aws

Guía del usuario

Estudio de investigación e ingeniería

Estudio de investigación e ingeniería: Guía del usuario

Table of Contents

Descripción general

> **Important**
>
> Esta versión de la Guía del usuario incluye la versión 2024.08 de Research and Engineering Studio en adelante. AWS Para ver la versión actual, consulte la Guía del AWS usuario de Research and Engineering Studio on.

Research and Engineering Studio (RES) es un producto de código abierto AWS compatible que permite a los administradores de TI proporcionar un portal web para que los científicos e ingenieros ejecuten cargas de trabajo informáticas técnicas. AWS RES ofrece un panel único para que los usuarios puedan lanzar escritorios virtuales seguros para realizar investigaciones científicas, diseñar productos, simulaciones de ingeniería o cargas de trabajo de análisis de datos. Los usuarios pueden conectarse al portal RES con sus credenciales corporativas actuales y trabajar en proyectos individuales o colaborativos.

Los administradores pueden crear espacios de colaboración virtuales denominados proyectos para que un conjunto específico de usuarios accedan a los recursos compartidos y colaboren. Los administradores pueden crear sus propios paquetes de software de aplicaciones (AMIs) y permitir a los usuarios de RES iniciar escritorios virtuales de Windows o Linux, además de permitir el acceso a los datos del proyecto a través de sistemas de archivos compartidos. Los administradores pueden asignar pilas de software y sistemas de archivos y restringir el acceso únicamente a los usuarios del proyecto. Los administradores pueden utilizar la telemetría integrada para supervisar el uso del entorno y solucionar los problemas de los usuarios. También pueden establecer presupuestos para proyectos individuales a fin de evitar el consumo excesivo de recursos. Como el producto es de código abierto, los clientes también pueden personalizar la experiencia de usuario del portal RES para adaptarla a sus propias necesidades.

RES está disponible sin costo adicional y usted paga solo por los AWS recursos necesarios para ejecutar sus aplicaciones.

Esta guía proporciona una descripción general de Research and Engineering Studio on AWS, su arquitectura y componentes de referencia, consideraciones para planificar la implementación y los pasos de configuración para implementar RES en la nube de Amazon Web Services (AWS).

Características y ventajas

Research and Engineering Studio on AWS ofrece las siguientes funciones:

Interfaz de usuario basada en web

RES proporciona un portal basado en la web que los administradores, investigadores e ingenieros pueden utilizar para acceder a sus espacios de trabajo de investigación e ingeniería y gestionarlos. Los científicos e ingenieros no necesitan tener experiencia Cuenta de AWS o experiencia en la nube para usar RES.

Configuración basada en proyectos

Use los proyectos para definir los permisos de acceso, asignar recursos y administrar los presupuestos de un conjunto de tareas o actividades. Asigne paquetes de software específicos (sistemas operativos y aplicaciones aprobadas) y recursos de almacenamiento a un proyecto para garantizar la coherencia y el cumplimiento. Supervise y gestione los gastos por proyecto.

Herramientas de colaboración

Los científicos e ingenieros pueden invitar a otros miembros de su proyecto a colaborar con ellos y establecer los niveles de permisos que desean que tengan esos colegas. Esas personas pueden iniciar sesión en RES para conectarse a esos escritorios.

Integración con la infraestructura de administración de identidades existente

Intégrelo con su infraestructura existente de administración de identidades y servicios de directorio para permitir la conexión al portal RES con la identidad corporativa existente de un usuario y asignar permisos a los proyectos utilizando las membresías de usuarios y grupos existentes.

Almacenamiento y acceso persistentes a los datos compartidos

Para proporcionar a los usuarios acceso a los datos compartidos en las sesiones de escritorios virtuales, conéctese a sus sistemas de archivos existentes o cree nuevos sistemas de archivos en RES. Los servicios de almacenamiento compatibles incluyen Amazon Elastic File System para escritorios Linux y Amazon FSx for NetApp ONTAP para escritorios Windows y Linux.

Supervisión e informes

Utilice el panel de análisis para supervisar el uso de los recursos, por ejemplo, los tipos de instancias, las pilas de software y los tipos de sistemas operativos. El panel también proporciona un desglose del uso de los recursos por proyectos para la elaboración de informes.

Gestión del presupuesto y los costes

AWS Budgets Conéctese a sus proyectos de RES para monitorear los costos de cada proyecto. Si supera su presupuesto, puede limitar el lanzamiento de sesiones de VDI.

Conceptos y definiciones

En esta sección se describen los conceptos clave y se define la terminología específica de este producto:

Explorador de archivos

Un explorador de archivos es una parte de la interfaz de usuario de RES donde los usuarios actualmente conectados pueden ver su sistema de archivos.

Sistema de archivos

El sistema de archivos actúa como un contenedor de los datos del proyecto (a menudo denominados conjuntos de datos). Proporciona una solución de almacenamiento dentro de los límites de un proyecto y mejora la colaboración y el control del acceso a los datos.

Administrador global

Un delegado administrativo con acceso a los recursos de RES que se comparten en un entorno de RES. El alcance y los permisos abarcan varios proyectos. Pueden crear o modificar proyectos y asignar sus propietarios. Pueden delegar o asignar permisos a los propietarios y miembros del proyecto. A veces, la misma persona actúa como administradora de la RES, según el tamaño de la organización.

Proyecto

Un proyecto es una partición lógica dentro de la aplicación que sirve como límite distintivo para los recursos de datos y computación, lo que garantiza la gobernanza del flujo de datos y evita que los datos y los hosts de VDI se compartan entre proyectos.

Permisos basados en proyectos

Los permisos basados en proyectos describen una partición lógica de los hosts de datos y de VDI en un sistema en el que pueden existir varios proyectos. El acceso de un usuario a los datos y a los hosts de VDI de un proyecto viene determinado por sus funciones asociadas. Se debe asignar a un usuario el acceso (o la pertenencia a un proyecto) para cada proyecto al que necesite

acceder. De lo contrario, un usuario no podrá acceder a los datos del proyecto VDIs si no se le ha concedido la membresía.

Miembro del proyecto

Usuario final de los recursos de RES (VDI, almacenamiento, etc.). El alcance y los permisos están restringidos a los proyectos a los que están asignados. No pueden delegar ni asignar ningún permiso.

Propietario del proyecto

Un delegado administrativo con acceso y propiedad sobre un proyecto específico. El alcance y los permisos están restringidos a los proyectos de su propiedad. Pueden asignar permisos a los miembros del proyecto en los proyectos de su propiedad.

Pila de software

Las pilas de software son Amazon Machine Images (AMI) con metadatos específicos de RES basados en cualquier sistema operativo que el usuario haya seleccionado para aprovisionar su host de VDI.

Hosts VDI

Los hosts de instancias de escritorios virtuales (VDI) permiten a los miembros del proyecto acceder a los entornos informáticos y de datos específicos del proyecto, lo que garantiza espacios de trabajo seguros y aislados.

Para obtener una referencia general de los AWS términos, consulte el AWS glosario de la Referencia general.AWS

Información general de la arquitectura

En esta sección se proporciona un diagrama de arquitectura de los componentes implementados con este producto.

Diagrama de arquitectura

Al implementar este producto con los parámetros predeterminados, se implementan los siguientes componentes en su Cuenta de AWS.

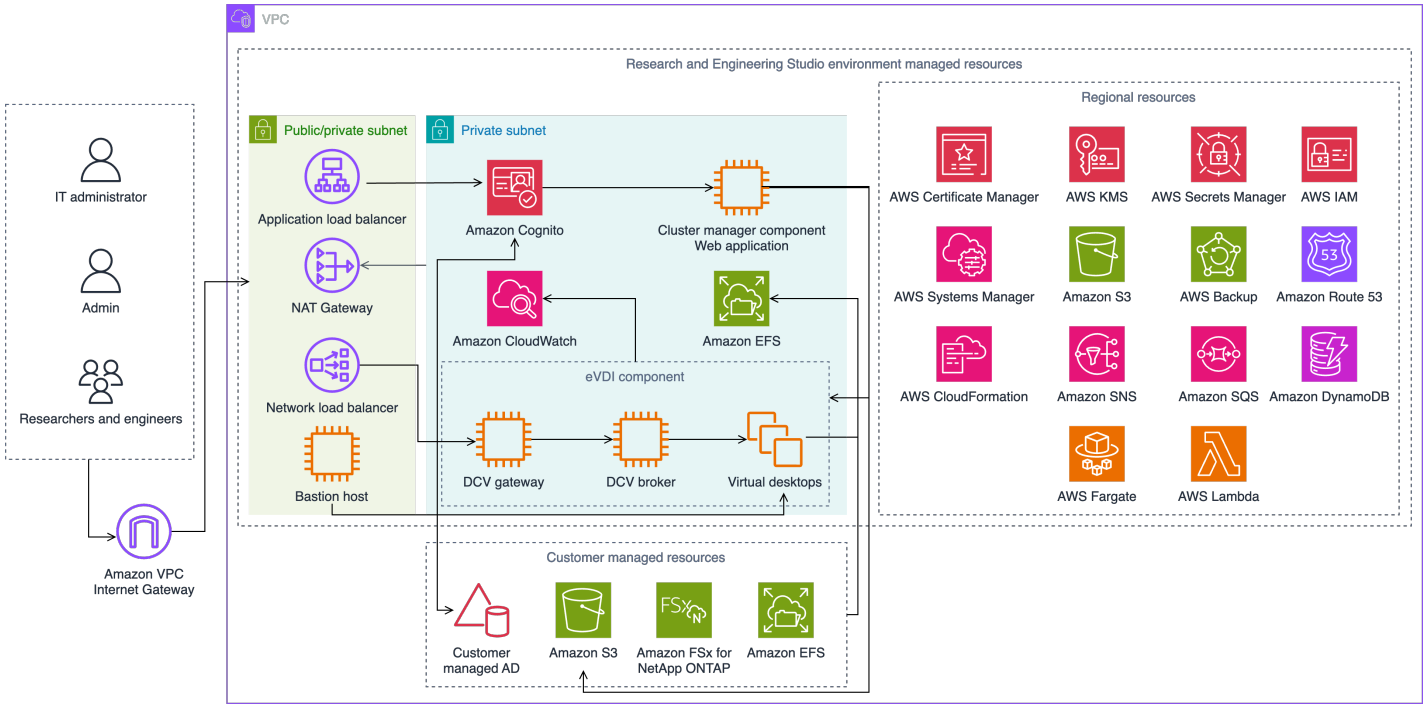


Figura 1: Estudio de investigación e ingeniería sobre AWS arquitectura

> **Note**
>
> AWS CloudFormation los recursos se crean a partir de AWS Cloud Development Kit (AWS CDK) construcciones.

El flujo de proceso de alto nivel para los componentes del producto implementados con la AWS CloudFormation plantilla es el siguiente:

1. RES instala componentes para el portal web, además de:

a. Componente de escritorio virtual de ingeniería (eVDI) para cargas de trabajo interactivas

b. Componente de métricas

   Amazon CloudWatch recibe las métricas de los componentes de eVDI.

c. Componente Bastion Host

   Los administradores pueden conectarse al componente de host Bastion mediante SSH para administrar la infraestructura subyacente.

2. RES instala los componentes en subredes privadas detrás de una puerta de enlace NAT. Los administradores acceden a las subredes privadas mediante el Application Load Balancer (ALB) o el componente Bastion Host.
3. Amazon DynamoDB almacena la configuración del entorno.
4. AWS Certificate Manager (ACM) genera y almacena un certificado público para el Application Load Balancer (ALB).

   > **Note**
   >
   > Le recomendamos que lo utilice AWS Certificate Manager para generar un certificado de confianza para su dominio.

5. Amazon Elastic File System (EFS) aloja el sistema de `/home` archivos predeterminado montado en todos los hosts de infraestructura aplicables y en las sesiones de Linux de EVDi.
6. RES usa Amazon Cognito para crear un usuario de bootstrap inicial llamado clusteradmin y envía credenciales temporales a la dirección de correo electrónico proporcionada durante la instalación. El administrador del clúster debe cambiar la contraseña al iniciar sesión por primera vez.
7. Amazon Cognito se integra con el Active Directory y las identidades de usuario de su organización para la administración de permisos.
8. Las zonas de seguridad permiten a los administradores restringir el acceso a componentes específicos del producto en función de los permisos.

AWS servicios de este producto

AWS servicio	Descripción
Amazon Elastic Compute Cloud	Principal. Proporciona los servicios informáticos subyacentes para crear escritorios virtuales con el sistema operativo y la pila de software que elijan.
Elastic Load Balancing	Principal. Los hosts Bastion, cluster-manager y VDI se crean en grupos de Auto Scaling detrás del balanceador de cargas. ELB equilibra el tráfico del portal web entre los hosts de RES.
Amazon Virtual Private Cloud	Principal. Todos los componentes principales del producto se crean en su VPC.
Amazon Cognito	Principal. Administra las identidades y la autenticación de los usuarios. Los usuarios de Active Directory se asignan a usuarios y grupos de Amazon Cognito para autenticar los niveles de acceso.
Amazon Elastic File System	Principal. Proporciona el sistema de `/home` archivos para el explorador de archivos y los hosts de VDI, así como para los sistemas de archivos externos compartidos.
Amazon DynamoDB	Principal. Almacena datos de configuración, como usuarios, grupos, proyectos, sistemas de archivos y ajustes de componentes.
AWS Systems Manager	Principal. Almacena documentos para ejecutar comandos para la administración de sesiones de VDI.
AWS Lambda	Principal. Admite funcionalidades del producto, como la actualización de la configuración de la

AWS servicio	Descripción
	tabla de DynamoDB, el inicio de los flujos de trabajo de sincronización de Active Directory y la actualización de la lista de prefijos.
Amazon CloudWatch	Admite. Proporciona métricas y registros de actividad para todos los EC2 hosts de Amazon y las funciones de Lambda.
Amazon Simple Storage Service	Admite. Almacena los archivos binarios de las aplicaciones para el arranque y la configuración del host.
AWS Key Management Service	Admite. Se utiliza para el cifrado en reposo con colas de Amazon SQS, tablas de DynamoDB y temas de Amazon SNS.
AWS Secrets Manager	Admite. Almacena las credenciales de las cuentas de servicio en Active Directory y los certificados autofirmados para. VDIs
AWS CloudFormation	Admite. Proporciona un mecanismo de implementación para el producto.
AWS Identity and Access Management	Admite. Restringe el nivel de acceso de los hosts.
Amazon Route 53	Admite. Crea una zona alojada privada para resolver el balanceador de cargas interno y el nombre de dominio del host del bastión.
Amazon Simple Queue Service	Admite. Crea colas de tareas para admitir las ejecuciones asíncronas.
Amazon Simple Notification Service	Admite. Admite el modelo de publicación-suscriptor entre los componentes de la VDI, como el controlador y los hosts.

AWS servicio	Descripción
AWS Fargate	Admite. Instala, actualiza y elimina entornos mediante las tareas de Fargate.
Amazon FSx File Gateway	Opcional. Proporciona un sistema de archivos compartidos externo.
Amazon FSx para NetApp ONTAP	Opcional. Proporciona un sistema de archivos compartidos externo.
AWS Certificate Manager	Opcional. Genera un certificado de confianza para su dominio personalizado.
AWS Backup	Opcional. Ofrece funciones de copia de seguridad para los EC2 hosts de Amazon, los sistemas de archivos y DynamoDB.

Cree un entorno de demostración

Siga los pasos de esta sección para probar Research and Engineering Studio AWS. Esta demostración implementa un entorno que no es de producción con un conjunto mínimo de parámetros utilizando la plantilla de pila de entornos de AWS demostración de Research and Engineering Studio. Utiliza un servidor Keycloak para el inicio de sesión único.

Tenga en cuenta que, después de implementar la pila, debe seguir los pasos que se indican a Pasos posteriores a la implementación continuación para configurar los usuarios en el entorno antes de iniciar sesión.

Cree una pila de demostración con un solo clic

Esta AWS CloudFormation pila crea todos los componentes necesarios para Research and Engineering Studio.

Tiempo de implementación: aproximadamente 90 minutos

Requisitos previos

Temas

- Cree una Cuenta de AWS con un usuario administrativo
- Crear un key pair de claves Amazon EC2 SSH
- Aumentar las cuotas de servicio

Cree una Cuenta de AWS con un usuario administrativo

Debe tener una Cuenta de AWS con un usuario administrativo:

1. Abre el https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como

práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Crear un key pair de claves Amazon EC2 SSH

Si no tienes un par de claves EC2 SSH de Amazon, tendrás que crear uno. Para obtener más información, consulta Cómo crear un key pair con Amazon EC2 en la Guía del EC2 usuario de Amazon.

Aumentar las cuotas de servicio

Recomendamos aumentar las cuotas de servicio para:

- Amazon VPC
  - Aumente la cuota de direcciones IP elásticas por puerta de enlace NAT de cinco a ocho
  - Aumente las puertas de enlace NAT por zona de disponibilidad de cinco a diez
- Amazon EC2
  - Aumente la elasticidad EC2 de -VPC IPs de cinco a diez

Su AWS cuenta tiene cuotas predeterminadas, antes denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar. Para obtener más información, consulte the section called “Cuotas de AWS servicios de este producto”.

Cree recursos e introduzca parámetros

1. Inicie sesión en https://console.aws.amazon.com/cloudformation AWS Management Console y abra la AWS CloudFormation consola.

   > **Note**
   >
   > Asegúrese de estar en su cuenta de administrador.

2. Inicie la plantilla en la consola.
3. En Parámetros, revise los parámetros de esta plantilla de producto y modifíquelos según sea necesario.

Parámetro	Predeterminado/a	Descripción
EnvironmentName	*<res-demo>*	Un nombre exclusivo asignado a su entorno RES que comienza con res- y no debe superar los 11 caracteres.
AdministratorEmail		La dirección de correo electrónico del usuario que completa la configuración del producto. Este usuario también funciona como un usuario rompeolas si se produce un error en la integración del inicio de sesión único de Active Directory.
KeyPair		El key pair que se utiliza para conectarse a los hosts de la infraestructura.
Cliente IPCidr	<0.0.0.0/0>	Filtro de direcciones IP que limita la conexión al sistema. Puede actualizarlo ClientIpCidr después de la implementación.
InboundPrefixList		(Opcional) Proporcione una lista de prefijos gestionada para IPs permitir el acceso directo a la interfaz de usuario web y a SSH desde el host bastión.

Pasos posteriores a la implementación

1. Restablezca las contraseñas de los usuariosAWS Directory Service: la pila de demostración crea cuatro usuarios con nombres de usuario que puede usar:admin1, user1admin2, y. user2

   a. Vaya a la consola de Directory Service.

   b. Seleccione el identificador de directorio de su entorno. Puede obtener el identificador del directorio a partir de la salida de la <StackName>*DirectoryService* pila.

   c. En el menú desplegable Acciones de la parte superior derecha, selecciona Restablecer la contraseña del usuario.

   d. Para todos los usuarios que quieras usar, coloca el nombre de usuario, escribe la contraseña que quieres tener y selecciona Restablecer contraseña.

2. Una vez que haya restablecido las contraseñas de los usuarios, tendrá que esperar a que Research and Engineering Studio sincronice los usuarios del entorno. Research and Engineering Studio sincroniza a los usuarios cada hora a las 24 horas. Puede esperar a que eso suceda o seguir los pasos que se indican El usuario se agregó en Active Directory, pero no aparece en RES para sincronizar los usuarios inmediatamente.

Su implementación ya está lista. Usa la EnvironmentUrl que recibiste en el correo electrónico para acceder a la interfaz de usuario, o también puedes obtener la misma URL del resultado de la pila implementada. Ahora puede iniciar sesión en el entorno de Research and Engineering Studio con el usuario y la contraseña para los que restableció la contraseña en Active Directory.

Planificación de la implementación

Costo

Research and Engineering Studio on AWS está disponible sin coste adicional y usted paga únicamente por los AWS recursos necesarios para ejecutar sus aplicaciones. Para obtener más información, consulte AWS servicios de este producto.

> **Note**
>
> Usted es responsable del coste de los AWS servicios utilizados durante la ejecución de este producto.
> Recomendamos crear un presupuesto AWS Cost Explorerpara ayudar a gestionar los costes. Los precios están sujetos a cambios. Para obtener más información, consulta la página web de precios de cada AWS servicio utilizado en este producto.

Seguridad

Cuando crea sistemas en una AWS infraestructura, las responsabilidades de seguridad se comparten entre usted y AWS. Este modelo de responsabilidad compartida reduce la carga operativa, ya que AWS opera, administra y controla los componentes, incluidos el sistema operativo anfitrión, la capa de virtualización y la seguridad física de las instalaciones en las que operan los servicios. Para obtener más información acerca AWS de la seguridad, visite Nube de AWS Seguridad.

Roles de IAM

AWS Identity and Access Management Las funciones (IAM) permiten a los clientes asignar políticas y permisos de acceso detallados a los servicios y usuarios del Nube de AWS. Este producto crea funciones de IAM que otorgan a las AWS Lambda funciones del producto y a las EC2 instancias de Amazon acceso para crear recursos regionales.

RES admite políticas basadas en la identidad dentro de IAM. Cuando se implementa, RES crea políticas para definir el permiso y el acceso del administrador. El administrador que implementa el producto crea y administra los usuarios finales y los líderes del proyecto dentro del Active Directory

del cliente existente integrado con RES. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de AWS Identity and Access Management.

El administrador de su organización puede administrar el acceso de los usuarios con un directorio activo. Cuando los usuarios finales acceden a la interfaz de usuario de RES, RES se autentica con Amazon Cognito.

Grupos de seguridad

Los grupos de seguridad creados en este producto están diseñados para controlar y aislar el tráfico de red entre las funciones, las instancias, los sistemas de archivos, las EC2 instancias de CSR y los puntos finales VPN remotos de Lambda. Le recomendamos que revise los grupos de seguridad y restrinja aún más el acceso según sea necesario una vez que se implemente el producto.

Cifrado de datos

De forma predeterminada, Research and Engineering Studio on AWS (RES) cifra los datos de los clientes en reposo y en tránsito mediante una clave propiedad de RES. Al implementar RES, puede especificar una AWS KMS key. RES utiliza sus credenciales para conceder el acceso clave. Si la proporciona a un cliente que es propiedad y está gestionado AWS KMS key, los datos inactivos del cliente se cifrarán con esa clave.

RES cifra los datos de los clientes en tránsito mediante SSL/TLS. Requerimos TLS 1.2, pero recomendamos TLS 1.3.

Cuotas

Service Quotas, también denominadas límites, establecen el número máximo de recursos u operaciones de servicio para su cuenta de Cuenta de AWS.

Cuotas para los AWS servicios de este producto

Asegúrese de tener una cuota suficiente para cada uno de los servicios implementados en este producto. Para más información, consulte Service Quotas de AWS.

Para este producto, recomendamos aumentar las cuotas para los siguientes servicios:

- Amazon Virtual Private Cloud
- Amazon EC2

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

AWS CloudFormation cuotas

Tienes AWS CloudFormation cuotas que debes tener en cuenta al lanzar la pila de este producto. Cuenta de AWS Si comprende estas cuotas, puede evitar errores de limitación que le impidan implementar este producto correctamente. Para obtener más información, consulte AWS CloudFormation las cuotas en la Guía del AWS CloudFormation usuario.

Planificar la resiliencia

El producto implementa una infraestructura predeterminada con la cantidad y el tamaño mínimos de EC2 instancias de Amazon para operar el sistema. Para mejorar la resiliencia en entornos de producción a gran escala, recomendamos aumentar la configuración de capacidad mínima predeterminada dentro de los grupos de Auto Scaling (ASG) de la infraestructura. Aumentar el valor de una instancia a dos instancias proporciona la ventaja de tener varias zonas de disponibilidad (AZ) y reduce el tiempo necesario para restaurar la funcionalidad del sistema en caso de una pérdida de datos inesperada.

La configuración de ASG se puede personalizar en la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/. El producto crea cuatro de forma ASGs predeterminada y cada nombre termina en. `-asg` Puede cambiar los valores mínimos y deseados por una cantidad adecuada para su entorno de producción. Elija el grupo que desee modificar y, a continuación, elija Acciones y Editar. Para obtener más información ASGs, consulte Escalar el tamaño de su grupo de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Compatible Regiones de AWS

Este producto utiliza servicios que actualmente no están disponibles en todos Regiones de AWS. Debe lanzar este producto en un Región de AWS lugar en el que estén disponibles todos los servicios. Para obtener la disponibilidad más actualizada de AWS los servicios por región, consulte la lista de Región de AWS todos los servicios.

Research and Engineering Studio on AWS es compatible con lo siguiente Regiones de AWS:

Nombre de la región	Región	Versión 2024.06 y anteriores	Versión 2024.08
Este de EE. UU. (Norte de Virginia)	us-east-1	yes	sí
Este de EE. UU. (Ohio)	us-east-2	yes	sí
Oeste de EE. UU. (Norte de California)	us-west-1	yes	sí
Oeste de EE. UU. (Oregón)	us-west-2	yes	sí
Asia-Pacífico (Tokio)	ap-northeast-1	yes	sí
Asia-Pacífico (Seúl)	ap-northeast-2	yes	sí
Asia-Pacífico (Bombay)	ap-south-1	yes	sí
Asia-Pacífico (Singapur)	ap-southeast-1	yes	sí
Asia-Pacífico (Sídney)	ap-southeast-2	yes	sí
Canadá (centro)	ca-central-1	yes	sí
Europa (Fráncfort)	eu-central-1	yes	sí
Europa (Milán)	eu-south-1	yes	sí
Europa (Irlanda)	eu-west-1	yes	sí
Europa (Londres)	eu-west-2	yes	sí
Europa (París)	eu-west-3	yes	sí
Europa (Estocolmo)	eu-north-1	no	yes

Nombre de la región	Región	Versión 2024.06 y anteriores	Versión 2024.08
Israel (Tel Aviv)	il-central-1	yes	sí
AWS GovCloud (US-Oeste)	us-gov-west-1	yes	no

Implemente el producto

> **Note**
>
> Este producto utiliza AWS CloudFormation plantillas y pilas para automatizar su implementación. Las CloudFormation plantillas describen los AWS recursos incluidos en este producto y sus propiedades. La CloudFormation pila proporciona los recursos que se describen en las plantillas.

Antes de lanzar el producto, revise el costo, la arquitectura, la seguridad de la red y otras consideraciones analizadas anteriormente en esta guía.

Temas

- Requisitos previos
- Crear recursos externos
- Paso 1: lanzar el producto
- Paso 2: Inicie sesión por primera vez

Requisitos previos

Temas

- Crear una Cuenta de AWS con un usuario administrativo
- Crear un key pair de claves Amazon EC2 SSH
- Aumentar las cuotas de servicio
- Crea un dominio público (opcional)
- Crear dominio (GovCloud solo)
- Proporcione recursos externos
- Configure LDAPS en su entorno (opcional)
- Configurar una VPC privada (opcional)

Crear una Cuenta de AWS con un usuario administrativo

Debe tener una Cuenta de AWS con un usuario administrativo:

1. Abre el https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Crear un key pair de claves Amazon EC2 SSH

Si no tienes un par de claves EC2 SSH de Amazon, tendrás que crear uno. Para obtener más información, consulta Cómo crear un key pair con Amazon EC2 en la Guía del EC2 usuario de Amazon.

Aumentar las cuotas de servicio

Recomendamos aumentar las cuotas de servicio para:

- Amazon VPC
  - Aumente la cuota de direcciones IP elásticas por puerta de enlace NAT de cinco a ocho
  - Aumente las puertas de enlace NAT por zona de disponibilidad de cinco a diez
- Amazon EC2
  - Aumente la elasticidad EC2 de -VPC IPs de cinco a diez

Su AWS cuenta tiene cuotas predeterminadas, anteriormente denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar. Para obtener más información, consulte the section called “Cuotas de AWS servicios de este producto”.

Crea un dominio público (opcional)

Recomendamos usar un dominio personalizado para el producto a fin de tener una URL fácil de usar. Deberá registrar un dominio mediante Amazon Route 53 u otro proveedor e importar un certificado para el dominio que utilice AWS Certificate Manager. Si ya tiene un dominio público y un certificado, puede omitir este paso.

1. Siga las instrucciones para registrar un dominio con Route53. Deberías recibir un correo electrónico de confirmación.
2. Recupera la zona alojada de tu dominio. Route53 la crea automáticamente.
   a. Abra la consola Route53.
   b. Selecciona Zonas alojadas en el menú de navegación de la izquierda.
   c. Abre la zona alojada creada para tu nombre de dominio y copia el ID de la zona alojada.
3. Abre AWS Certificate Manager y sigue estos pasos para solicitar un certificado de dominio. Asegúrese de estar en la región en la que planea implementar la solución.
4. Seleccione Listar certificados en la barra de navegación y busque su solicitud de certificado. La solicitud debería estar pendiente.
5. Elija su ID de certificado para abrir la solicitud.
6. En la sección Dominios, elija Crear registros en Route53. La solicitud tardará aproximadamente diez minutos en procesarse.
7. Una vez emitido el certificado, copie el ARN de la sección de estado del certificado.

Crear dominio (GovCloud solo)

Si va a realizar el despliegue en la región AWS GovCloud (EE. UU.-Oeste), tendrá que completar estos pasos previos.

1. Implemente la AWS CloudFormation pila de certificados en la AWS cuenta de la partición comercial en la que se creó el dominio hospedado público.
2. En los CloudFormation resultados del certificado, busque y anote las `CertificateARN` letras y. `PrivateKeySecretARN`
3. En la cuenta de GovCloud partición, cree un secreto con el valor de la `CertificateARN` salida. Anote el nuevo ARN secreto y añada dos etiquetas al secreto para `vdc-gateway` poder acceder al valor secreto:

a. res: = ModuleName virtual-desktop-controller

b. res: EnvironmentName = [nombre del entorno] (podría ser res-demo)

4. En la cuenta de GovCloud partición, cree un secreto con el valor de la `PrivateKeySecretArn` salida. Anote el nuevo ARN secreto y añada dos etiquetas al secreto para `vdc-gateway` poder acceder al valor secreto:

   a. res: = ModuleName virtual-desktop-controller

   b. res: EnvironmentName = [nombre del entorno] (podría ser res-demo)

Proporcione recursos externos

Research and Engineering Studio on AWS espera que existan los siguientes recursos externos cuando se implemente.

- Redes (VPC, subredes públicas y subredes privadas)

  Aquí es donde ejecutará las EC2 instancias utilizadas para alojar el entorno RES, el Active Directory (AD) y el almacenamiento compartido.

- Almacenamiento (Amazon EFS)

  Los volúmenes de almacenamiento contienen los archivos y los datos necesarios para la infraestructura de escritorio virtual (VDI).

- Servicio de directorio ()AWS Directory Service for Microsoft Active Directory

  El servicio de directorio autentica a los usuarios en el entorno RES.

- Un secreto que contiene la contraseña de la cuenta de servicio

  Research and Engineering Studio accede a los secretos que usted proporciona, incluida la contraseña de la cuenta de servicio, mediante AWS Secrets Manager.

> **Tip**
>
> Si está implementando un entorno de demostración y no dispone de estos recursos externos, puede utilizar fórmulas informáticas de AWS alto rendimiento para generar los recursos externos. Consulte la siguiente sección para implementar recursos en su cuenta. Crear recursos externos

Para las implementaciones de demostración en la región AWS GovCloud (EE. UU.-Oeste), tendrá que completar los pasos previos que se indican a continuación. Crear dominio (GovCloud solo)

Configure LDAPS en su entorno (opcional)

Si planea utilizar la comunicación LDAPS en su entorno, debe completar estos pasos para crear y adjuntar certificados al controlador de dominio AWS Managed Microsoft AD (AD) a fin de proporcionar comunicación entre AD y RES.

1. Siga los pasos que se indican en Cómo habilitar el LDAPS del lado del servidor para su. AWS Managed Microsoft AD Puede omitir este paso si ya ha activado el LDAPS.
2. Tras confirmar que LDAPS está configurado en el AD, exporte el certificado de AD:
   a. Vaya a su servidor de Active Directory.
   b. PowerShell Ábralo como administrador.
   c. Ejecute `certmgr.msc` para abrir la lista de certificados.
   d. Abra la lista de certificados abriendo primero las autoridades emisoras de certificados raíz de confianza y, a continuación, los certificados.
   e. Seleccione y mantenga pulsado (o haga clic con el botón derecho del ratón) en el certificado con el mismo nombre que su servidor de AD y, a continuación, seleccione Todas las tareas y, a continuación, Exportar.
   f. Elija X.509 (.CER) codificado en base 64 y elija Siguiente.
   g. Seleccione un directorio y, a continuación, elija Siguiente.
3. Crea un secreto en AWS Secrets Manager:

   Al crear su secreto en Secrets Manager, seleccione Otro tipo de secretos en Tipo de secreto y pegue su certificado cifrado en PEM en el campo Texto no cifrado.
4. Anote el ARN creado e introdúzcalo como `DomainTLSCertificateSecretARN` parámetro en. the section called “Paso 1: lanza el producto”

Configurar una VPC privada (opcional)

La implementación de Research and Engineering Studio en una VPC aislada ofrece una seguridad mejorada para cumplir con los requisitos de cumplimiento y gobierno de su organización. Sin

embargo, la implementación estándar de RES se basa en el acceso a Internet para instalar las dependencias. Para instalar RES en una VPC privada, debe cumplir los siguientes requisitos previos:

Temas

Prepare imágenes de máquinas de Amazon (AMIs)

1. Descarga las dependencias. Para implementarse en una VPC aislada, la infraestructura RES requiere la disponibilidad de dependencias sin tener acceso público a Internet.
2. Cree un rol de IAM con acceso de solo lectura a Amazon S3 y una identidad de confianza como Amazon. EC2

   a. Abra la consola de IAM en https://console.aws.amazon.com/iam/.

   b. En Roles, elija Crear rol.

   c. En la página Seleccionar entidad de confianza:

      - En Tipo de entidad de confianza, elija Servicio de AWS.
      - En Caso de uso en Servicio o Caso de uso, seleccione EC2y elija Siguiente.

   d. En Añadir permisos, selecciona las siguientes políticas de permisos y, a continuación, selecciona Siguiente:

      - Amazon S3 ReadOnlyAccess
      - Amazon SSMManaged InstanceCore
      - EC2InstanceProfileForImageBuilder

   e. Añada un nombre y una descripción del rol y, a continuación, elija Crear rol.
3. Cree el componente generador de EC2 imágenes:

   a. Abra la consola EC2 de Image Builder enhttps://console.aws.amazon.com/imagebuilder.

   b. En Recursos guardados, elija Componentes y elija Crear componente.

   c. En la página Crear componente, introduzca los siguientes detalles:

- En Tipo de componente, elija Construir.
- Para ver los detalles del componente, elija:

Parámetro	Entrada de usuario
Sistema operativo (OS) de imagen	Linux
Versiones de sistema operativo compatibles	Amazon Linux 2
Nombre del componente	Elija un nombre como: *<research-and-engineering-studio-infrastructure>*
Versión del componente	Recomendamos empezar con la versión 1.0.0.
Descripción	Entrada de usuario opcional.

d. En la página Crear componente, elija Definir el contenido del documento.

i. Antes de introducir el contenido del documento de definición, necesitará un URI de archivo para el archivo tar.gz. Cargue el archivo tar.gz proporcionado por RES a un bucket de Amazon S3 y copie el URI del archivo de las propiedades del bucket.

ii. Introduzca lo siguiente:

> **Note**
>
> `AddEnvironmentVariables`es opcional y puede eliminarlo si no necesita variables de entorno personalizadas en los hosts de su infraestructura.
> Si está configurando variables de `https_proxy` entorno, `no_proxy` los parámetros son necesarios para evitar que la instancia utilice el proxy para consultar el host local, las direcciones IP de los metadatos de la instancia y los servicios que admiten los puntos de enlace de la VPC. `http_proxy`

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
```

```
#  Licensed under the Apache License, Version 2.0 (the "License"). You may
 not use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is
 distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
 software dependencies for infrastructure hosts.
schemaVersion: 1.0

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: '<s3 tar.gz file uri>'
              destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd /root/bootstrap/res_dependencies'
                - 'tar -xf res_dependencies.tar.gz'
                - 'cd all_dependencies'
```

```
                - '/bin/bash install.sh'
        - name: AddEnvironmentVariables
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
             commands:
                 - |
                   echo -e "
                   http_proxy=http://<ip>:<port>
                   https_proxy=http://<ip>:<port>

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com
                  " > /etc/environment
```

e. Seleccione Crear componente.

4. Cree una receta de imágenes de Image Builder.

a. En la página Crear receta, introduzca lo siguiente:

Sección	Parámetro	Entrada de usuario
Detalles de la receta	Nombre	Introduzca un nombre apropiado, como res-recipe-linux-x86.
	Versión	Introduzca una versión, que normalmente empieza por la 1.0.0.
	Descripción	Añada una descripción opcional.
Imagen base	Seleccione una imagen	Seleccione imágenes gestionadas.
	SO	Amazon Linux
	Origen de la imagen	Inicio rápido (gestionado por Amazon)
	Nombre de la imagen	Amazon Linux 2 x86
	Opciones de control de versiones automático	Utilice la última versión del sistema operativo disponible.
Configuración de instancias	–	Mantén todo en la configuración predeterminada y asegúrate de que no esté seleccionada la opción Eliminar el agente SSM tras la ejecución de la canalización.

Sección	Parámetro	Entrada de usuario
Directorio de trabajo	Ruta del directorio de trabajo	/root/bootstrap/res_dependencias
Componentes	Construya componentes	Busque y seleccione lo siguiente: • Administrado por Amazon: -2-linux aws-cli-version • Administrado por Amazon: amazon-cloudwatch-agent-linux • De tu propiedad: EC2 componente de Amazon creado anteriormente. Pon tu Cuenta de AWS ID y la actual Región de AWS en los campos.
	Pruebe los componentes	Busque y seleccione: • Administrado por Amazon: simple-boot-test-linux

b. Elija Crear receta.

5. Cree la configuración de infraestructura de Image Builder.

a. En Recursos guardados, elija Configuraciones de infraestructura.

b. Elija Crear configuración de infraestructura.

c. En la página Crear configuración de infraestructura, introduzca lo siguiente:

Sección	Parámetro	Entrada de usuario
General	Nombre	Introduzca un nombre apropiado, como res-infra-linux-x 86.
	Descripción	Añada una descripción opcional.
	Rol de IAM	Seleccione el rol de IAM creado anteriormente.
AWS infraestructura	Tipo de instancia	Elija t3.medium.

	VPC, subred y grupos de seguridad	Seleccione una opción que permita el acceso a Internet y al bucket de Amazon S3. Si necesitas crear un grupo de seguridad, puedes crear uno desde la EC2 consola de Amazon con las siguientes entradas:
		• VPC: seleccione la misma VPC que se utiliza para la configura ción de la infraestructura. Esta VPC debe tener acceso a Internet.
		• Regla de entrada:
		  • Tipo: SSH
		  • Source (Fuente): Custom
		  • Bloque CIDR: 0.0.0.0/0

d. Elija Crear configuración de infraestructura.

6. Cree una nueva canalización EC2 de Image Builder:

   a. Vaya a las canalizaciones de imágenes y elija Crear canalización de imágenes.

   b. En la página Especificar los detalles de la canalización, introduce lo siguiente y selecciona Siguiente:

      - Nombre de la canalización y descripción opcional
      - En Crear un cronograma, defina un cronograma o elija Manual si desea iniciar el proceso de horneado AMI manualmente.

   c. En la página Elegir receta, elija Usar receta existente e introduzca el nombre de la receta creada anteriormente. Elija Siguiente.

   d. En la página Definir el proceso de imagen, seleccione los flujos de trabajo predeterminados y elija Siguiente.

   e. En la página Definir configuración de infraestructura, elija Usar la configuración de infraestructura existente e introduzca el nombre de la configuración de infraestructura creada anteriormente. Elija Siguiente.

   f. En la página Definir la configuración de distribución, tenga en cuenta lo siguiente para sus selecciones:

      - La imagen de salida debe residir en la misma región que el entorno RES implementado, de modo que RES pueda lanzar correctamente las instancias del host de infraestructura desde allí. Si se utilizan los valores predeterminados del servicio, la imagen de salida se creará en la región en la que se utilice el servicio EC2 Image Builder.
      - Si desea implementar RES en varias regiones, puede elegir Crear una nueva configuración de distribución y agregar allí más regiones.

   g. Revisa tus selecciones y selecciona Crear canalización.

7. Ejecute la canalización EC2 de Image Builder:

   a. En Image Pipelines, busca y selecciona la canalización que has creado.

   b. Selecciona Acciones y selecciona Ejecutar canalización.

      La canalización puede tardar entre 45 minutos y una hora en crear una imagen AMI.

8. Anote el ID de AMI de la AMI generada y utilícelo como entrada para el parámetro InfrastructureHost AMI enthe section called “Paso 1: lanza el producto”.

Configurar puntos finales de VPC

Para implementar RES y lanzar escritorios virtuales, Servicios de AWS necesita acceso a su subred privada. Debe configurar los puntos de enlace de VPC para proporcionar el acceso necesario y tendrá que repetir estos pasos para cada punto de enlace.

1. Si los puntos de conexión no se han configurado previamente, siga las instrucciones que se proporcionan en Acceso y Servicio de AWS uso de un punto de conexión de VPC de interfaz.
2. Seleccione una subred privada en cada una de las dos zonas de disponibilidad.

Servicio de AWS	Nombre del servicio
Aplicación de escalado automático	com.amazonaws. *region*.escalado automático de aplicaciones
AWS CloudFormation	com.amazonaws. *region*.formación en la nube
Amazon CloudWatch	com.amazonaws. *region*.monitoreo
Amazon CloudWatch Logs	com.amazonaws. *region*.logs
Amazon DynamoDB	com.amazonaws. *region*.dynamodb (requiere un punto final de puerta de enlace)
Amazon EC2	com.amazonaws. *region*.ec2
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon Elastic File System	com.amazonaws. *region*.sistema de archivos elástico
Elastic Load Balancing	com.amazonaws. *region*.balanceo de carga elástico
Amazon EventBridge	com.amazonaws. *region*.eventos
Amazon FSx	com.amazonaws. *region*.fsx
AWS Key Management Service	com.amazonaws. *region*.kms

Servicio de AWS	Nombre del servicio
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams
Amazon S3	com.amazonaws. *region*.s3 (requiere un punto final de puerta de enlace que se crea de forma predeterminada en RES).
AWS Secrets Manager	com.amazonaws. *region*.administrador de secretos
Amazon SES	com.amazonaws. *region*.email-smtp (no se admite en las siguientes zonas de disponibilidad: use-1-az2, use1-az3, use1-az5, usw1-az2, usw2-az4, apne2-az4, cac1-az3 y cac1-az4).
AWS Security Token Service	com.amazonaws. *region*.sts
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
AWS Systems Manager	com.amazonaws. *region*Mensajes.ec2
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*Mensajes.ssm

Conéctese a servicios sin puntos finales de VPC

Para integrarlo con servicios que no admiten puntos de enlace de VPC, puede configurar un servidor proxy en una subred pública de su VPC. Siga estos pasos para crear un servidor proxy con el acceso mínimo necesario para una implementación de Research and Engineering Studio utilizando AWS Identity Center como proveedor de identidad.

1. Lance una instancia de Linux en la subred pública de la VPC que utilizará para la implementación de RES.
   - Familia Linux: Amazon Linux 2 o Amazon Linux 3
   - Arquitectura: x86

- Tipo de instancia: t2.micro o superior
- Grupo de seguridad: TCP en el puerto 3128 desde 0.0.0.0/0

2. Conéctese a la instancia para configurar un servidor proxy.

   a. Abre la conexión http.

   b. Permita la conexión a los siguientes dominios desde todas las subredes relevantes:

      - .amazonaws.com (para servicios genéricos) AWS
      - .amazoncognito.com (para Amazon Cognito)
      - .awsapps.com (para Identity Center)
      - .signin.aws (para Identity Center)
      - . amazonaws-us-gov.com (para Gov Cloud)

   c. Denegar todas las demás conexiones.

   d. Active e inicie el servidor proxy.

   e. Anote el PUERTO en el que escucha el servidor proxy.

3. Configure su tabla de rutas para permitir el acceso al servidor proxy.

   a. Vaya a la consola de VPC e identifique las tablas de enrutamiento de las subredes que utilizará para los hosts de infraestructura y los hosts de VDI.

   b. Edite la tabla de rutas para permitir que todas las conexiones entrantes vayan a la instancia del servidor proxy creada en los pasos anteriores.

   c. Haga esto para las tablas de enrutamiento de todas las subredes (sin acceso a Internet) que vaya a utilizar en VDIs Infrastructure/.

4. Modifique el grupo de seguridad de la EC2 instancia del servidor proxy y asegúrese de que permite las conexiones TCP entrantes en el puerto por el que escucha el servidor proxy.

Defina los parámetros de despliegue de una VPC privada

Enthe section called “Paso 1: lanza el producto”, se espera que introduzcas determinados parámetros en la AWS CloudFormation plantilla. Asegúrese de configurar los siguientes parámetros, tal y como se indica, para implementarlos correctamente en la VPC privada que acaba de configurar.

Parámetro	Input
InfrastructureHostAMI	Utilice el ID de AMI de infraestructura creado enthe section called “Prepare imágenes de máquinas de Amazon (AMIs)”.
IsLoadBalancerInternetFacing	Establézcalo en falso.
LoadBalancerSubnets	Elija subredes privadas sin acceso a Internet.
InfrastructureHostSubnets	Elija subredes privadas sin acceso a Internet.
VdiSubnets	Elija subredes privadas sin acceso a Internet.
ClientIP	Puede elegir el CIDR de la VPC para permitir el acceso a todas las direcciones IP de la VPC.

Crear recursos externos

Esta CloudFormation pila crea certificados de red, almacenamiento, Active Directory y dominio (si PortalDomainName se proporciona uno). Debe tener estos recursos externos disponibles para implementar el producto.

Puede descargar la plantilla de recetas antes de la implementación.

Tiempo de despliegue: aproximadamente entre 40 y 90 minutos

1. Inicie sesión en AWS Management Console https://console.aws.amazon.com/cloudformation y abra la AWS CloudFormation consola.

   > **Note**
   >
   > Asegúrese de estar en su cuenta de administrador.

2. Inicie la plantilla en la consola.

   Si va a realizar la implementación en la región AWS GovCloud (EE. UU.-Oeste), inicie la plantilla en la cuenta de GovCloud partición.

3. Introduzca los parámetros de la plantilla:

Parámetro	Predeterminado/a	Descripción
DomainName	`corp.res.com`	Dominio utilizado para el directorio activo. El valor predeterminado se proporcio na en el `LDIF` archivo que configura los usuarios de bootstrap. Si desea utilizar los usuarios predeterm inados, deje el valor como predeterminado. Para cambiar el valor, actualice y proporcione un `LDIF` archivo independiente. No es necesario que coincida con el dominio utilizado para Active Directory.
SubDomain (GovCloud solo)		Este parámetro es opcional para las regiones comercial es, pero obligatorio para GovCloud las regiones. Si proporciona un SubDomain, el parámetro tendrá el prefijo del DomainName proporcio nado. El nombre de dominio de Active Directory proporcio nado pasará a ser un subdominio.

Parámetro	Predeterminado/a	Descripción
AdminPassword		La contraseña del administrador de Active Directory (nombre de usuario`Admin`). Este usuario se crea en Active Directory para la fase inicial de arranque y no se utiliza después. Importante: el formato de este campo puede ser (1) una contraseña de texto simple o (2) el ARN de un AWS secreto formatead o como un par. key/value `{"password":"somepassword"}` Nota: La contraseña de este usuario debe cumplir los requisitos de complejidad de contraseñas de Active Directory.

Parámetro	Predeterminado/a	Descripción
ServiceAccountPassword		Contraseña utilizada para crear una cuenta de servicio (`ReadOnlyUser `). Esta cuenta se utiliza para la sincronización. Importante: el formato de este campo puede ser (1) una contraseña de texto simple o (2) el ARN de un AWS secreto formatead o como un par. key/value `{"password":"somep assword"}` Nota: La contraseña de este usuario debe cumplir los requisitos de complejidad de contraseñas de Active Directory.
Par de claves		Conecta las instancias administrativas mediante un cliente SSH. Nota: El administrador de AWS Systems Manager sesiones también se puede usar para conectarse a instancias.

Parámetro	Predeterminado/a	Descripción
LDIFS3Ruta	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	La ruta de Amazon S3 a un archivo LDIF importado durante la fase de arranque de la configuración de Active Directory. Para obtener más información, consulte LDIF Support. El parámetro se rellena previamente con un archivo que crea varios usuarios en el directorio activo. Para ver el archivo, consulte el archivo res.ldif disponible en. GitHub
ClientIpCidr		La dirección IP desde la que accederá al sitio. Por ejemplo, puede seleccionar su dirección IP y utilizarla `[IPADDRESS]/32` para permitir el acceso únicamente desde su servidor. Puede actualizarla después de la implementación.

Parámetro	Predeterminado/a	Descripción
ClientPrefixList		Introduzca una lista de prefijos para proporcionar acceso a los nodos de administración de Active Directory. Para obtener información sobre la creación de una lista de prefijos administrada, consulte Trabajar con listas de prefijos administradas por el cliente.
EnvironmentName	`res-[environment name]`	Si `PortalDomainName` se proporciona, este parámetro se usa para agregar etiquetas a los secretos generados para que puedan usarse en el entorno. Deberá coincidir con el `EnvironmentName` parámetro utilizado al crear la pila RES. Si vas a implementar varios entornos en tu cuenta, tendrá que ser único.

Parámetro	Predeterminado/a	Descripción
PortalDomainName		Para GovCloud las implementaciones, no introduzcas este parámetro . Los certificados y los secretos se crearon manualmente durante los requisitos previos. El nombre de dominio de Amazon Route 53 de la cuenta. Si se proporciona, se generará un certifica do público y un archivo de claves y se cargarán en ellos AWS Secrets Manager. Si tiene su propio dominio y certificados, `Environme ntName` puede dejar este parámetro en blanco.

4. Marque todas las casillas de verificación en Capacidades y elija Crear pila.

Paso 1: lanzar el producto

Siga las step-by-step instrucciones de esta sección para configurar e implementar el producto en su cuenta.

Tiempo de implementación: aproximadamente 60 minutos

Puede descargar la CloudFormation plantilla de este producto antes de implementarlo.

Si va a realizar el despliegue en AWS GovCloud (EE. UU. al oeste), utilice esta plantilla.

res-stack: utilice esta plantilla para lanzar el producto y todos los componentes asociados. La configuración predeterminada implementa la pila principal de RES y los recursos de autenticación, interfaz y backend.

> **Note**
>
> AWS CloudFormation los recursos se crean a partir de construcciones AWS Cloud Development Kit (AWS CDK) ()AWS CDK.

La AWS CloudFormation plantilla implementa Research and Engineering Studio AWS en el. Nube de AWS Debe cumplir los requisitos previos antes de lanzar la pila.

1. Inicia sesión en AWS Management Console https://console.aws.amazon.com/cloudformation y abre la AWS CloudFormation consola.
2. Abre la plantilla.

   Para implementarla en AWS GovCloud (EE. UU. al oeste), lance esta plantilla.
3. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar la solución en otro lugar Región de AWS, utilice el selector de regiones de la barra de navegación de la consola.

   > **Note**
   >
   > Este producto utiliza el servicio Amazon Cognito, que actualmente no está disponible en todos. Regiones de AWS Debe lanzar este producto en un Región de AWS lugar en el que Amazon Cognito esté disponible. Para obtener la disponibilidad más reciente por región, consulte la lista de Región de AWS todos los servicios.
4. En Parámetros, revisa los parámetros de esta plantilla de producto y modifícalos según sea necesario. Si ha implementado los recursos externos automatizados, puede encontrar estos parámetros en la pestaña Resultados de la pila de recursos externos.

Parámetro	Predeterminado/a	Descripción
EnvironmentName	`<res-demo>`	Nombre exclusivo asignado a su entorno RES que comienza por res- y no debe superar los 11 caracteres.
AdministratorEmail		La dirección de correo electrónico del usuario que

Parámetro	Predeterminado/a	Descripción
		completa la configuración del producto. Este usuario también funciona como un usuario rompeolas si se produce un error en la integración del inicio de sesión único de Active Directory.
InfrastructureHostAMI	ami- *[numbers or letters only]*	(Opcional) Puede proporcionar un identificador de AMI personalizado para usarlo en todos los hosts de la infraestructura. El sistema operativo base compatible actualmente es Amazon Linux 2. Para obtener más información, consulte Configurar RES-Ready AMIs.
SSHKeyPar		El key pair que se utiliza para conectarse a los hosts de la infraestructura.
ClientIP	*x.x.x*.0/24 o .0/32 *x.x.x*	Filtro de direcciones IP que limita la conexión al sistema. Puede actualizarlo ClientIpCidr después de la implementación.
ClientPrefixList		(Opcional) Proporcione una lista de prefijos gestionada para IPs permitir el acceso directo a la interfaz de usuario web y a SSH desde el host bastión.

Parámetro	Predeterminado/a	Descripción
IAMPermissionLímite		(Opcional) Puede proporcio nar un ARN de política administrada que se adjuntará como límite de permisos a todos los roles creados en RES. Para obtener más información, consulte Establecer límites de permisos personalizados.
VpcId		IP de la VPC en la que se lanzarán las instancias.
IsLoadBalancerInternetFacin g		Seleccione true para implementar un balanceador de carga orientado a Internet (requiere subredes públicas para el balanceador de carga). Para las implement aciones que necesitan acceso restringido a Internet, selecciona false.

Parámetro	Predeterminado/a	Descripción
LoadBalancerSubnets		Seleccione al menos dos subredes en distintas zonas de disponibilidad donde se lanzarán los balanceadores de carga. Para las implement aciones que necesitan acceso restringido a Internet, elija subredes privadas. Para las implementaciones que necesitan acceso a Internet, elija subredes públicas. Si la pila de redes externas creó más de dos, seleccione todas las que se crearon.
InfrastructureHostSubnets		Seleccione al menos dos subredes privadas en distintas zonas de disponibi lidad donde se lanzarán los hosts de infraestructura. Si la pila de redes externas creó más de dos, seleccion e todas las que se hayan creado.
VdiSubnets		Seleccione al menos dos subredes privadas en distintas zonas de disponibi lidad donde se lanzarán las instancias de VDI. Si la pila de redes externas creó más de dos, seleccione todas las que se hayan creado.

Parámetro	Predeterminado/a	Descripción
ActiveDirectoryName	`corp.res.com`	Dominio para el directorio activo. No es necesario que coincida con el nombre de dominio del portal.
ADShortNombre	`corp`	El nombre abreviado del directorio activo. También se denomina nombre de NetBIOS.
Base LDAP	**`DC=corp,DC=res,DC=com`**	Una ruta LDAP a la base dentro de la jerarquía LDAP.
LDAPConnectionURI		Una única ruta ldap://a la que puede acceder el servidor host de Active Directory. Si implement aste los recursos externos automatizados con el dominio AD predeterminado, puedes usar ldap: //corp.re s.com.
ServiceAccountUserName	ServiceAccount	Nombre de usuario de una cuenta de servicio utilizada para conectarse a AD. Esta cuenta debe tener acceso para crear ordenadores dentro de ComputerSOU.
ServiceAccountPass wordSecretArn		Proporcione un ARN secreto que contenga la contraseñ a de texto simple para. ServiceAccount

Parámetro	Predeterminado/a	Descripción
Usuario SOU		Unidad organizativa dentro de AD para los usuarios que se sincronizarán.
Grupo SOU		Unidad organizativa dentro de AD para los grupos que se sincronizarán.
SudoerSou		Unidad organizativa de AD para sudoers globales.
SudoersGroupName	RESAdministrators	Nombre de grupo que contiene todos los usuarios con acceso a sudoer en las instancias en el momento de la instalación y acceso de administrador en RES.
Computador/SOU		Unidad organizativa de AD a la que se unirán las instancia s.
TLSCertificateSecretarN de dominio		(Opcional) Proporcione un ARN secreto de certifica do TLS de dominio para habilitar la comunicación TLS con AD.

Parámetro	Predeterminado/a	Descripción
EnableLdapIDMapping		Determina si el SSSD genera los números UID y GID o si se utilizan los números proporcionados por el AD. Establézcalo en True para usar el UID y el GID generados por SSSD, o en False para usar el UID y el GID proporcionados por el AD. En la mayoría de los casos, este parámetro debe estar establecido en True.
Desactivar ADJoin	False	Para evitar que los hosts Linux se unan al dominio del directorio, cambie a True. De lo contrario, deje la configura ción predeterminada de False.
ServiceAccountUserDN		Proporcione el nombre distintivo (DN) del usuario de la cuenta de servicio en el Directorio.
SharedHomeFilesystemID		Un ID de EFS que se utilizará en el sistema de archivos doméstico compartido para los hosts VDI de Linux.
CustomDomainNamefo rWebApp		(Opcional) Subdominio utilizado por el portal web para proporcionar enlaces a la parte web del sistema.

Parámetro	Predeterminado/a	Descripción
CustomDomainNameforVDI		(Opcional) Subdominio utilizado por el portal web para proporcionar enlaces a la parte de VDI del sistema.
ACMCertificateARNforWebApp		(Opcional) Si se utiliza la configuración predeterminada, el producto aloja la aplicación web en el dominio amazonaws.com. Puede alojar los servicios del producto en su dominio. Si implementaste los recursos externos automatizados, se generaron para ti y la información se encuentra en los resultados de la pila res-bi. Si necesita generar un certificado para su aplicación web, consulte. Guía de configuración
CertificateSecretARNforVDI		(Opcional) Este secreto de ARN almacena el certificado público del certificado público de su portal web. Si establece un nombre de dominio de portal para sus recursos externos automatizados, puede encontrar este valor en la pestaña Resultados de la pila res-bi.

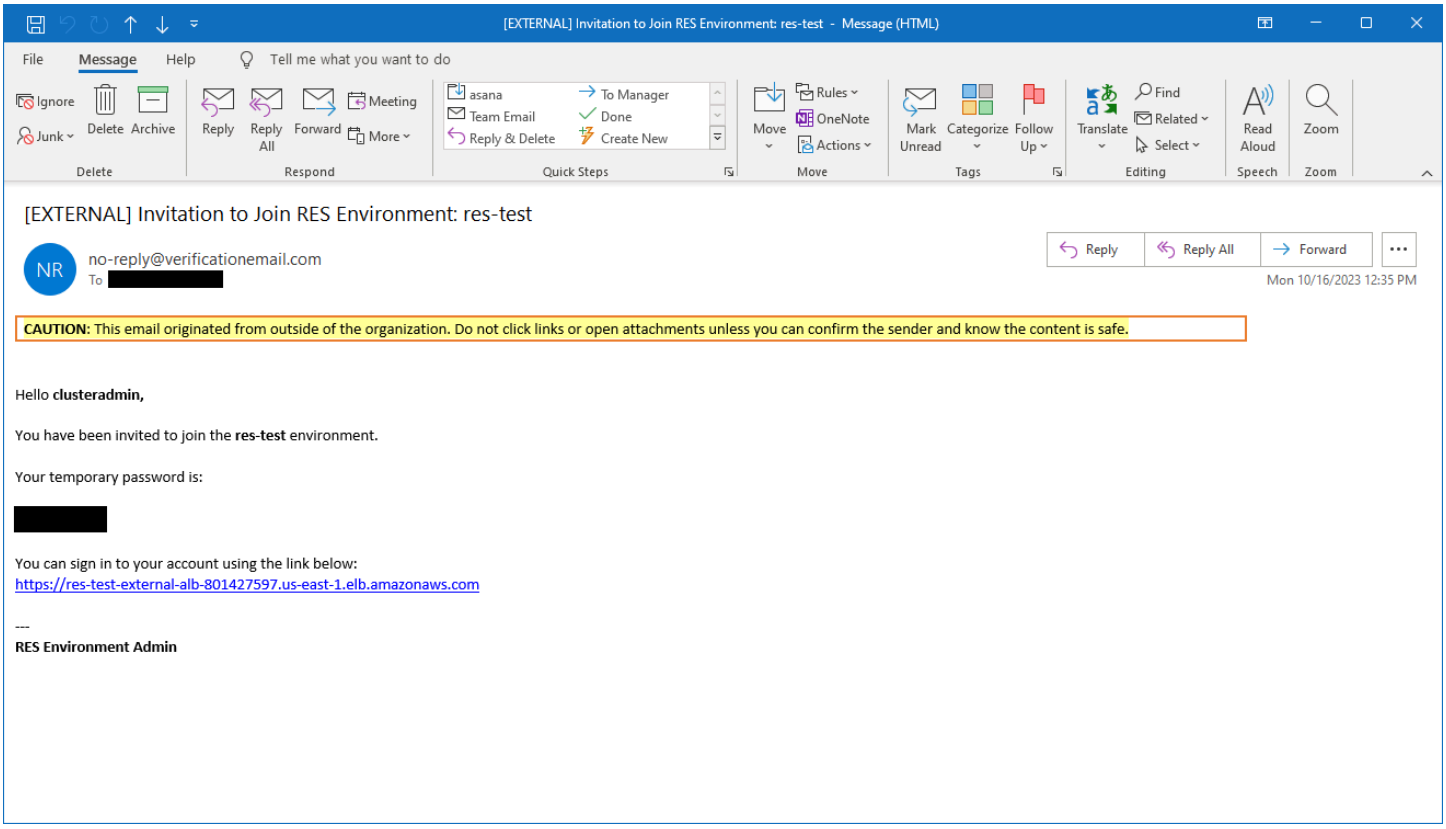
Parámetro	Predeterminado/a	Descripción
PrivateKeySecretARNforVDI		(Opcional) Este secreto ARN almacena la clave privada del certificado de su portal web. Si establece s un nombre de dominio de portal para tus recursos externos automatizados, puedes encontrar este valor en la pestaña Resultados de la pila res-bi.

5. Elija Create stack (Crear pila) para implementar la pila.

Puede ver el estado de la pila en la AWS CloudFormation consola, en la columna Estado. Deberías recibir el estado CREATE_COMPLETE en aproximadamente 60 minutos.

Paso 2: Inicie sesión por primera vez

Una vez que la gama de productos se haya desplegado en su cuenta, recibirá un correo electrónico con sus credenciales. Usa la URL para iniciar sesión en tu cuenta y configurar el espacio de trabajo para otros usuarios.



Una vez que haya iniciado sesión por primera vez, podrá configurar los ajustes del portal web para conectarse al proveedor de SSO. Para obtener información sobre la configuración posterior a la implementación, consulte la. Guía de configuración Tenga en cuenta que `clusteradmin` es una cuenta única: puede usarla para crear proyectos y asignar miembros de usuarios o grupos a esos proyectos; no puede asignar paquetes de software ni implementar un escritorio por sí misma.

Actualiza el producto

Research and Engineering Studio (RES) tiene dos métodos para actualizar el producto que dependen de si la actualización de la versión es importante o secundaria.

RES utiliza un esquema de control de versiones basado en fechas. Una versión principal utiliza el año y el mes, y una versión secundaria agrega un número de secuencia cuando es necesario. Por ejemplo, la versión 2024.01 se publicó en enero de 2024 como una versión principal; la versión 2024.01.01 fue una actualización menor de esa versión.

Temas

Actualizaciones de versiones principales

Research and Engineering Studio utiliza instantáneas para facilitar la migración de un entorno RES anterior al más reciente sin perder la configuración del entorno. También puede usar este proceso para probar y verificar las actualizaciones de su entorno antes de incorporar usuarios.

Para actualizar su entorno con la versión más reciente de RES:

1. Cree una instantánea de su entorno actual. Consulte the section called “Crear una instantánea”.
2. Vuelva a implementar RES con la nueva versión. Consulte the section called “Paso 1: lanza el producto”.
3. Aplique la instantánea a su entorno actualizado. Consulte the section called “Aplica una instantánea”.
4. Compruebe que todos los datos se hayan migrado correctamente al nuevo entorno.

Actualizaciones de versiones menores

Para las actualizaciones de versiones menores de RES, no es necesaria una nueva instalación. Puede actualizar la pila RES existente actualizando su AWS CloudFormation plantilla. Compruebe la versión de su entorno RES actual AWS CloudFormation antes de implementar la actualización. Puede encontrar el número de versión al principio de la plantilla.

Por ejemplo: `"Description": "RES_2024.1"`

Para realizar una actualización menor de la versión:

1. Descarga la AWS CloudFormation plantilla más reciente enthe section called “Paso 1: lanza el producto”.
2. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
3. En Stacks, busca y selecciona la pila principal. Debería aparecer como*<stack-name>*.
4. Elija Actualizar.
5. Selecciona Reemplazar la plantilla actual.
6. Para Origen de plantilla, elija Cargar un archivo de plantilla.
7. Selecciona Elegir archivo y carga la plantilla que has descargado.
8. En Especificar los detalles de la pila, selecciona Siguiente. No es necesario actualizar los parámetros.
9. En Configurar las opciones de pila, seleccione Siguiente.
10. En Revisar<stack-name>, selecciona Enviar.

Desinstalar el producto

Puede desinstalar Research and Engineering Studio en el AWS producto desde AWS Management Console o utilizando el AWS Command Line Interface. Debe eliminar manualmente los buckets de Amazon Simple Storage Service (Amazon S3) creados por este producto. Este producto no elimina automáticamente < EnvironmentName >- shared-storage-security-group en caso de que haya almacenado datos que deba conservar.

Usando el AWS Management Console

1. Inicie sesión en la consola de AWS CloudFormation.
2. En la página Stacks, seleccione la pila de instalación de este producto.
3. Elija Eliminar.

Usando AWS Command Line Interface

Determine si el AWS Command Line Interface (AWS CLI) está disponible en su entorno. Para obtener instrucciones de instalación, consulte Qué es AWS Command Line Interface en la Guía del AWS CLI usuario. Tras confirmar que AWS CLI está disponible y configurado en la cuenta de administrador de la región en la que se implementó el producto, ejecute el siguiente comando.

```
$ aws cloudformation delete-stack --stack-name
<RES-stack-name>
```

Eliminar el shared-storage-security-group

> **Warning**
>
> El producto conserva este sistema de archivos de forma predeterminada para protegerlo contra la pérdida de datos involuntaria. Si decide eliminar el grupo de seguridad y los sistemas de archivos asociados, todos los datos que se conserven en esos sistemas se eliminarán permanentemente. Se recomienda hacer una copia de seguridad de los datos o reasignarlos a un nuevo grupo de seguridad.

1. Inicie sesión en la consola de Amazon EFS AWS Management Console y ábrala en https://console.aws.amazon.com/efs/.
2. Elimine todos los sistemas de archivos asociados a *<RES-stack-name>* -shared-storage-security-group. Como alternativa, puede reasignar estos sistemas de archivos a otro grupo de seguridad para conservar los datos.
3. Inicia sesión en la EC2 consola de Amazon AWS Management Console y ábrela en https://console.aws.amazon.com/ec2/.
4. Elimina el *<RES-stack-name>* -shared-storage-security-group.

Eliminar los buckets de Amazon S3

Este producto está configurado para conservar el bucket de Amazon S3 creado por el producto (para implementarlo en una región opcional) si decide eliminar la AWS CloudFormation pila para evitar la pérdida accidental de datos. Tras desinstalar el producto, puede eliminar manualmente este depósito de S3 si no necesita conservar los datos. Siga estos pasos para eliminar el bucket de Amazon S3.

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala en https://console.aws.amazon.com/s3/.
2. En el panel de navegación, elija Buckets.
3. Localice los depósitos de `stack-name` S3.
4. Selecciona cada depósito de Amazon S3 y, a continuación, selecciona Vacío. Debe vaciar cada cubo.
5. Seleccione el depósito S3 y elija Eliminar.

Para eliminar buckets de S3 mediante AWS CLI, ejecute el siguiente comando:

```
$ aws s3 rb s3://<bucket-name> --force
```

> **Note**
>
> El `--force` comando vacía el contenido del depósito.

Guía de configuración

Esta guía de configuración proporciona instrucciones posteriores a la implementación para un público técnico sobre cómo personalizar e integrar aún más el estudio de investigación e ingeniería del producto. AWS

Temas

Administrar usuarios y grupos

Research and Engineering Studio puede utilizar cualquier proveedor de identidad compatible con SAML 2.0. Si implementó RES con recursos externos o planea usar el centro de identidad de IAM, consulte. Configuración del inicio de sesión único (SSO) con IAM Identity Center Si tiene su propio proveedor de identidad compatible con SAML 2.0, consulte. Configuración del proveedor de identidad para el inicio de sesión único (SSO)

Temas

Configuración del inicio de sesión único (SSO) con IAM Identity Center

Si aún no tiene un centro de identidad conectado al Active Directory administrado, comience con. Paso 1: Configurar un centro de identidad Si ya tiene un centro de identidad conectado al Active Directory administrado, comience conPaso 2: Conectarse a un centro de identidad.

> **Note**
>
> Si va a realizar la implementación en la región AWS GovCloud (EE. UU. Oeste), configure el SSO en la cuenta de AWS GovCloud (US) partición en la que implementó Research and Engineering Studio.

Paso 1: Configurar un centro de identidad

Habilitación de IAM Identity Center

1. Inicie sesión en la consola de AWS Identity and Access Management.
2. Abra el Centro de identidad.
3. Seleccione Habilitar.
4. Seleccione Activar con AWS Organizations.
5. Seleccione Continuar.

> **Note**
>
> Asegúrese de estar en la misma región en la que tiene su Active Directory administrado.

Conexión del IAM Identity Center a un Active Directory administrado

Tras activar el Centro de identidades de IAM, complete estos pasos de configuración recomendados:

1. En el panel de navegación, seleccione Configuración.
2. En Fuente de identidad, seleccione Acciones y elija Cambiar fuente de identidad.
3. En Directorios existentes, selecciona tu directorio.
4. Seleccione Siguiente.
5. Revise los cambios e **`ACCEPT`** introdúzcalos en el cuadro de confirmación.
6. Seleccione Cambiar fuente de identidad.

Sincronizar usuarios y grupos con el centro de identidad

Una vez que se hayan completado Conexión del IAM Identity Center a un Active Directory administrado los cambios realizados, aparecerá un banner de confirmación verde.

1. En el banner de confirmación, selecciona Iniciar la configuración guiada.
2. En Configurar asignaciones de atributos, seleccione Siguiente.
3. En la sección Usuario, introduce los usuarios que deseas sincronizar.
4. Seleccione Añadir.
5. Seleccione Siguiente.
6. Revisa los cambios y, a continuación, selecciona Guardar configuración.
7. El proceso de sincronización puede tardar unos minutos. Si recibes un mensaje de advertencia sobre los usuarios que no se están sincronizando, selecciona Reanudar la sincronización.

Habilitar usuarios

1. En el menú, selecciona Usuarios.
2. Elija los usuarios para los que desea habilitar el acceso.
3. Seleccione Habilitar el acceso de los usuarios.

Paso 2: Conectarse a un centro de identidad

Configuración de la aplicación en el Centro de identidades de IAM

1. Abra la consola de IAM Identity Center.
2. Seleccione Aplicaciones.
3. Selecciona Añadir aplicación.
4. En las preferencias de configuración, selecciona Tengo una aplicación que quiero configurar.
5. En Tipo de aplicación, selecciona SAML 2.0.
6. Seleccione Siguiente.
7. Introduzca el nombre para mostrar y la descripción que desee utilizar.
8. En Metadatos del Centro de Identidad de IAM, copie el enlace del archivo de metadatos SAML del Centro de Identidad de IAM. Lo necesitará al configurar el Centro de identidades de IAM con el portal RES.

9. En Propiedades de la aplicación, introduzca la URL de inicio de la aplicación. Por ejemplo, `<your-portal-domain>/sso`.
10. En la URL ACS de la aplicación, introduzca la URL de redireccionamiento desde el portal RES. Para encontrar esto:
    a. En Administración del entorno, selecciona Configuración general.
    b. Elija la pestaña Identity provider.
    c. En el inicio de sesión único, encontrarás la URL de redireccionamiento de SAML.
11. En Audiencia SAML de la aplicación, introduzca la URN de Amazon Cognito.

    Para crear la urna:

    a. Desde el portal RES, abra la configuración general.
    b. En la pestaña Proveedor de identidades, localice el ID del grupo de usuarios.
    c. Agregue el ID del grupo de usuarios a esta cadena:

    ```
    urn:amazon:cognito:sp:<user_pool_id>
    ```

12. Tras introducir la URN de Amazon Cognito, seleccione Enviar.

Configuración de las asignaciones de atributos para la aplicación

1. En el Centro de identidad, abra los detalles de la aplicación que ha creado.
2. Seleccione Acciones y, a continuación, seleccione Editar asignaciones de atributos.
3. En Asunto, introduzca **`${user:email}`**.
4. En Formato, selecciona Dirección de correo electrónico.
5. Selecciona Añadir nueva asignación de atributos.
6. En el campo Atributo de usuario de la aplicación, introduzca «correo electrónico».
7. En Asignar a este valor de cadena o atributo de usuario del Centro de Identidad de IAM, introduzca. **`${user:email}`**
8. En Formato, escriba «sin especificar».
9. Seleccione Guardar cambios.

Añadir usuarios a la aplicación en el Centro de identidades de IAM

1. En el Centro de identidades, abra Usuarios asignados para la aplicación que haya creado y elija Asignar usuarios.
2. Elija los usuarios a los que desee asignar el acceso a la aplicación.
3. Seleccione Asignar usuarios.

Configuración del centro de identidad de IAM en el entorno RES

1. En el entorno de Research and Engineering Studio, en Administración del entorno, abra Configuración general.
2. Abra la pestaña Proveedor de identidades.
3. En Inicio de sesión único, selecciona Editar (junto a Estado).
4. Complete el formulario con la siguiente información:
    a. Elija SAML.
    b. En Nombre del proveedor, introduzca un nombre fácil de usar.
    c. Seleccione Introducir la URL del punto final del documento de metadatos.
    d. Introduce la URL que copiaste durante el procesoConfiguración de la aplicación en el Centro de identidades de IAM.
    e. En el atributo de correo electrónico del proveedor, introduce «correo electrónico».
    f. Elija Enviar.
5. Actualiza la página y comprueba que el estado se muestre como activado.

Configuración del proveedor de identidad para el inicio de sesión único (SSO)

Research and Engineering Studio se integra con cualquier proveedor de identidades de SAML 2.0 para autenticar el acceso de los usuarios al portal RES. Estos pasos proporcionan instrucciones para la integración con el proveedor de identidades de SAML 2.0 que elija. Si tiene intención de utilizar el Centro de identidades de IAM, consulte. the section called “Configuración del SSO con IAM Identity Center”

> **Note**
>
> El correo electrónico del usuario debe coincidir en la afirmación SAML del IDP y en Active Directory. Deberá conectar su proveedor de identidad con su Active Directory y sincronizar los usuarios periódicamente.

Temas

Configure su proveedor de identidad

En esta sección se proporcionan los pasos para configurar su proveedor de identidad con información del grupo de usuarios de Amazon Cognito de RES.

1. RES presupone que tiene un AD (AD AWS gestionado o un AD autoaprovisionado) con las identidades de usuario autorizadas para acceder al portal y a los proyectos de RES. Conecte su AD a su proveedor de servicios de identidad y sincronice las identidades de los usuarios. Consulta la documentación de tu proveedor de identidad para obtener información sobre cómo conectar tu AD y sincronizar las identidades de los usuarios. Por ejemplo, consulte Uso de Active Directory como fuente de identidad en la Guía del AWS IAM Identity Center usuario.
2. Configure una aplicación SAML 2.0 para RES en su proveedor de identidad (IdP). Esta configuración requiere los siguientes parámetros:
   - URL de redireccionamiento de SAML: la URL que utiliza su IdP para enviar la respuesta de SAML 2.0 al proveedor de servicios.

     > **Note**
     >
     > Según el IdP, la URL de redireccionamiento de SAML puede tener un nombre diferente:
     > - URL de aplicación
     > - URL del Servicio de Consumer de Afirmación (ACS)
     > - URL de enlace POST de ACS

Para obtener la URL

1. Inicie sesión en RES como administrador o administrador de clústeres.
2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.
3. Elija la URL de redireccionamiento de SAML.

- URI de audiencia de SAML: el ID único de la entidad de audiencia de SAML por parte del proveedor de servicios.

> **Note**
>
> Según el IdP, el URI de audiencia de SAML puede tener un nombre diferente:
>
> - ClientID
> - Aplicación: SAML Audience
> - ID de entidad del SP

Proporcione la entrada en el siguiente formato.

```
urn:amazon:cognito:sp:user-pool-id
```

Para encontrar tu URI de audiencia de SAML

1. Inicia sesión en RES como administrador o administrador de clústeres.
2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.
3. Elija el ID del grupo de usuarios.

3. La afirmación de SAML publicada en RES debe tener la siguiente fields/claims configuración en la dirección de correo electrónico del usuario:
   - Asunto o NameID de SAML
   - Correo electrónico SAML
4. Su IdP se agrega fields/claims a la afirmación SAML en función de la configuración. RES requiere estos campos. La mayoría de los proveedores rellenan estos campos automáticamente de

forma predeterminada. Consulte las siguientes entradas y valores de los campos si tiene que configurarlos.

- AudienceRestriction: se establece en `urn:amazon:cognito:sp:`*`user-pool-id`*. *`user-pool-id`*Sustitúyalo por el ID de tu grupo de usuarios de Amazon Cognito.

```
<saml:AudienceRestriction>
    <saml:Audience> urn:amazon:cognito:sp:user-pool-id
</saml:AudienceRestriction>
```

- Respuesta: se establece en`InResponseTo`. `https://`*`user-pool-domain`*`/saml2/idpresponse` *`user-pool-domain`*Sustitúyalo por el nombre de dominio de tu grupo de usuarios de Amazon Cognito.

```
<saml2p:Response
  Destination="http://user-pool-domain/saml2/idpresponse"
  ID="id123"
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  IssueInstant="Date-time stamp"
  Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

- SubjectConfirmationData— `Recipient` Configúrelo en el `saml2/idpresponse` punto final de su grupo de usuarios y `InResponseTo` en el ID de solicitud SAML original.

```
<saml2:SubjectConfirmationData
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  NotOnOrAfter="Date-time stamp"
  Recipient="https://user-pool-domain/saml2/idpresponse"/>
```

- AuthnStatement— Configúrelo de la siguiente manera:

```
<saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ"
  SessionIndex="32413b2e54db89c764fb96ya2k"
 SessionNotOnOrAfter="2016-10-30T13:13:28">
    <saml2:SubjectLocality />
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
```

```
</saml2:AuthnStatement>
```

5. Si su aplicación SAML tiene un campo de URL de cierre de sesión, configúrelo en:. <*domain-url*>/saml2/logout

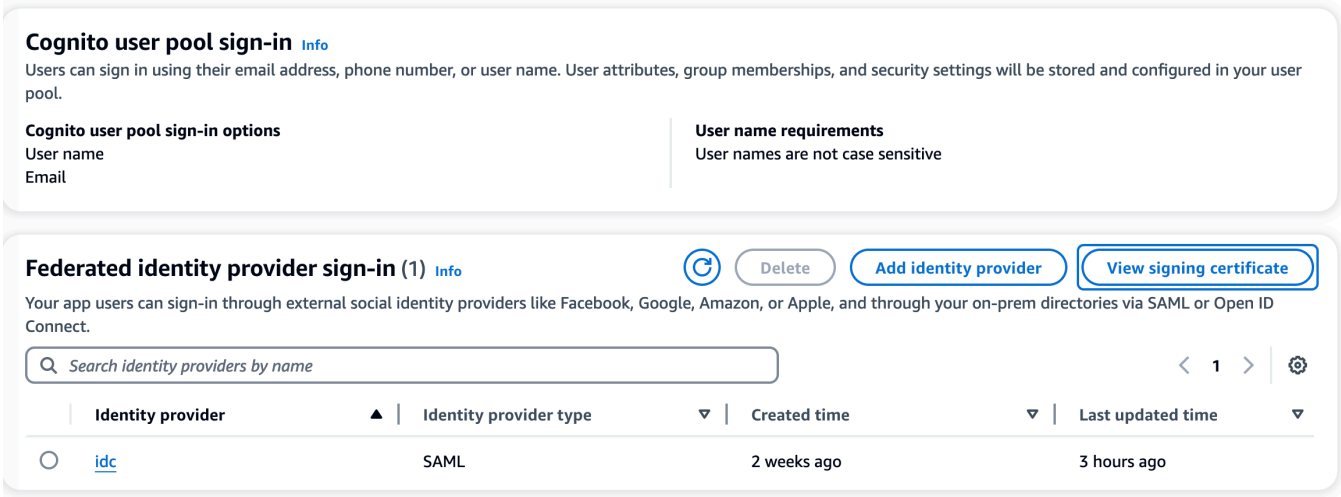
   Para obtener la URL del dominio

   1. Inicie sesión en RES como administrador o administrador de clústeres.
   2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.
   3. Elija la URL del dominio.

6. Si su IdP acepta un certificado de firma para establecer la confianza en Amazon Cognito, descargue el certificado de firma de Amazon Cognito y cárguelo en su IdP.

   Para obtener el certificado de firma

   1. Abra la consola de Amazon Cognito en la sección Introducción a AWS Management Console
   2. Seleccione su grupo de usuarios. Su grupo de usuarios debería serlores-*<environment name>*-user-pool.
   3. Elija la pestaña Experiencia de inscripción.
   4. En la sección de inicio de sesión con un proveedor de identidad federado, selecciona Ver certificado de firma.



Puede usar este certificado para configurar el IDP de Active Directory, agregar un `relying party trust` y habilitar la compatibilidad con SAML en la parte que confía.

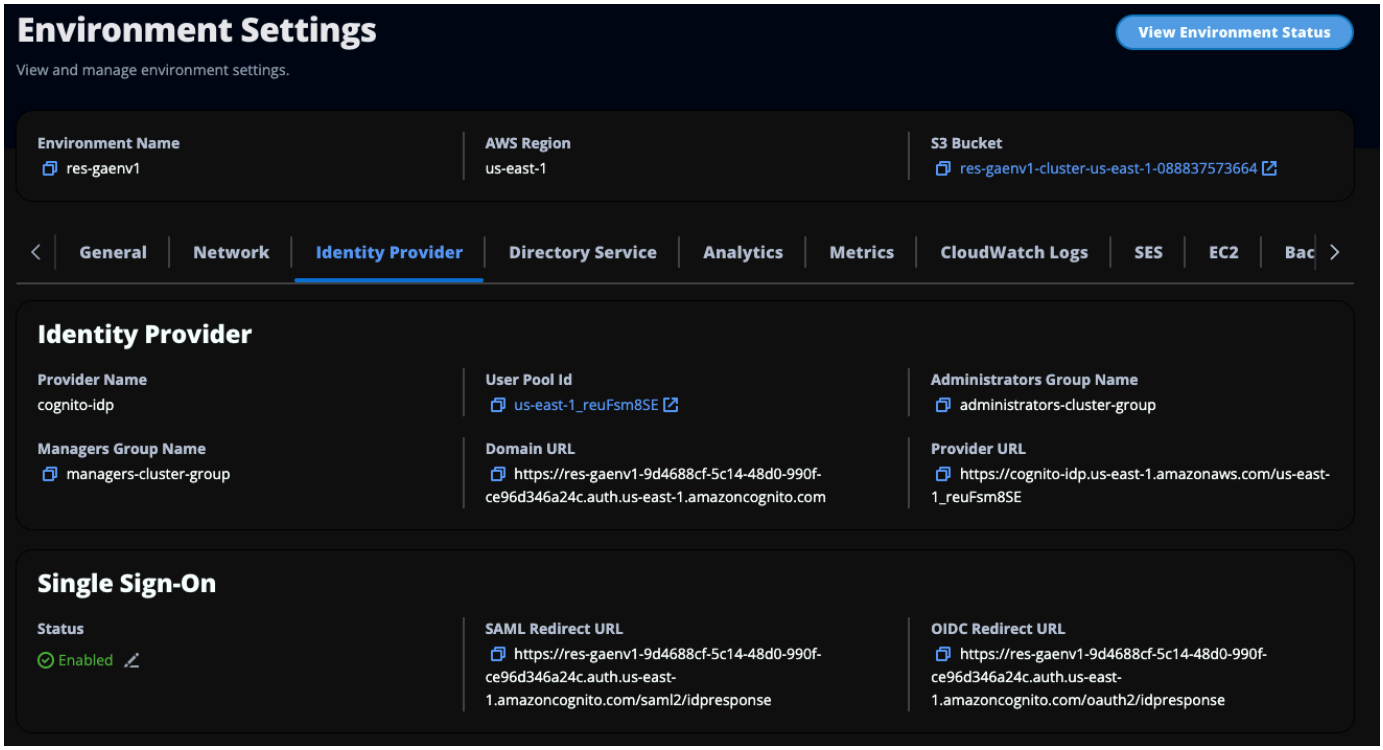
> **Note**
>
> Esto no se aplica a Keycloak ni a IDC.

5. Una vez completada la configuración de la aplicación, descargue el XML o la URL de los metadatos de la aplicación SAML 2.0. Lo usarás en la siguiente sección.

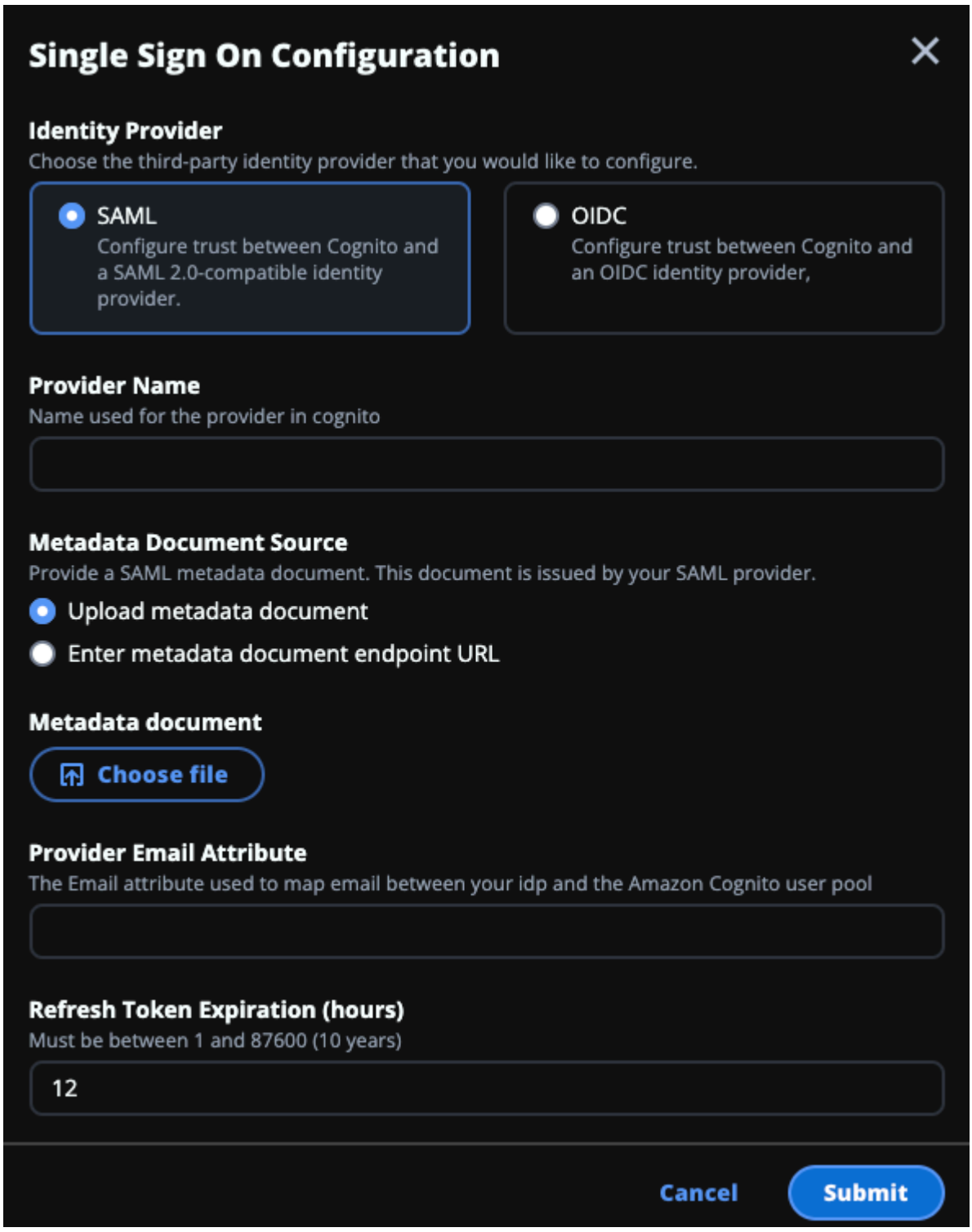
Configure RES para usar su proveedor de identidad

Para completar la configuración del inicio de sesión único para RES

1. Inicie sesión en RES como administrador o administrador de clústeres.
2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.



3. En el inicio de sesión único, seleccione el icono de edición situado junto al indicador de estado para abrir la página de configuración del inicio de sesión único.



a. En Identity Provider, elija SAML.

b. En Nombre del proveedor, introduce un nombre único para tu proveedor de identidad.

> **Note**
>
> No se permiten los siguientes nombres:
>
> - Cognito
> - IdentityCenter

c. En Fuente del documento de metadatos, elija la opción adecuada y cargue el documento XML de metadatos o proporcione la URL del proveedor de identidad.

d. En el campo Atributo de correo electrónico del proveedor, introduzca el valor del texto`email`.

e. Elija Enviar.

4. Vuelva a cargar la página de configuración del entorno. El inicio de sesión único está habilitado si la configuración es correcta.

Configurar el proveedor de identidades en un entorno que no sea de producción

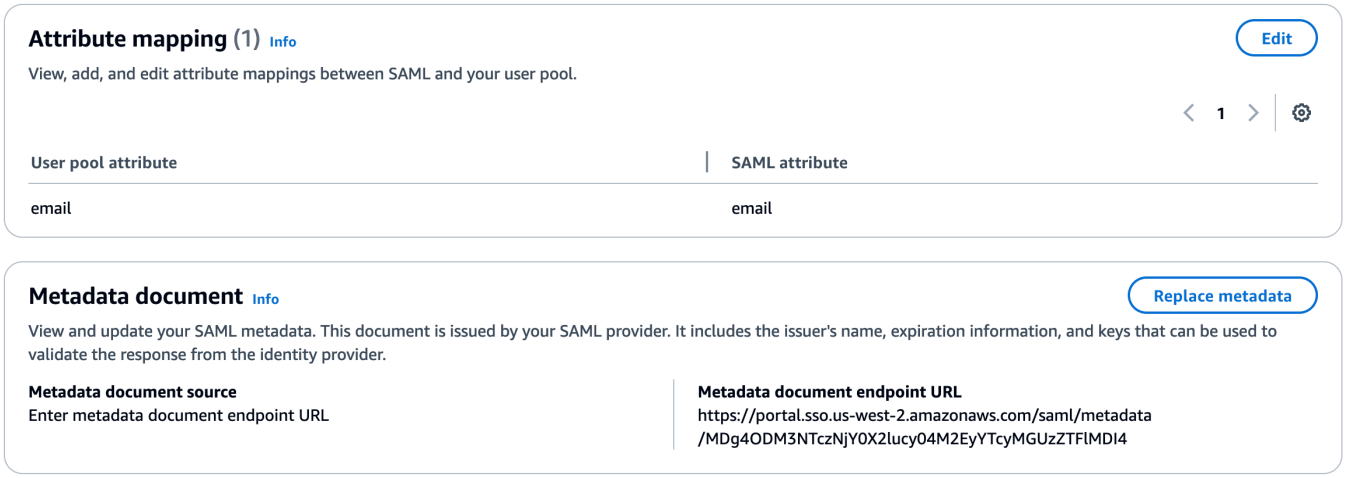
Si utilizó los recursos externos proporcionados para crear un entorno RES que no fuera de producción y configuró IAM Identity Center como su proveedor de identidades, puede que desee configurar un proveedor de identidades diferente, como Okta. El formulario de activación del SSO de RES solicita tres parámetros de configuración:

1. Nombre del proveedor: no se puede modificar
2. Documento de metadatos o URL: se puede modificar
3. Atributo de correo electrónico del proveedor: se puede modificar

Para modificar el documento de metadatos y el atributo de correo electrónico del proveedor, haga lo siguiente:

1. Vaya a la consola de Amazon Cognito.
2. En la barra de navegación, elija Grupos de usuarios.
3. Elija su grupo de usuarios para ver la descripción general del grupo de usuarios.
4. En la pestaña Experiencia de inicio de sesión, vaya a Inicio de sesión con un proveedor de identidad federado y abra el proveedor de identidad configurado.

5. Por lo general, solo tendrás que cambiar los metadatos y dejar la asignación de atributos sin cambios. Para actualizar el mapeo de atributos, elija Editar. Para actualizar el documento de metadatos, seleccione Reemplazar metadatos.



6. Si ha editado la asignación de atributos, tendrá que actualizar la `<environment name>.cluster-settings` tabla en DynamoDB.

   a. Abra la consola de DynamoDB y seleccione Tablas en la barra de navegación.

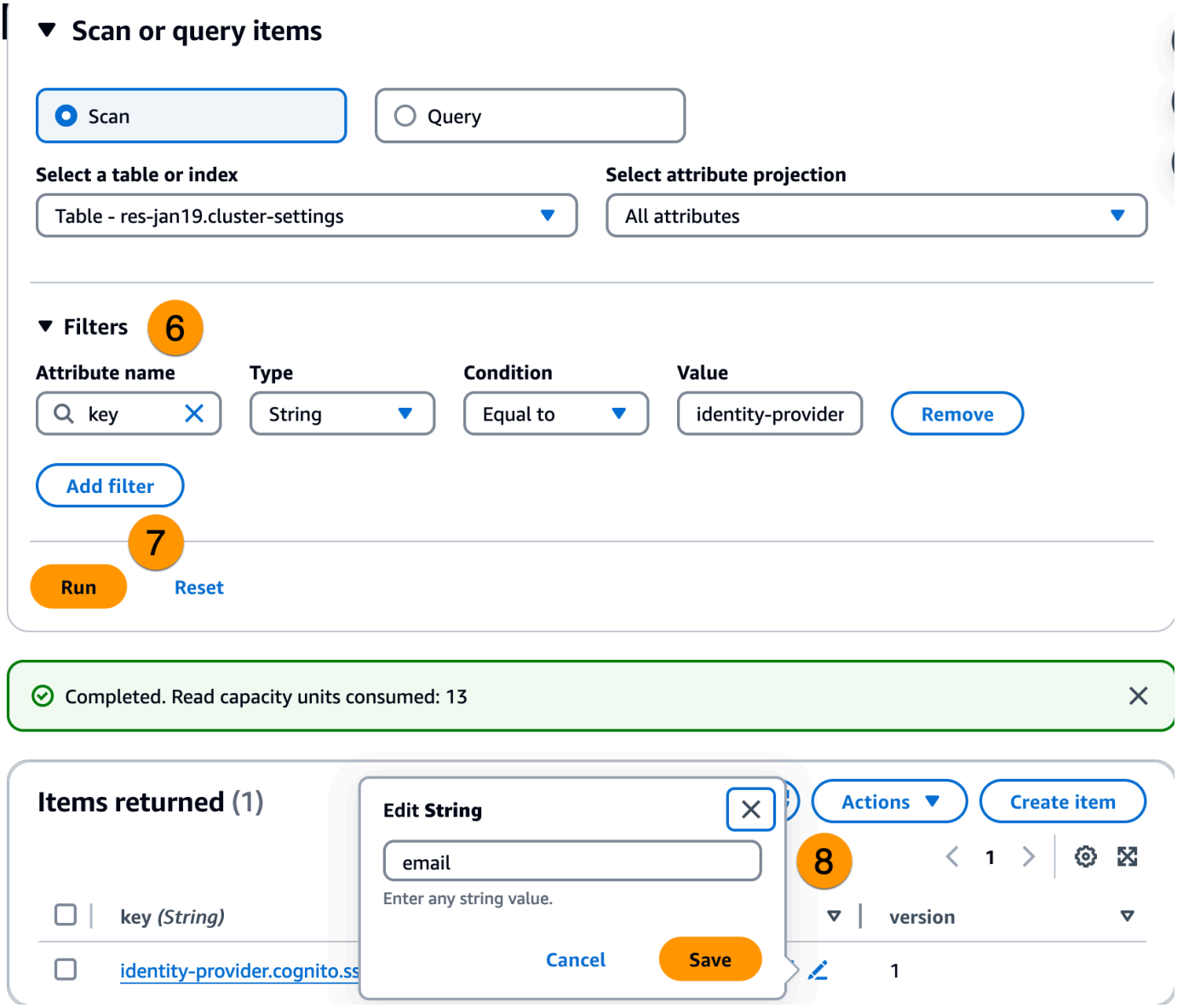
   b. Busque y seleccione la `<environment name>.cluster-settings` tabla y, en el menú Acciones, elija Explorar elementos.

   c. En Escanear o consultar elementos, vaya a Filtros e introduzca los siguientes parámetros:

      - Nombre del atributo: `key`
      - Valor — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. Seleccione Ejecutar.

7. En Elementos devueltos, busque la `identity-provider.cognito.sso_idp_provider_email_attribute` cadena y seleccione Editar para modificarla y adaptarla a los cambios en Amazon Cognito.



Depuración de problemas de IdP de SAML

SAML-Tracer: puedes usar esta extensión para el navegador Chrome para rastrear las solicitudes de SAML y comprobar los valores de las aserciones de SAML. Para obtener más información, consulta SAML-Tracer en la tienda web de Chrome.

Herramientas para desarrolladores de SAML: OneLogin proporcionan herramientas que puedes usar para decodificar el valor codificado en SAML y comprobar los campos obligatorios en la afirmación de SAML. Para obtener más información, consulte Base 64 Decode + Inflate en el sitio web. OneLogin

Amazon CloudWatch Logs: puede comprobar los registros de RES en CloudWatch Logs para ver si hay errores o advertencias. Sus registros están en un grupo de registros con el formato de nombre*res-environment-name*/cluster-manager.

Documentación de Amazon Cognito: para obtener más información sobre la integración de SAML con Amazon Cognito, consulte Añadir proveedores de identidad de SAML a un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

Establecer contraseñas para los usuarios

1. En la AWS Directory Service consola, elige el directorio de la pila creada.
2. En el menú Acciones, selecciona Restablecer contraseña de usuario.
3. Elija el usuario e introduzca una contraseña nueva.
4. Selecciona Restablecer contraseña.

Crear subdominios

Si utiliza un dominio personalizado, tendrá que configurar subdominios para admitir las partes web y VDI de su portal.

> **Note**
>
> Si va a realizar la implementación en la región AWS GovCloud (EE. UU. Oeste), configure la aplicación web y los subdominios de VDI en la cuenta de partición comercial que aloja la zona de alojamiento público del dominio.

1. Abra la consola de Route 53.
2. Busca el dominio que creaste y selecciona Crear registro.
3. Introduce «web» como nombre del registro.
4. Elija CNAME como tipo de registro.
5. En Value, introduce el enlace que recibiste en el correo electrónico inicial.
6. Elija Crear registros.
7. Para crear un registro para el VDC, recupere la dirección NLB.

    a. Abra la consola de AWS CloudFormation.

b. Elija `<environment-name>-vdc`.

c. Elija Recursos y abra. `<environmentname>-vdc-external-nlb`

d. Copia el nombre DNS del NLB.

8. Abra la consola de Route 53.
9. Busca tu dominio y selecciona Crear registro.
10. En Nombre del registro, ingresa`vdc`.
11. En Tipo de registro, seleccione CNAME.
12. Para el NLB, introduzca el DNS.
13. Elija Crear registro.

Cree un certificado ACM

De forma predeterminada, RES aloja el portal web en un balanceador de carga de aplicaciones que utiliza el dominio amazonaws.com. Para usar tu propio dominio, tendrás que configurar un SSL/TLS certificado público que hayas proporcionado o que hayas solicitado a AWS Certificate Manager (ACM). Si usa ACM, recibirá un nombre de AWS recurso que deberá proporcionar como parámetro para cifrar el SSL/TLS canal entre el cliente y el host de los servicios web.

> **Tip**
>
> Si va a implementar el paquete de demostración de recursos externos, tendrá que introducir el dominio que haya elegido `PortalDomainName` al implementar la pila de recursos externos. Crear recursos externos

Para crear un certificado para dominios personalizados:

1. Desde la consola, AWS Certificate Managerábrala para solicitar un certificado público. Si va a realizar la implementación en EE. UU. AWS GovCloud (oeste de EE. UU.), cree el certificado en su cuenta de GovCloud partición.
2. Elija Solicitar un certificado público y, a continuación, Siguiente.
3. En Nombres de dominio, solicita un certificado para ambos `*.PortalDomainNamePortalDomainName`.
4. En Método de validación, selecciona Validación de DNS.

5. Seleccione Request (Solicitar).
6. En la lista de certificados, abra los certificados solicitados. Cada certificado tendrá el estado Pendiente de validación.

> **Note**
>
> Si no ve sus certificados, actualice la lista.

7. Realice una de las siguientes acciones:
   - Implementación comercial:

     En los detalles del certificado de cada certificado solicitado, elija Crear registros en Route 53. El estado del certificado debe cambiar a Emitido.
   - GovCloud despliegue:

     Si va a realizar la implementación en AWS GovCloud (EE. UU. al oeste), copie la clave y el valor del CNAME. Desde la cuenta de partición comercial, usa los valores para crear un registro nuevo en la zona alojada pública. El estado del certificado debe cambiar a Emitido.
8. Copie el nuevo ARN del certificado para ingresarlo como parámetro para. `ACMCertificateARNforWebApp`

Amazon CloudWatch Logs

Research and Engineering Studio crea los siguientes grupos de registros CloudWatch durante la instalación. Consulte la siguiente tabla para ver las retenciones predeterminadas:

CloudWatch Grupos de registros	Retención
/aws/lambda/ < >-cluster-endpoints installation-stack-name	¡Nunca caducan
/aws/lambda/ < >- -sync installation-stack-name cluster-manager-scheduled-ad	Nunca caduca
/aws/lambda/ < >-cluster-settings installation-stack-name	¡Nunca caducan

CloudWatch Grupos de registros	Retención
/aws/lambda/ < >-oauth-credentials installation-stack-name	¡Nunca caducan
/aws/lambda/ < >- installation-stack-name self-signed-certificate	¡Nunca caducan
/aws/lambda/ < >- installation-stack-name update-cluster-prefix-list	¡Nunca caducan
/aws/lambda/ < >- installation-stack-name vdc-scheduled-event-transformer	¡Nunca caducan
/aws/lambda/ < >- -ámbito del cliente installation-stack-name vdc-update-cluster-manager	¡Nunca caducan
/< >/cluster-manager installation-stack-name	6 meses
/< installation-stack-name >/vdc/controller	6 meses
/< installation-stack-name >/vdc/dcv-broker	6 meses
/< installation-stack-name >/vdc/ dcv-connection-gateway	6 meses

Si desea cambiar la retención predeterminada de un grupo de registros, puede ir a la CloudWatch consola y seguir las instrucciones que se indican en la sección Cambiar la retención de los datos de registro en los registros. CloudWatch

Establecer límites de permisos personalizados

A partir del 24 de abril de 2020, puede modificar de forma opcional las funciones creadas por RES adjuntando límites de permisos personalizados. Se puede definir un límite de permiso personalizado como parte de la AWS CloudFormation instalación de RES proporcionando el ARN del límite del permiso como parte del parámetro IAMPermission Boundary. No se establece ningún límite de permisos en ninguna función de RES si este parámetro se deja vacío. A continuación se muestra la

lista de acciones que los roles de RES requieren para funcionar. Asegúrese de que cualquier límite de permiso que vaya a utilizar de forma explícita permita las siguientes acciones:

```
[
    {
        "Effect": "Allow",
        "Resource": "*",
        "Sid": "ResRequiredActions",
        "Action": [
            "access-analyzer:*",
            "account:GetAccountInformation",
            "account:ListRegions",
            "acm:*",
            "airflow:*",
            "amplify:*",
            "amplifybackend:*",
            "amplifyuibuilder:*",
            "aoss:*",
            "apigateway:*",
            "appflow:*",
            "application-autoscaling:*",
            "appmesh:*",
            "apprunner:*",
            "aps:*",
            "athena:*",
            "auditmanager:*",
            "autoscaling-plans:*",
            "autoscaling:*",
            "backup-gateway:*",
            "backup-storage:*",
            "backup:*",
            "batch:*",
            "bedrock:*",
            "budgets:*",
            "ce:*",
            "cloud9:*",
            "cloudformation:*",
            "cloudfront:*",
            "cloudtrail-data:*",
            "cloudtrail:*",
            "cloudwatch:*",
            "codeartifact:*",
            "codebuild:*",
```

```
            "codeguru-profiler:*",
            "codeguru-reviewer:*",
            "codepipeline:*",
            "codestar-connections:*",
            "codestar-notifications:*",
            "codestar:*",
            "cognito-identity:*",
            "cognito-idp:*",
            "cognito-sync:*",
            "comprehend:*",
            "compute-optimizer:*",
            "cur:*",
            "databrew:*",
            "datapipeline:*",
            "datasync:*",
            "dax:*",
            "detective:*",
            "devops-guru:*",
            "dlm:*",
            "dms:*",
            "drs:*",
            "dynamodb:*",
            "ebs:*",
            "ec2-instance-connect:*",
            "ec2:*",
            "ec2messages:*",
            "ecr:*",
            "ecs:*",
            "eks:*",
            "elastic-inference:*",
            "elasticache:*",
            "elasticbeanstalk:*",
            "elasticfilesystem:*",
            "elasticloadbalancing:*",
            "elasticmapreduce:*",
            "elastictranscoder:*",
            "es:*",
            "events:*",
            "firehose:*",
            "fis:*",
            "fms:*",
            "forecast:*",
            "fsx:*",
            "geo:*",
```

```
            "glacier:*",
            "glue:*",
            "grafana:*",
            "guardduty:*",
            "health:*",
            "iam:*",
            "identitystore:*",
            "imagebuilder:*",
            "inspector2:*",
            "inspector:*",
            "internetmonitor:*",
            "iot:*",
            "iotanalytics:*",
            "kafka:*",
            "kafkaconnect:*",
            "kinesis:*",
            "kinesisanalytics:*",
            "kms:*",
            "lambda:*",
            "lightsail:*",
            "logs:*",
            "memorydb:*",
            "mgh:*",
            "mobiletargeting:*",
            "mq:*",
            "neptune-db:*",
            "organizations:DescribeOrganization",
            "osis:*",
            "personalize:*",
            "pi:*",
            "pipes:*",
            "polly:*",
            "qldb:*",
            "quicksight:*",
            "rds-data:*",
            "rds:*",
            "redshift-data:*",
            "redshift-serverless:*",
            "redshift:*",
            "rekognition:*",
            "resiliencehub:*",
            "resource-groups:*",
            "route53:*",
            "route53domains:*",
```

```
            "route53resolver:*",
            "rum:*",
            "s3:*",
            "sagemaker:*",
            "scheduler:*",
            "schemas:*",
            "sdb:*",
            "secretsmanager:*",
            "securityhub:*",
            "serverlessrepo:*",
            "servicecatalog:*",
            "servicequotas:*",
            "ses:*",
            "signer:*",
            "sns:*",
            "sqs:*",
            "ssm:*",
            "ssmmessages:*",
            "states:*",
            "storagegateway:*",
            "sts:*",
            "support:*",
            "tag:GetResources",
            "tag:GetTagKeys",
            "tag:GetTagValues",
            "textract:*",
            "timestream:*",
            "transcribe:*",
            "transfer:*",
            "translate:*",
            "vpc-lattice:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*",
            "wisdom:*",
            "xray:*"
        ]
    }
]
```

Configurar RES-Ready AMIs

Con RES-Ready AMIs, puede preinstalar las dependencias de RES para las instancias de escritorios virtuales () según sus necesidades. VDIs AMIs El uso de RES-Ready AMIs mejora los tiempos de arranque de las instancias de VDI mediante las imágenes preconfiguradas. Con EC2 Image Builder, puede crear y registrar sus AMIs nuevas pilas de software. Para obtener más información sobre Image Builder, consulte la Guía del usuario de Image Builder.

Antes de empezar, debe implementar la última versión de RES.

Temas

- Prepare la función de IAM para acceder al entorno RES
- Componente Create EC2 Image Builder
- Prepara tu receta EC2 de Image Builder
- Configurar EC2 la infraestructura de Image Builder
- Configurar la canalización de imágenes de Image Builder
- Ejecute la canalización de imágenes de Image Builder
- Registre una nueva pila de software en RES

Prepare la función de IAM para acceder al entorno RES

Para acceder al servicio de entorno RES desde EC2 Image Builder, debe crear o modificar un rol de IAM denominado RES- EC2InstanceProfileForImageBuilder. Para obtener información sobre la configuración de un rol de IAM para su uso en Image Builder, consulte AWS Identity and Access Management (IAM) en la Guía del usuario de Image Builder.

Su función requiere:

- Las relaciones de confianza incluyen el EC2 servicio de Amazon
- Amazon SSMManaged InstanceCore y sus EC2 InstanceProfileForImageBuilder políticas
- Política de RES personalizada con acceso limitado a DynamoDB y Amazon S3 al entorno RES implementado

  (Esta política puede ser un documento de política gestionado por el cliente o integrado en línea).

Entidad de relación de confianza:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            }
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Política de RES:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:{AWS-Region}:{AWS-Account-ID}:table/{RES-
EnvironmentName}.cluster-settings",
            "Condition": {
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-
Account-ID}/idea/vdc/res-ready-install-script-packages/*"
        }
    ]
}
```

Componente Create EC2 Image Builder

Siga las instrucciones para crear un componente mediante la consola de Image Builder de la Guía del usuario de Image Builder.

Introduzca los detalles del componente:

1. En Tipo, elija Construir.
2. En el caso del sistema operativo (SO) Image, elija Linux o Windows.
3. En Nombre del componente, introduzca un nombre descriptivo, como**`research-and-engineering-studio-vdi-<operating-system>`**.
4. Introduzca el número de versión del componente y, si lo desea, añada una descripción.
5. Para el documento de definición, introduzca el siguiente archivo de definición. Si encuentra algún error, el archivo YAML es sensible al espacio y es la causa más probable.

   Linux

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-linux
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Linux VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
```

```
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
```

```
        inputs:
           delaySeconds: 0
      - name: RunInstallPostRebootScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
           commands:
               - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
      - name: SecondReboot
        action: Reboot
        onFailure: Abort
        maxAttempts: 3
        inputs:
           delaySeconds: 0
```

Windows

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-windows
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
```

```
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'Tar -xf
 res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
                - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
                - 'Install-WindowsEC2Instance'
       - name: Reboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
```

```
            delaySeconds: 0
```

6. Crea cualquier etiqueta opcional y selecciona Crear componente.

Prepara tu receta EC2 de Image Builder

Una receta de EC2 Image Builder define la imagen base que se utilizará como punto de partida para crear una nueva imagen, junto con el conjunto de componentes que se añaden para personalizar la imagen y comprobar que todo funciona como se espera. Debe crear o modificar una receta para construir la AMI de destino con las dependencias de software RES necesarias. Para obtener más información sobre las recetas, consulte Administrar recetas.

RES es compatible con los siguientes sistemas operativos de imagen:

- Amazon Linux 2 (x86 y ARM64)
- Ubuntu 22.04.3 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Abra la consola EC2 de Image Builder enhttps://console.aws.amazon.com/imagebuilder.
2. En Recursos guardados, selecciona Recetas de imágenes.
3. Seleccione Crear receta de imagen.
4. Introduce un nombre único y un número de versión.
5. Elija una imagen base compatible con RES.
6. En Configuración de instancias, instale un agente SSM si no viene preinstalado. Introduzca la información en Datos de usuario y cualquier otro dato de usuario necesario.

> **Note**
>
> Para obtener información sobre cómo instalar un agente de SSM, consulte:
>
> - Instalación manual del agente SSM en EC2 instancias para Linux
> - Instalación y desinstalación manual del agente SSM en EC2 instancias para Windows Server

7. Para recetas basadas en Linux, añada el componente de `aws-cli-version-2-linux` compilación gestionado por Amazon a la receta. Los scripts de instalación de RES lo utilizan AWS CLI para proporcionar acceso de VDI a los valores de configuración de los ajustes del clúster de DynamoDB. Windows no requiere este componente.
8. Añada el componente EC2 Image Builder creado para su entorno Linux o Windows e introduzca los valores de parámetros necesarios. Los siguientes parámetros son entradas obligatorias: AWSAccount ID, RESEnv nombre, RESEnv región y RESEnvReleaseVersion.

   > **Important**
   >
   > Para los entornos Linux, debe agregar estos componentes en orden y agregar primero el componente de `aws-cli-version-2-linux` compilación.

9. (Recomendado) Añada el componente de `simple-boot-test-<linux-or-windows>` prueba gestionado por Amazon para comprobar que se puede lanzar la AMI. Se trata de una recomendación mínima. Puede seleccionar otros componentes de prueba que cumplan con sus requisitos.
10. Complete las secciones opcionales si es necesario, añada cualquier otro componente que desee y elija Crear receta.

Modify a recipe

Si ya tiene una receta de EC2 Image Builder, puede usarla añadiendo los siguientes componentes:

1. Para recetas basadas en Linux, añada el componente de `aws-cli-version-2-linux` compilación gestionado por Amazon a la receta. Los scripts de instalación de RES lo utilizan AWS CLI para proporcionar acceso de VDI a los valores de configuración de los ajustes del clúster de DynamoDB. Windows no requiere este componente.
2. Añada el componente EC2 Image Builder creado para su entorno Linux o Windows e introduzca los valores de parámetros necesarios. Los siguientes parámetros son entradas obligatorias: AWSAccount ID, RESEnv nombre, RESEnv región y RESEnvReleaseVersion.

> **Important**
>
> Para los entornos Linux, debe agregar estos componentes en orden y agregar primero el componente de `aws-cli-version-2-linux` compilación.

3. Complete las secciones opcionales si es necesario, añada cualquier otro componente que desee y elija Crear receta.

Configurar EC2 la infraestructura de Image Builder

Puede utilizar las configuraciones de infraestructura para especificar la EC2 infraestructura de Amazon que Image Builder utiliza para crear y probar su imagen de Image Builder. Para usarla con RES, puede elegir entre crear una nueva configuración de infraestructura o usar una existente.

- Para crear una nueva configuración de infraestructura, consulte Crear una configuración de infraestructura.
- Para usar una configuración de infraestructura existente, actualice una configuración de infraestructura.

Para configurar la infraestructura de Image Builder:

1. Para el rol de IAM, introduzca el rol que configuró anteriormente. the section called “Prepare la función de IAM para acceder al entorno RES”
2. Para el tipo de instancia, elija un tipo con al menos 4 GB de memoria y que sea compatible con la arquitectura AMI base que haya elegido. Consulte los tipos de EC2 instancias de Amazon.
3. En el caso de los grupos de VPC, subredes y seguridad, debe permitir el acceso a Internet para descargar paquetes de software. También se debe permitir el acceso a la tabla de `cluster-settings` DynamoDB y al bucket de clústeres de Amazon S3 del entorno RES.

Configurar la canalización de imágenes de Image Builder

La canalización de imágenes de Image Builder ensambla la imagen base, los componentes para la creación y las pruebas, la configuración de la infraestructura y los ajustes de distribución. Para configurar una canalización de imágenes para RES-Ready AMIs, puede optar por crear una

canalización nueva o utilizar una existente. Para obtener más información, consulte Creación y actualización de canalizaciones de imágenes AMI en la Guía del usuario de Image Builder.

Create a new Image Builder pipeline

1. Abra la consola de Image Builder enhttps://console.aws.amazon.com/imagebuilder.
2. En la barra de navegación, elija Image Pipelines.
3. Selecciona Crear canalización de imágenes.
4. Especifica los detalles de tu canalización introduciendo un nombre único, una descripción opcional, un cronograma y una frecuencia.
5. En Elegir receta, elija Usar receta existente y seleccione la receta creada enthe section called “Prepara tu receta EC2 de Image Builder”. Comprueba que los detalles de la receta sean correctos.
6. En Definir el proceso de creación de imágenes, elija el flujo de trabajo predeterminado o personalizado según el caso de uso. En la mayoría de los casos, los flujos de trabajo predeterminados son suficientes. Para obtener más información, consulte Configurar flujos de trabajo de imágenes para la canalización de EC2 Image Builder.
7. En Definir la configuración de infraestructura, elija Elegir la configuración de infraestructura existente y seleccione la configuración de infraestructura creada enthe section called “Configurar EC2 la infraestructura de Image Builder”. Compruebe que los detalles de su infraestructura sean correctos.
8. En Definir la configuración de distribución, elija Crear la configuración de distribución mediante los valores predeterminados del servicio. La imagen de salida debe residir en el mismo lugar Región de AWS que su entorno RES. Si se utilizan los valores predeterminados del servicio, la imagen se creará en la región en la que se utilice Image Builder.
9. Revisa los detalles de la canalización y selecciona Crear canalización.

Modify an existing Image Builder pipeline

1. Para usar una canalización existente, modifique los detalles para usar la receta creada enthe section called “Prepara tu receta EC2 de Image Builder”.
2. Seleccione Save changes (Guardar cambios).

Ejecute la canalización de imágenes de Image Builder

Para producir la imagen de salida configurada, debe iniciar la canalización de imágenes. El proceso de creación puede tardar hasta una hora en función del número de componentes de la receta de la imagen.

Para ejecutar la canalización de imágenes:

1. En las canalizaciones de imágenes, seleccione la canalización creada enthe section called “Configurar la canalización de imágenes de Image Builder”.
2. En Acciones, selecciona Ejecutar canalización.

Registre una nueva pila de software en RES

1. Siga las instrucciones the section called “Pilas de software () AMIs” para registrar una pila de software.
2. Para el ID de AMI, introduzca el ID de AMI de la imagen de salida integradathe section called “Ejecute la canalización de imágenes de Image Builder”.

Guía del administrador

Esta guía del administrador proporciona instrucciones adicionales para un público técnico sobre cómo personalizar e integrar aún más el estudio de investigación e ingeniería AWS del producto.

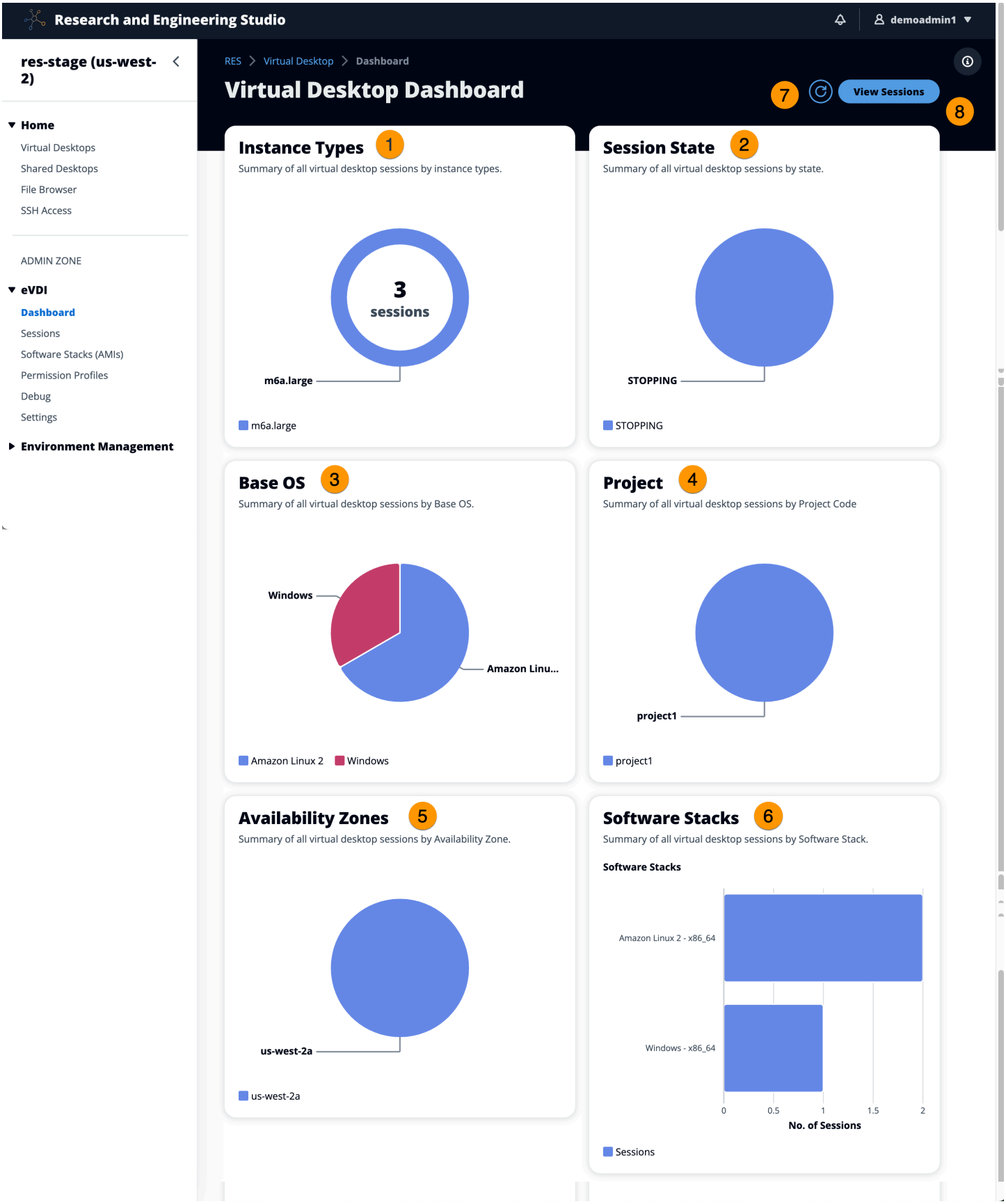
Temas

Administración de sesiones

La administración de sesiones proporciona un entorno flexible e interactivo para desarrollar y probar las sesiones. Como usuario administrativo, puede permitir que los usuarios creen y administren sesiones interactivas en sus entornos de proyecto.

Temas

Panel de control



El panel de administración de sesiones proporciona a los administradores una vista rápida de:

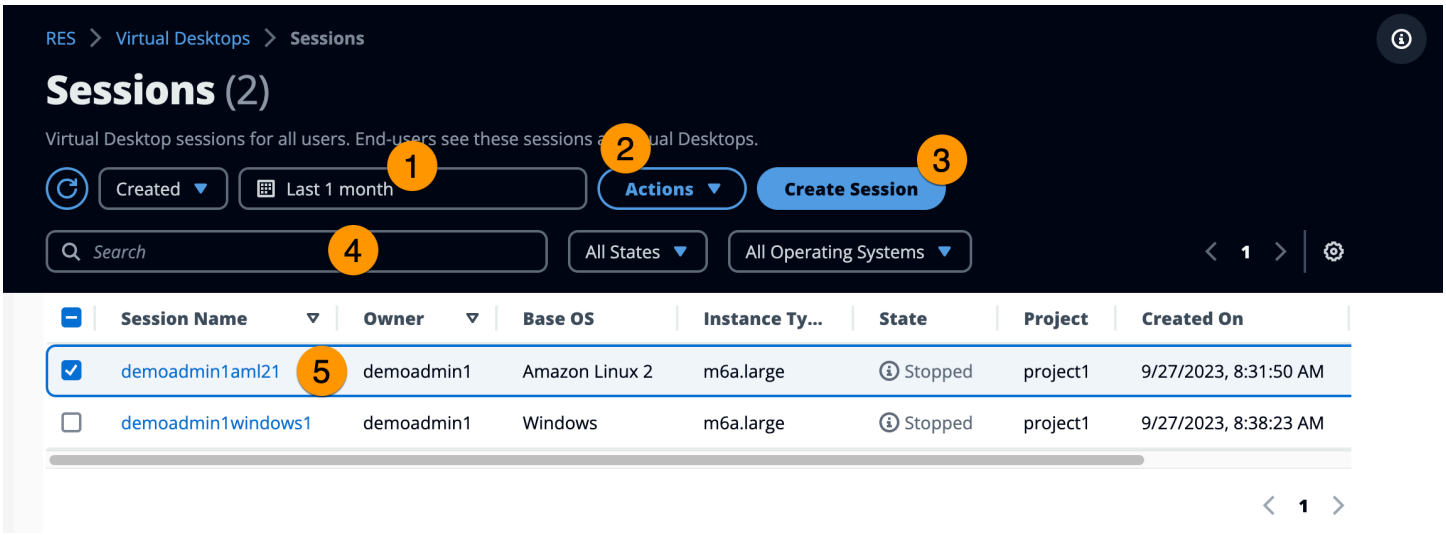
1. Tipos de instancias
2. Estados de la sesión
3. Sistema operativo base
4. Proyectos
5. Zonas de disponibilidad
6. Pilas de software

Además, los administradores pueden:

7. Actualice el panel de control para actualizar la información.
8. Seleccione Ver sesiones para ir a Sesiones.

Sesiones

Sesiones muestra todos los escritorios virtuales creados en Research and Engineering Studio. Desde la página Sesiones, puede filtrar y ver la información de la sesión o crear una sesión nueva.



1. Use el menú para filtrar los resultados por sesiones creadas o actualizadas dentro de un período de tiempo específico.
2. Seleccione una sesión y utilice el menú Acciones para:
   a. Reanudar sesión (s)
   b. Stop/Hibernate Sesión (s)

c. Stop/Hibernate Forzar sesión (s)

d. Finalizar sesión (s)

e. Forzar la finalización de la (s) sesión (s)

f. Salud de la (s) sesión (s)

g. Cree una pila de software

3. Elija Crear sesión para crear una sesión nueva.
4. Busque una sesión por nombre y filtre por estado y sistema operativo.
5. Elija el nombre de la sesión para ver más detalles.

Crear una sesión

1. Elija Crear sesión. Se abre el modal Iniciar un nuevo escritorio virtual.
2. Introduzca los detalles de la nueva sesión.
3. (Opcional.) Active Mostrar opciones avanzadas para proporcionar detalles adicionales, como el ID de subred y el tipo de sesión de DCV.
4. Elija Enviar.

Launch New Virtual Desktop

Session Name

Enter a name for the virtual desktop

Session Name is required. Use any characters and form a name of length between 3 and 24 characters, inclusive.

User

Select the user to create the session for

Project

Select the project under which the session will get created

Operating System

Select the operating system for the virtual desktop

Amazon Linux 2

Software Stack

Select the software stack for your virtual desktop

Enable Instance Hibernation

Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. You can not change instance type if you enable this option.

Virtual Desktop Size

Select a virtual desktop instance type

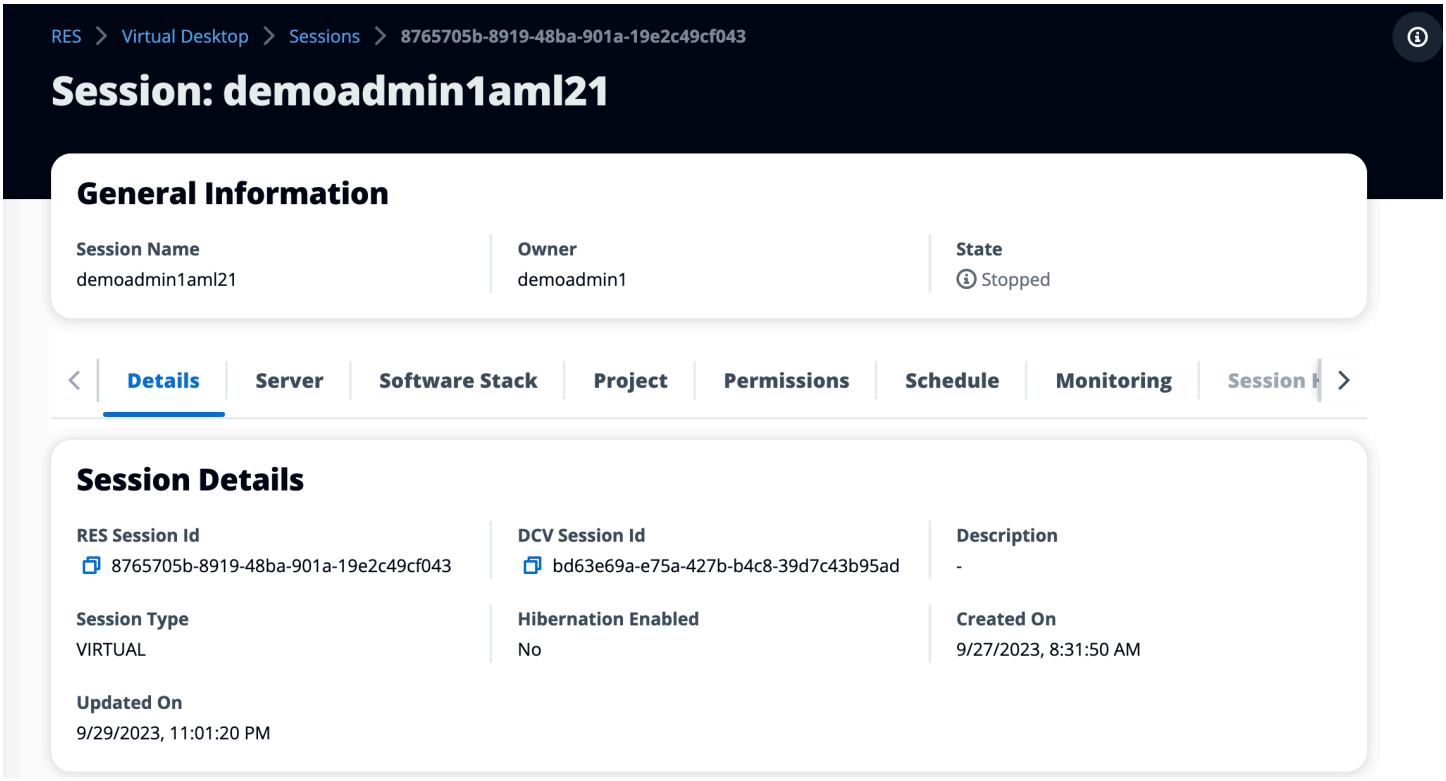
Storage Size (GB)

Enter the storage size for your virtual desktop in GBs

10

Detalles de la sesión

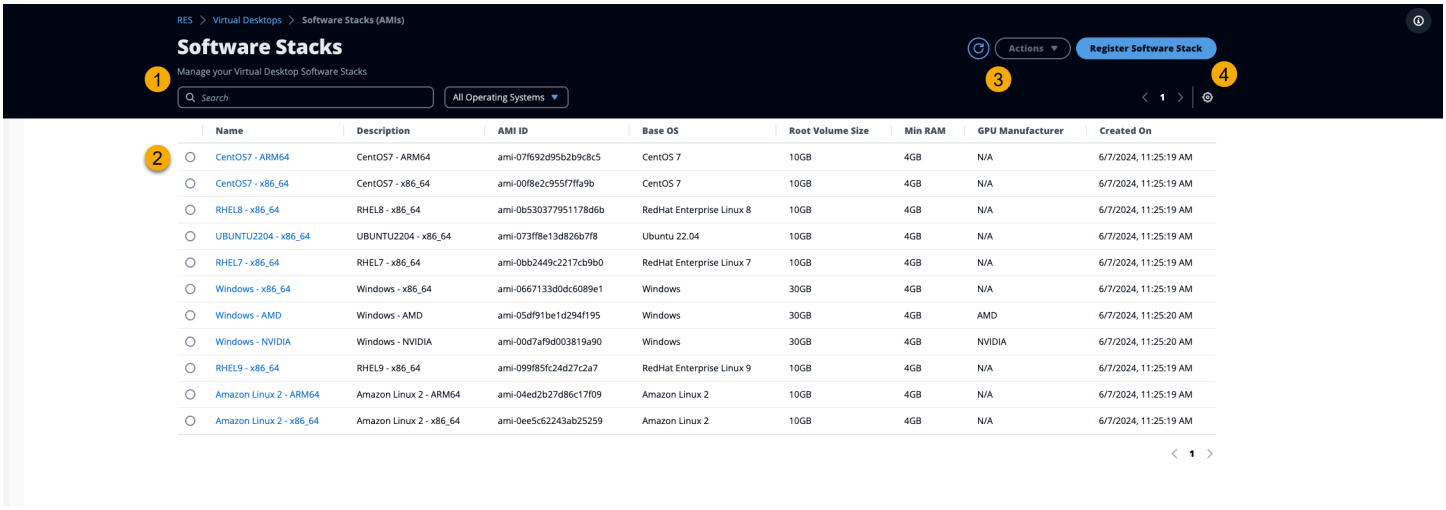
En la lista de sesiones, elija el nombre de la sesión para ver los detalles de la sesión.



Pilas de software () AMIs

> **Note**
>
> Para ejecutar la pila de SO7 software de Cent proporcionada AWS GovCloud (US), tendrá que suscribirse a la AMI desde dentro AWS Marketplace mediante su cuenta estándar vinculada.

Desde la página Software Stacks, puedes configurar Amazon Machine Images (AMIs) y gestionar las existentes AMIs.



1. Para buscar una pila de software existente, utilice el menú desplegable del sistema operativo para filtrar por sistema operativo.
2. Elija el nombre de una pila de software para ver los detalles de la pila.
3. Una vez que haya seleccionado una pila de software, utilice el menú Acciones para editar la pila y asignarla a un proyecto.
4. El botón Registrar pila de software le permite crear una pila nueva:
    1. Seleccione Registrar pila de software.
    2. Introduzca los detalles de la nueva pila de software.
    3. Elija Enviar.

Register new Software Stack

Name

Enter a name for the software stack

Use any characters and form a name of length between 3 and 24 characters, inclusive.

Description

Enter a user friendly description for the software stack

AMI Id

Enter the AMI Id

AMI Id must start with ami-xxx

Operating System

Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer

Select the GPU Manufacturer for the software stack

N/A

Min. Storage Size (GB)

Enter the min. storage size for your virtual desktop in GBs

10

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

10

Projects

Select applicable projects for the software stack

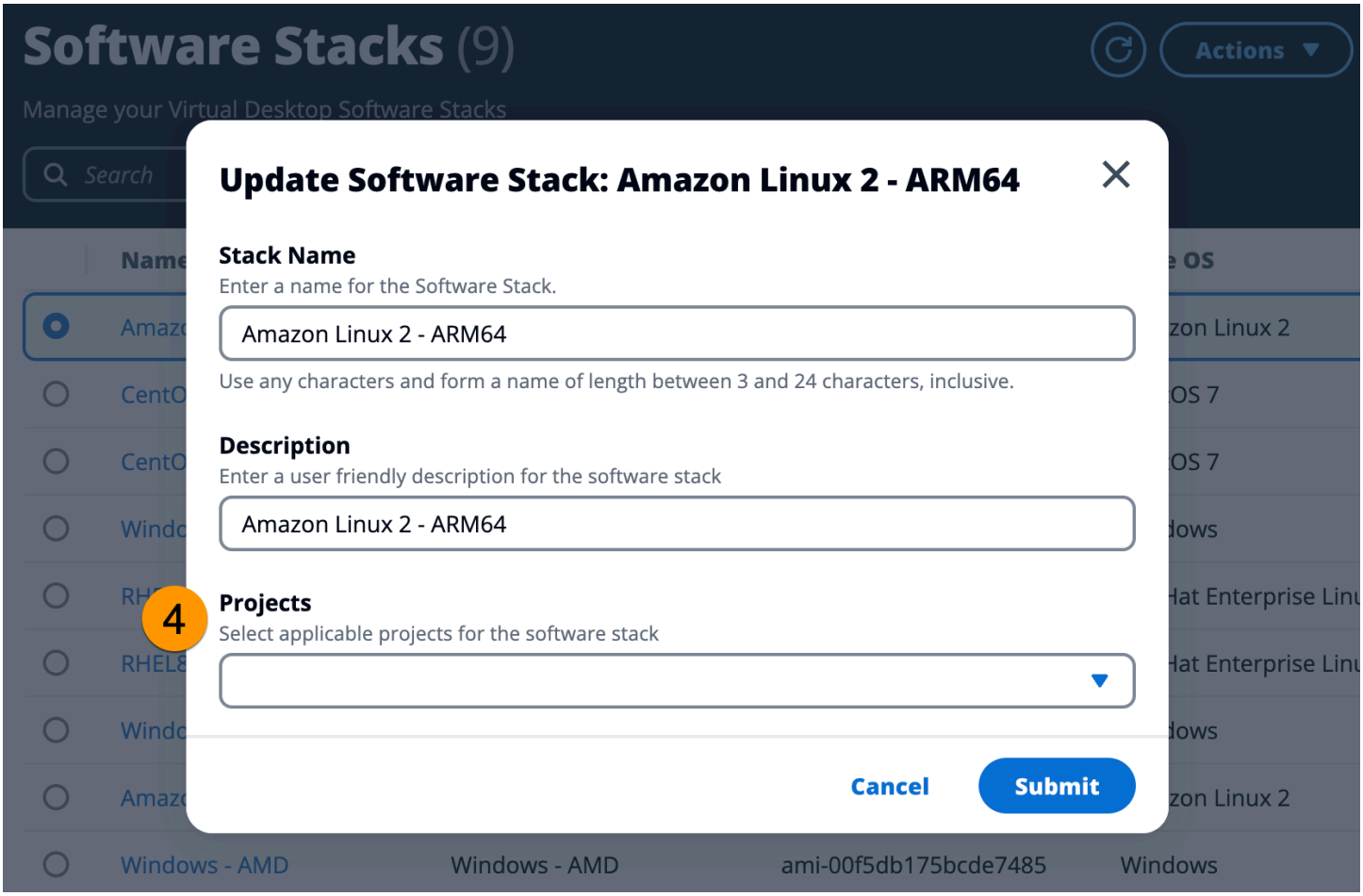
Asigne una pila de software a un proyecto

Al crear una nueva pila de software, puede asignar la pila a los proyectos. Si necesita añadir la pila a un proyecto después de la creación inicial, haga lo siguiente:

> **Note**
>
> Solo puede asignar paquetes de software a los proyectos de los que sea miembro.

1. Seleccione la pila de software que necesita añadir a un proyecto en la página Software Stacks.
2. Elija Acciones.
3. Seleccione Editar.
4. Utilice el menú desplegable Proyectos para seleccionar el proyecto.
5. Elija Enviar.

También puede editar la pila de software desde la página de detalles de la pila.

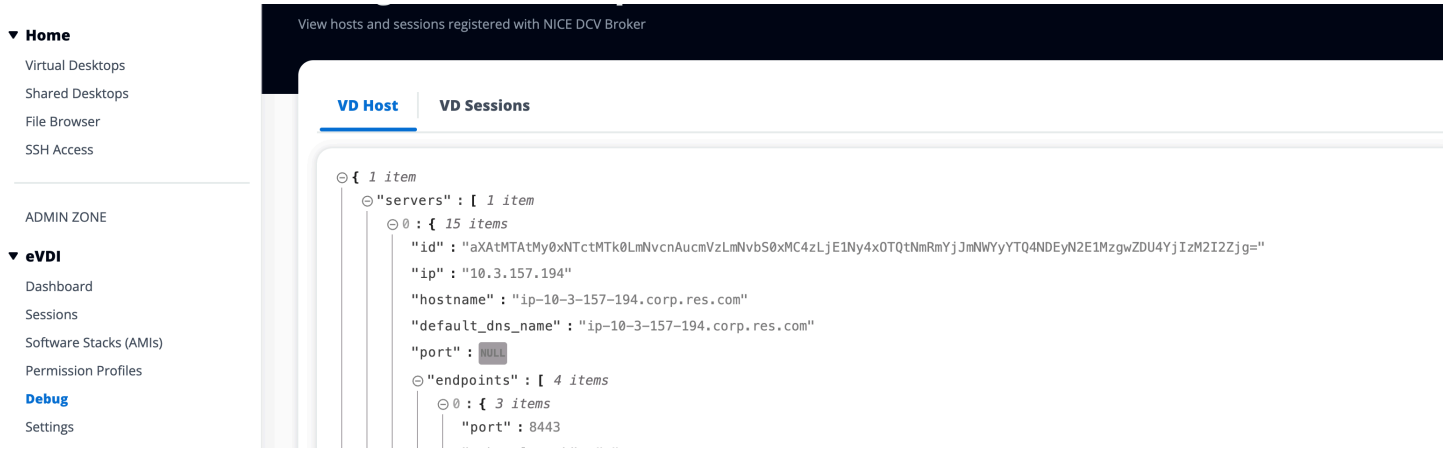


Vea los detalles de la pila de software

En la lista de pilas de software, elija el nombre de la pila de software para ver los detalles. En la página de detalles, también puede seleccionar Editar para editar la pila de software.

Debugging

El panel de depuración muestra el tráfico de mensajes asociado a los escritorios virtuales. Puede utilizar este panel para observar la actividad entre los hosts. La pestaña VD Host muestra la actividad específica de la instancia y la pestaña VD Sessions muestra la actividad de la sesión en curso.



Configuración de escritorio

Puede utilizar la página de configuración del escritorio para configurar los recursos asociados a los escritorios virtuales. La pestaña Servidor proporciona acceso a ajustes como:

Tiempo de espera de inactividad de la sesión DCV

: Tiempo transcurrido el cual la sesión de DCV se desconectará automáticamente. Esto no cambia el estado de la sesión de escritorio, solo cierra la sesión desde el cliente DCV o desde el navegador web.

Advertencia de tiempo de espera de inactividad

: Tiempo transcurrido el cual se enviará al cliente una advertencia de inactividad.

Umbral de uso de la CPU

: El uso de la CPU debe considerarse inactivo.

Sesiones permitidas por usuario

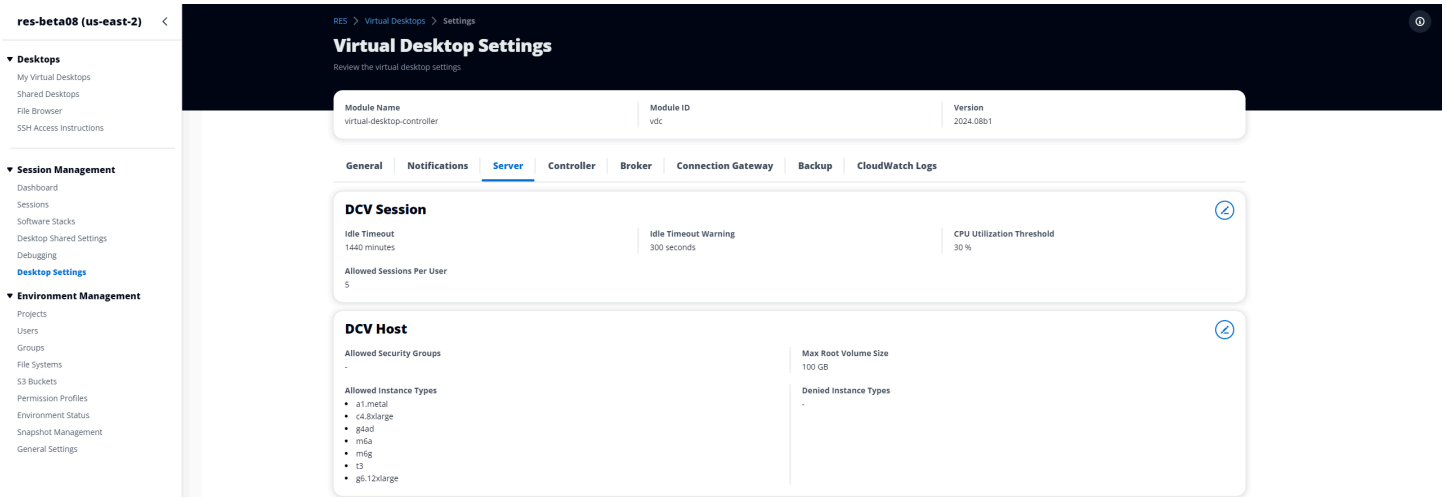
: El número de sesiones de VDI que un usuario individual puede tener en un momento dado. Si un usuario alcanza o supera este valor, no podrá iniciar nuevas sesiones desde la página Mis escritorios virtuales. Este valor no afecta a la capacidad de iniciar sesiones a través de la página Sesiones.

Tamaño máximo del volumen raíz

: El tamaño predeterminado del volumen raíz en las sesiones de escritorios virtuales.

Tipos de instancias permitidos

La lista de familias y tamaños de instancias que se pueden lanzar para este entorno RES. Se aceptan las combinaciones de familia de instancias y tamaño de instancia. Por ejemplo, si especificas «m7a», todos los tamaños de la familia m7a estarán disponibles para su lanzamiento como sesiones de VDI. Si especifica «m7a.24xlarge», solo m7a.24xlarge estará disponible para lanzarse como sesión de VDI. Esta lista afecta a todos los proyectos del entorno.



Gestión del entorno

Desde la sección de gestión ambiental de RES, los usuarios administrativos pueden crear y gestionar entornos aislados para sus proyectos de investigación e ingeniería. Estos entornos pueden incluir recursos informáticos, almacenamiento y otros componentes necesarios, todo ello dentro de un entorno seguro. Los usuarios pueden configurar y personalizar estos entornos para cumplir con los requisitos específicos de sus proyectos, lo que facilita la experimentación, las pruebas y la iteración de sus soluciones sin afectar a otros proyectos o entornos.

Temas

- Proyectos
- Usuarios
- Grupos
- Perfiles de permisos
- Sistemas de archivos
- Estado del entorno

- Administración de instantáneas
- Configuración del entorno
- Buckets de Amazon S3

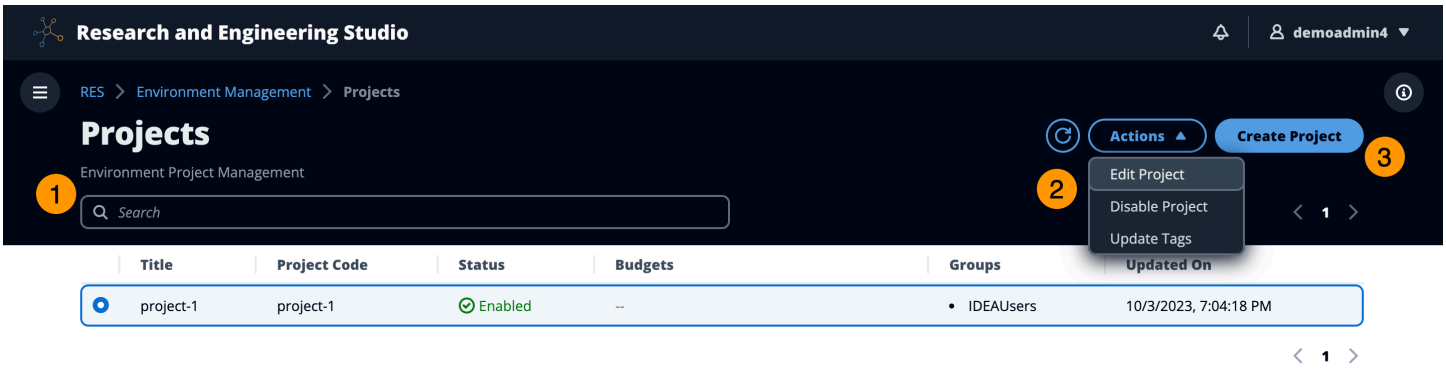
Proyectos

Los proyectos constituyen un límite para los escritorios, los equipos y los presupuestos virtuales. Al crear un proyecto, se definen sus ajustes, como el nombre, la descripción y la configuración del entorno. Los proyectos suelen incluir uno o más entornos, que se pueden personalizar para cumplir con los requisitos específicos del proyecto, como el tipo y el tamaño de los recursos informáticos, la pila de software y la configuración de la red.

Temas

- Vea los proyectos
- Crear un proyecto
- Edita un proyecto
- Añadir o eliminar etiquetas de un proyecto
- Vea los sistemas de archivos asociados a un proyecto
- Añadir una plantilla de lanzamiento

Vea los proyectos



El panel de proyectos proporciona una lista de los proyectos disponibles. Desde el panel de proyectos, puede:

1. Puedes usar el campo de búsqueda para buscar proyectos.

2. Cuando se selecciona un proyecto, puede utilizar el menú Acciones para:
   a. Editar un proyecto
   b. Habilitar o deshabilitar un proyecto
   c. Actualizar las etiquetas del proyecto
3. Puede elegir Crear proyecto para crear un proyecto nuevo.

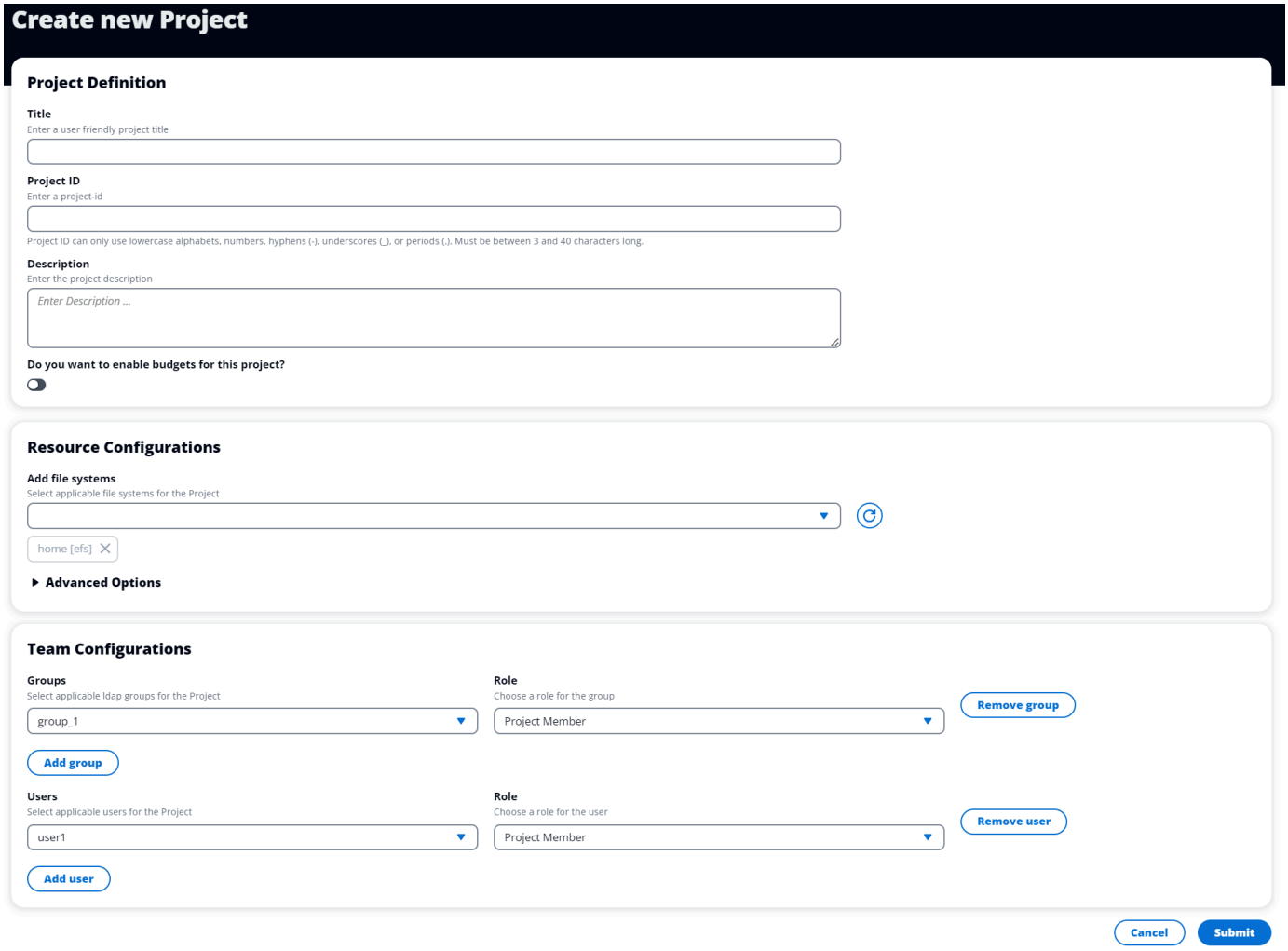
Crear un proyecto

1. Elija Crear proyecto.
2. Introduzca los detalles del proyecto.

   El identificador del proyecto es una etiqueta de recursos que se puede utilizar para realizar un seguimiento de la asignación de costes AWS Cost Explorer Service. Para obtener más información, consulte Activación de etiquetas de asignación de costes definidas por el usuario.

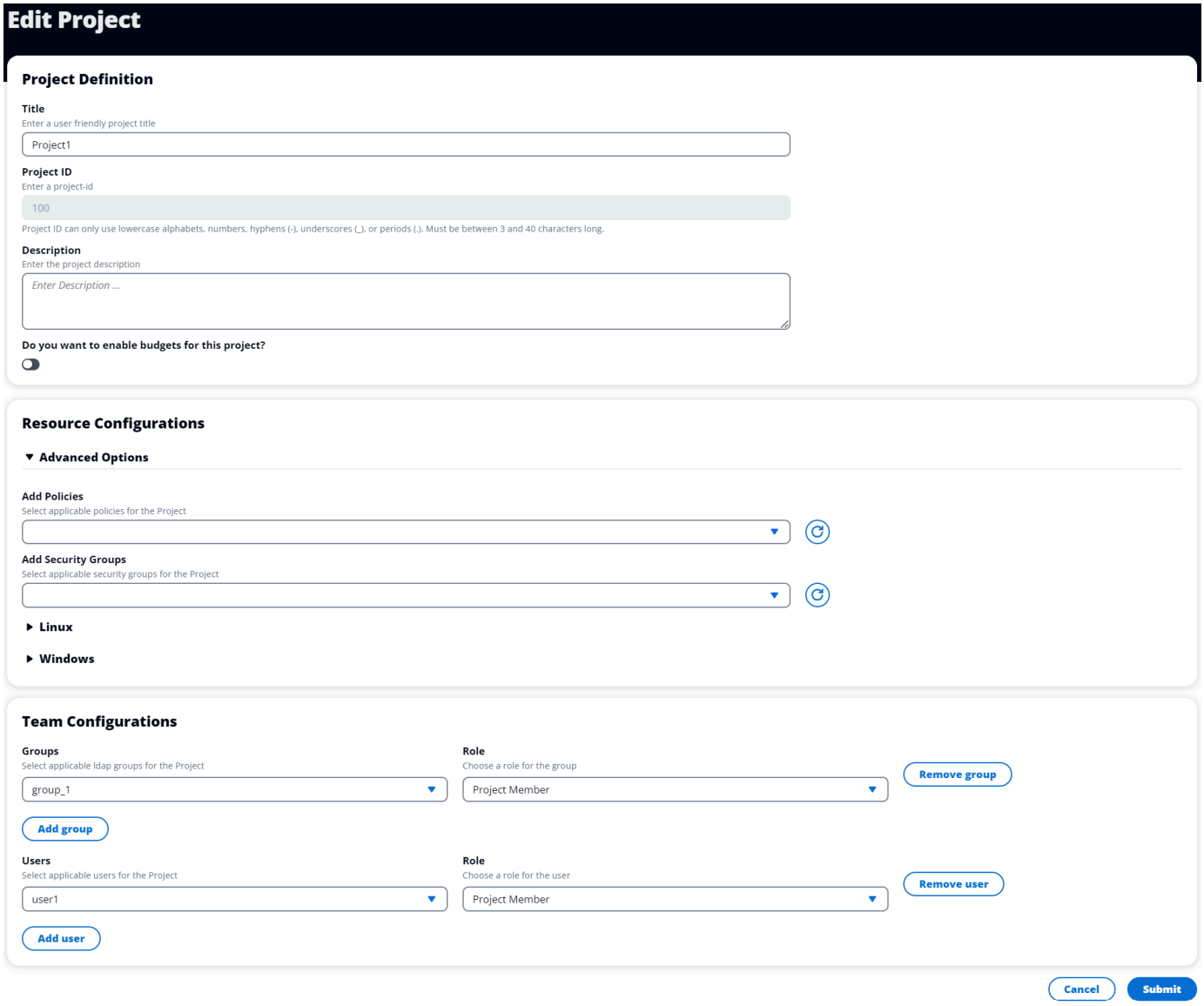
   > **Important**
   >
   > El identificador del proyecto no se puede cambiar después de la creación.

   Para obtener información sobre las opciones avanzadas, consulteAñadir una plantilla de lanzamiento.
3. (Opcional) Active los presupuestos del proyecto. Para obtener más información sobre los presupuestos, consulteSupervisión y control de costes.
4. Asigne a los and/or grupos de usuarios la función adecuada («miembro del proyecto» o «propietario del proyecto»). Consulte Perfiles de permisos predeterminados las acciones que puede realizar cada rol.
5. Elija Enviar.



Edita un proyecto

1. Seleccione un proyecto de la lista de proyectos.
2. En el menú Acciones, elija Editar proyecto.
3. Introduce tus actualizaciones. Si tiene intención de activar los presupuestos, consulte Supervisión y control de costes para obtener más información. Para obtener información sobre las opciones avanzadas, consulteAñadir una plantilla de lanzamiento.
4. Elija Enviar.



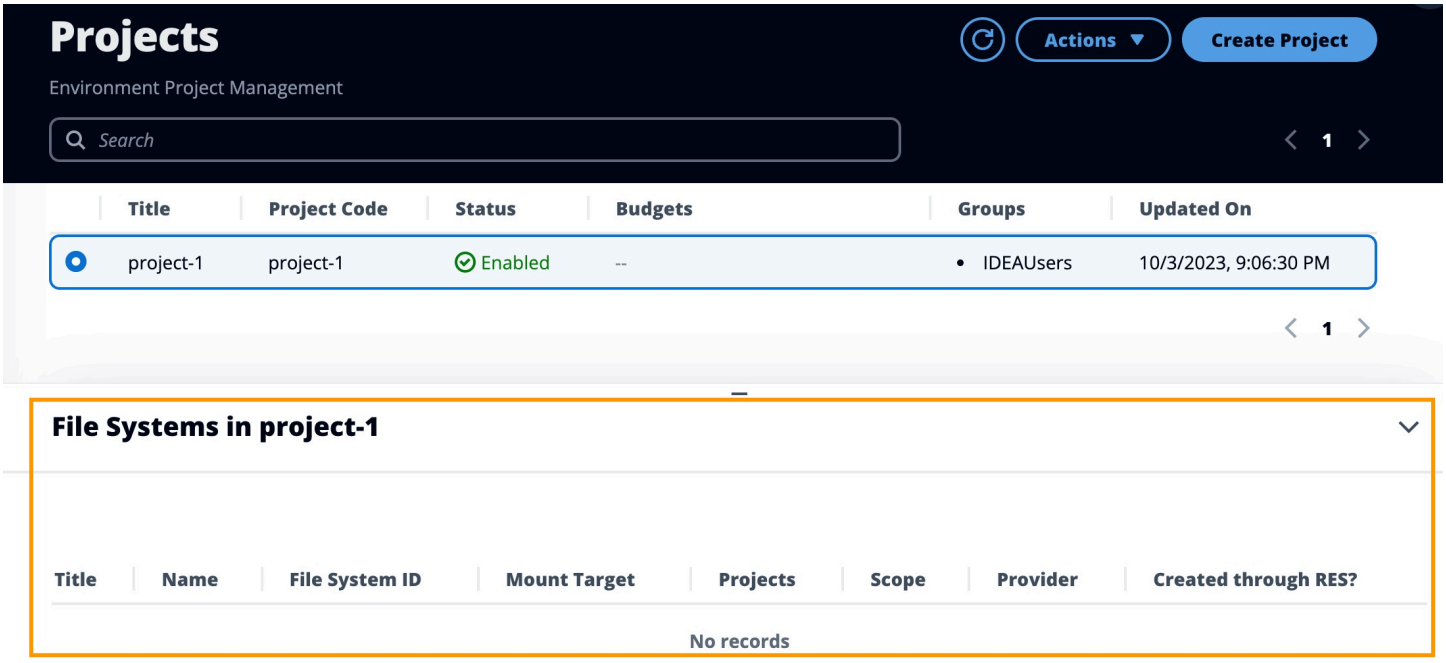
Añadir o eliminar etiquetas de un proyecto

Las etiquetas de proyecto asignarán etiquetas a todas las instancias creadas en el marco de ese proyecto.

1. Seleccione un proyecto de la lista de proyectos.
2. En el menú Acciones, elija Actualizar etiquetas.
3. Seleccione Añadir etiquetas e introduzca un valor para la clave.
4. Para eliminar etiquetas, selecciona Eliminar junto a la etiqueta que deseas eliminar.

Vea los sistemas de archivos asociados a un proyecto

Cuando se selecciona un proyecto, puede expandir el panel Sistemas de archivos en la parte inferior de la pantalla para ver los sistemas de archivos asociados al proyecto.



Añadir una plantilla de lanzamiento

Al crear o editar un proyecto, puede añadir plantillas de lanzamiento mediante las opciones avanzadas de la configuración del proyecto. Las plantillas de lanzamiento proporcionan configuraciones adicionales, como grupos de seguridad, políticas de IAM y scripts de lanzamiento, para todas las instancias de VDI del proyecto.

Agregue políticas

Puede añadir una política de IAM para controlar el acceso a la VDI de todas las instancias implementadas en su proyecto. Para incorporar una política, etiquétela con el siguiente par clave-valor:

```
res:Resource/vdi-host-policy
```

Para obtener más información sobre las funciones de IAM, consulte Políticas y permisos en IAM.

Añadir grupos de seguridad

Puede añadir un grupo de seguridad para controlar los datos de entrada y salida de todas las instancias de VDI de su proyecto. Para incorporar un grupo de seguridad, etiquete el grupo de seguridad con el siguiente par clave-valor:

```
res:Resource/vdi-security-group
```

Para obtener más información sobre los grupos de seguridad, consulte Controlar el tráfico de sus AWS recursos mediante grupos de seguridad en la Guía del usuario de Amazon VPC.

Añada scripts de lanzamiento

Puede añadir scripts de lanzamiento que se iniciarán en todas las sesiones de VDI del proyecto. RES admite el inicio de scripts para Linux y Windows. Para iniciar el script, puede elegir entre las siguientes opciones:

Ejecute el script cuando se inicie VDI

: Esta opción inicia el script al principio de una instancia de VDI antes de que se ejecute cualquier configuración o instalación de RES.

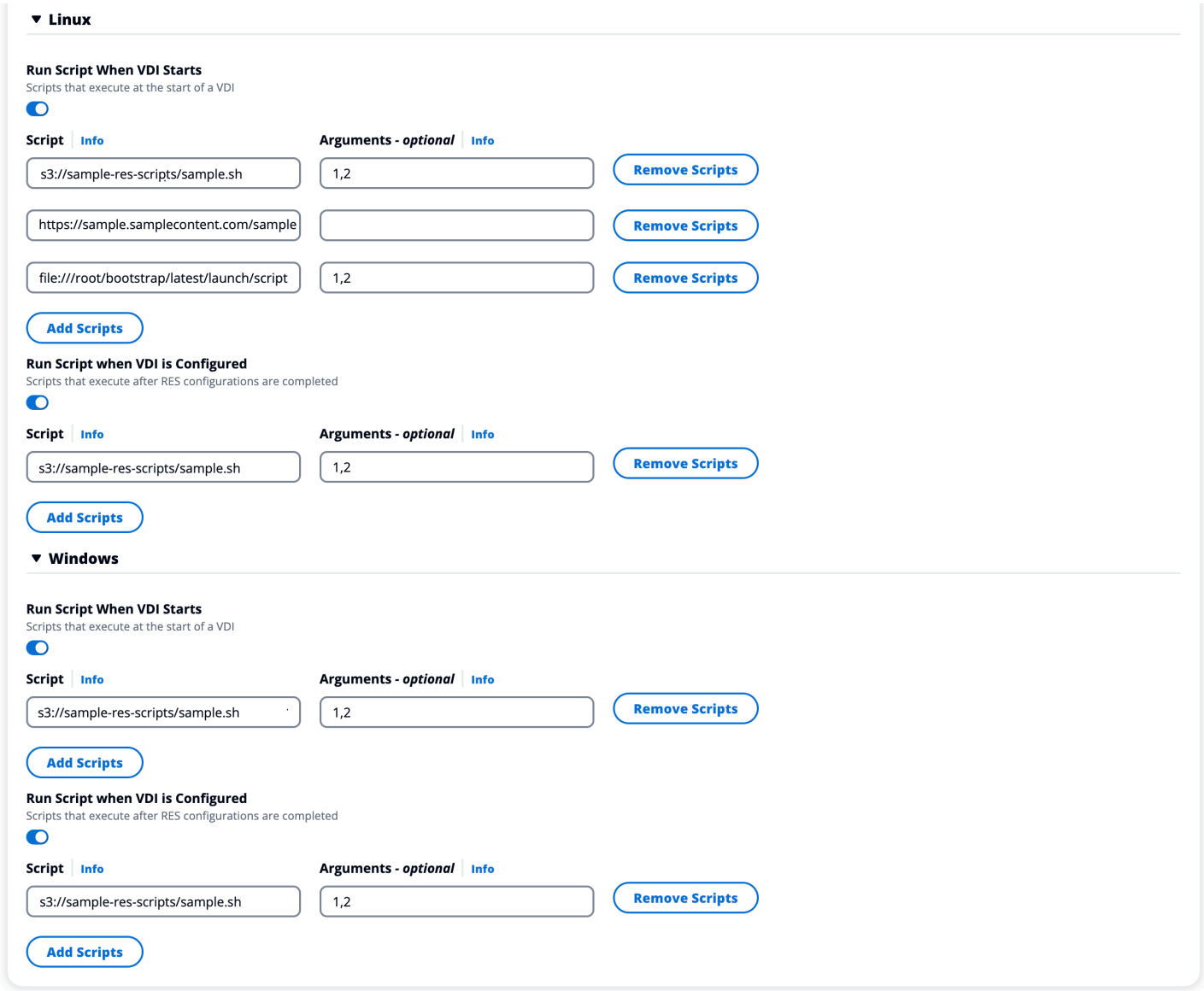
Ejecute el script cuando VDI esté configurado

: Esta opción inicia el script una vez finalizadas las configuraciones de RES.

Los scripts admiten las siguientes opciones:

Configuración de scripts	Ejemplo
S3 URI	s3://bucketname/script.sh
URL HTTPS	https://sample.samplecontent.com/sample
Archivo local	archivo:///.sh user/scripts/example

En el caso de los argumentos, proporcione los argumentos separados por una coma.



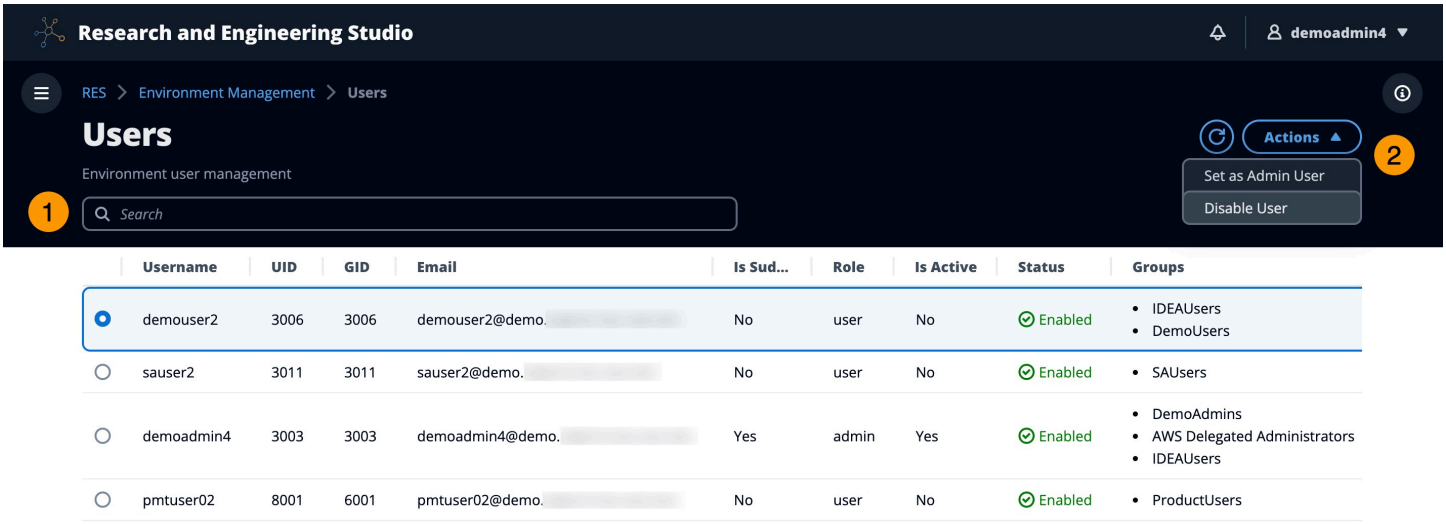
Ejemplo de configuración de un proyecto

Usuarios

Todos los usuarios sincronizados desde su Active Directory aparecerán en la página de usuarios. El usuario administrador del clúster sincroniza los usuarios durante la configuración del producto. Para obtener más información sobre la configuración inicial del usuario, consulte la. Guía de configuración

> **Note**
>
> Los administradores solo pueden crear sesiones para usuarios activos. De forma predeterminada, todos los usuarios estarán inactivos hasta que inicien sesión en el entorno

del producto. Si un usuario está inactivo, pídale que inicie sesión antes de crear una sesión para él.

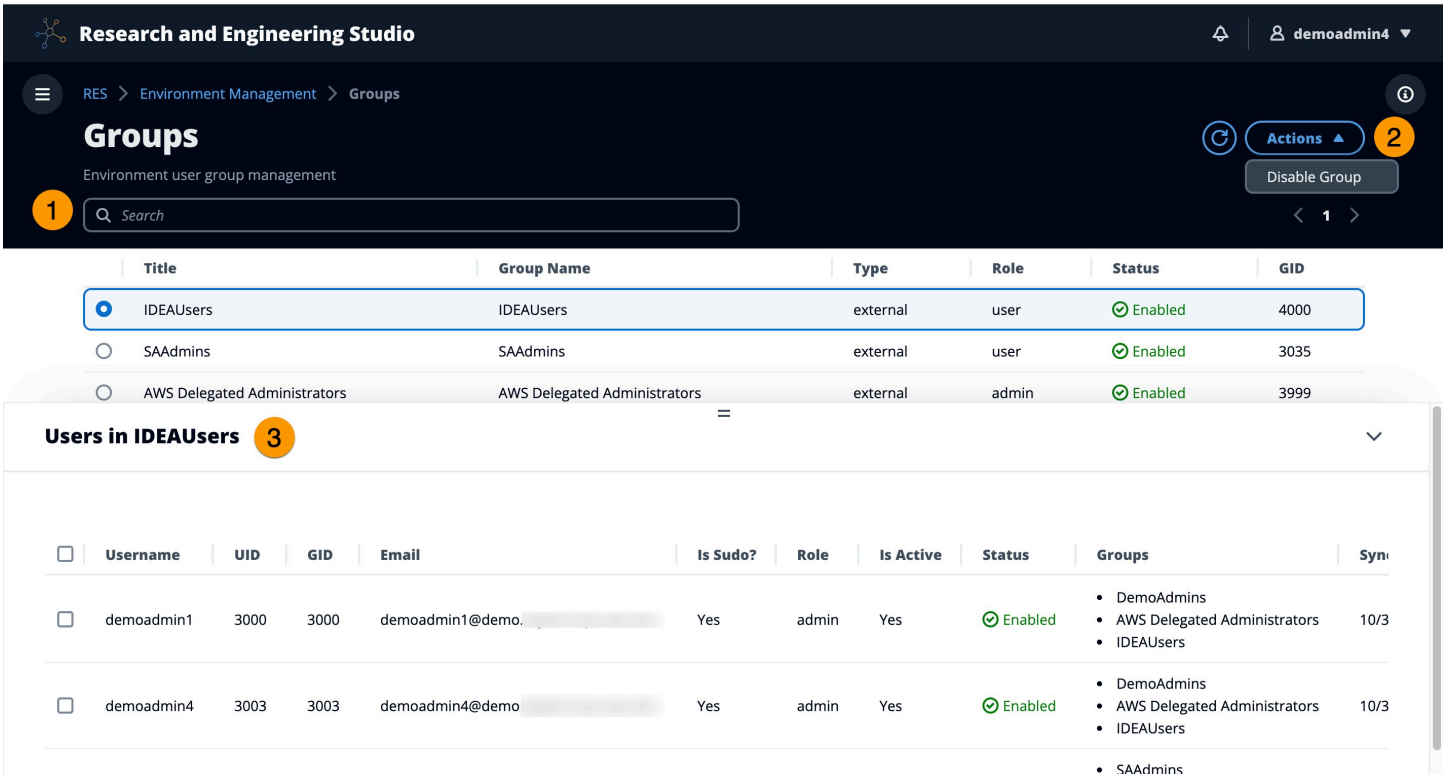


Desde la página de usuarios, puedes:

1. Busca usuarios.
2. Cuando se selecciona un nombre de usuario, utilice el menú Acciones para:
    a. Establézcalo como usuario administrador
    b. Inhabilitar usuario

Grupos

Todos los grupos sincronizados desde el directorio activo aparecen en la página Grupos. Para obtener más información sobre la configuración y la administración de grupos, consulte laGuía de configuración.



Desde la página Grupos, puede:

1. Buscar grupos de usuarios.
2. Cuando se selecciona un grupo de usuarios, utilice el menú Acciones para activar o desactivar un grupo.
3. Cuando se selecciona un grupo de usuarios, puede expandir el panel Usuarios en la parte inferior de la pantalla para ver los usuarios del grupo.

Perfiles de permisos

Descripción general

Research and Engineering Studio (RES) permite a un usuario administrativo crear perfiles de permisos personalizados que otorgan a los usuarios seleccionados permisos adicionales para administrar el proyecto del que forman parte. Cada proyecto incluye dos perfiles de permisos predeterminados: «Miembro del proyecto» y «Propietario del proyecto», que se pueden personalizar tras la implementación.

Actualmente, los administradores pueden conceder dos conjuntos de permisos mediante un perfil de permisos:

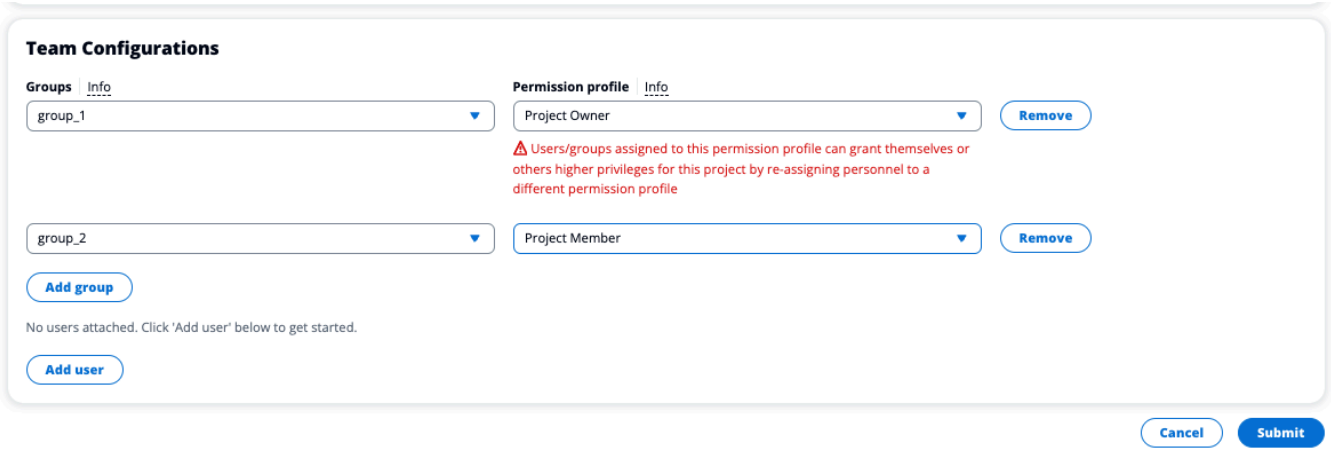
1. Los permisos de administración de proyectos consisten en «Actualizar la membresía del proyecto», que permite a un usuario designado añadir otros usuarios y grupos a un proyecto o eliminarlos de él, y «Actualizar el estado del proyecto», que permite a un usuario designado habilitar o deshabilitar un proyecto.
2. Los permisos de administración de sesiones de VDI consisten en «Crear sesión», que permite a un usuario designado crear una sesión de VDI dentro de su proyecto, y «Crear/finalizar la sesión de otro usuario», que permite a un usuario designado crear o finalizar las sesiones de otros usuarios dentro de un proyecto.

De esta forma, los administradores pueden delegar los permisos basados en proyectos a personas no administradoras de su entorno.

Permisos de gestión de proyectos

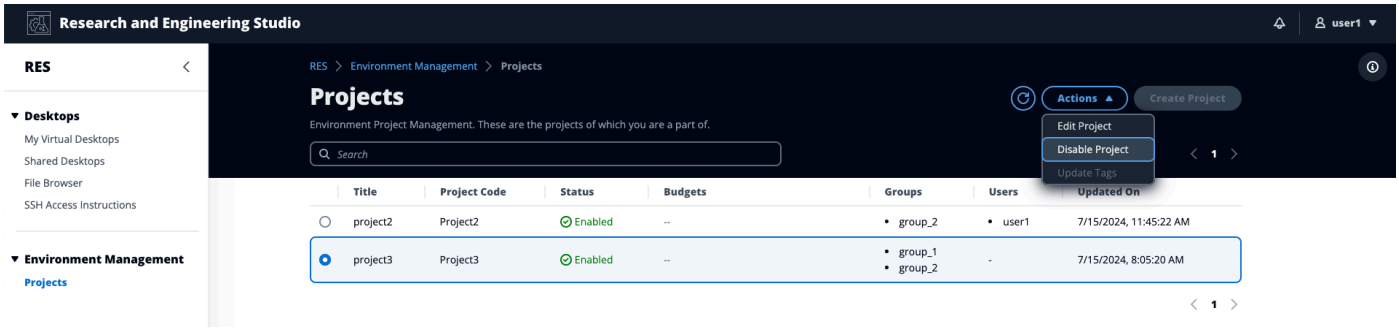
Actualizar la membresía del proyecto

Este permiso permite a los usuarios no administradores a los que se ha concedido añadir y eliminar usuarios o grupos de un proyecto. También les permite establecer el perfil de permisos y decidir el nivel de acceso para todos los demás usuarios y grupos de ese proyecto.



Actualizar el estado del proyecto

Este permiso permite a los usuarios no administradores a los que se ha concedido habilitar o deshabilitar un proyecto mediante el botón Acciones de la página de proyectos.

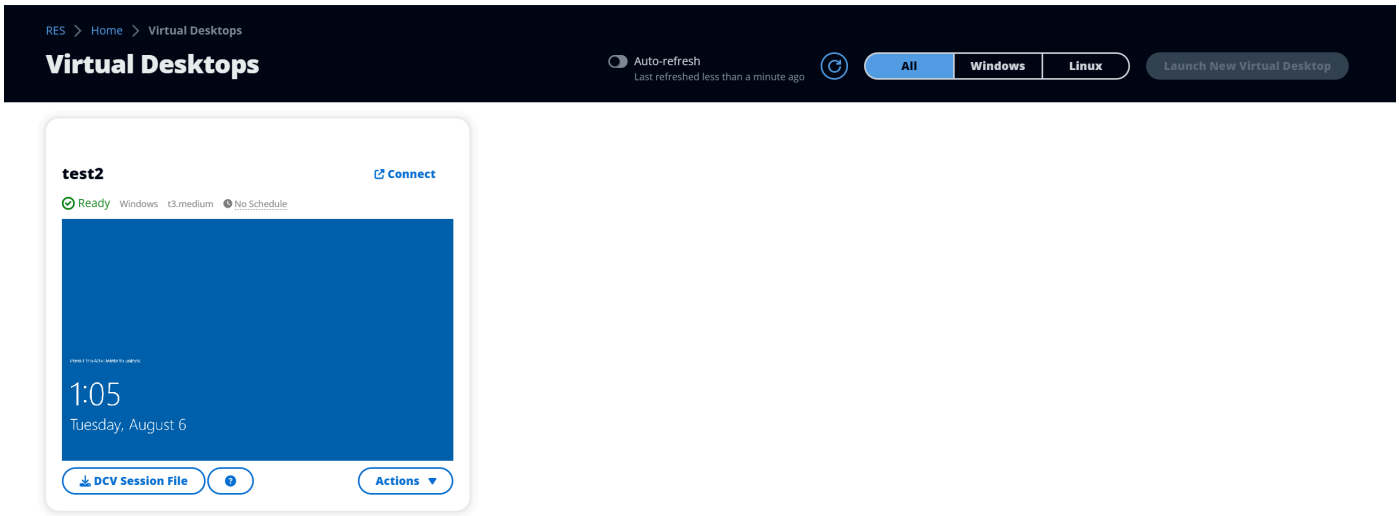


Permisos de administración de sesiones de VDI

Crear una sesión

Controla si un usuario puede o no iniciar su propia sesión de VDI desde la página Mis escritorios virtuales. Desactívela para denegar a los usuarios que no sean administradores la posibilidad de iniciar sus propias sesiones de VDI. Los usuarios siempre pueden detener y finalizar sus propias sesiones de VDI.

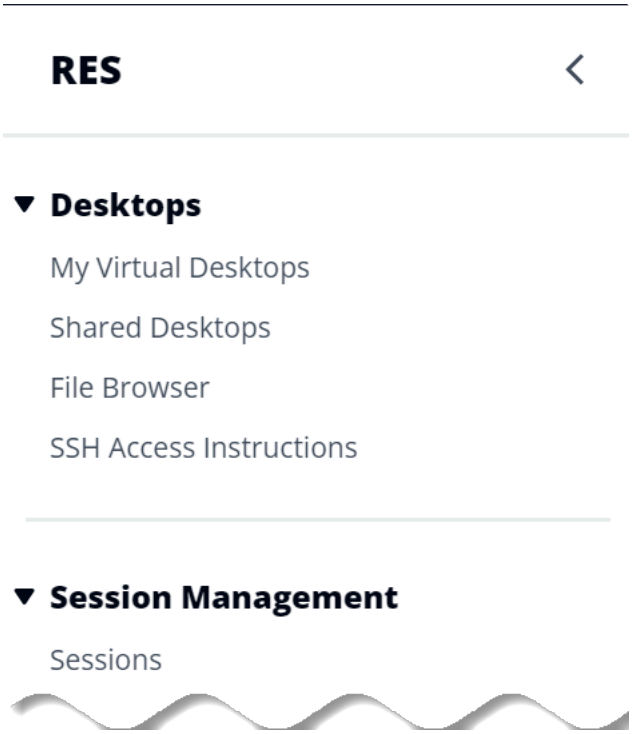
Si un usuario que no es administrador no tiene permisos para crear una sesión, se le deshabilitará el botón Iniciar un nuevo escritorio virtual, tal y como se muestra a continuación:



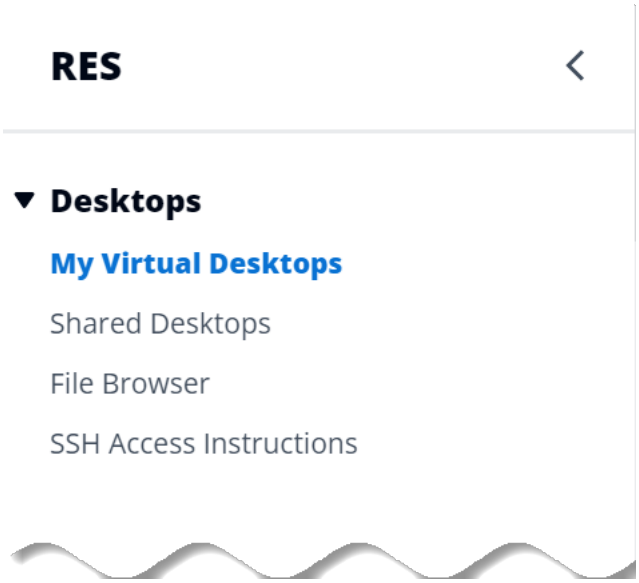
Cree o finalice las sesiones de otros

Permite a los usuarios no administradores acceder a la página de sesiones desde el panel de navegación de la izquierda. Estos usuarios podrán iniciar sesiones de VDI para otros usuarios de los proyectos en los que se les haya concedido este permiso.

Si un usuario que no es administrador tiene permiso para iniciar sesiones para otros usuarios, el panel de navegación de la izquierda mostrará el enlace Sesiones en Administración de sesiones, como se muestra a continuación:



Si un usuario que no es administrador no tiene permiso para crear sesiones para otros usuarios, el panel de navegación de la izquierda no mostrará la administración de sesiones, como se muestra aquí:

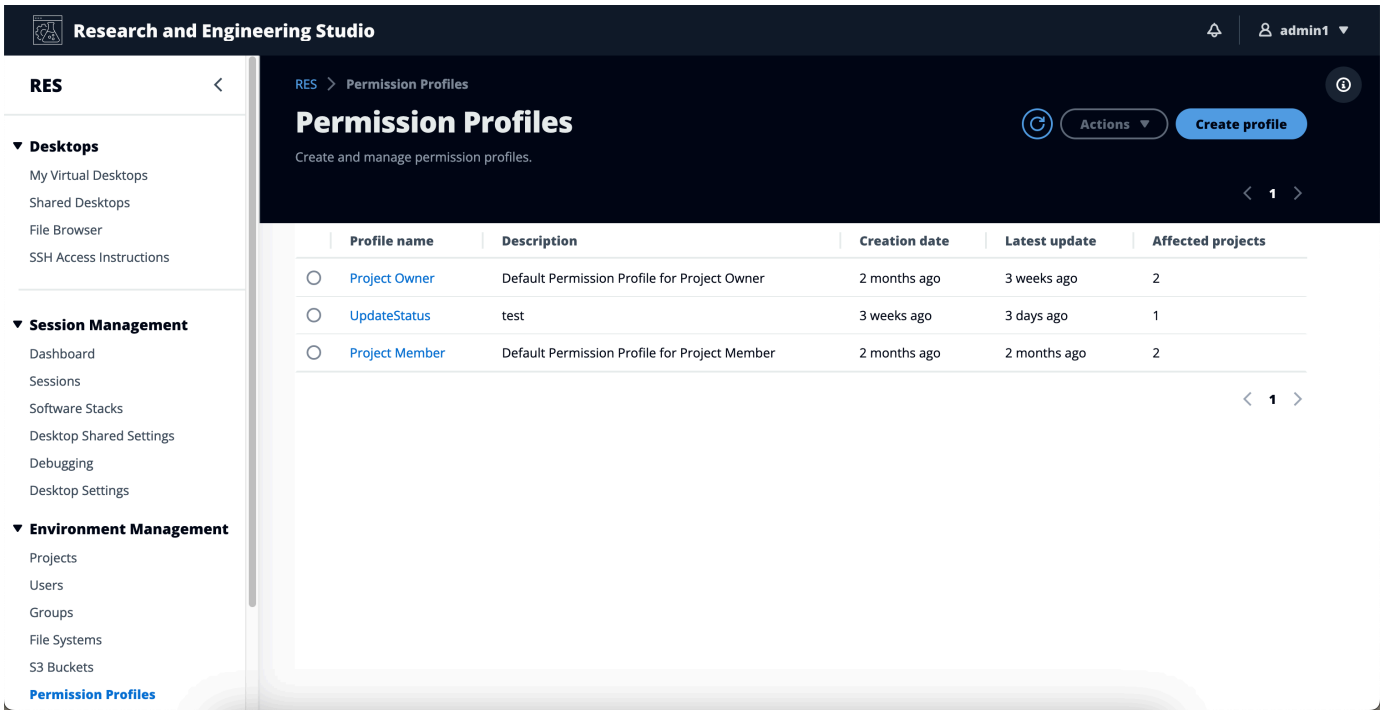


Administrar los perfiles de permisos

Como administrador de RES, puede realizar las siguientes acciones para administrar los perfiles de permisos.

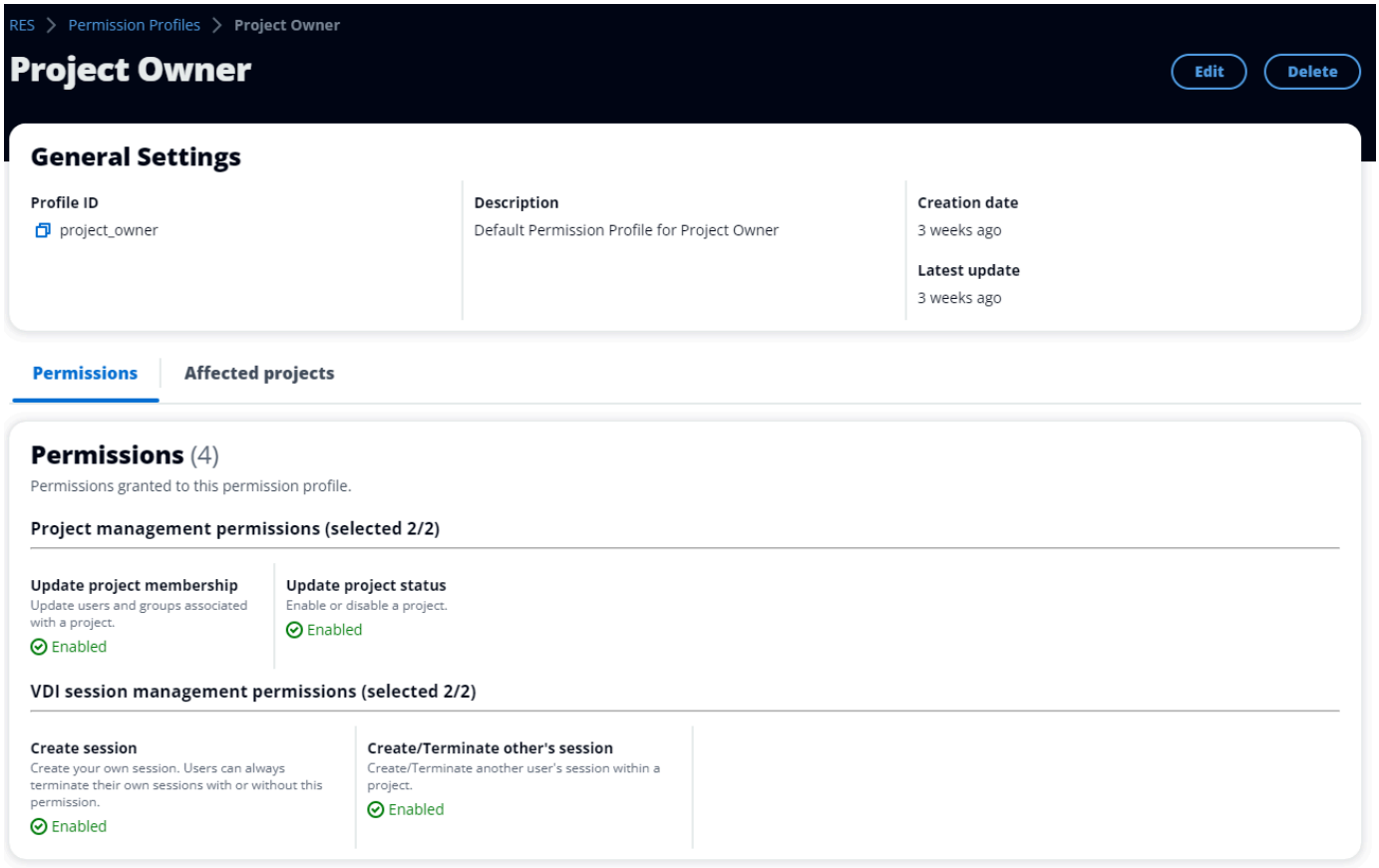
Enumere los perfiles de permisos

- En la página de la consola de Research and Engineering Studio, seleccione Perfiles de permisos en el panel de navegación de la izquierda. Desde esta página puede crear, actualizar, enumerar, ver y eliminar perfiles de permisos.

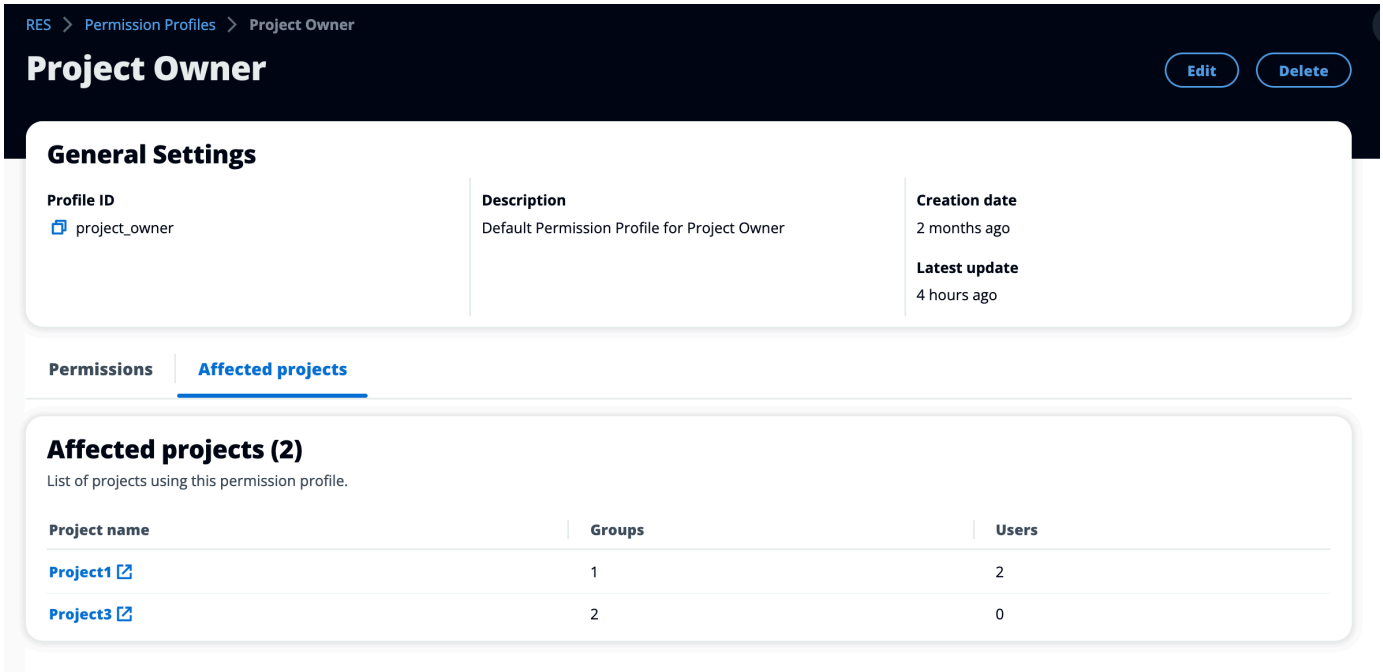


Ver los perfiles de permisos

1. En la página principal de perfiles de permisos, seleccione el nombre del perfil de permisos que desee ver. Desde esta página, puede editar o eliminar el perfil de permisos seleccionado.

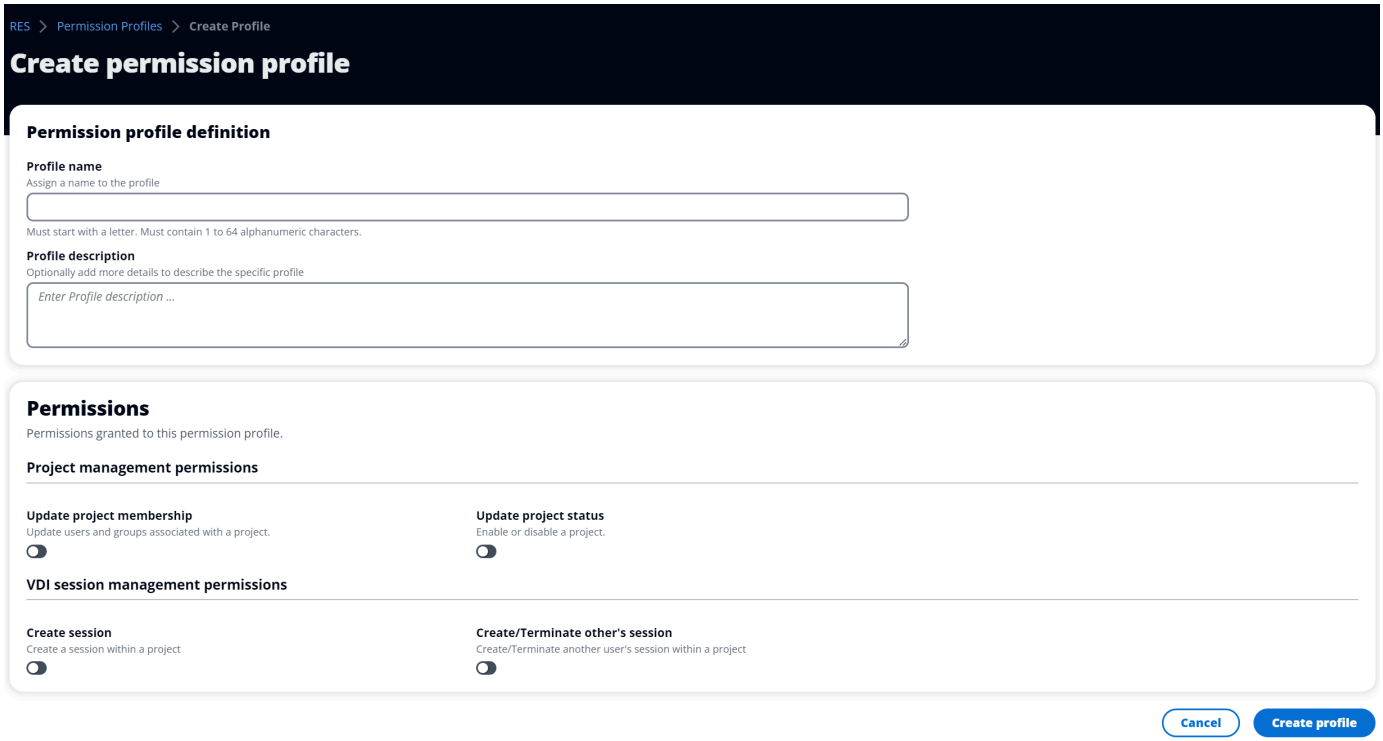


2. Seleccione la pestaña Proyectos afectados para ver los proyectos que utilizan actualmente el perfil de permisos.



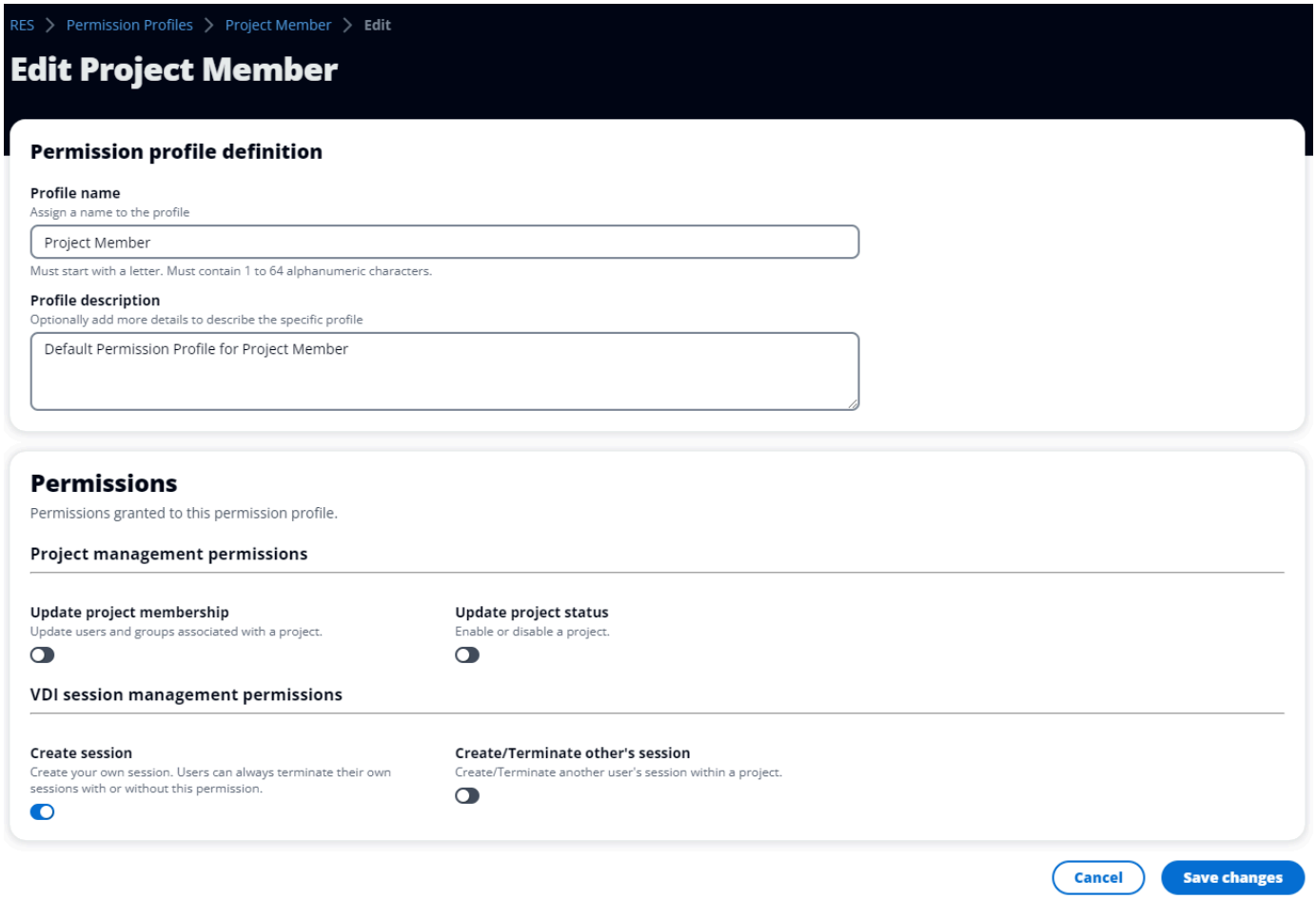
Cree perfiles de permisos

1. En la página principal de perfiles de permisos, seleccione Crear perfil para crear un perfil de permisos.
2. Introduzca un nombre y una descripción del perfil de permisos y, a continuación, elija los permisos que desee conceder a los usuarios o grupos que asigne a este perfil.



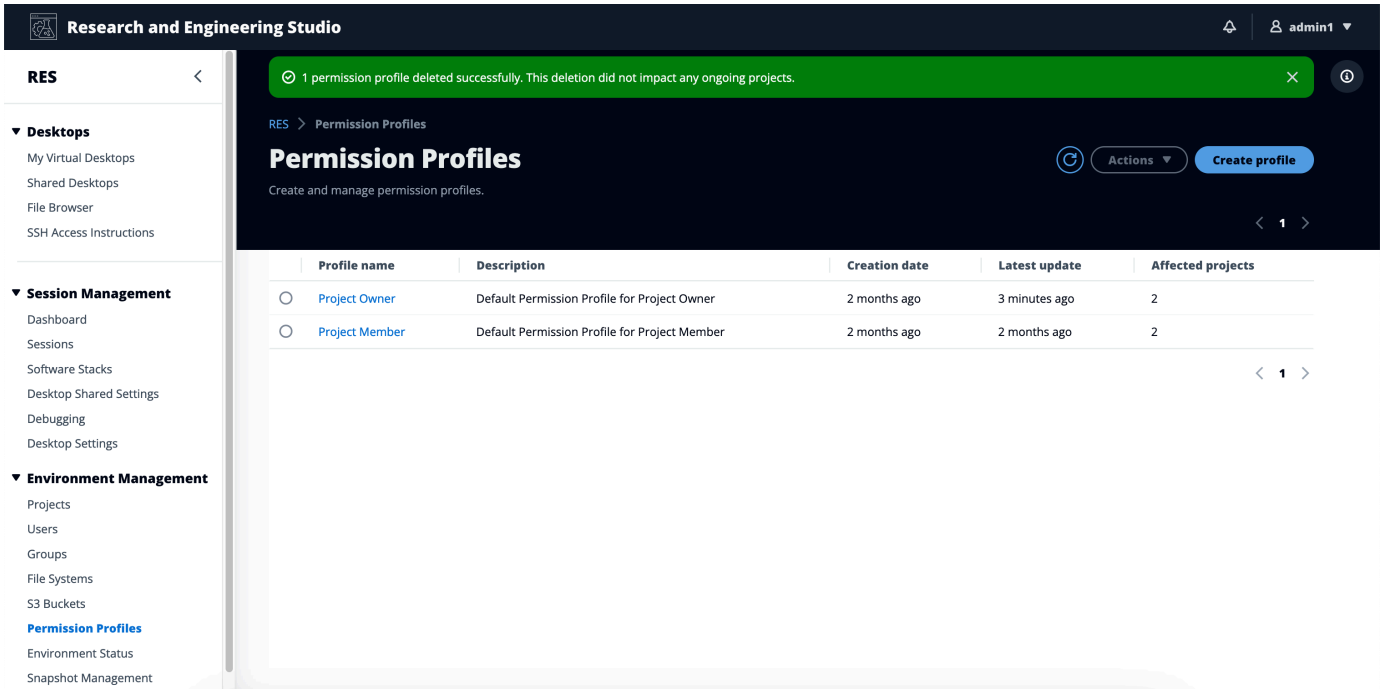
Editar perfiles de permisos

- En la página principal de perfiles de permisos, elija un perfil haciendo clic en el círculo situado junto a él, seleccione Acciones y, a continuación, elija Editar perfil para actualizar ese perfil de permisos.



Eliminar perfiles de permisos

- En la página principal de perfiles de permisos, elija un perfil haciendo clic en el círculo situado junto a él, seleccione Acciones y, a continuación, seleccione Eliminar perfil. No puede eliminar un perfil de permisos que esté siendo utilizado por ningún proyecto existente.



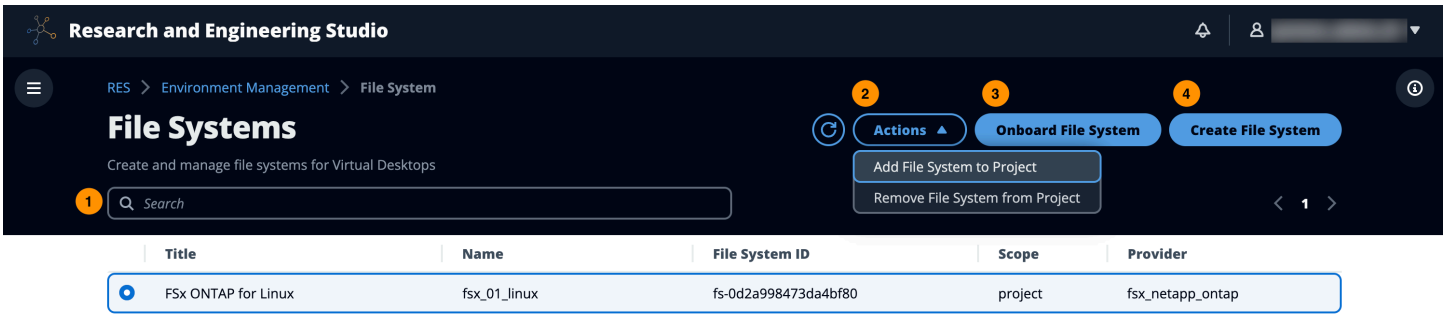
Perfiles de permisos predeterminados

Cada proyecto de RES incluye dos perfiles de permisos predeterminados que los administradores globales pueden configurar. (Además, los administradores globales pueden crear y modificar nuevos perfiles de permisos para un proyecto). En la siguiente tabla se muestran los permisos permitidos para los perfiles de permisos predeterminados: «Miembro del proyecto» y «Propietario del proyecto». Los perfiles de permisos y los permisos que conceden a determinados usuarios de un proyecto solo se aplican al proyecto al que pertenecen; los administradores globales son superusuarios que tienen todos los permisos que se indican a continuación en todos los proyectos.

Permisos	Descripción	Miembro del proyecto	Dueño del proyecto	
Crear sesión	Crea tu propia sesión. Los usuarios siempre pueden detener y terminar sus propias sesiones	X	X	

Permisos	Descripción	Miembro del proyecto	Dueño del proyecto	
	con o sin este permiso.			
Crea o termina las sesiones de otros	Crea o termina la sesión de otro usuario dentro de un proyecto.		X	
Actualiza la membresía del proyecto	Actualice los usuarios y grupos asociados a un proyecto.		X	
Actualizar el estado del proyecto	Habilita o deshabilita un proyecto.		X	

Sistemas de archivos



Desde la página Sistemas de archivos, puede:

1. Buscar sistemas de archivos.
2. Cuando se selecciona un sistema de archivos, utilice el menú Acciones para:
    a. Añada el sistema de archivos a un proyecto
    b. Elimine el sistema de archivos de un proyecto

3. Incorpore un nuevo sistema de archivos.
4. Cree un sistema de archivos.
5. Cuando se selecciona un sistema de archivos, puede expandir el panel de la parte inferior de la pantalla para ver los detalles del sistema de archivos.

Cree un sistema de archivos

1. Seleccione Crear sistema de archivos.
2. Introduzca los detalles del nuevo sistema de archivos.
3. Proporcione una subred IDs desde la VPC. Puede encontrarla IDs en la pestaña Administración del entorno > Configuración > Red.
4. Elija Enviar.

Create new File System

Title

Enter a user friendly file system title

Eg. EFS 01

Name

Enter a file system name

File System name can only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

File System Provider

Select applicable file system type

EFS

Projects

Select applicable project

Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

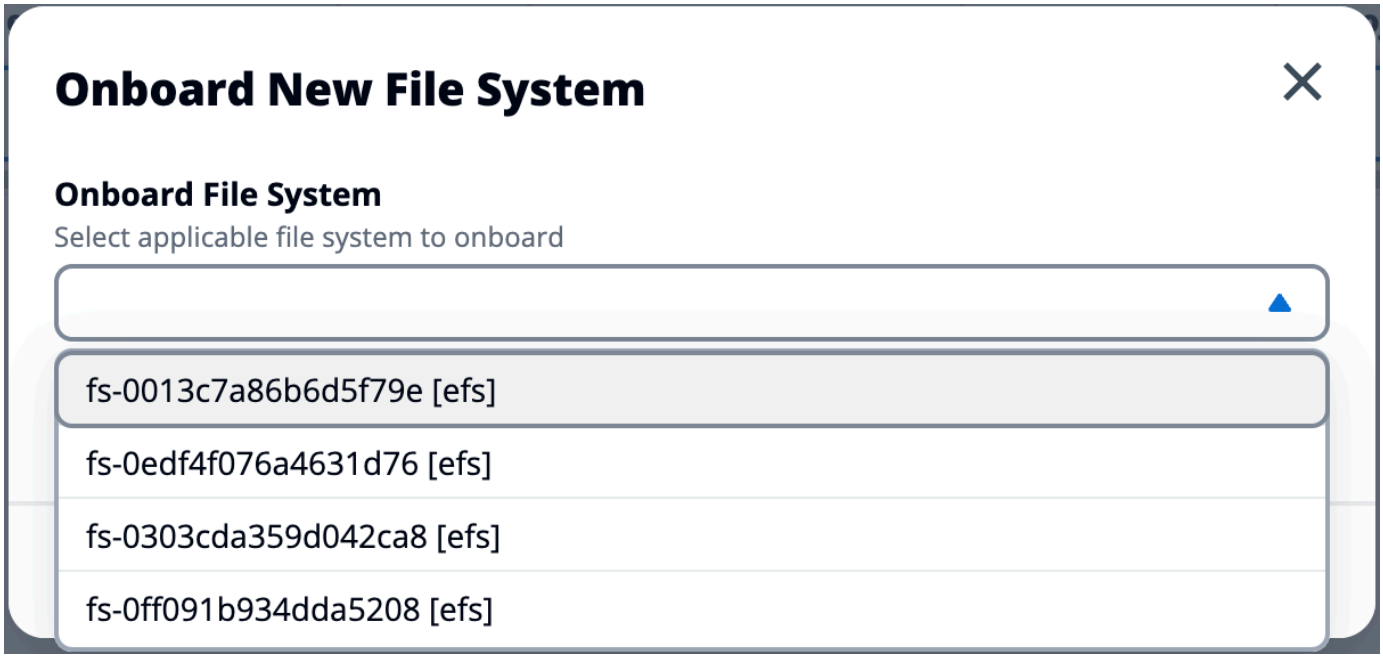
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

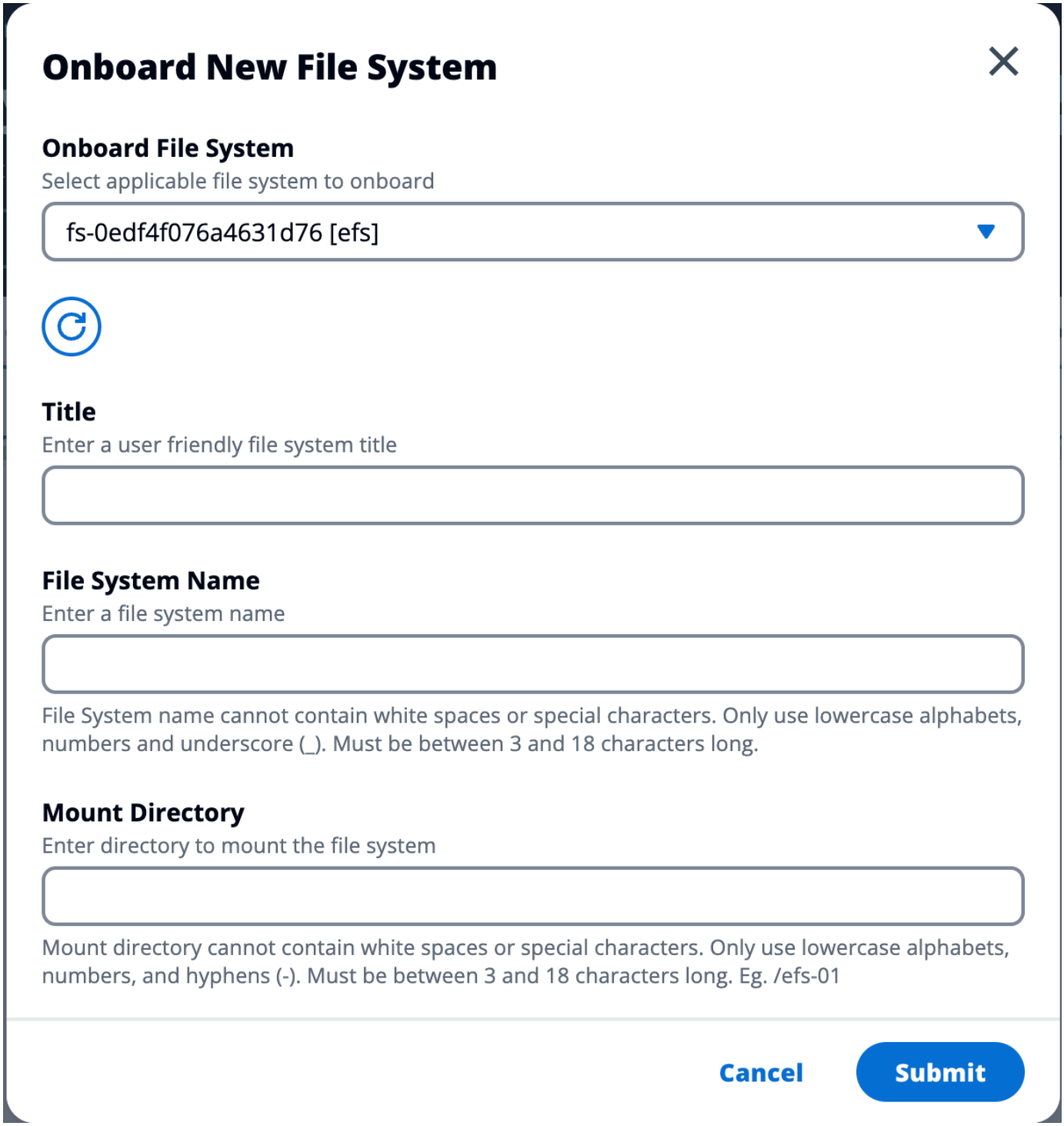
Enter directory to mount the file system

Incorpore un sistema de archivos

1. Elija un sistema de archivos integrado.
2. Seleccione un sistema de archivos en el menú desplegable. El modal se ampliará con entradas de detalles adicionales.

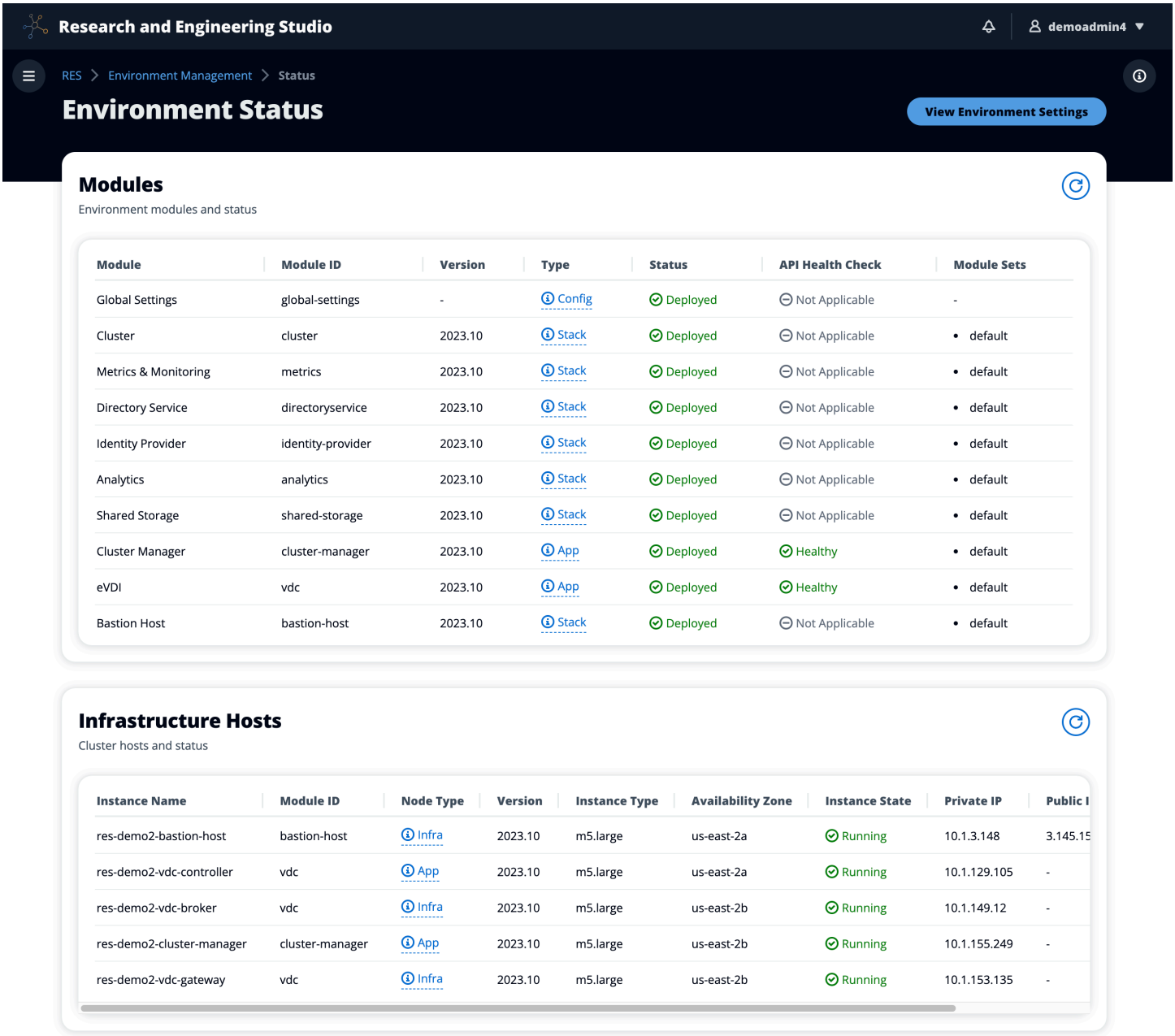


3. Introduzca los detalles del sistema de archivos.
4. Elija Enviar.


Onboard New File System
Onboard File System
Select applicable file system to onboard
fs-0edf4f076a4631d76 [efs]
Title
Enter a user friendly file system title
File System Name
Enter a file system name
File System name cannot contain white spaces or special characters. Only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.
Mount Directory
Enter directory to mount the file system
Mount directory cannot contain white spaces or special characters. Only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long. Eg. /efs-01
Cancel
Submit

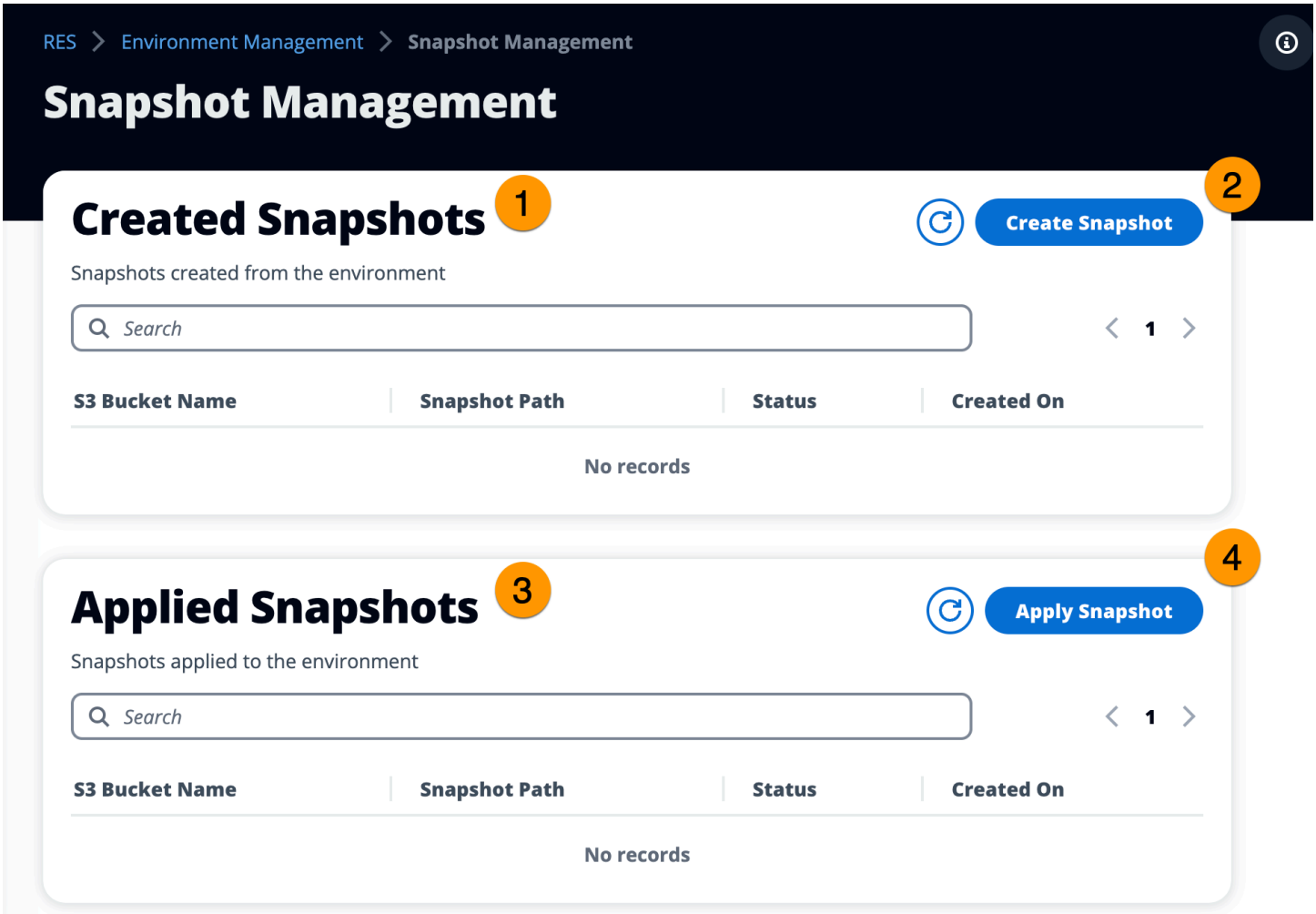
Estado del entorno

La página de estado del entorno muestra el software y los hosts implementados en el producto. Incluye información como la versión del software, los nombres de los módulos y otra información del sistema.



Administración de instantáneas

La administración de instantáneas simplifica el proceso de guardar y migrar datos entre entornos, lo que garantiza la coherencia y la precisión. Con las instantáneas, puede guardar el estado de su entorno y migrar los datos a un nuevo entorno con el mismo estado.



Desde la página de administración de instantáneas, puede:

1. Ver todas las instantáneas creadas y su estado.
2. Cree una instantánea. Antes de poder crear una instantánea, tendrá que crear un depósito con los permisos adecuados.
3. Vea todas las instantáneas aplicadas y su estado.
4. Aplique una instantánea.

Crear una instantánea

Antes de poder crear una instantánea, debe proporcionar un bucket de Amazon S3 con los permisos necesarios. Para obtener información sobre la creación de un bucket, consulte la sección de creación de un bucket. Recomendamos habilitar el control de versiones de los buckets y el registro de acceso al servidor. Estos ajustes se pueden habilitar desde la pestaña Propiedades del bucket después del aprovisionamiento.

> **Note**
>
> El ciclo de vida de este bucket de Amazon S3 no se gestionará dentro del producto. Deberá administrar el ciclo de vida del bucket desde la consola.

Para añadir permisos al depósito:

1. Elige el depósito que has creado en la lista de depósitos.
2. Elija la pestaña Permisos.
3. En Política de bucket, elija Editar.
4. Agrega la siguiente declaración a la política de cubos. Reemplace estos valores por sus propios valores:

   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

   > **Important**
   >
   > Hay cadenas de versiones limitadas compatibles con. AWS Para obtener más información, consulte https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html

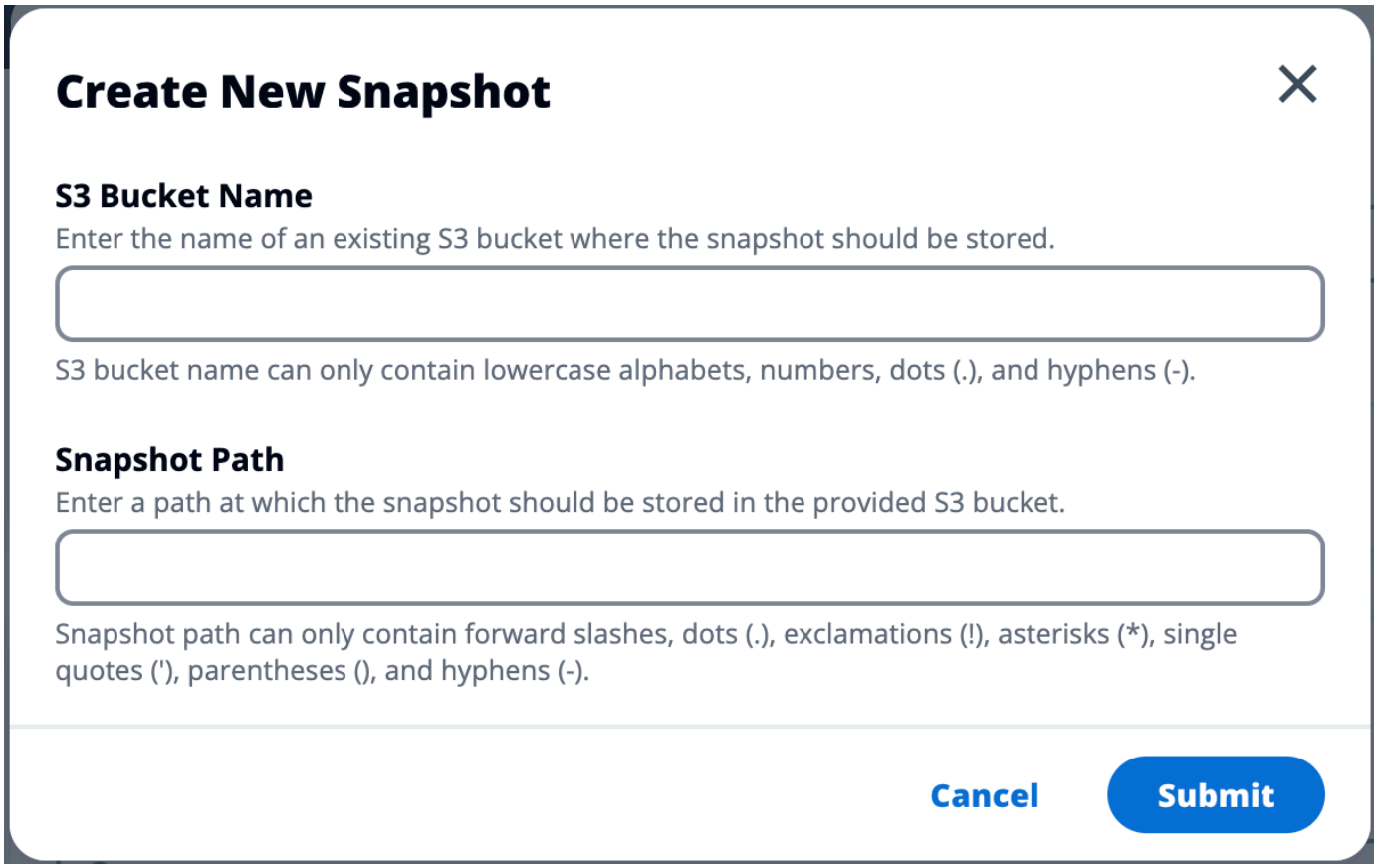
JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
```

```
}
```

Para crear la instantánea:

1. Elija Create Snapshot (Crear instantánea).
2. Introduzca el nombre del bucket de Amazon S3 que creó.
3. Introduzca la ruta en la que desea almacenar la instantánea en el depósito. Por ejemplo, **`october2023/23`**.
4. Elija Enviar.



5. Después de cinco a diez minutos, seleccione Actualizar en la página de instantáneas para comprobar el estado. Una instantánea no será válida hasta que el estado cambie de IN_PROGRESS a COMPLETADA.

Aplica una instantánea

Una vez que haya creado una instantánea de un entorno, puede aplicarla a un nuevo entorno para migrar los datos. Tendrá que añadir una nueva política al depósito que permita al entorno leer la instantánea.

Al aplicar una instantánea, se copian datos como los permisos de usuario, los proyectos, las pilas de software, los perfiles de permisos y los sistemas de archivos, junto con sus asociaciones, a un nuevo entorno. Las sesiones de usuario no se replicarán. Cuando se aplica la instantánea, comprueba la información básica de cada registro de recursos para determinar si ya existe. En el caso de los registros duplicados, la instantánea omite la creación de recursos en el nuevo entorno. Para los registros que son similares, como compartir un nombre o clave, pero la información sobre otros recursos básicos varía, creará un nuevo registro con un nombre y una clave modificados utilizando la siguiente convención:`RecordName_SnapshotRESVersion_ApplySnapshotID`. `ApplySnapshotID`Parece una marca de tiempo e identifica cada intento de aplicar una instantánea.

Durante la aplicación de la instantánea, la instantánea comprueba la disponibilidad de los recursos. No se creará el recurso que no esté disponible para el nuevo entorno. En el caso de los recursos con un recurso dependiente, la instantánea comprueba la disponibilidad del recurso dependiente. Si el recurso dependiente no está disponible, creará el recurso principal sin el recurso dependiente.

Si el nuevo entorno no es el esperado o se produce un error, puede comprobar los CloudWatch registros que se encuentran en el grupo de registros `/res-<env-name>/cluster-manager` para obtener más información. Cada registro tendrá la etiqueta [aplicar instantánea]. Una vez que haya aplicado una instantánea, podrá comprobar su estado desde la the section called “Administración de instantáneas” página.

Para añadir permisos al depósito:

1. Elige el depósito que has creado en la lista de depósitos.
2. Elija la pestaña Permisos.
3. En Política de bucket, elija Editar.
4. Agrega la siguiente declaración a la política de cubos. Reemplace estos valores por sus propios valores:

   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION

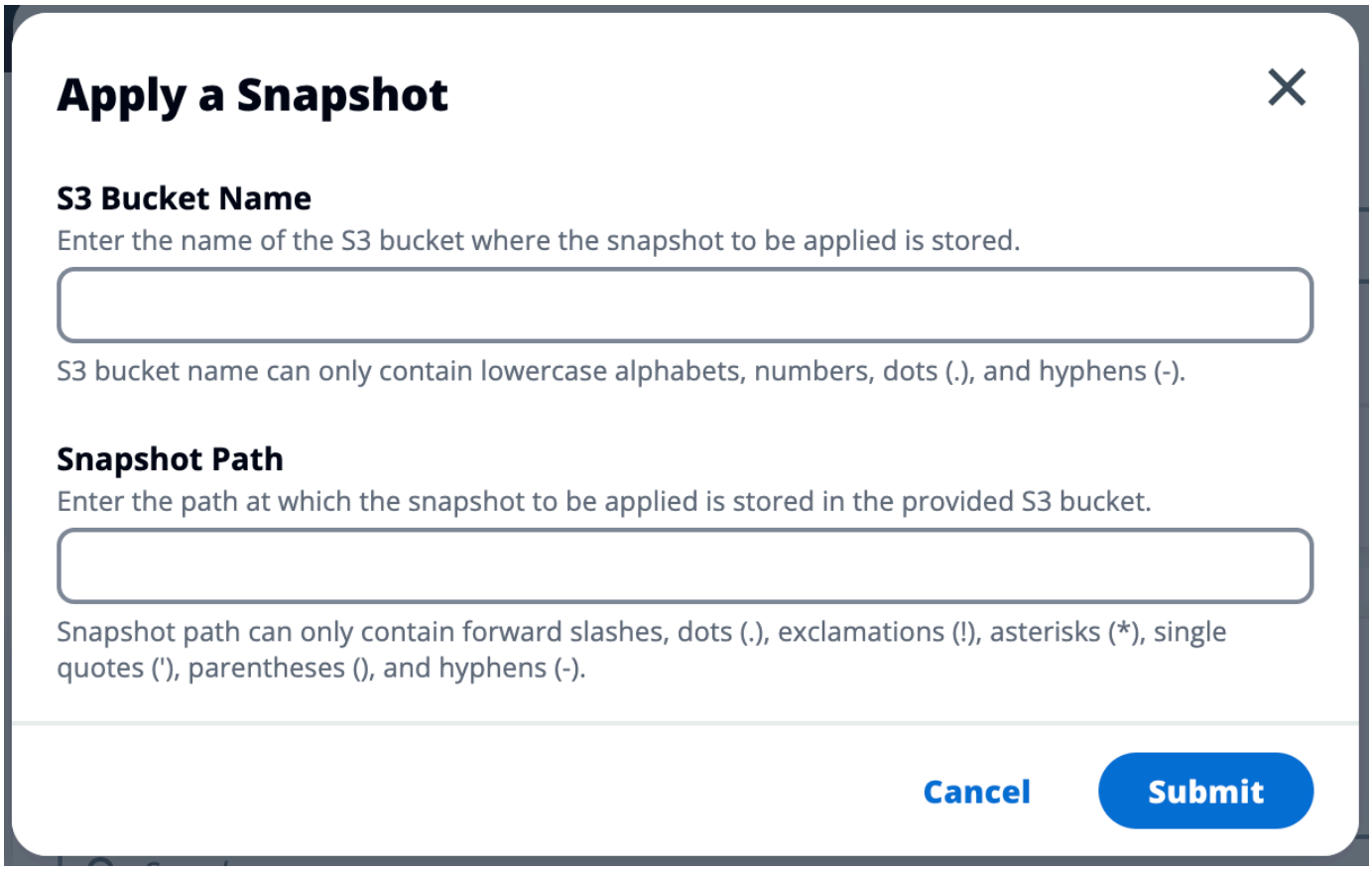
- S3_BUCKET_NAME

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

Para aplicar una instantánea:

1. Seleccione Aplicar instantánea.
2. Introduzca el nombre del bucket de Amazon S3 que contiene la instantánea.
3. Introduzca la ruta del archivo a la instantánea dentro del bucket.
4. Elija Enviar.



5. Transcurridos entre cinco y diez minutos, seleccione Actualizar en la página de administración de instantáneas para comprobar el estado.

Configuración del entorno

La configuración del entorno muestra los detalles de configuración del producto, como:

- General

  Muestra información como el nombre de usuario del administrador y el correo electrónico del usuario que suministró el producto. Puede editar el título del portal web y el texto de los derechos de autor.

- Proveedor de identidades

  Muestra información como el estado del inicio de sesión único.

- Network

  Muestra el ID de VPC y la lista IDs de prefijos para el acceso.

- Directory Service

  Muestra la configuración de Active Directory y el ARN del administrador de secretos de cuentas de servicio para el nombre de usuario y la contraseña.

Buckets de Amazon S3

Temas

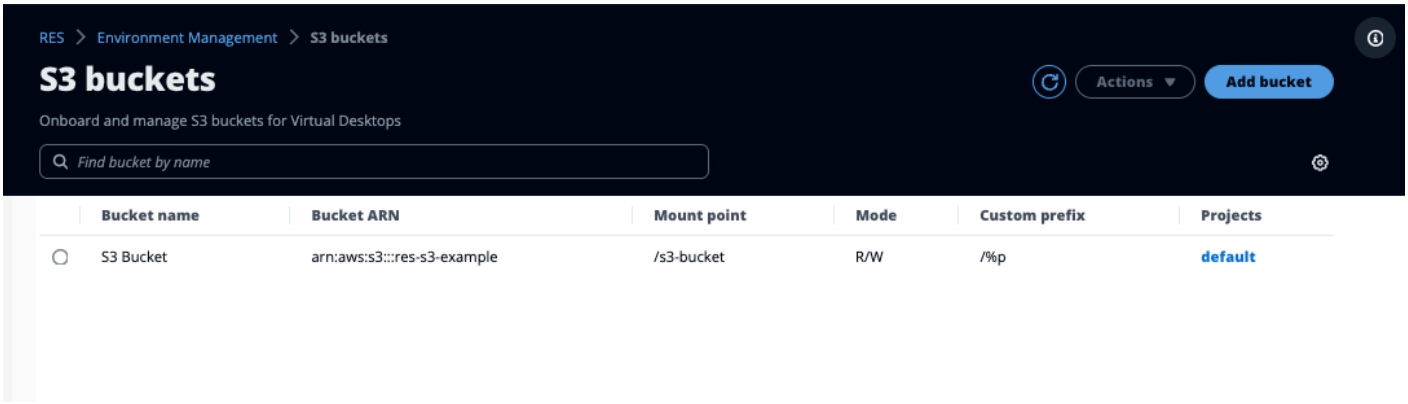
Montar un bucket de Amazon S3

Research and Engineering Studio (RES) admite el montaje de buckets de Amazon S3 en instancias de infraestructura de escritorio virtual (VDI) de Linux. Los administradores de RES pueden incorporar cubos de S3 a RES, adjuntarlos a proyectos, editar su configuración y eliminar los cubos en la pestaña de cubos de S3, en la sección Administración del entorno.

El panel de control de los buckets de S3 proporciona una lista de los buckets de S3 integrados que están disponibles para usted. Desde el panel de mandos de S3, puedes:

1. Utilice Añadir depósito para incorporar un depósito de S3 a RES.

2. Seleccione un depósito de S3 y utilice el menú Acciones para:
   - Edite un bucket
   - Eliminar un balde
3. Usa el campo de búsqueda para buscar por nombre de bucket y encontrar los buckets S3 integrados.



Añadir un bucket de Amazon S3

Para añadir un bucket de S3 a su entorno RES:

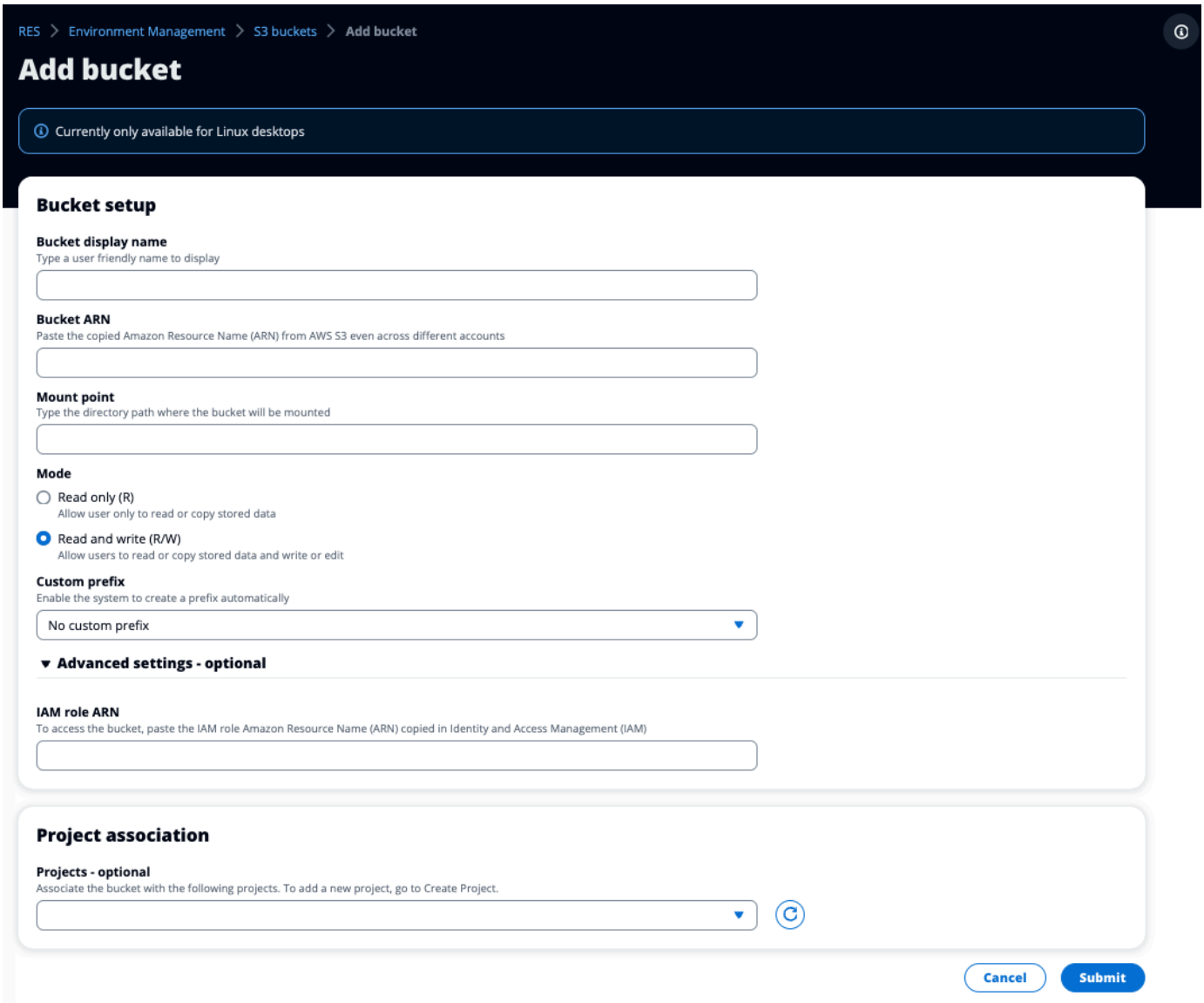
1. Elija Add bucket (Añadir bucket).
2. Introduzca los detalles del depósito, como el nombre del depósito, el ARN y el punto de montaje.

> **Important**
>
> - El ARN del bucket, el punto de montaje y el modo proporcionados no se pueden cambiar después de la creación.
> - El ARN del depósito puede contener un prefijo que aísle el depósito S3 incorporado de ese prefijo.

3. Seleccione un modo en el que desee incorporar el bucket.

> **Important**
>
> - Consulte Aislamiento de datos para obtener más información relacionada con el aislamiento de datos con modos específicos.

4. En Opciones avanzadas, puede proporcionar un ARN de rol de IAM para montar los cubos para el acceso entre cuentas. Sigue los pasos que se indican a continuación Acceso al bucket entre cuentas para crear el rol de IAM necesario para el acceso entre cuentas.
5. (Opcional) Asocia el bucket a los proyectos, que se pueden cambiar más adelante. Sin embargo, un bucket de S3 no se puede montar en las sesiones de VDI existentes de un proyecto. Solo las sesiones iniciadas después de que el proyecto se haya asociado al bucket se montarán en el bucket.
6. Elija Enviar.



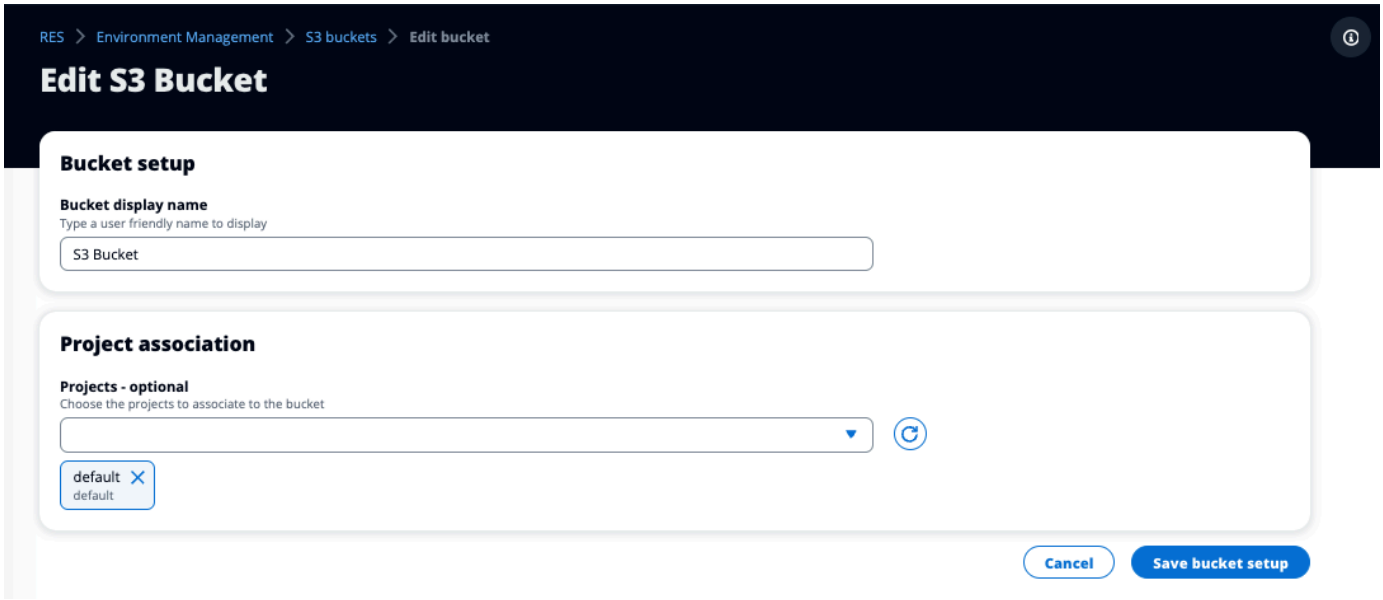
Editar un bucket de Amazon S3

1. Seleccione un depósito de S3 de la lista de depósitos de S3.

2. En el menú Acciones, selecciona Editar.
3. Introduce tus actualizaciones.

> **Important**
>
> - Al asociar un proyecto a un bucket de S3, no se montará el bucket en las instancias de infraestructura de escritorio virtual (VDI) existentes de ese proyecto. El bucket solo se montará en las sesiones de VDI lanzadas en un proyecto una vez que el bucket se haya asociado a ese proyecto.
> - La disociación de un proyecto de un bucket de S3 no afectará a los datos del bucket de S3, pero provocará que los usuarios de escritorio pierdan el acceso a esos datos.

4. Selecciona Guardar configuración del bucket.



Eliminar un bucket de Amazon S3

1. Seleccione un depósito de S3 de la lista de depósitos de S3.
2. En el menú Acciones, selecciona Eliminar.

> **Important**
>
> - Primero debe eliminar todas las asociaciones de proyectos del depósito.

- La operación de eliminación no afecta a los datos del depósito de S3. Solo elimina la asociación del bucket de S3 con RES.
- Al eliminar un depósito, las sesiones de VDI existentes perderán el acceso al contenido de ese depósito cuando caduquen las credenciales de esa sesión (aproximadamente 1 hora).

Aislamiento de datos

Cuando agrega un depósito de S3 a RES, tiene opciones para aislar los datos del depósito para proyectos y usuarios específicos. En la página Añadir cubo, puedes elegir un modo de Solo lectura (R) o Lectura y escritura (R/W).

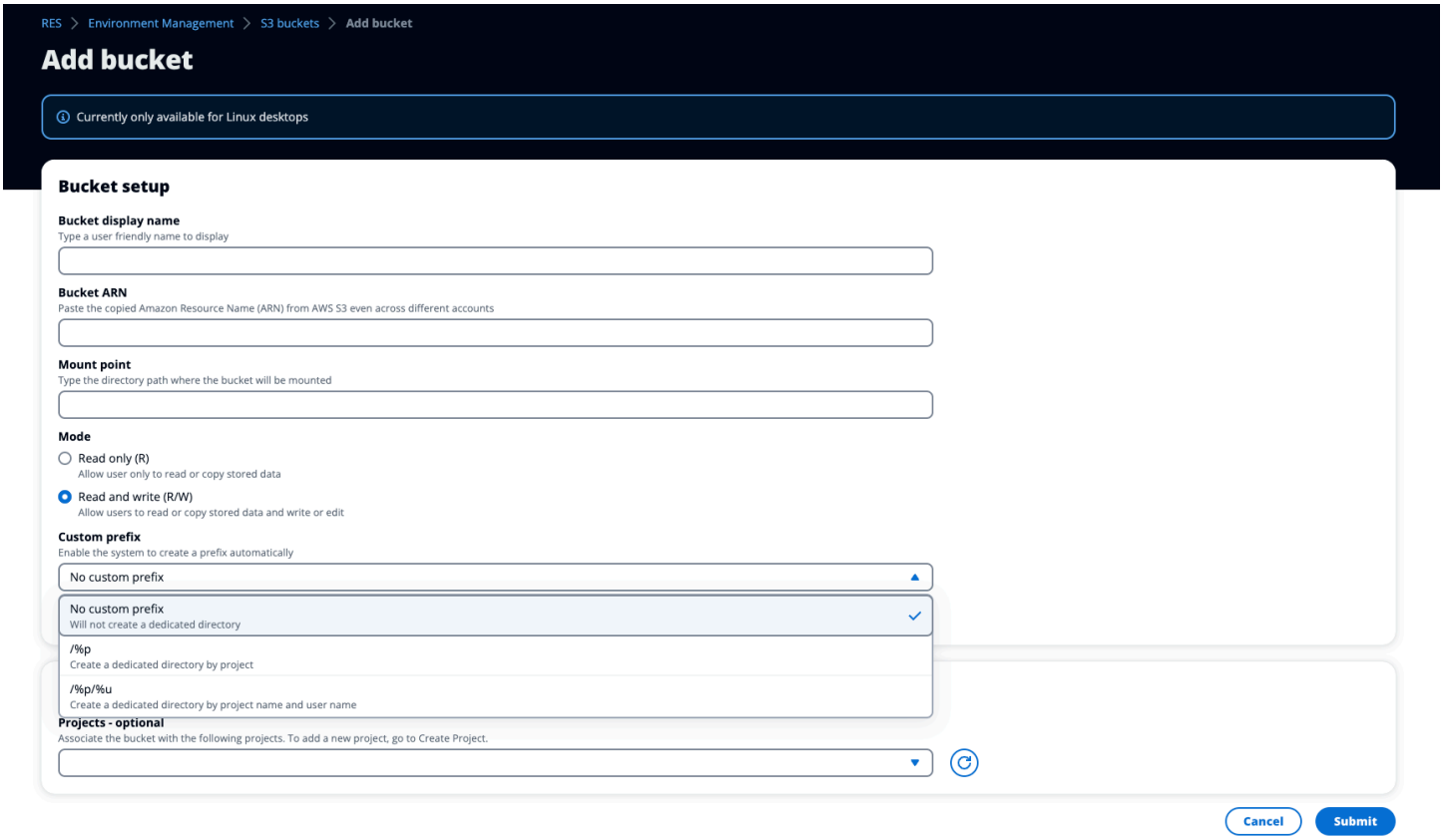
Solo lectura

Si `Read Only (R)` se selecciona, el aislamiento de datos se aplica en función del prefijo del ARN (Amazon Resource Name) del bucket. Por ejemplo, si un administrador añade un depósito a RES mediante el ARN `arn:aws:s3:::`*`bucket-name/example-data/`* y asocia este depósito al Proyecto A y al Proyecto B, los usuarios que se inicien VDIs desde el Proyecto A y el Proyecto B solo podrán leer los datos que se encuentran *`bucket-name`* debajo de la ruta. *`/example-data`* No tendrán acceso a los datos fuera de esa ruta. Si no hay ningún prefijo adjunto al ARN del bucket, todo el bucket estará disponible para cualquier proyecto asociado al mismo.

Lee y escribe

Si `Read and Write (R/W)` se selecciona, el aislamiento de datos se sigue aplicando en función del prefijo del ARN del bucket, tal y como se ha descrito anteriormente. Este modo tiene opciones adicionales que permiten a los administradores proporcionar prefijos basados en variables para el depósito de S3. Cuando `Read and Write (R/W)` se selecciona, aparece una sección de prefijos personalizados que ofrece un menú desplegable con las siguientes opciones:

- Sin prefijo personalizado
- /%p
- /%p/%u



Sin aislamiento de datos personalizado

Cuando `No custom prefix` se selecciona como Prefijo personalizado, el depósito se añade sin ningún aislamiento de datos personalizado. Esto permite que cualquier proyecto asociado al depósito tenga acceso de lectura y escritura. Por ejemplo, si un administrador añade un depósito a RES mediante el ARN `arn:aws:s3:::bucket-name` con el `No custom prefix` seleccionado y asocia este depósito al Proyecto A y al Proyecto B, los usuarios que se lancen VDIs desde el Proyecto A y el Proyecto B tendrán acceso ilimitado de lectura y escritura al depósito.

Aislamiento de datos por proyecto

Cuando `/%p` se selecciona el prefijo personalizado, los datos del depósito se aíslan para cada proyecto específico asociado al mismo. La `%p` variable representa el código del proyecto. Por ejemplo, si un administrador agrega un depósito a RES `arn:aws:s3:::bucket-name` con el ARN `/%p` seleccionado y un punto de montaje de`/bucket`, y asocia este depósito a los proyectos A y B, el usuario A del proyecto A puede escribir un archivo en él. `/bucket` El usuario B del proyecto A también puede ver el archivo en `/bucket` el que escribió el usuario A. Sin embargo,

si el usuario B lanza una VDI en el proyecto B y la consulta*/bucket*, no verá el archivo que escribió el usuario A, ya que los datos están aislados por proyecto. El archivo que escribió el usuario A se encuentra en el bucket de S3, bajo el prefijo, `/ProjectA` mientras que el usuario B solo puede acceder `/ProjectB` cuando utiliza el suyo VDIs del Proyecto B.

Aislamiento de datos por proyecto y por usuario

Cuando `/%p/%u` se selecciona el prefijo personalizado, los datos del depósito se aíslan para cada proyecto y usuario específicos asociados a ese proyecto. La `%p` variable representa el código del proyecto y `%u` representa el nombre de usuario. Por ejemplo, un administrador agrega un bucket a RES utilizando el ARN `arn:aws:s3:::`*`bucket-name`* con la `/%p/%u` opción seleccionada y un punto de montaje de. */bucket* Este depósito está asociado al proyecto A y al proyecto B. El usuario A del proyecto A puede escribir un archivo en él. */bucket* A diferencia del escenario anterior, en el que solo estaba `%p` aislado, en este caso el usuario B no verá el archivo en el que escribió el usuario A en el proyecto A*/bucket*, ya que los datos están aislados tanto por el proyecto como por el usuario. El archivo que escribió el usuario A se encuentra en el depósito de S3 bajo el prefijo, `/ProjectA/UserA` mientras que el usuario B solo puede acceder `/ProjectA/UserB` cuando lo usa VDIs en el Proyecto A.

Acceso al bucket entre cuentas

RES tiene la capacidad de montar depósitos desde otras AWS cuentas, siempre que estos grupos cuenten con los permisos adecuados. En el siguiente escenario, un entorno RES de la cuenta A quiere montar un bucket de S3 en la cuenta B.

Paso 1: Cree un rol de IAM en la cuenta en la que está desplegado RES (se denominará cuenta A):

1. Inicie sesión en la consola AWS de administración de la cuenta RES que necesita acceder al bucket de S3 (cuenta A).
2. Abra la consola de IAM:
   a. Navegue hasta el panel de control de IAM.
   b. En el panel de navegación, seleccione Policies (Políticas).
3. Cree una política:
   a. Seleccione Crear política.
   b. Seleccione la pestaña JSON.

c. Pegue la siguiente política de JSON (*<BUCKET-NAME>*sustitúyala por el nombre del bucket de S3 ubicado en la cuenta B):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

d. Seleccione Siguiente.

4. Revisa y crea la política:

   a. Proporcione un nombre para la política (por ejemplo, AccessPolicy «S3»).

   b. Añada una descripción opcional para explicar el propósito de la política.

   c. Revisa la política y selecciona Crear política.

5. Abra la consola de IAM:

   a. Navegue hasta el panel de control de IAM.

   b. En el panel de navegación, seleccione Roles (Roles).

6. Cree un rol:

   a. Elija Crear rol.

   b. Elija una política de confianza personalizada como tipo de entidad de confianza.

c. Pegue la siguiente política de JSON (*<ACCOUNT_ID>*sustitúyala por el ID de cuenta real de la cuenta A, *<ENVIRONMENT_NAME>* por el nombre del entorno de la implementación de RES y *<REGION>* por la AWS región en la que se implementa RES):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::<ACCOUNT_ID>:role/<ENVIRONMENT_NAME>-custom-credential-
broker-lambda-role-<REGION>"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

d. Seleccione «Siguiente».

7. Adjunte políticas de permisos:

a. Busque y seleccione la política que creó anteriormente.

b. Seleccione «Siguiente».

8. Etiquete, revise y cree el rol:

a. Introduzca el nombre de un rol (por ejemplo, AccessRole «S3»).

b. En el paso 3, selecciona Añadir etiqueta y, a continuación, introduce la clave y el valor siguientes:

- Clave: `res:Resource`
- Valor: `s3-bucket-iam-role`

c. Revisa el rol y selecciona Crear rol.

9. Utilice el rol de IAM en RES:

a. Copie el ARN del rol de IAM que creó.

b. Inicie sesión en la consola RES.

c. En el panel de navegación izquierdo, seleccione S3 Bucket.

d. Seleccione Añadir depósito y rellene el formulario con el ARN del depósito S3 multicuenta.

e. Selecciona el menú desplegable Configuración avanzada (opcional).

f. Introduzca el ARN del rol en el campo ARN del rol de IAM.

g. Seleccione Añadir depósito.

Paso 2: Modifique la política de depósitos en la cuenta B

1. Inicie sesión en la consola AWS de administración de la cuenta B.
2. Abra la consola S3:

   a. Navegue hasta el panel de control de S3.

   b. Selecciona el depósito al que quieres conceder acceso.
3. Edita la política de buckets:

   a. Elija la pestaña Permisos y seleccione la política de buckets.

   b. Añada la siguiente política para conceder a la función de IAM de la cuenta A acceso al bucket (*<AccountA_ID>*sustitúyala por el ID de cuenta real de la cuenta A y *<BUCKET-NAME>* por el nombre del bucket de S3):

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

c. Seleccione Guardar.

Evitar la exfiltración de datos en una VPC privada

Para evitar que los usuarios extraigan datos de depósitos de S3 seguros a sus propios depósitos de S3 de su cuenta, puede adjuntar un punto de enlace de VPC para proteger su VPC privada. En los siguientes pasos, se muestra cómo crear un punto final de VPC para el servicio S3 que permita el acceso a los buckets de S3 de su cuenta, así como a cualquier cuenta adicional que tenga buckets entre cuentas.

1. Abra la consola de Amazon VPC:
   a. Inicie sesión en la consola AWS de administración.
   b. Abra la consola de Amazon VPC en. https://console.aws.amazon.com/vpc/
2. Cree un punto final de VPC para S3:
   a. En el panel de navegación izquierdo, seleccione Endpoints.
   b. Seleccione Crear punto de conexión.
   c. En Service category (Categoría de servicio), asegúrese de que se seleccionó AWS services (Servicios de AWS).
   d. En el campo Nombre del servicio, introduzca `com.amazonaws.<region>.s3` (*<region>*sustitúyalo por su AWS región) o busque «S3".
   e. Seleccione el servicio S3 de la lista.
3. Configure los ajustes del punto final:
   a. En el caso de la VPC, seleccione la VPC en la que desee crear el punto final.
   b. En el caso de las subredes, seleccione las dos subredes privadas utilizadas para las subredes de VDI durante la implementación.

c. En Habilitar el nombre DNS, asegúrese de que la opción esté marcada. Esto permite que el nombre de host DNS privado se resuelva en las interfaces de red del punto final.

4. Configure la política para restringir el acceso:

   a. En Política, selecciona Personalizado.

   b. En el editor de políticas, introduce una política que restrinja el acceso a los recursos de tu cuenta o de una cuenta específica. Este es un ejemplo de política (*mybucket*sustitúyalo por el nombre de tu bucket de S3 *111122223333* y *444455556666* por la AWS cuenta adecuada a la IDs que quieras acceder):

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::mybucket",
                "arn:aws:s3:::mybucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",   // Your Account ID
                        "444455556666"    // Another Account ID
                    ]
                }
            }
        }
    ]
}
```

5. Crea el punto final:

   a. Revise la configuración.

   b. Seleccione Crear punto final.

6. Verifique el punto final:

a. Una vez creado el punto final, diríjase a la sección Puntos finales de la consola de VPC.
b. Seleccione el punto final recién creado.
c. Compruebe que el estado esté disponible.

Si sigue estos pasos, crea un punto final de VPC que permite el acceso a S3 restringido a los recursos de su cuenta o a un ID de cuenta específico.

Solución de problemas

¿Cómo comprobar si un bucket no se monta en una VDI

Si un bucket no se monta en una VDI, hay algunas ubicaciones en las que puede comprobar si hay errores. Siga los pasos que se indican a continuación.

1. Compruebe los registros de VDI:
   a. Inicie sesión en la consola AWS de administración.
   b. Abra la EC2 consola y vaya a Instancias.
   c. Seleccione la instancia de VDI que lanzó.
   d. Conéctese a la VDI mediante el administrador de sesiones.
   e. Ejecute los siguientes comandos :

```
sudo su
cd ~/bootstrap/logs
```

   Aquí encontrará los registros de arranque. Los detalles de cualquier error se encontrarán en el `configure.log.{time}` archivo.

   Además, consulte el `/etc/message` registro para obtener más información.
2. Compruebe los registros CloudWatch Lambda personalizados de Credential Broker:
   a. Inicie sesión en la consola de AWS administración.
   b. Abra la CloudWatch consola y vaya a Grupos de registros.
   c. Busque el grupo de registros`/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.

d. Examine el primer grupo de registros disponible y localice cualquier error en los registros. Estos registros contendrán detalles sobre posibles problemas y proporcionarán credenciales personalizadas temporales para el montaje de depósitos de S3.

3. Compruebe los CloudWatch registros de API Gateway personalizados de Credential Broker:

a. Inicie sesión en la consola AWS de administración.

b. Abra la CloudWatch consola y vaya a Grupos de registros.

c. Busque el grupo de registros`<stack-name>-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>`.

d. Examine el primer grupo de registros disponible y localice cualquier error en los registros. Estos registros contendrán detalles sobre cualquier solicitud y respuesta a la API Gateway para obtener las credenciales personalizadas necesarias para montar los buckets de S3.

¿Cómo editar la configuración del rol de IAM de un bucket después de la incorporación

1. Inicie sesión en la consola de AWS DynamoDB.
2. Seleccione la tabla:

a. En el panel de navegación izquierdo, selecciona Tablas.

b. Busque y seleccione`<stack-name>.cluster-settings`.

3. Escanea la tabla:

a. Selecciona Explorar los elementos de la tabla.

b. Asegúrese de que esté seleccionada la opción Escanear.

4. Añadir un filtro:

a. Seleccione Filtros para abrir la sección de entrada de filtros.

b. Configure el filtro para que coincida con su clave

- Atributo: introduce la clave.
- Condición: Elegir Empieza por.
- Valor: introduzca la `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` sustitución por `<filesystem_id>` el valor del sistema de archivos que se debe modificar.

5. Ejecute el escaneo:

Seleccione Ejecutar para ejecutar el escaneo con el filtro.

6. Compruebe el valor:

   Si la entrada existe, asegúrese de que el valor esté configurado correctamente con el ARN del rol de IAM correcto.

   Si la entrada no existe:

   a. Selecciona Crear artículo.

   b. Introduce los detalles del artículo:

      - Para el atributo clave, introduzca`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
      - Añada el ARN del rol de IAM correcto.

   c. Seleccione Guardar para añadir el elemento.

7. Reinicie las instancias de VDI:

   Reinicie la instancia para asegurarse de VDIs que los ARN afectados por el rol de IAM incorrecto se vuelvan a montar.

Habilitando CloudTrail

Para activarla CloudTrail en tu cuenta mediante la CloudTrail consola, sigue las instrucciones que se proporcionan en la sección Creación de una ruta con la CloudTrail consola de la Guía del AWS CloudTrail usuario. CloudTrail registrará el acceso a los buckets de S3 registrando el rol de IAM que accedió a ellos. Esto se puede vincular a un ID de instancia, que está vinculado a un proyecto o usuario.

Administración de secretos

Research and Engineering Studio mantiene los siguientes secretos de uso AWS Secrets Manager. RES crea secretos automáticamente durante la creación del entorno. Los secretos introducidos por el administrador durante la creación del entorno se introducen como parámetros.

Nombre del secreto	Descripción	RES generado	Ingresó el administrador
<envname>- sso-client-secret	Secreto de OAuth2 cliente de inicio de sesión único para el entorno	✓	
<envname>- vdc-client-secret	vdc ClientSecret	✓	
<envname>- vdc-client-id	vdc ClientId	✓	
<envname>- tecla vdc-gateway-certificate-private	Certificado autofirmado: clave privada para el dominio	✓	
<envname>- vdc-gateway-certificate-certificate	Certificado autofirmado para dominio	✓	
<envname>- cluster-manager-client-secret	administrador de clústeres ClientSecret	✓	
<envname>- cluster-manager-client-id	administrador de clústeres ClientId	✓	
<envname>- external-private-key	Certificado autofirmado: clave privada para el dominio	✓	
<envname>-certificado externo	Certificado autofirmado para el dominio	✓	
<envname>- internal-private-key	Certificado autofirmado: clave privada para el dominio	✓	

Nombre del secreto	Descripción	RES generado	Ingresó el administrador
<envname>-certificado interno	Certificado autofirmado para el dominio	✓	
<envname>- servicio de directorio - ServiceAccountUsername			✓
<envname>- servicio de directorio - ServiceAccountPassword			✓

Los siguientes valores de ARN secretos se incluyen en la tabla <envname>-cluster-settings de DynamoDB:

Clave	Origen
identity-provider.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	pila
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	pila
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	pila
directoryservice.root_username_secret_arn	
vdc.client_secret	pila
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	pila

Clave	Origen
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	pila
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	pila
cluster-manager.client_secret	

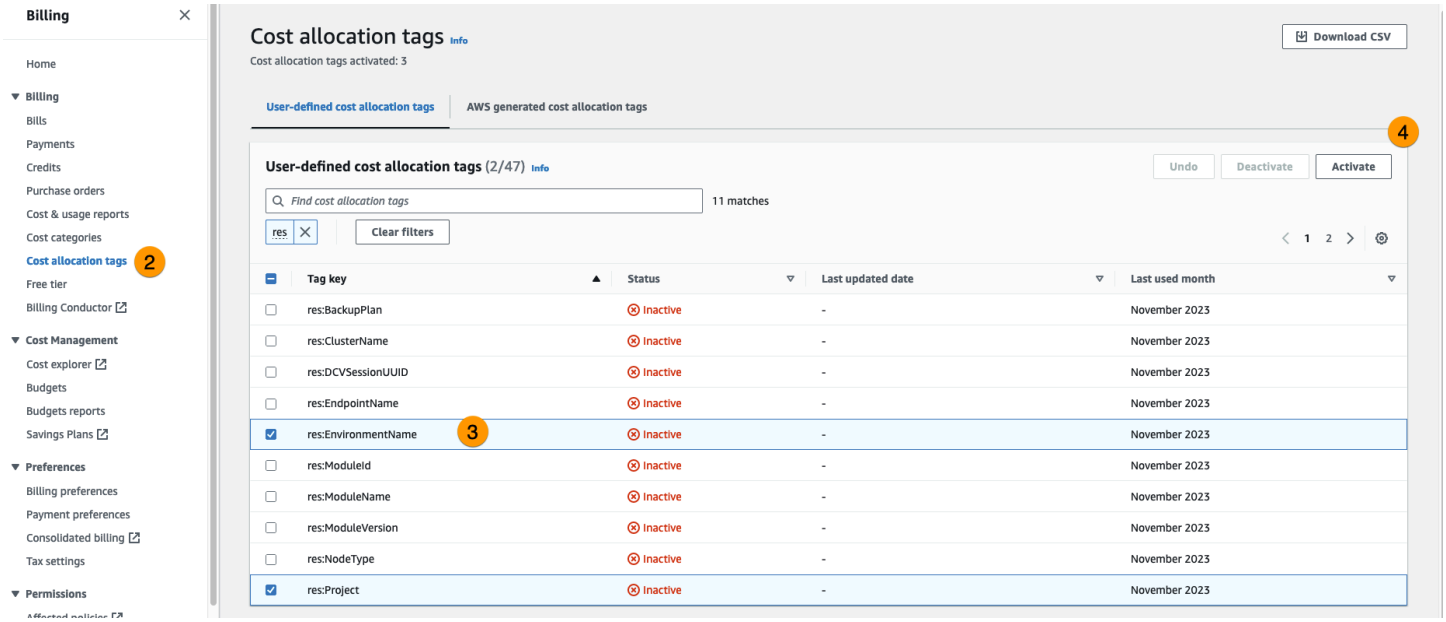
Supervisión y control de costes

> **Note**
>
> No se admite la asociación de proyectos de Research and Engineering Studio a AWS Budgets . AWS GovCloud (US)

Recomendamos crear un presupuesto a través de AWS Cost Explorer para ayudar a administrar los costos. Los precios están sujetos a cambios. Para obtener más información, consulte la página web de precios de cada uno de losthe section called “AWS servicios de este producto”.

Para facilitar el seguimiento de los costos, puede asociar los proyectos de RES a los presupuestos creados en ellos AWS Budgets. Primero tendrá que activar las etiquetas de entorno dentro de las etiquetas de asignación de costes de facturación.

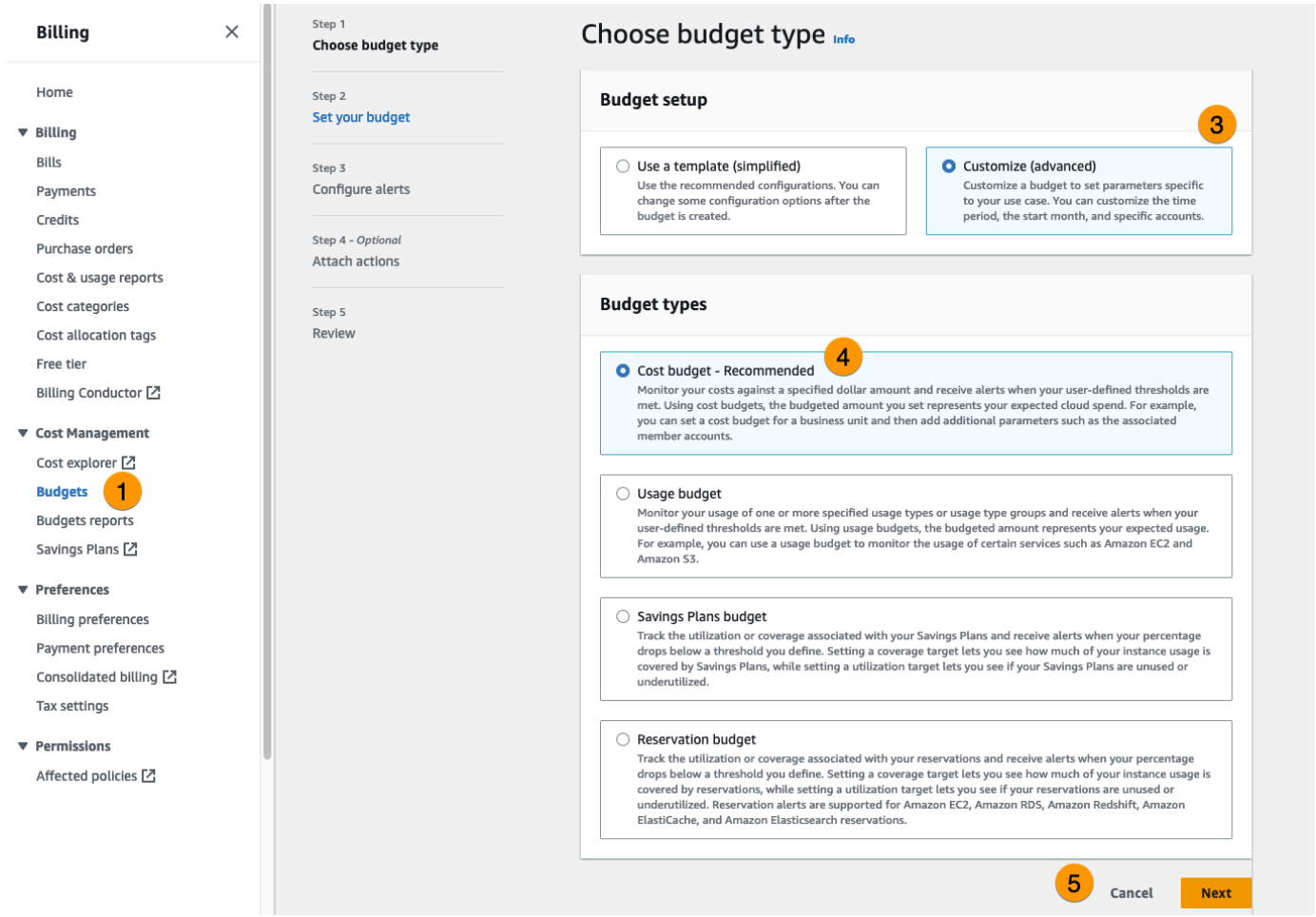
1. Inicie sesión en AWS Management Console y abra la Administración de facturación y costos de AWS consola en https://console.aws.amazon.com/costmanagement/.
2. Elija las etiquetas de asignación de costes.
3. Busque y seleccione las `res:EnvironmentName` etiquetas `res:Project` y.
4. Seleccione Activar.



> **Note**
>
> Las etiquetas RES pueden tardar hasta un día en aparecer después de la implementación.

Para crear un presupuesto para los recursos de RES:

1. En la consola de facturación, selecciona Presupuestos.
2. Selecciona Crear un presupuesto.
3. En Configuración del presupuesto, seleccione Personalización (avanzada).
4. En Tipos de presupuesto, selecciona Presupuesto de costes: recomendado.
5. Elija Siguiente.

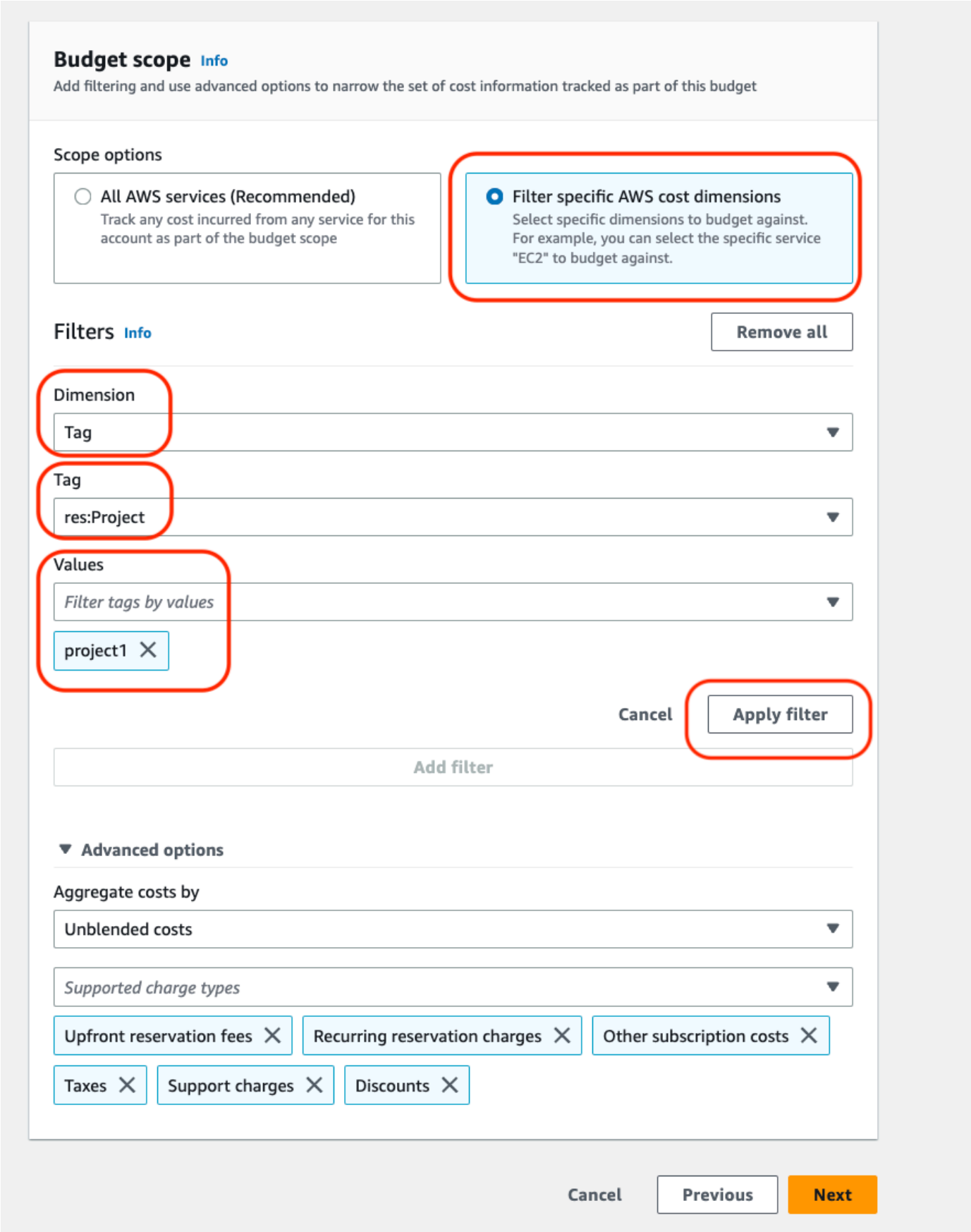


6. En Detalles, introduce un nombre de presupuesto significativo para tu presupuesto a fin de distinguirlo de los demás presupuestos de tu cuenta. Por ejemplo, [EnvironmentName] - [ProjectName] - [BudgetName].
7. En Establecer importe presupuestario, introduce el importe presupuestado para tu proyecto.
8. En Alcance del presupuesto, selecciona Filtrar dimensiones de AWS coste específicas.
9. Elija Add filter (Agregar filtro).
10. En Dimensión, elija Etiqueta.
11. En Etiqueta, selecciona RES:Project.

> **Note**
>
> Las etiquetas y los valores pueden tardar hasta dos días en estar disponibles. Puede crear un presupuesto una vez que el nombre del proyecto esté disponible.

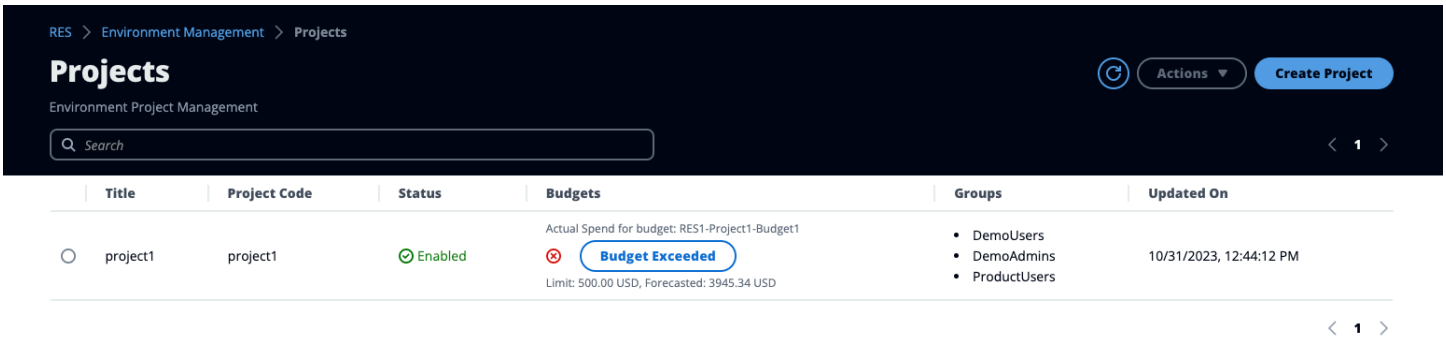
12. En Valores, seleccione el nombre del proyecto.

13. Elija Aplicar filtro para adjuntar el filtro del proyecto al presupuesto.
14. Elija Siguiente.


Budget scope Info
Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget
Scope options
All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope
Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.
Filters Info
Remove all
Dimension
Tag
Tag
res:Project
Values
Filter tags by values
project1
Cancel
Apply filter
Add filter
Advanced options
Aggregate costs by
Unblended costs
Supported charge types
Upfront reservation fees
Recurring reservation charges
Other subscription costs
Taxes
Support charges
Discounts
Cancel
Previous
Next

15. (Opcional.) Añada un umbral de alerta.
16. Elija Siguiente.
17. (Opcional.) Si se configuró una alerta, utilice Adjuntar acciones para configurar las acciones deseadas con la alerta.
18. Elija Siguiente.
19. Revise la configuración del presupuesto y confirme que se haya establecido la etiqueta correcta en Parámetros presupuestarios adicionales.
20. Seleccione Crear presupuesto.

Ahora que se ha creado el presupuesto, puede activar el presupuesto para los proyectos. Para activar los presupuestos de un proyecto, consultethe section called “Editar un proyecto”. Si se supera el presupuesto, se bloqueará el lanzamiento de los escritorios virtuales. Si se supera el presupuesto durante el lanzamiento de un escritorio, el escritorio seguirá funcionando.



Si necesitas cambiar el presupuesto, vuelve a la consola para editar el importe del presupuesto. El cambio puede tardar hasta quince minutos en surtir efecto en RES. Como alternativa, puede editar un proyecto para deshabilitar un presupuesto.

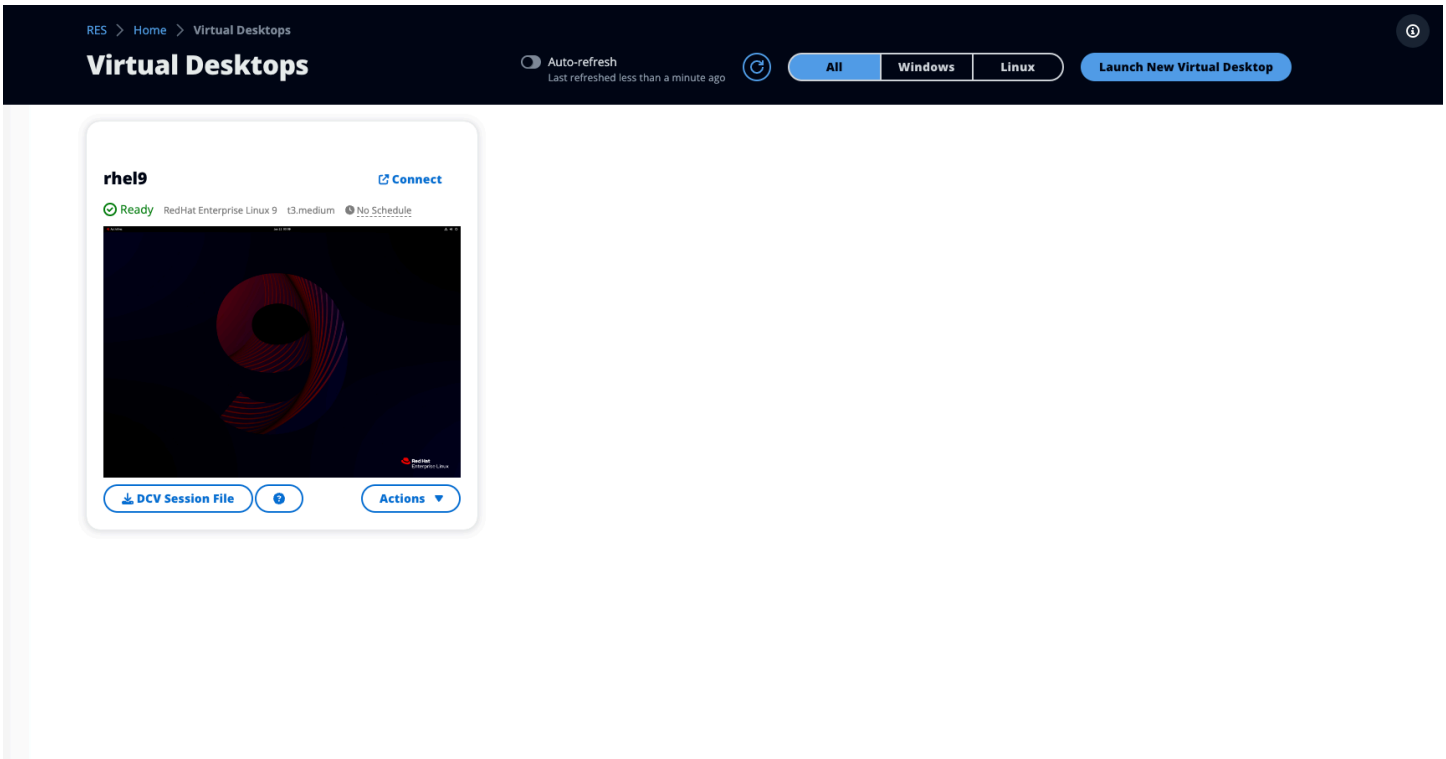
Usa el producto

En esta sección se ofrece orientación a los usuarios sobre el uso de escritorios virtuales para colaborar con otros usuarios.

Temas

Escritorios virtuales

El módulo de interfaz de escritorio virtual (VDI) permite a los usuarios crear y administrar escritorios virtuales Windows o Linux en ellos. AWS Los usuarios pueden lanzar EC2 instancias de Amazon con sus herramientas y aplicaciones favoritas preinstaladas y configuradas.



Sistemas operativos compatibles

Actualmente, RES admite el lanzamiento de escritorios virtuales mediante los siguientes sistemas operativos:

- Amazon Linux 2 (x86 y ARM64)
- Ubuntu 22.04.03 (x86)
- Windows 2019, 2022 (x86)

Lanza un escritorio nuevo

1. En el menú, elija Mis escritorios virtuales.
2. Seleccione Lanzar un nuevo escritorio virtual.
3. Introduzca los detalles de su nuevo escritorio.
4. Elija Enviar.

Aparece al instante una nueva tarjeta con la información del escritorio y el escritorio estará listo para usarse en un plazo de 10 a 15 minutos. El tiempo de inicio depende de la imagen seleccionada. RES detecta las instancias de GPU e instala los controladores correspondientes.

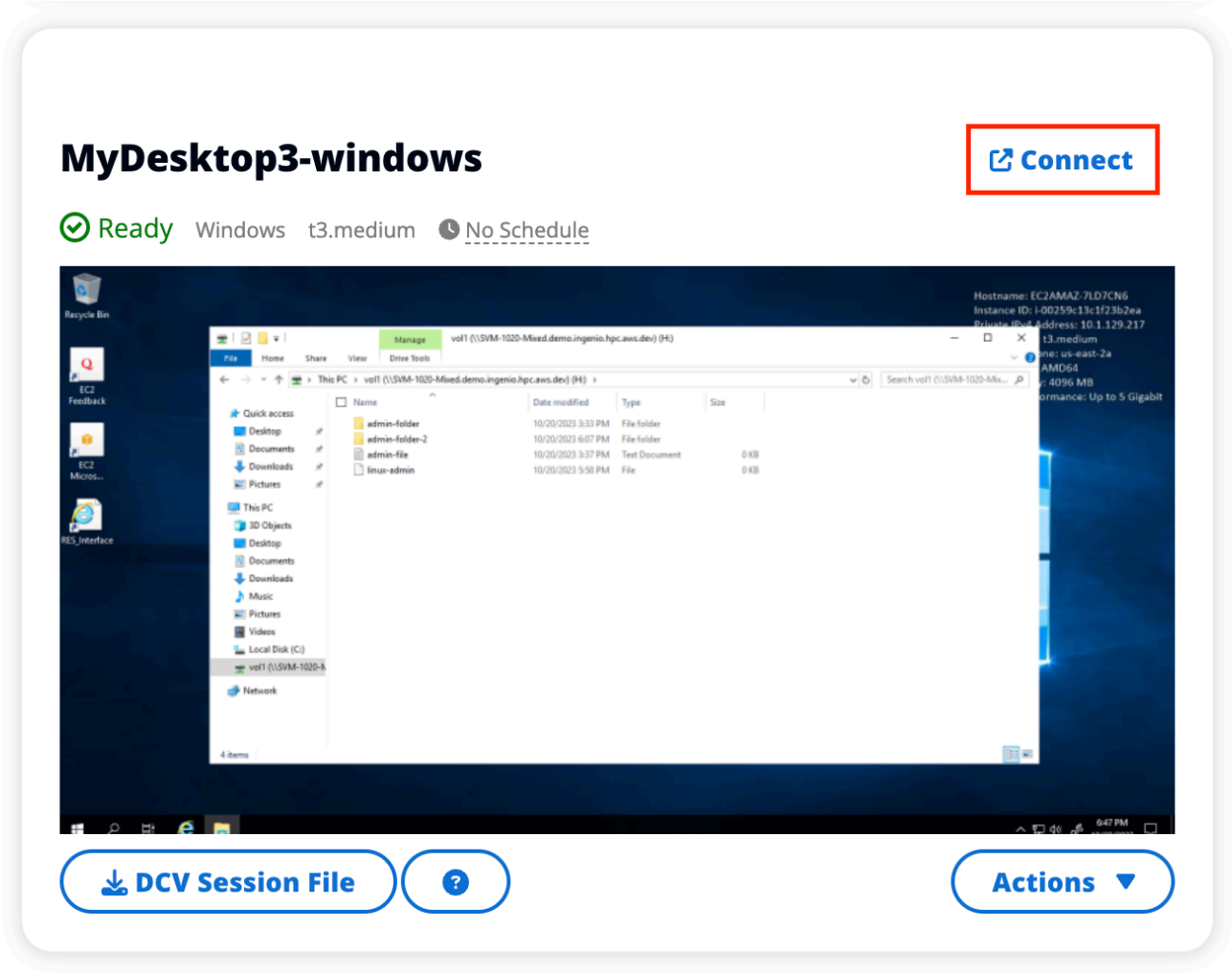
Acceda a su escritorio

Para acceder a un escritorio virtual, elija la tarjeta para el escritorio y conéctese mediante un cliente web o DCV.

Web connection

Acceder al escritorio a través del navegador web es el método de conexión más sencillo.

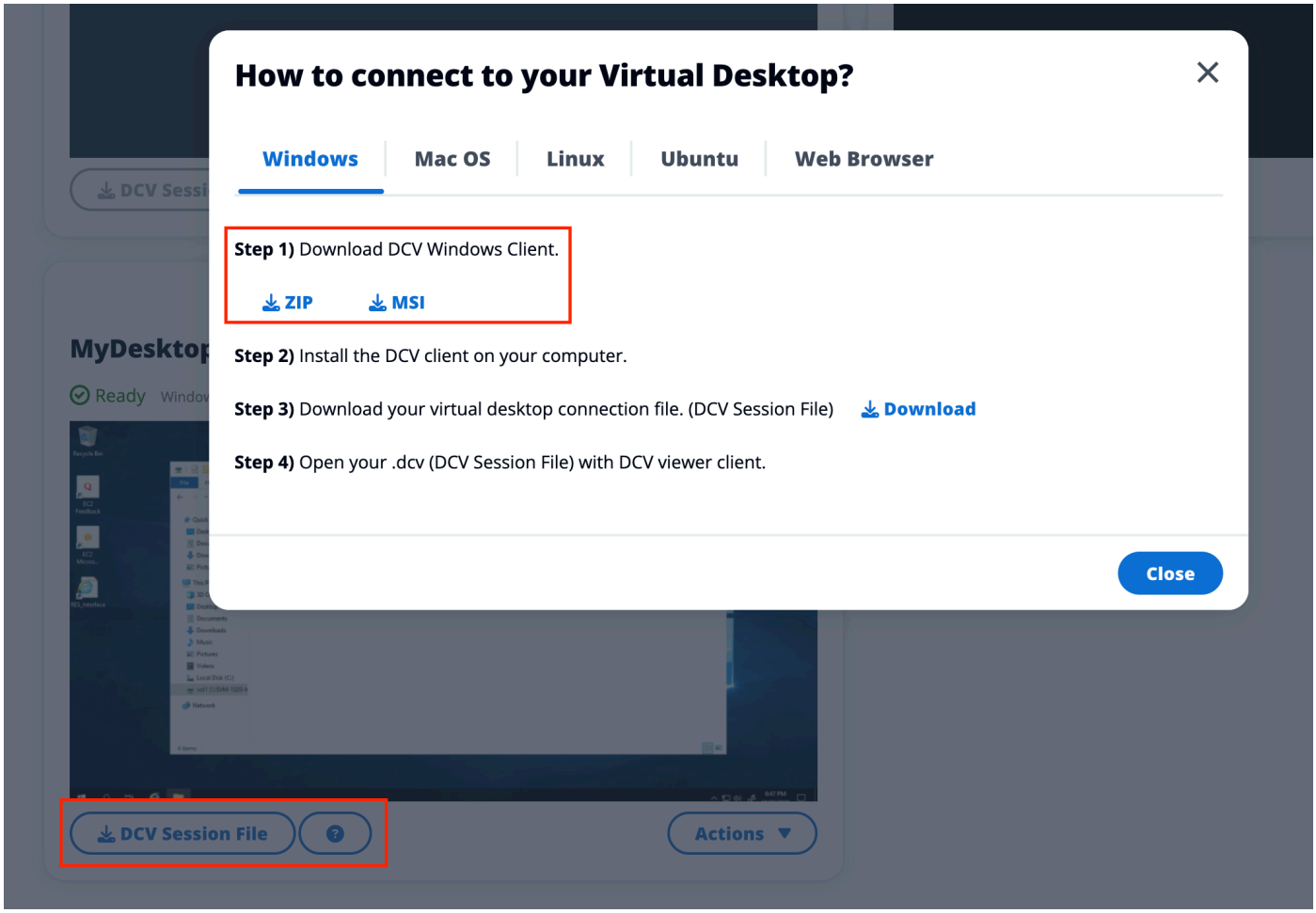
- Selecciona Connect o elige la miniatura para acceder al escritorio directamente a través del navegador.



DCV connection

Acceder a su escritorio a través de un cliente DCV ofrece el mejor rendimiento. Para acceder a través de DCV:

1. Elija el archivo de sesión DCV para descargar el. `dcv`archivo. Necesitará tener un cliente DCV instalado en su sistema.
2. Para ver las instrucciones de instalación, elija la opción? icono.



Controle el estado de su escritorio

Para controlar el estado del escritorio:

1. Elija Acciones.
2. Elija el estado del escritorio virtual. Puede elegir entre cuatro estados:

   - Detener

     Una sesión detenida no sufrirá pérdida de datos y podrá reiniciarla en cualquier momento.
   - Reiniciar

     Reinicia la sesión actual.
   - Finalizar

Finaliza una sesión de forma permanente. La finalización de una sesión puede provocar la pérdida de datos si utiliza un almacenamiento efímero. Debe hacer una copia de seguridad de sus datos en el sistema de archivos RES antes de finalizar.

- Hibernar

  El estado del escritorio se guardará en la memoria. Al reiniciar el escritorio, las aplicaciones se reanudarán, pero es posible que se pierdan las conexiones remotas. No todas las instancias admiten la hibernación y la opción solo está disponible si se activó durante la creación de la instancia. Para comprobar si la instancia admite este estado, consulta los requisitos previos de hibernación.

Modifica un escritorio virtual

Puede actualizar el hardware de su escritorio virtual o cambiar el nombre de la sesión.

1. Antes de realizar cambios en el tamaño de la instancia, debe detener la sesión:
   a. Elija Acciones.
   b. Elija el estado del escritorio virtual.
   c. Elija Detener.

> **Note**
>
> No puede actualizar el tamaño del escritorio para las sesiones en hibernación.

2. Una vez que hayas confirmado que el escritorio se ha detenido, selecciona Acciones y, a continuación, selecciona Actualizar sesión.
3. Cambie el nombre de la sesión o elija el tamaño de escritorio que desee.
4. Elija Enviar.
5. Una vez que las instancias se actualicen, reinicia el escritorio:
   a. Elija Acciones.
   b. Elija el estado del escritorio virtual.
   c. Elija Iniciar.

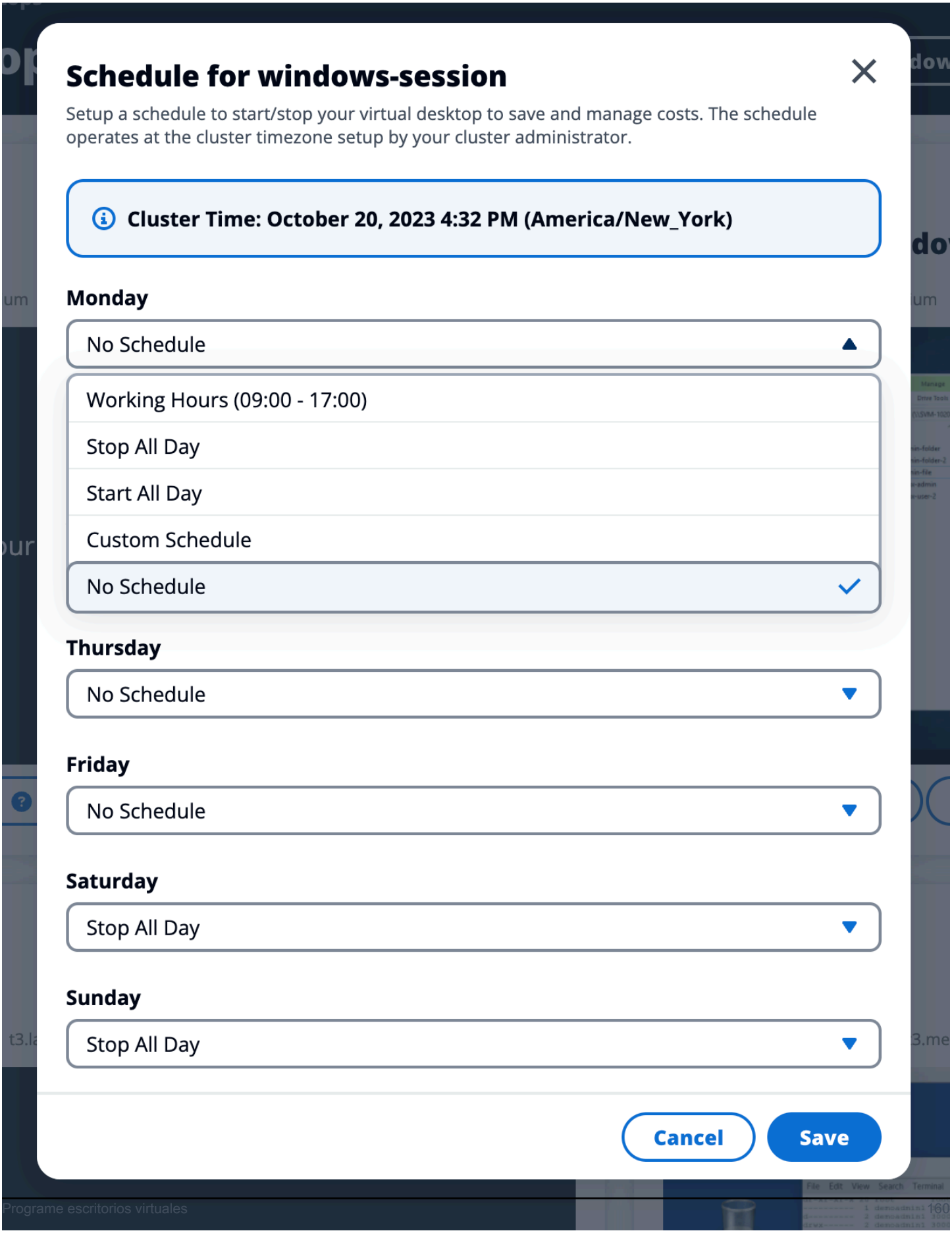
Recupere la información de la sesión

1. Elija Acciones.
2. Selecciona Mostrar información.

Programe escritorios virtuales

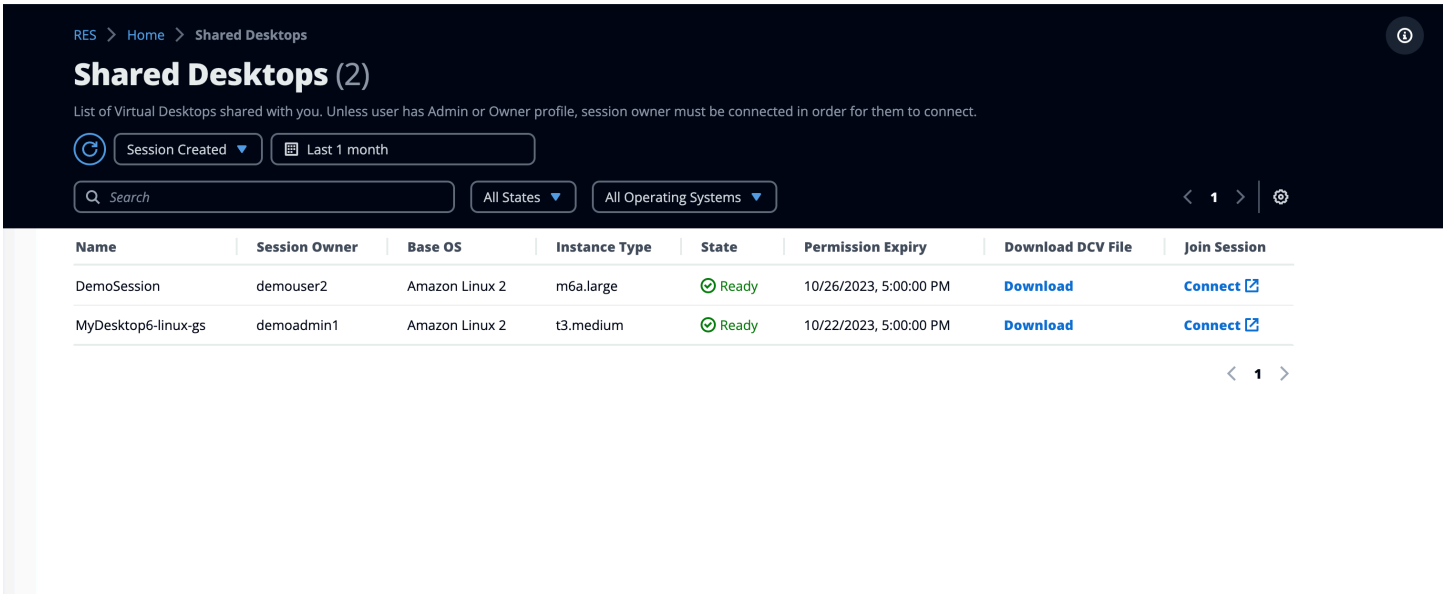
De forma predeterminada, los escritorios virtuales no tienen una programación y permanecerán activos hasta que detenga o finalice la sesión. Los escritorios también se detienen si están inactivos para evitar paradas accidentales. El estado inactivo se determina si no hay conexión activa y si el uso de la CPU es inferior al 15% durante al menos 15 minutos. Puede configurar una programación para iniciar y detener automáticamente el escritorio.

1. Elija Acciones.
2. Elija Schedule.
3. Establece tu horario para cada día.
4. Seleccione Save.


Schedule for windows-session
Setup a schedule to start/stop your virtual desktop to save and manage costs. The schedule operates at the cluster timezone setup by your cluster administrator.
Cluster Time: October 20, 2023 4:32 PM (America/New_York)
Monday
No Schedule
Working Hours (09:00 - 17:00)
Stop All Day
Start All Day
Custom Schedule
No Schedule
Thursday
No Schedule
Friday
No Schedule
Saturday
Stop All Day
Sunday
Stop All Day
Cancel
Save

Escritorios compartidos

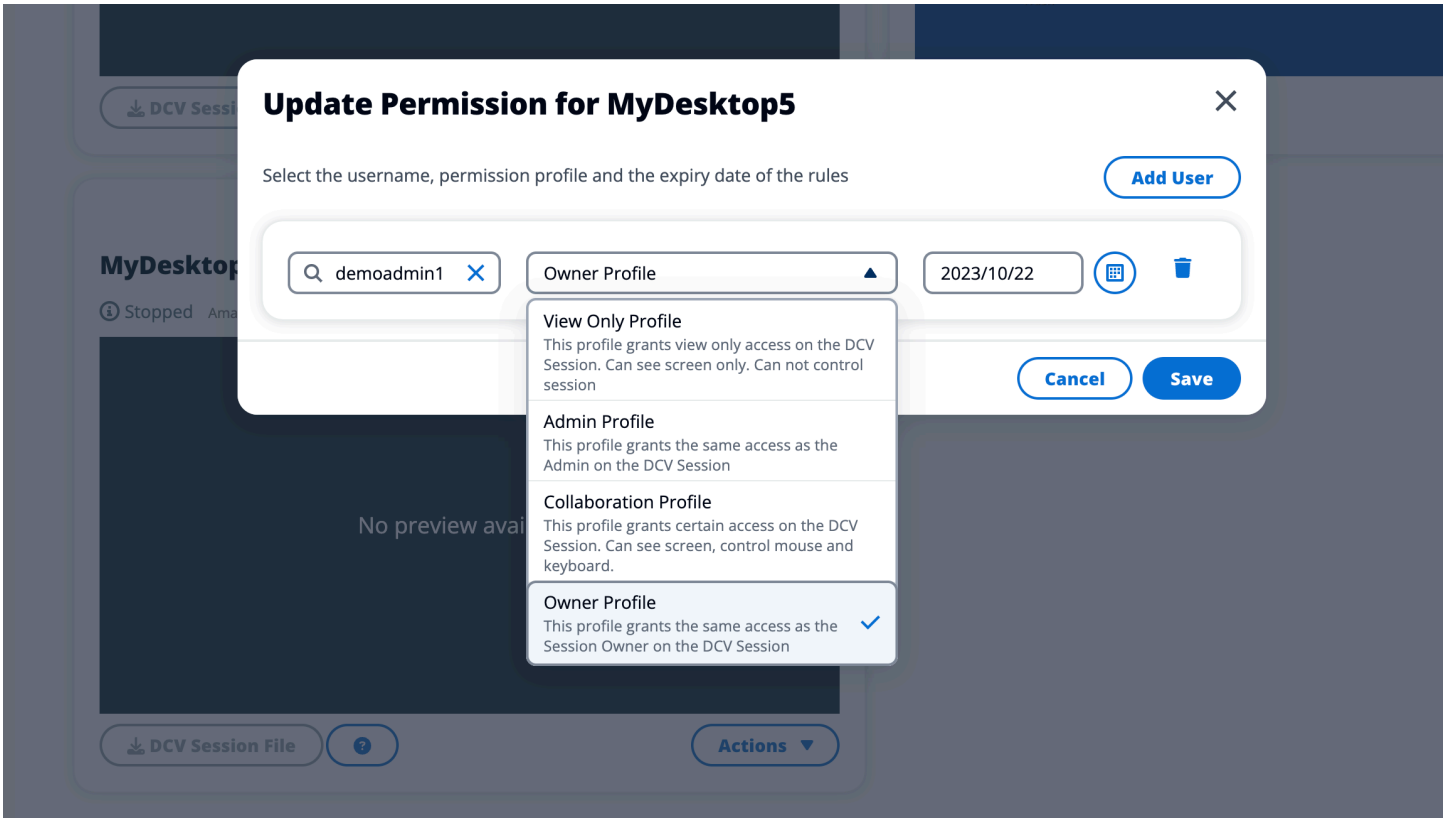
En los escritorios compartidos, puede ver los escritorios que se han compartido con usted. Para conectarse a un escritorio, el propietario de la sesión también debe estar conectado, a menos que usted sea administrador o propietario.



Al compartir una sesión, puede configurar los permisos para sus colaboradores. Por ejemplo, puedes conceder acceso de solo lectura a un compañero de equipo con el que estés colaborando.

Comparte un escritorio

1. En tu sesión de escritorio, selecciona Acciones.
2. Selecciona Permisos de sesión.
3. Elija el usuario y el nivel de permiso. También puede establecer una fecha de caducidad.
4. Seleccione Save.



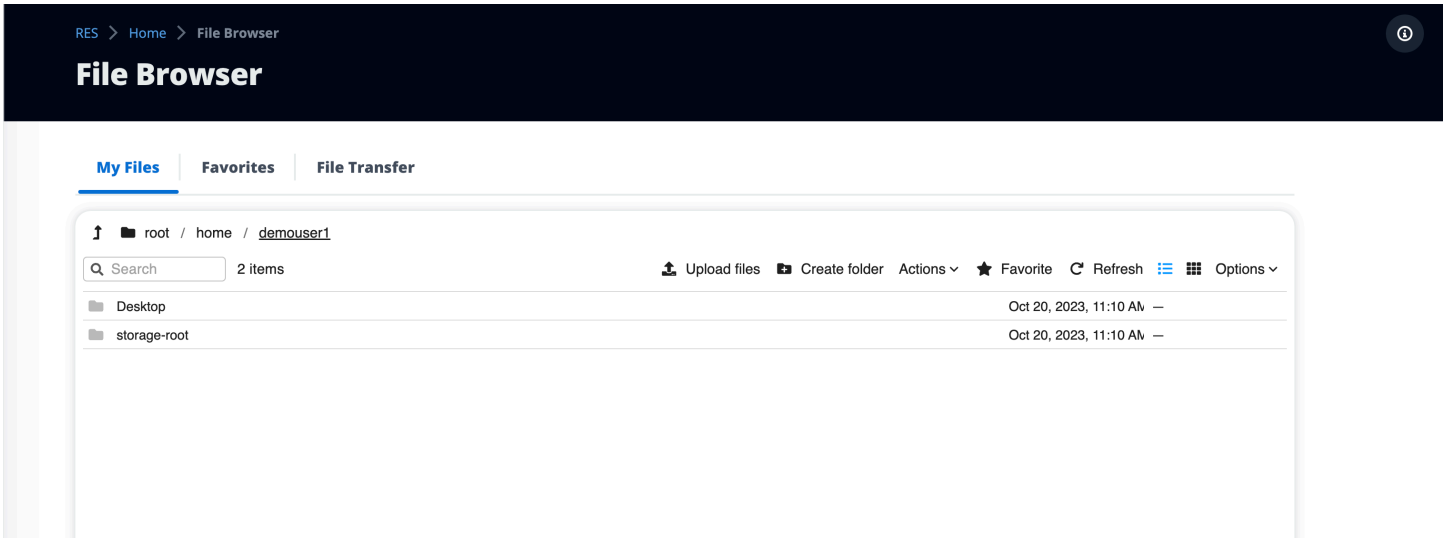
Para obtener más información sobre los permisos, consultethe section called “Perfiles de permisos”.

Acceda a un escritorio compartido

Desde los escritorios compartidos, puedes ver los escritorios compartidos contigo y conectarte a una instancia. Puedes unirte mediante un navegador web o DCV. Para conectarse, siga las instrucciones que se indican enthe section called “Acceda a su escritorio”.

Explorador de archivos

El explorador de archivos le permite acceder a los sistemas de archivos a través del portal web. Puede administrar todos los archivos disponibles a los que tiene permiso de acceso en el sistema de archivos subyacente. El almacenamiento de backend (Amazon EFS) está disponible para todos los nodos de Linux. Para los nodos de Linux y Windows, está FSx disponible ONTAP. Actualizar los archivos del escritorio virtual es lo mismo que actualizar un archivo a través del terminal o del explorador de archivos basado en la web.



Cargar archivo (s)

1. Elija Cargar archivo.
2. Suelta los archivos o busca los archivos para subirlos.
3. Selecciona Cargar (n) archivos.

Eliminar archivo (s)

1. Seleccione los archivos que desee eliminar.
2. Elija Acciones.
3. Elija Eliminar archivos.

Como alternativa, también puede hacer clic con el botón derecho en cualquier archivo o carpeta y seleccionar Eliminar archivos.

Administra los favoritos

Para fijar archivos y carpetas importantes, puedes añadirlos a Favoritos.

1. Selecciona un archivo o una carpeta.
2. Selecciona Favorito.

También puede hacer clic con el botón derecho en cualquier archivo o carpeta y seleccionar Favorito.

> **Note**
>
> Los favoritos se guardan en el navegador local. Si cambias de navegador o borras la memoria caché, tendrás que volver a fijar tus favoritos.

Edición de archivos

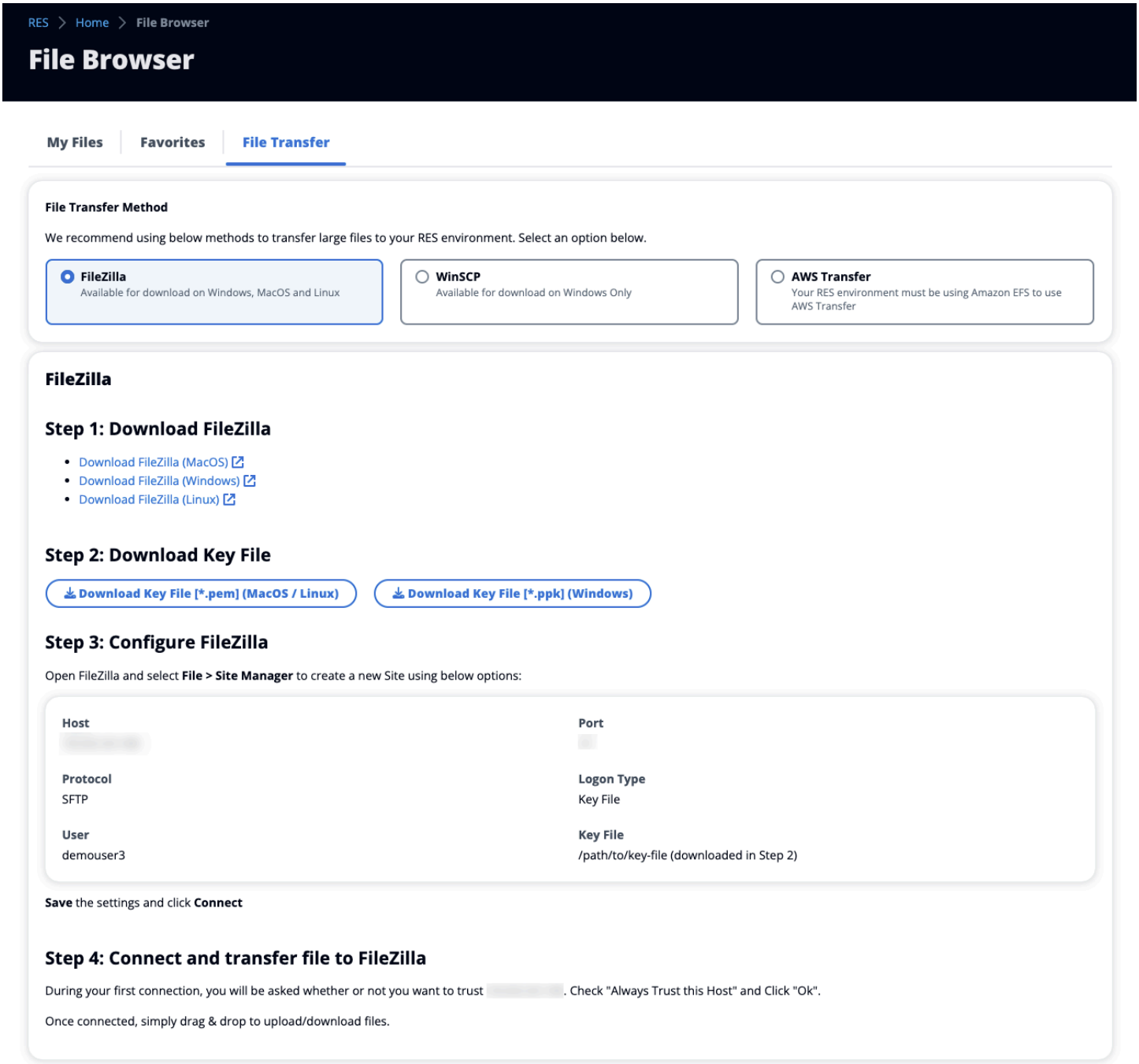
Puede editar el contenido de los archivos basados en texto en el portal web.

1. Elija el archivo que desee actualizar. Se abrirá un modal con el contenido del archivo.
2. Realice las actualizaciones y elija Guardar.

Transferencia de archivos

Use File Transfer para usar aplicaciones de transferencia de archivos externas para transferir archivos. Puede seleccionar una de las siguientes aplicaciones y seguir las instrucciones que aparecen en pantalla para transferir archivos.

- FileZilla (Windows, macOS, Linux)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)



Acceso mediante SSH

Para usar SSH para acceder al host del bastión:

1. En el menú RES, selecciona SSH access.
2. Sigue las instrucciones que aparecen en pantalla para usar SSH o PuTTY para acceder.

Solución de problemas

Esta sección contiene información sobre cómo supervisar el sistema y cómo solucionar problemas específicos que puedan surgir.

Temas

Contenido detallado:

- (2024.04-2024.04.02) Siempre que el límite de permisos de IAM no esté asociado a la función de las instancias de VDI
- (2024.04.02 y versiones anteriores) Las instancias de Windows NVIDIA en ap-southeast-2 (Sídney) no se inician
- (2024.04 y 2024.04.01) Error al eliminar RES en GovCloud
- (2024.04 - 2024.04.02) Es posible que el escritorio virtual Linux quede atrapado en el estado «REANUDANDO» al reiniciarse
- (04.02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo atributo de SAMAccount nombre incluye letras mayúsculas o caracteres especiales
- (02 de abril de 2020 y versiones anteriores) La clave privada para acceder al host del bastión no es válida
- (2024.06 y versiones anteriores) Los miembros del grupo no se sincronizaron con RES durante la sincronización de AD
- (2024.06 y versiones anteriores) CVE-2024-6387, Regre, vulnerabilidad de seguridad en Ubuntu SSHion RHEL9 VDIs

Depuración y supervisión generales

Esta sección contiene información sobre dónde se puede encontrar información en RES.

- Fuentes útiles de información sobre registros y eventos
  - Archivos de registro en el entorno Amazon EC2 instances
  - CloudFormation Pilas
  - Fallos del sistema debidos a un problema y reflejados en la actividad grupal de Amazon EC2 Auto Scaling
- Apariencia típica de Amazon EC2 Console
  - Hosts de infraestructura
  - Hosts de infraestructura y escritorios virtuales
  - Se aloja en un estado terminado
  - Comandos útiles relacionados con Active Directory (AD) como referencia
- Depuración de DCV en Windows
- Encuentre información sobre la versión NICE DCV

Fuentes útiles de información sobre registros y eventos

Se conservan varias fuentes de información a las que se puede hacer referencia para la solución de problemas y los usos de supervisión.

Archivos de registro en el entorno Amazon EC2 instances

Los archivos de registro existen en las EC2 instancias de Amazon que utiliza RES. El administrador de sesiones SSM se puede utilizar para abrir una sesión en la instancia y examinar estos archivos.

En las instancias de infraestructura, como el administrador de clústeres y el controlador vdc, los registros de aplicaciones y de otro tipo se encuentran en las siguientes ubicaciones.

- /.log opt/idea/app/logs/application
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssd/
- /var/log/messages
- /-data.log var/log/user
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

En un escritorio virtual Linux, lo siguiente contiene archivos de registro útiles

- /var/log/dcv/
- /root/bootstrap/logs/userdata.log
- /var/log/messages

En las instancias de escritorios virtuales de Windows, los registros se encuentran en

- PS C:\ProgramData\ n ice\ dcv\ log
- PS C:\\ ProgramData n ice\\ log DCVSession ManagerAgent

En Windows, el registro de algunas aplicaciones se encuentra en:

- PS C:\Program Files\ NICE\ DCV\ Server\ bin

En Windows, los archivos del certificado NICE DCV se encuentran en:

- C:\Windows\System32\config\systemprofile\\ LocalAppData\ NICE\ dcv\

Grupos de Amazon CloudWatch Log

Amazon EC2 y los recursos AWS Lambda informáticos registran la información en Amazon CloudWatch Log Groups. Las entradas de registro que contienen pueden proporcionar información útil para solucionar posibles problemas o para obtener información general.

Estos grupos se denominan de la siguiente manera:

- `/aws/lambda/<envname>-/ - lambda related`
- `/<envname>/`
  - `cluster-manager/ - main infrastructure host`
  - `vdc/ - virtual desktop related`
    - `dcv-broker/ - desktop related`
    - `dcv-connection-gateway/ - desktop related`
    - `controller/ - main desktop controller host`
    - `dcv-session/ - desktop session related`

Al examinar los grupos de registros, puede resultar útil filtrar mediante cadenas en mayúsculas y minúsculas, como las siguientes. Esto generará solo los mensajes que contengan las cadenas indicadas.

```
?"ERROR" ?"error"
```

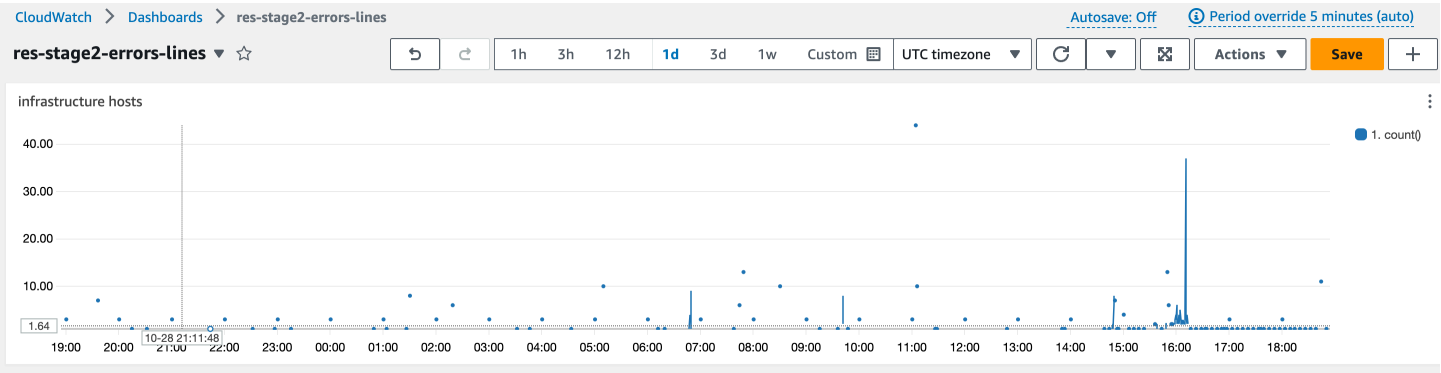
Otro método de supervisión de los problemas consiste en crear Amazon CloudWatch Dashboards que contengan widgets que muestren los datos de interés.

Un ejemplo consiste en crear un widget que cuente la incidencia de las cadenas error y ERROR y graficarlas como líneas. Este método facilita la detección de posibles problemas o tendencias que indiquen que se ha producido un cambio de patrón.

El siguiente es un ejemplo de ello para los hosts de infraestructura. Para ello, concatene las líneas de consulta y sustituya los `<region>` atributos `<envname>` y por los valores adecuados.

```
{
    "widgets": [
        {
            "type": "log",
            "x": 0,
            "y": 0,
            "width": 24,
            "height": 6,
            "properties": {
                "query": "SOURCE '/<envname>/vdc/controller' |
                    SOURCE '/<envname>/cluster-manager' |
                    SOURCE '/<envname>/vdc/dcv-broker' |
                   SOURCE '/<envname>/vdc/dcv-connection-gateway' |
                    fields @timestamp, @message, @logStream, @log\n|
                    filter @message like /(?i)(error|ERROR)/\n|
                    sort @timestamp desc|
                    stats count() by bin(30s)",
                "region": "<region>",
                "title": "infrastructure hosts",
                "view": "timeSeries",
                "stacked": false
            }
        }
    ]
}
```

Un ejemplo del panel de control podría tener el siguiente aspecto:



CloudFormation Pilas

Las CloudFormation pilas que se crean durante la creación del entorno contienen información sobre los recursos, los eventos y los resultados asociados a la configuración del entorno.

Para cada una de las pilas, puede consultarse la pestaña Eventos, Recursos y Salidas para obtener información sobre las pilas.

Pilas RES:

- <envname>-bootstrap
- <envname>-clúster
- <envname>-métricas
- <envname>- servicio de directorio
- <envname>-proveedor de identidad
- <envname>-almacenamiento compartido
- <envname>-administrador de clústeres
- <envname>-vdc
- <envname>-bastión anfitrión

Paquete de entornos de demostración (si está implementando un entorno de demostración y no dispone de estos recursos externos, puede utilizar métodos de computación de AWS alto rendimiento para generar recursos para un entorno de demostración).

- <envname>
- <envname>-Redes
- <envname>- DirectoryService
- <envname>-Almacenamiento
- <envname>- WindowsManagementHost

Fallos del sistema debidos a un problema y reflejados en la actividad grupal de Amazon EC2 Auto Scaling

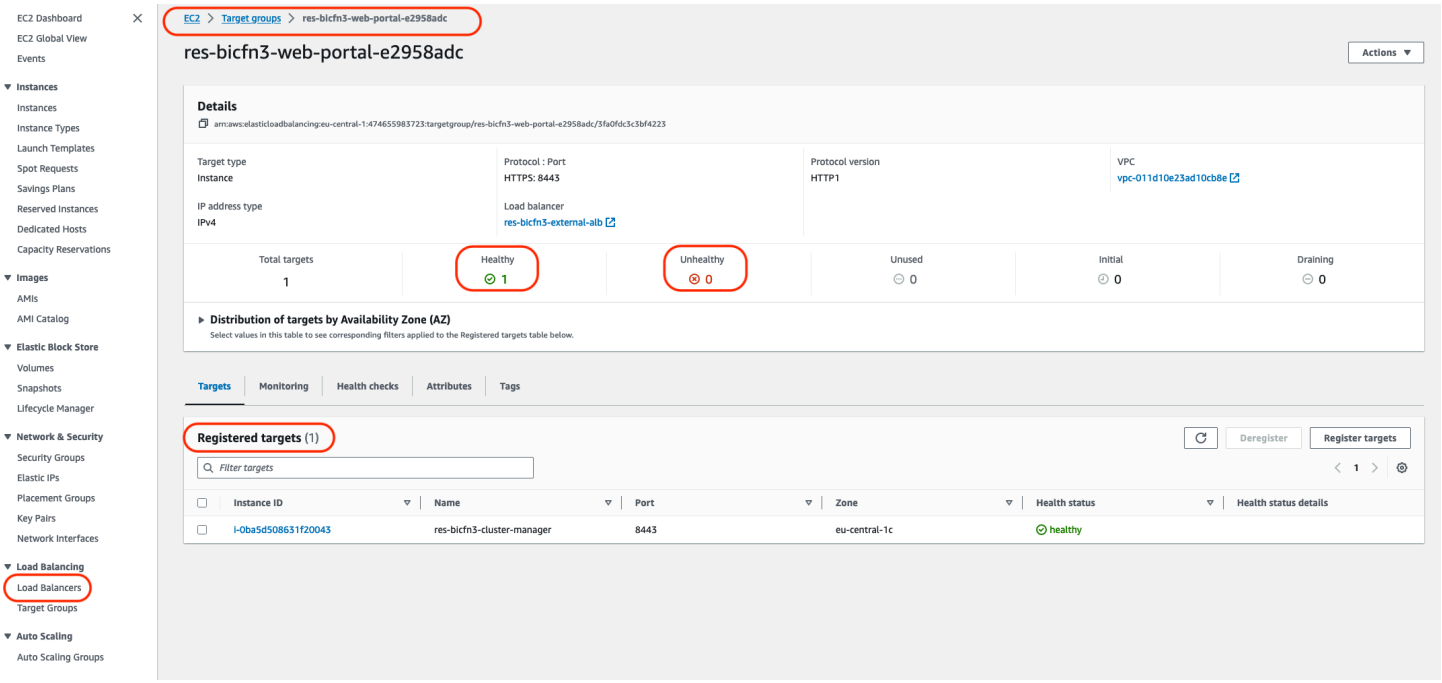
Si el RES UIs indica errores en el servidor, la causa puede ser una aplicación, el software u otro problema.

Cada uno de los grupos de escalado automático de EC2 instancias de Amazon de infraestructura (ASGs) contiene una pestaña de actividad que puede resultar útil para detectar la actividad de escalado de las instancias. Si las páginas de la interfaz de usuario muestran algún error o no están accesibles, consulte la EC2 consola de Amazon para ver si hay varias instancias terminadas y

consulte la pestaña Actividad de grupo de Auto Scaling para ver el ASG relacionado para determinar si las EC2 instancias de Amazon son cíclicas.

Si es así, usa el grupo de CloudWatch registros de Amazon relacionado con la instancia para determinar si se están registrando errores que puedan indicar la causa del problema. También es posible utilizar la consola de sesiones SSM para abrir una sesión en una instancia en ejecución de ese tipo y examinar los archivos de registro de la instancia para determinar la causa antes de que el ASG marque la instancia como en mal estado y la cancele.

Si se produce este problema, la consola ASG puede mostrar una actividad similar a la siguiente.

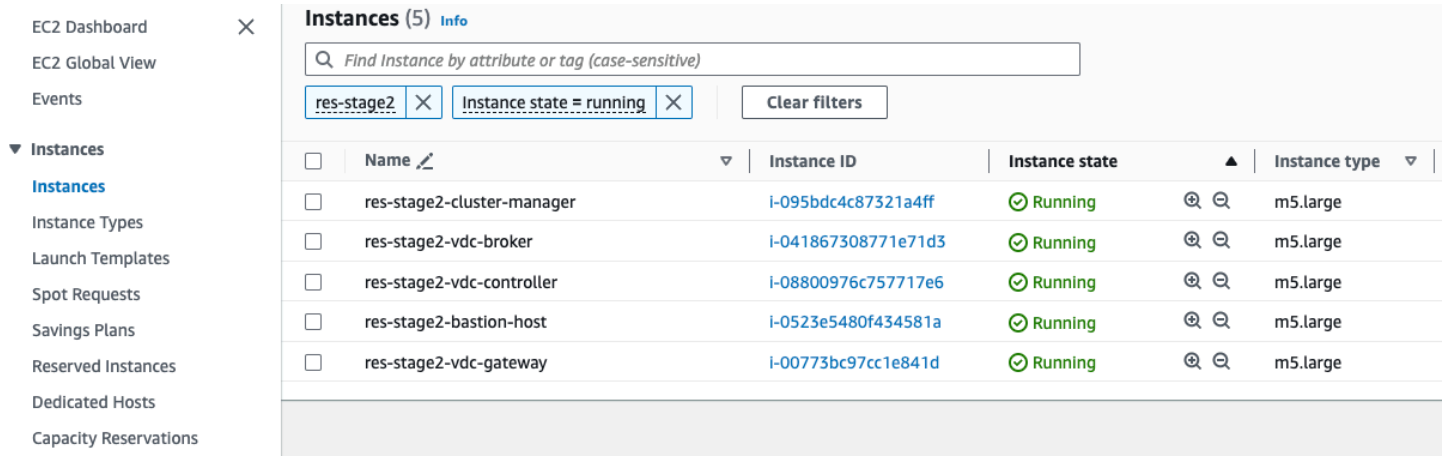


Apariencia típica de Amazon EC2 Console

Esta sección contiene capturas de pantalla del sistema que funciona en varios estados.

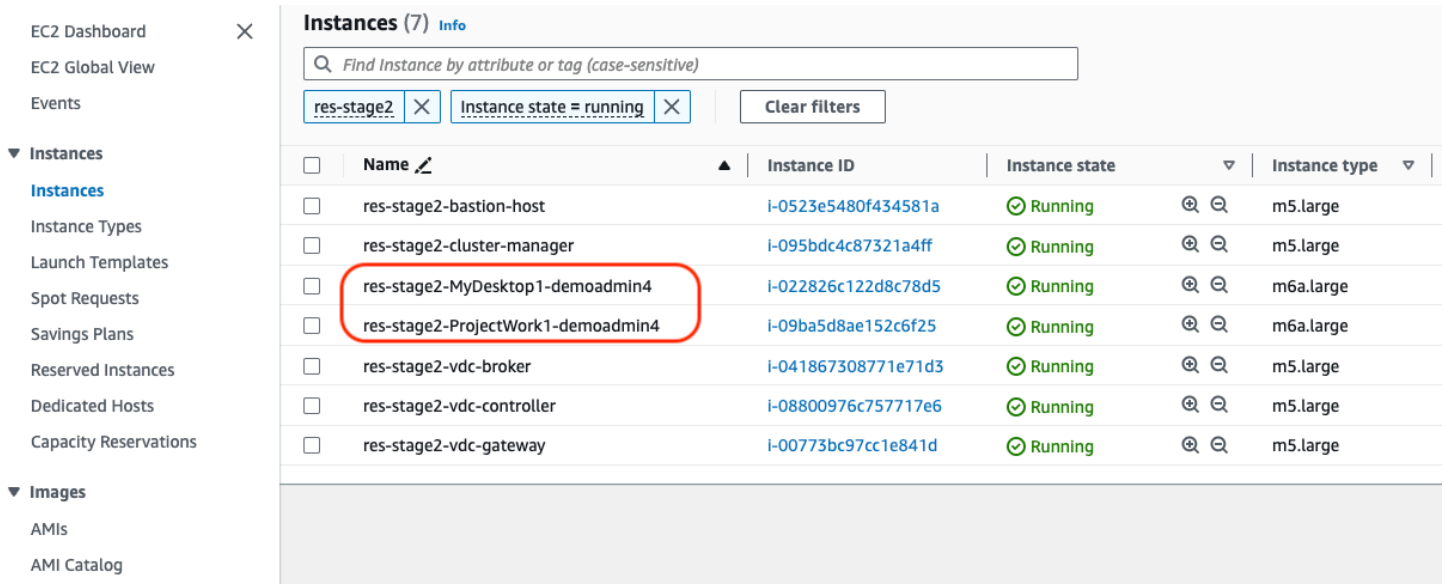
Hosts de infraestructura

La EC2 consola de Amazon, cuando no hay escritorios en ejecución, suele tener un aspecto similar al siguiente. Las instancias que se muestran son la infraestructura RES que Amazon EC2 aloja. El prefijo del nombre de una instancia es el nombre del entorno RES.



Hosts de infraestructura y escritorios virtuales

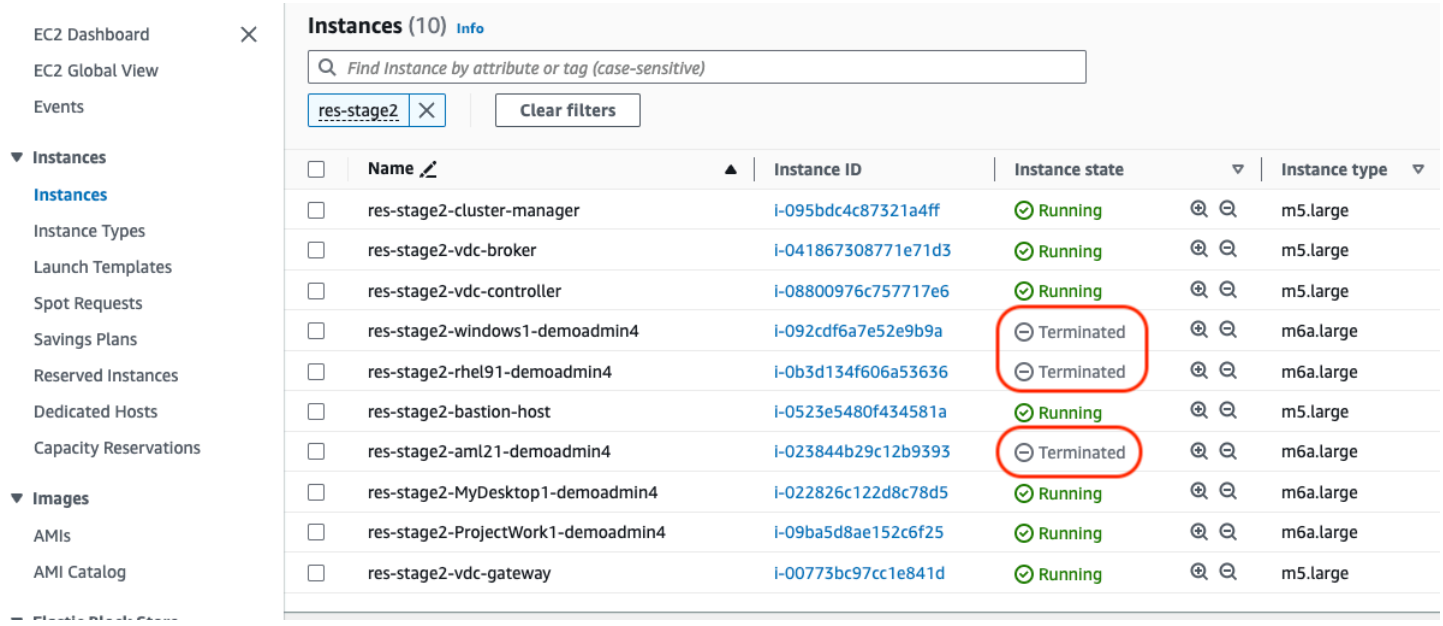
En la EC2 consola de Amazon, cuando se ejecutan escritorios virtuales, tienen un aspecto similar al siguiente. En este caso, los escritorios virtuales aparecen en rojo. El sufijo del nombre de la instancia es el usuario que creó el escritorio. El nombre que aparece en el centro es el nombre de sesión establecido en el momento del lanzamiento y puede ser el nombre predeterminado MyDesktop «» o el nombre establecido por el usuario.



Se aloja en un estado terminado

Cuando la EC2 consola de Amazon muestra instancias terminadas, generalmente son hosts de escritorio que han sido cancelados. Si la consola incluye hosts de infraestructura en un estado terminado, especialmente si hay varios del mismo tipo, esto puede indicar que se está produciendo un problema en el sistema.

La siguiente imagen muestra las instancias de escritorio que se han cancelado.



Comandos útiles relacionados con Active Directory (AD) como referencia

A continuación, se muestran ejemplos de comandos relacionados con el LDAP que se pueden introducir en los hosts de la infraestructura para ver la información relacionada con la configuración de AD. El dominio y otros parámetros utilizados deben reflejar los introducidos en el momento de la creación del entorno.

```
ldapsearch "(cn=AWS Delegated Add Workstations To Domain Users)" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>

ldapsearch "(&(objectClass=group))" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>
```

Depuración de DCV en Windows

En un escritorio de Windows, puede enumerar la sesión asociada a ella mediante lo siguiente:

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe'list-sessions
Session: 'a7953489-9dbf-492b-8135-7709dccc4cab' (owner:admin2 type:console
 name:windows1)
```

Encuentre información sobre la versión NICE DCV

NICE DCV se utiliza para sesiones de escritorio virtual. AWS NICE DCV. Los siguientes ejemplos muestran cómo determinar la versión del software DCV instalada.

Linux

```
[root@ip-10-3-157-194 ~]# /usr/bin/dcv version

NICE DCV 2023.0 (r14852)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Windows

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe' version

NICE DCV 2023.0 (r15065)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Problema RunBooks

La siguiente sección contiene los problemas que pueden producirse, cómo detectarlos y sugerencias para resolverlos.

- Problemas de instalación
  - AWS CloudFormation la pila no se puede crear con el mensaje «se WaitCondition recibió el mensaje fallido». Error: estados. TaskFailed»
  - No se recibió la notificación por correo electrónico después de que las AWS CloudFormation pilas se crearan correctamente
  - Instancias cíclicas o controladora de vdc en estado fallido

Problemas de instalación

Temas

- AWS CloudFormation la pila no se puede crear con el mensaje «se WaitCondition recibió el mensaje fallido». Error: estados. TaskFailed»
- No se recibió la notificación por correo electrónico después de que las AWS CloudFormation pilas se crearan correctamente
- Instancias cíclicas o controladora de vdc en estado fallido
- La CloudFormation pila de entornos no se puede eliminar debido a un error en el objeto dependiente
- Se encontró un error en el parámetro de bloque CIDR durante la creación del entorno
- CloudFormation error al crear la pila durante la creación del entorno
- La creación de una pila de recursos externos (demostración) falla con AdDomainAdminNode CREATE_FAILED

.....

AWS CloudFormation la pila no se puede crear con el mensaje «se WaitCondition recibió el mensaje fallido». Error: estados. TaskFailed»

Para identificar el problema, examine el grupo de CloudWatch registros de Amazon denominado`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`. Si hay varios grupos de registros con el mismo nombre, examine el primero disponible. Un mensaje de error en los registros proporcionará más información sobre el problema.

> **Note**
>
> Confirme que los valores de los parámetros no tengan espacios.

.....

No se recibió la notificación por correo electrónico después de que las AWS CloudFormation pilas se crearan correctamente

Si no se recibió una invitación por correo electrónico después de haber creado correctamente las AWS CloudFormation pilas, compruebe lo siguiente:

1. Confirme que el parámetro de dirección de correo electrónico se haya introducido correctamente.

   Si la dirección de correo electrónico es incorrecta o no se puede acceder a ella, elimine y vuelva a implementar el entorno de Research and Engineering Studio.

2. Consulta la EC2 consola de Amazon para ver pruebas de casos de ciclismo.

   Si hay EC2 instancias de Amazon con el `<envname>` prefijo que aparecen como terminadas y, a continuación, se sustituyen por una nueva instancia, es posible que haya un problema con la configuración de la red o de Active Directory.

3. Si implementó las recetas de computación de AWS alto rendimiento para crear sus recursos externos, confirme que la pila haya creado la VPC, las subredes públicas y privadas y otros parámetros seleccionados.

   Si alguno de los parámetros es incorrecto, es posible que tengas que eliminar y volver a implementar el entorno RES. Para obtener más información, consulte Desinstale el producto.

4. Si implementó el producto con sus propios recursos externos, confirme que la red y Active Directory coincidan con la configuración esperada.

   Es fundamental confirmar que las instancias de infraestructura se han unido correctamente a Active Directory. Pruebe los pasos que se indican the section called “Instancias cíclicas o controladora de vdc en estado fallido” a continuación para resolver el problema.

.....

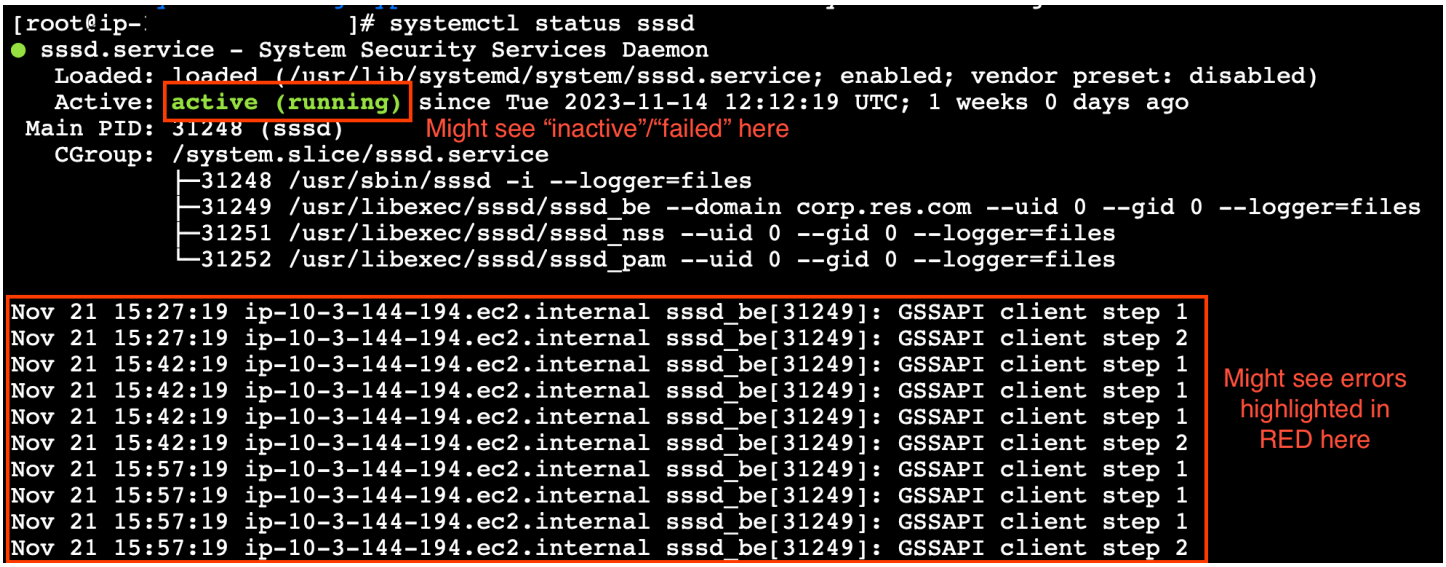
Instancias cíclicas o controladora de vdc en estado fallido

La causa más probable de este problema es la incapacidad de los recursos para conectarse o unirse a Active Directory.

Para comprobar el problema:

1. Desde la línea de comandos, inicie una sesión con SSM en la instancia en ejecución del vdc-controller.
2. Ejecute `sudo su -`.
3. Ejecute `systemctl status sssd`.

Si el estado es inactivo, ha fallado o aparecen errores en los registros, significa que la instancia no se ha podido unir a Active Directory.



Registro de errores de SSM

Para resolver el problema:

- Desde la misma instancia de línea de comandos, ejecuta `cat /root/bootstrap/logs/userdata.log` para investigar los registros.

El problema puede tener una de las tres causas principales posibles.

Causa principal 1: se ingresaron detalles de conexión LDAP incorrectos

Revise los registros. Si ve que lo siguiente se repite varias veces, la instancia no ha podido unirse a Active Directory.

```
+ local AD_AUTHORIZATION_ENTRY=
+ [[ -z '' ]]
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
```

```
+ (( ATTEMPT_COUNT++ ))
```

1. Compruebe que los valores de los siguientes parámetros se hayan introducido correctamente durante la creación de la pila RES.
   - directoryservice.ldap_connection_uri
   - directoryservice.ldap_base
   - directoryservice.users.ou
   - directoryservice.groups.eu
   - directoryservice.sudoers.ou
   - directoryservice.computers.ou
   - directoryservice.name
2. Actualice los valores incorrectos de la tabla de DynamoDB. La tabla se encuentra en la consola de DynamoDB, en Tablas. El nombre de la tabla debe ser. **<stack name>.**`cluster-settings`
3. Tras actualizar la tabla, elimine el administrador de clústeres y el vdc-controller que actualmente ejecutan las instancias del entorno. El escalado automático iniciará nuevas instancias con los valores más recientes de la tabla de DynamoDB.

Causa principal 2: el nombre de usuario introducido es incorrecto ServiceAccount

Si los registros vuelven a aparecer`Insufficient permissions to modify computer account`, es posible que el ServiceAccount nombre introducido durante la creación de la pila sea incorrecto.

1. Desde la AWS consola, abre Secrets Manager.
2. Busque la opción `directoryserviceServiceAccountUsername`. El secreto debería ser**<stack name>**`-directoryservice-ServiceAccountUsername`.
3. Abre el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y selecciona Texto sin formato.
4. Si el valor se actualizó, elimine las instancias del entorno con el administrador de clústeres y el controlador de vdc que se estén ejecutando actualmente. El escalado automático iniciará nuevas instancias con el valor más reciente de Secrets Manager.

Causa principal 3: se ingresó ServiceAccount una contraseña incorrecta

Si aparecen los registros`Invalid credentials`, es posible que la ServiceAccount contraseña introducida durante la creación de la pila sea incorrecta.

1. Desde la AWS consola, abre Secrets Manager.
2. Busque la opción `directoryserviceServiceAccountPassword`. El secreto debería ser**`<stack name>`**`-directoryservice-ServiceAccountPassword`.
3. Abre el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y selecciona Texto sin formato.
4. Si ha olvidado la contraseña o no está seguro de si es correcta, puede restablecerla en Active Directory y Secrets Manager.
    a. Para restablecer la contraseña en AWS Managed Microsoft AD:
        i. Abra la AWS consola y vaya a AWS Directory Service.
        ii. Seleccione el ID de directorio para su directorio RES y elija Acciones.
        iii. Elija Restablecer la contraseña de usuario.
        iv. Introduzca el ServiceAccount nombre de usuario.
        v. Introduce una contraseña nueva y selecciona Restablecer contraseña.
    b. Para restablecer la contraseña en Secrets Manager:
        i. Abre la AWS consola y ve a Secrets Manager.
        ii. Busque la opción `directoryserviceServiceAccountPassword`. El secreto debería ser**`<stack name>`**`-directoryservice-ServiceAccountPassword`.
        iii. Abre el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y elige Texto sin formato.
        iv. Seleccione Editar.
        v. Establezca una nueva contraseña para el ServiceAccount usuario y seleccione Guardar.
5. Si actualizó el valor, elimine las instancias cluster-manager y vdc-controller del entorno que se estén ejecutando actualmente. El escalado automático iniciará nuevas instancias con el valor más reciente.

La CloudFormation pila de entornos no se puede eliminar debido a un error en el objeto dependiente

Si la eliminación de la **<env-name>**-vdc CloudFormation pila falla debido a un error de objeto dependiente, como elvdcdcvhostsecuritygroup, podría deberse a que una EC2 instancia de Amazon se lanzó a una subred o grupo de seguridad creado por RES mediante la consola. AWS

Para resolver el problema, busca y cancela todas las EC2 instancias de Amazon lanzadas de esta manera. A continuación, puede reanudar la eliminación del entorno.

.....

Se encontró un error en el parámetro de bloque CIDR durante la creación del entorno

Al crear un entorno, aparece un error en el parámetro de bloque CIDR con un estado de respuesta de [FALLIDO].

Ejemplo de error:

```
Failed to update cluster prefix list:
        An error occurred (InvalidParameterValue) when calling the
 ModifyManagedPrefixList operation:
        The specified CIDR (52.94.133.132/24) is not valid. For example, specify a CIDR
 in the following form: 10.0.0.0/16.
```

Para resolver el problema, el formato esperado es x.x.x.0/24 o x.x.x.0/32.

.....

CloudFormation error al crear la pila durante la creación del entorno

La creación de un entorno implica una serie de operaciones de creación de recursos. En algunas regiones, puede producirse un problema de capacidad que provoque un error al crear una CloudFormation pila.

Si esto ocurre, elimine el entorno y vuelva a intentar la creación. Como alternativa, puede volver a intentar la creación en una región diferente.

.....

La creación de una pila de recursos externos (demostración) falla con AdDomainAdminNode CREATE_FAILED

Si la creación de la pila del entorno de demostración falla y aparece el siguiente error, es posible que se deba a que Amazon ha aplicado EC2 parches de forma inesperada durante el aprovisionamiento tras el lanzamiento de la instancia.

```
AdDomainAdminNode CREATE_FAILED  Failed to receive 1 resource signal(s) within the
 specified duration
```

Para determinar la causa del error:

1. En el SSM State Manager, compruebe si la aplicación de parches está configurada y si está configurada para todas las instancias.
2. En el historial de ejecuciones del SSM, compruebe si la RunCommand/Automation ejecución de un documento SSM relacionado con la aplicación de parches coincide con el lanzamiento de una instancia.
3. En los archivos de registro de las instancias de Amazon del entorno, revisa el registro de EC2 instancias locales para determinar si la instancia se reinició durante el aprovisionamiento.

Si el problema se debió a la aplicación de parches, retrase la aplicación de los parches a las instancias de RES al menos 15 minutos después del lanzamiento.

.....

Problemas de administración de identidades

La mayoría de los problemas relacionados con el inicio de sesión único (SSO) y la administración de identidades se deben a una configuración incorrecta. Para obtener información sobre cómo configurar tu configuración de SSO, consulta:

- the section called “Configuración del SSO con IAM Identity Center”
- the section called “Configurar tu proveedor de identidad para el inicio de sesión único (SSO)”

Para solucionar otros problemas relacionados con la administración de identidades, consulta los siguientes temas de solución de problemas:

Temas

.....

No estoy autorizado a realizar iam: PassRole

Si recibe un mensaje de error que indica que no está autorizado a realizar la PassRole acción iam:, sus políticas deben actualizarse para que pueda transferir una función a RES.

Algunos AWS servicios le permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM llamado marymajor intenta usar la consola para realizar una acción en RES. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary deben actualizarse para que pueda realizar la acción iam:. PassRole Si necesitas ayuda, ponte en contacto con tu AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

.....

Quiero permitir que personas ajenas a mi AWS cuenta accedan a los AWS recursos de mi Estudio de Investigación e Ingeniería

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para

que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre cómo proporcionar acceso a sus recursos en todas AWS las cuentas de su propiedad, consulte Proporcionar acceso a un usuario de IAM en otra AWS cuenta de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a AWS cuentas de terceros, consulta Cómo proporcionar acceso a AWS cuentas propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para conocer la diferencia entre el uso de funciones y políticas basadas en recursos para el acceso entre cuentas, consulte en qué se diferencian las funciones de IAM de las políticas basadas en recursos en la Guía del usuario de IAM.

.....

Al iniciar sesión en el entorno, vuelvo inmediatamente a la página de inicio de sesión

Este problema se produce cuando la integración del SSO está mal configurada. Para determinar el problema, consulta los registros de las instancias del controlador y revisa los ajustes de configuración para ver si hay errores.

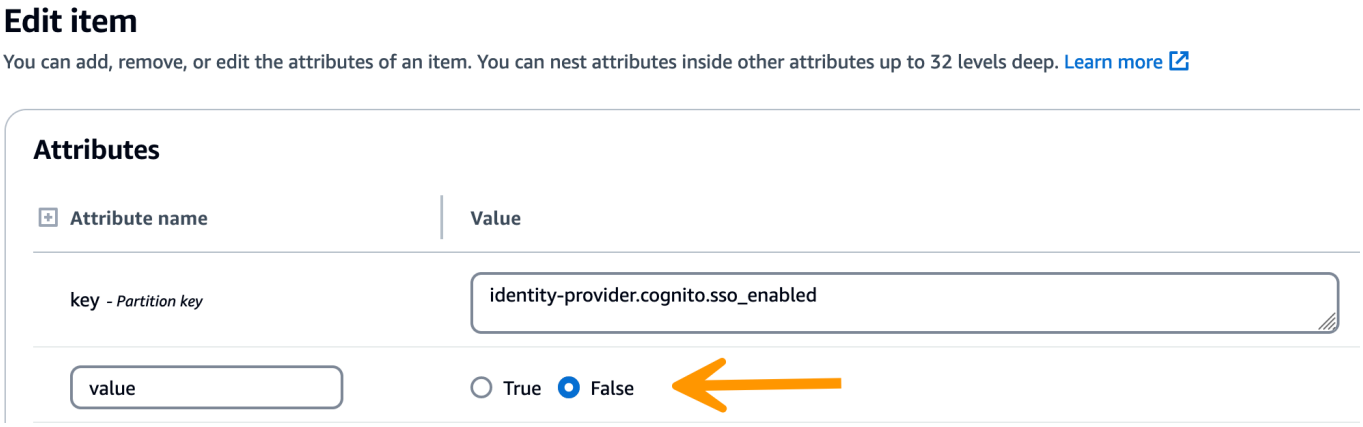
Para comprobar los registros:

1. Abra la consola de CloudWatch .
2. En Grupos de registros, busque el nombre del grupo/*<environment-name>*/cluster-manager.
3. Abra el grupo de registros para buscar cualquier error en las secuencias de registros.

Para comprobar los ajustes de configuración:

1. Abra la consola de DynamoDB

2. En Tablas, busque la tabla denominada. `<environment-name>.cluster-settings`
3. Abre la tabla y selecciona Explorar los elementos de la tabla.
4. Amplíe la sección de filtros e introduzca las siguientes variables:
   - Nombre del atributo: clave
   - Condición: contiene
   - Valor: sso
5. Seleccione Ejecución.
6. En la cadena devuelta, compruebe que los valores de configuración del SSO son correctos. Si son incorrectos, cambie el valor de la clave sso_enabled a False.



7. Vuelva a la interfaz de usuario de RES para volver a configurar el SSO.

.....

Se produjo el error «Usuario no encontrado» al intentar iniciar sesión

Si un usuario recibe el error «Usuario no encontrado» al intentar iniciar sesión en la interfaz RES y el usuario está presente en Active Directory:

- Si el usuario no está presente en RES y usted lo agregó recientemente a AD
  - Es posible que el usuario aún no esté sincronizado con RES. RES se sincroniza cada hora, por lo que es posible que tengas que esperar y comprobar que el usuario se ha añadido después de la siguiente sincronización. Para sincronizar inmediatamente, sigue los pasos que se indican. El usuario se agregó en Active Directory, pero no aparece en RES

- Si el usuario está presente en RES:

  1. Asegúrese de que la asignación de atributos esté configurada correctamente. Para obtener más información, consulte Configuración del proveedor de identidad para el inicio de sesión único (SSO).
  2. Asegúrese de que tanto el asunto SAML como el correo electrónico SAML coincidan con la dirección de correo electrónico del usuario.

.....

El usuario se agregó en Active Directory, pero no aparece en RES

Si ha agregado un usuario a Active Directory pero no aparece en RES, debe activarse la sincronización de AD. La sincronización de AD se realiza cada hora mediante una función Lambda que importa las entradas de AD al entorno RES. En ocasiones, se produce un retraso hasta que se ejecute el siguiente proceso de sincronización después de añadir nuevos usuarios o grupos. Puede iniciar la sincronización manualmente desde Amazon Simple Queue Service.

Inicie el proceso de sincronización manualmente:

1. Abra la consola de Amazon SQS.
2. En Colas, selecciona`<environment-name>-cluster-manager-tasks.fifo`.
3. Selecciona Enviar y recibir mensajes.
4. En Cuerpo del mensaje, ingresa:

   ```
   { "name": "adsync.sync-from-ad", "payload": {} }
   ```

5. Para el ID del grupo de mensajes, introduzca: **`adsync.sync-from-ad`**
6. En el campo ID de deduplicación de mensajes, introduce una cadena alfanumérica aleatoria. Esta entrada debe ser diferente de todas las llamadas realizadas en los cinco minutos anteriores o se ignorará la solicitud.

.....

El usuario no estaba disponible al crear una sesión

Si es un administrador que está creando una sesión, pero descubre que un usuario que está en Active Directory no está disponible al crear una sesión, es posible que el usuario tenga que iniciar

sesión por primera vez. Las sesiones solo se pueden crear para usuarios activos. Los usuarios activos deben iniciar sesión en el entorno al menos una vez.

.....

Se ha superado el límite de tamaño: error en el registro del administrador del CloudWatch clúster

```
2023-10-31T18:03:12.942-07:00 ldap.SIZELIMIT_EXCEEDED: {'msgtype': 100, 'msgid': 11,
 'result': 4, 'desc': 'Size limit exceeded', 'ctrls': []}
```

Si recibe este error en el registro del CloudWatch administrador del clúster, es posible que la búsqueda de LDAP haya devuelto demasiados registros de usuario. Para solucionar este problema, aumente el límite de resultados de búsqueda de LDAP de su IDP.

.....

Almacenamiento

Temas

- Creé el sistema de archivos a través de RES, pero no se monta en los hosts VDI
- He incorporado un sistema de archivos mediante RES, pero no se monta en los hosts VDI
- No puedo iniciar sesión desde los hosts read/write VDI
- He creado Amazon FSx for NetApp ONTAP desde RES pero no se ha unido a mi dominio

.....

Creé el sistema de archivos a través de RES, pero no se monta en los hosts VDI

Los sistemas de archivos deben estar en el estado «Disponible» antes de que los hosts VDI puedan montarlos. Siga los pasos que se indican a continuación para validar que el sistema de archivos se encuentra en el estado requerido.

Amazon EFS

1. Vaya a la consola de Amazon EFS.
2. Compruebe que el estado del sistema de archivos esté disponible.

3. Si el estado del sistema de archivos no está disponible, espere antes de iniciar los hosts VDI.

1. Ve a la FSx consola de Amazon.
2. Comprueba que el estado esté disponible.
3. Si el estado no está disponible, espere antes de lanzar los hosts de VDI.

.....

He incorporado un sistema de archivos mediante RES, pero no se monta en los hosts VDI

Los sistemas de archivos integrados en RES deben tener configuradas las reglas de grupo de seguridad requeridas para permitir que los hosts de VDI monten los sistemas de archivos. Como estos sistemas de archivos se crean de forma externa a RES, RES no administra las reglas de los grupos de seguridad asociados.

El grupo de seguridad asociado a los sistemas de archivos integrados debe permitir el siguiente tráfico entrante:

- Tráfico NFS (puerto: 2049) desde los hosts VDC de Linux
- Tráfico SMB (puerto: 445) desde los hosts VDC de Windows

.....

No puedo iniciar sesión desde los hosts read/write VDI

ONTAP admite los estilos de seguridad UNIX, NTFS y MIXED para los volúmenes. Los estilos de seguridad determinan el tipo de permisos que ONTAP utiliza para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

Por ejemplo, si un volumen utiliza el estilo de seguridad UNIX, los clientes SMB pueden seguir accediendo a los datos (siempre que se autentiquen y autoricen correctamente) debido a la naturaleza multiprotocolo de ONTAP. Sin embargo, ONTAP utiliza permisos de UNIX que solo los clientes de UNIX pueden modificar mediante herramientas nativas.

Ejemplo de casos de uso de la gestión de permisos

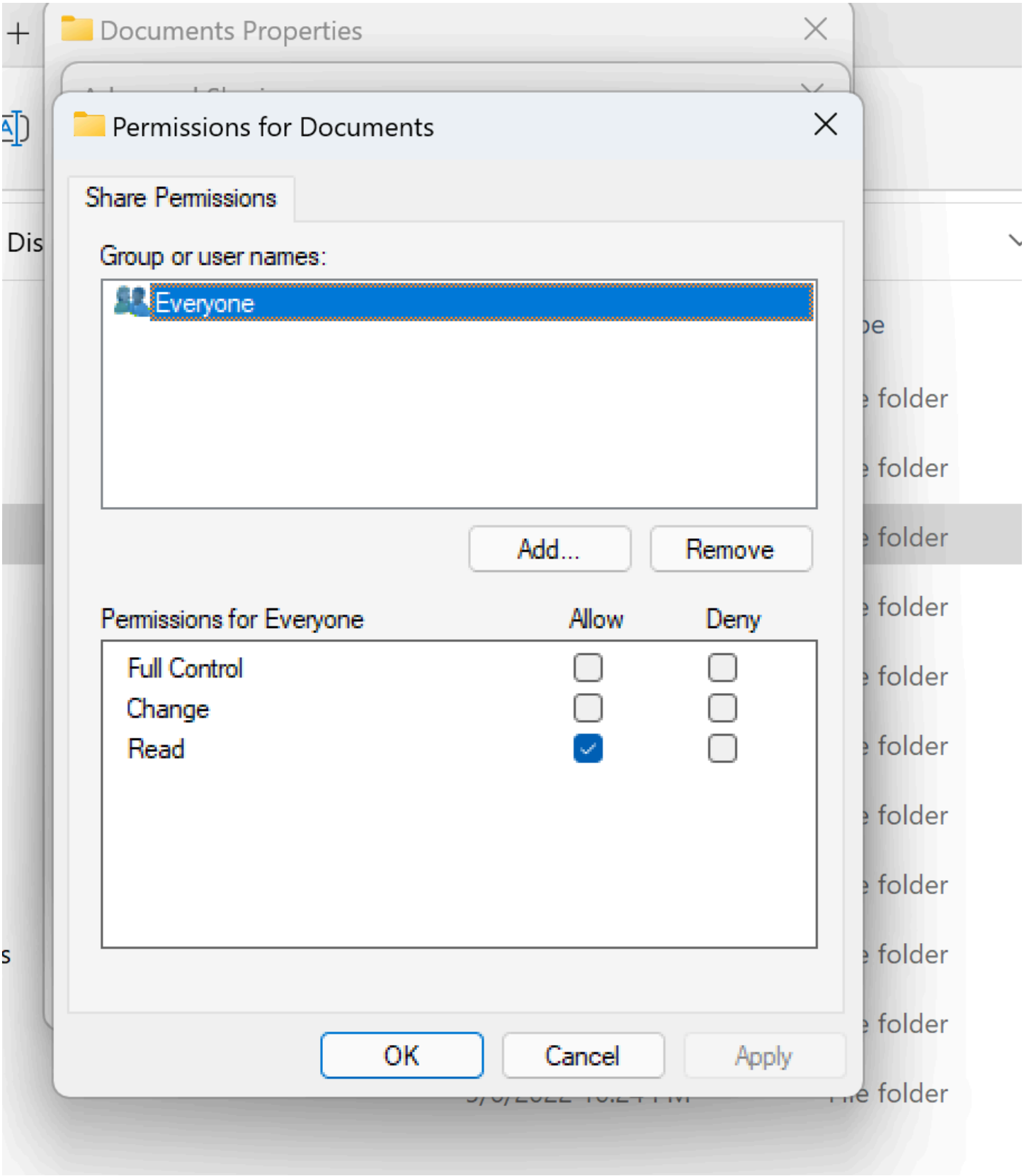
Uso de volúmenes de estilo UNIX con cargas de trabajo de Linux

El sudoer puede configurar los permisos para otros usuarios. Por ejemplo, lo siguiente daría a todos los miembros todos `<group-ID>` los read/write permisos en el `/<project-name>` directorio:

```
sudo chown root:<group-ID> /<project-name>
sudo chmod 770 /<project-name>
```

Uso de un volumen de estilo NTFS con cargas de trabajo de Linux y Windows

Los permisos de uso compartido se pueden configurar mediante las propiedades de uso compartido de una carpeta en particular. Por ejemplo, en función de un usuario `user_01` y una carpeta`myfolder`, puedes establecer los permisos de `Full Control`Change, `Allow` o `Read` para`Deny`:


Documents Properties
Permissions for Documents
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

Si los clientes de Linux y Windows van a utilizar el volumen, necesitamos configurar una asignación de nombres en SVM que asocie cualquier nombre de usuario de Linux al mismo nombre de usuario con el formato de nombre de dominio de NetBIOS domain\ username. Esto es necesario para traducir entre usuarios de Linux y Windows. Como referencia, consulte Habilitar cargas de trabajo multiprotocolo con Amazon FSx for NetApp ONTAP.

.....

He creado Amazon FSx for NetApp ONTAP desde RES pero no se ha unido a mi dominio

Actualmente, al crear Amazon FSx para NetApp ONTAP desde la consola RES, el sistema de archivos se aprovisiona pero no se une al dominio. Para unir el SVM del sistema de archivos ONTAP creado a tu dominio, consulta Cómo unirse SVMs a un Microsoft Active Directory y sigue los pasos de la consola de Amazon FSx . Asegúrese de que los permisos necesarios estén delegados a la cuenta de Amazon FSx Service en AD. Una vez que el SVM se una al dominio correctamente, vaya a Resumen del SVM > Puntos finales > Nombre DNS SMB y copie el nombre DNS porque lo necesitará más adelante.

Una vez unida al dominio, edite la clave de configuración de DNS SMB en la tabla DynamoDB de configuración del clúster:

1. Vaya a la consola de Amazon DynamoDB.
2. Seleccione Tablas y, a continuación, elija. `<stack-name>-cluster-settings`
3. En Explorar los elementos de la tabla, expanda Filtros e introduzca el siguiente filtro:
   - Nombre del atributo: clave
   - Condición: igual a
   - Valor - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. Selecciona el artículo devuelto y, a continuación, Acciones y Editar artículo.
5. Actualice el valor con el nombre DNS SMB que copió anteriormente.
6. Selecciona Guardar y cerrar.

Además, asegúrese de que el grupo de seguridad asociado al sistema de archivos permita el tráfico tal y como se recomienda en el Control de acceso al sistema de archivos con Amazon VPC. Los nuevos hosts de VDI que utilicen el sistema de archivos ahora podrán montar el SVM y el sistema de archivos unidos al dominio.

Como alternativa, puede incorporar un sistema de archivos existente que ya esté unido a su dominio mediante la función RES Onboard File System (en Environment Management, seleccione File Systems, Onboard File System).

.....

Instantáneas

Temas

.....

Una instantánea tiene el estado Fallido

En la página de instantáneas de RES, si una instantánea tiene el estado Fallido, se puede determinar la causa yendo al grupo de CloudWatch registros de Amazon del administrador de clústeres correspondiente al momento en que se produjo el error.

```
[2023-11-19 03:39:20,208] [INFO] [snapshots-service] creating snapshot in S3 Bucket:
  asdf at path s31
[2023-11-19 03:39:20,381] [ERROR] [snapshots-service] An error occurred while
  creating the snapshot: An error occurred (TableNotFoundException)
  when calling the UpdateContinuousBackups operation:
  Table not found: res-demo.accounts.sequence-config
```

.....

No se puede aplicar una instantánea y los registros indican que las tablas no se pudieron importar.

Si una instantánea tomada de un entorno anterior no se aplica a un entorno nuevo, busque en los CloudWatch registros el administrador de clústeres para identificar el problema. Si el problema menciona que la nube de tablas requerida no se puede importar, compruebe que la instantánea esté en un estado válido.

1. Descargue el archivo metadata.json y compruebe que el estado de ExportStatus las distintas tablas esté completado. Asegúrese de que las distintas tablas tengan el `ExportManifest` campo

establecido. Si no encuentra configurados los campos anteriores, la instantánea se encuentra en un estado no válido y no se puede utilizar con la funcionalidad de aplicación de instantáneas.

2. Tras iniciar la creación de una instantánea, asegúrese de que el estado de la instantánea pase a ser COMPLETADA en RES. El proceso de creación de la instantánea tarda entre 5 y 10 minutos. Vuelva a cargar o vuelva a visitar la página de administración de instantáneas para asegurarse de que la instantánea se creó correctamente. Esto garantizará que la instantánea creada esté en un estado válido.

.....

Infraestructura

Temas

.....

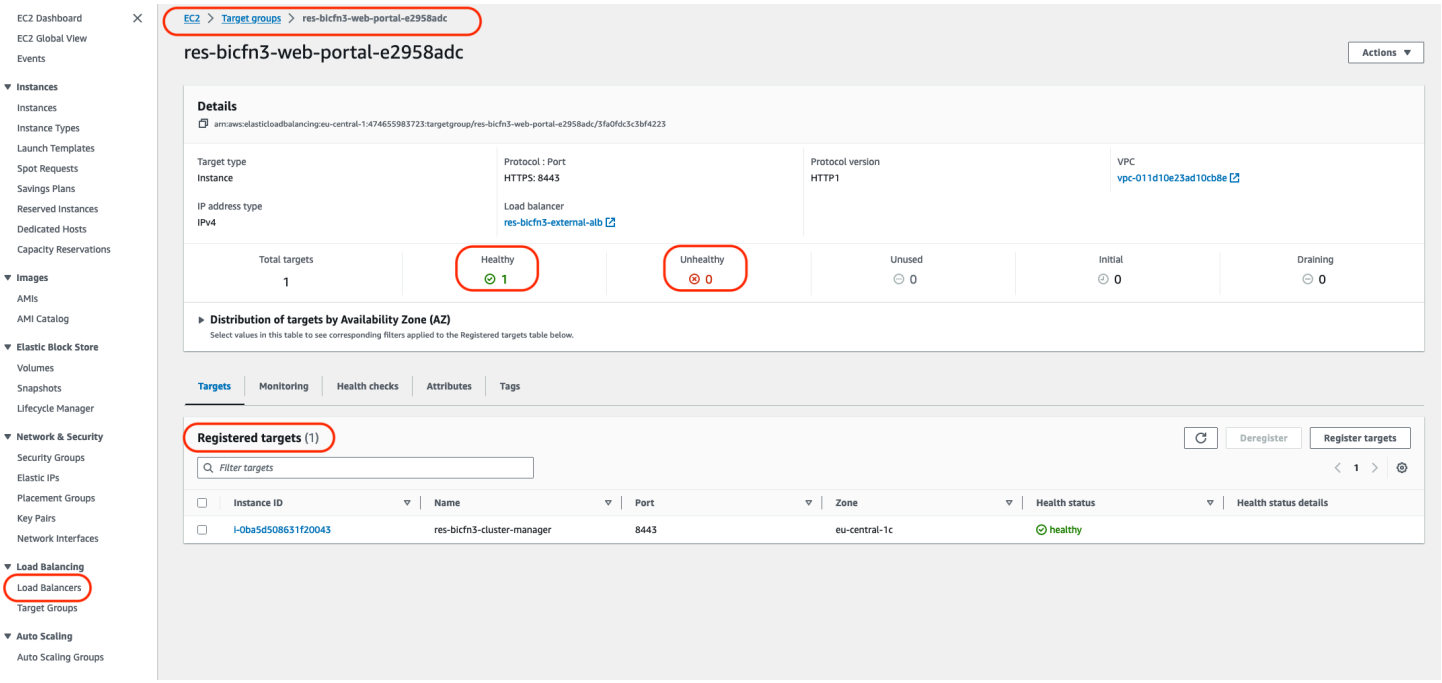
Grupos objetivo del balanceador de carga sin instancias en buen estado

Si aparecen problemas como mensajes de error del servidor en la interfaz de usuario o si las sesiones de escritorio no se pueden conectar, eso puede indicar un problema en la infraestructura de las EC2 instancias de Amazon.

Los métodos para determinar el origen del problema consisten en comprobar primero en la EC2 consola de Amazon cualquier EC2 instancia de Amazon que parezca estar finalizando repetidamente y siendo sustituida por instancias nuevas. Si ese es el caso, comprobar los CloudWatch registros de Amazon puede determinar la causa.

Otro método consiste en comprobar los balanceadores de carga del sistema. Un indicio de que puede haber problemas en el sistema es si algún balanceador de carga, que se encuentra en la EC2 consola de Amazon, no muestra ninguna instancia en buen estado registrada.

A continuación se muestra un ejemplo de aspecto normal:



Si la entrada Healthy es 0, indica que no hay ninguna EC2 instancia de Amazon disponible para procesar las solicitudes.

Si la entrada Unhealthy no es 0, eso indica que es posible que una EC2 instancia de Amazon esté circulando. Esto puede deberse a que el software de las aplicaciones instaladas no pasa los controles de estado.

Si las entradas en buen estado y en mal estado son 0, eso indica un posible error de configuración de la red. Por ejemplo, es posible que las subredes pública y privada no tengan las correspondientes. AZs Si se produce esta condición, es posible que haya texto adicional en la consola que indique que existe un estado de red.

.....

Lanzamiento de escritorios virtuales

Temas

- Un escritorio virtual que funcionaba anteriormente ya no se puede conectar correctamente
- Solo puedo iniciar 5 escritorios virtuales
- Los intentos de conexión a Windows desde un escritorio fallan y muestran el mensaje «Se ha cerrado la conexión». «Error de transporte»
- VDIs atascado en estado de aprovisionamiento

- VDIs pasar al estado de error después de iniciar

.....

Un escritorio virtual que funcionaba anteriormente ya no se puede conectar correctamente

Si se cierra una conexión de escritorio o ya no puedes conectarte a ella, el problema puede deberse a un error en la EC2 instancia de Amazon subyacente o a que la EC2 instancia de Amazon se haya cerrado o detenido fuera del entorno RES. Es posible que el estado de la interfaz de usuario del administrador siga mostrando un estado preparado, pero los intentos de conectarse a ella fallan.

Se debe usar Amazon EC2 Console para determinar si la instancia se ha cerrado o detenido. Si está detenida, intenta iniciarla de nuevo. Si el estado finaliza, será necesario crear otro escritorio. Todos los datos almacenados en el directorio principal del usuario deberían seguir estando disponibles cuando se inicie la nueva instancia.

Si la instancia que falló anteriormente sigue apareciendo en la interfaz de usuario del administrador, es posible que sea necesario cerrarla mediante la interfaz de usuario del administrador.

.....

Solo puedo iniciar 5 escritorios virtuales

El límite predeterminado de la cantidad de escritorios virtuales que un usuario puede lanzar es de 5. Un administrador puede cambiarlo mediante la interfaz de usuario de administración de la siguiente manera:

- Ve a la configuración del escritorio.
- Seleccione la pestaña Servidor.
- En el panel Sesión de DCV, haga clic en el icono de edición de la derecha.
- Cambie el valor de Sesiones permitidas por usuario al nuevo valor deseado.
- Seleccione Enviar.
- Actualice la página para confirmar que se ha establecido la nueva configuración.

.....

Los intentos de conexión a Windows desde un escritorio fallan y muestran el mensaje «Se ha cerrado la conexión». «Error de transporte»

Si se produce un error en la conexión de escritorio de Windows y aparece el error de interfaz de usuario «Se ha cerrado la conexión». Error de transporte», la causa puede deberse a un problema en el software del servidor DCV relacionado con la creación del certificado en la instancia de Windows.

El grupo de CloudWatch registros de Amazon `<envname>/vdc/dcv-connection-gateway` puede registrar el error de intento de conexión con mensajes similares a los siguientes:

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
 protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
 Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]

Nov 24 20:25:15.384  INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }

Nov 24 20:25:15.384  WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Error in websocket connection: Server unreachable: Server error: IO error:
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

Si esto ocurre, una solución podría ser utilizar el administrador de sesiones SSM para abrir una conexión a la instancia de Windows y eliminar los dos archivos relacionados con los certificados siguientes:

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

    Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/4/2022  12:59 PM           1704 dcv.key
```

```
-a----         8/4/2022  12:59 PM           1265 dcv.pem
```

Los archivos deberían volver a crearse automáticamente y es posible que un intento de conexión posterior se realice correctamente.

Si este método resuelve el problema y si los nuevos lanzamientos de escritorios Windows producen el mismo error, utilice la función Crear pila de software para crear una nueva pila de software de Windows de la instancia fija con los archivos de certificado regenerados. Esto puede producir una pila de software de Windows que se puede utilizar para iniciar y establecer conexiones satisfactorias.

.....

VDIs atascado en estado de aprovisionamiento

Si el inicio de un escritorio permanece en el estado de aprovisionamiento en la interfaz de usuario del administrador, puede deberse a varios motivos.

Para determinar la causa, examina los archivos de registro de la instancia de escritorio y busca errores que puedan estar causando el problema. Este documento contiene una lista de archivos de registro y grupos de CloudWatch registros de Amazon que contienen información relevante en la sección denominada Fuentes útiles de información de registros y eventos.

Las posibles causas de este problema son las siguientes.

- El identificador de AMI utilizado se registró como una pila de software, pero RES no lo admite.

  No se pudo completar el script de aprovisionamiento de bootstrap porque la AMI no tiene la configuración o las herramientas necesarias esperadas. Los archivos de registro de la instancia, como `/root/bootstrap/logs/` los de una instancia de Linux, pueden contener información útil al respecto. AMIs Es posible que los identificadores tomados del AWS Marketplace no funcionen para las instancias de escritorio de RES. Es necesario probarlas para confirmar si son compatibles.
- Los scripts de datos de usuario no se ejecutan cuando la instancia de escritorio virtual de Windows se lanza desde una AMI personalizada.

  De forma predeterminada, los scripts de datos de usuario se ejecutan una vez cuando se lanza una EC2 instancia de Amazon. Si crea una AMI a partir de una instancia de escritorio virtual existente, registra una pila de software con la AMI e intenta lanzar otro escritorio virtual con esta pila de software, los scripts de datos de usuario no se ejecutarán en la nueva instancia de escritorio virtual.

Para solucionar el problema, abra una ventana de PowerShell comandos como administrador en la instancia de escritorio virtual original que utilizó para crear la AMI y ejecute el siguiente comando:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

A continuación, cree una AMI nueva a partir de la instancia. Puede utilizar la nueva AMI para registrar pilas de software y lanzar nuevos escritorios virtuales posteriormente. Tenga en cuenta que también puede ejecutar el mismo comando en la instancia que permanece en el estado de aprovisionamiento y reiniciar la instancia para corregir la sesión del escritorio virtual, pero volverá a tener el mismo problema al lanzar otro escritorio virtual desde la AMI mal configurada.

.....

VDIs pasar al estado de error después de iniciar

Posible problema 1: el sistema de archivos principal tiene un directorio para el usuario con diferentes permisos POSIX.

Este podría ser el problema al que te enfrentas si se dan las siguientes situaciones:

1. La versión RES implementada es la 2024.01 o superior.
2. Durante el despliegue de la pila RES, el atributo para `EnableLdapIDMapping` se estableció en. `True`
3. El sistema de archivos principal especificado durante el despliegue de la pila RES se usó en una versión anterior a la RES 2024.01 o se usó en un entorno anterior con el valor establecido en. `EnableLdapIDMapping` `False`

Pasos de resolución: elimine los directorios de usuarios del sistema de archivos.

1. Envíe un SMS al host del administrador del clúster.
2. `cd /home`.
3. `ls`- debería enumerar los directorios con nombres de directorio que coincidan con los nombres de usuario, como`admin1`,.. y así sucesivamente. `admin2`
4. Elimine los directorios,. `sudo rm -r 'dir_name'` No elimine los directorios ssm-user y ec2-user.
5. Si los usuarios ya están sincronizados con el nuevo entorno, elimínelos de la tabla DDB del usuario (excepto clusteradmin).

6. Inicie la sincronización de AD: `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` ejecútela en el administrador de clústeres Amazon. EC2
7. Reinicie la instancia de VDI en el `Error` estado desde la página web de RES. Valide que la VDI pase al `Ready` estado en unos 20 minutos.

.....

Componente de escritorio virtual

Temas

.....

La EC2 instancia de Amazon aparece repetidamente finalizada en la consola

Si una instancia de infraestructura aparece repetidamente como terminada en la EC2 consola de Amazon, la causa puede estar relacionada con su configuración y depender del tipo de instancia de infraestructura. Los siguientes son métodos para determinar la causa.

Si la instancia de vdc-controller muestra estados terminados repetidamente en la EC2 consola de Amazon, esto puede deberse a una etiqueta secreta incorrecta. Los secretos que mantiene RES tienen etiquetas que se utilizan como parte de las políticas de control de acceso de IAM asociadas a la infraestructura de las EC2 instancias de Amazon. Si el controlador vdc está circulando y aparece el siguiente error en el grupo de CloudWatch registros, es posible que el secreto no se haya etiquetado correctamente. Tenga en cuenta que el secreto debe estar etiquetado con lo siguiente:

```
{
    "res:EnvironmentName": "<envname>" # e.g. "res-demo"
    "res:ModuleName": "virtual-desktop-controller"
}
```

El mensaje de CloudWatch registro de Amazon correspondiente a este error tendrá un aspecto similar al siguiente:

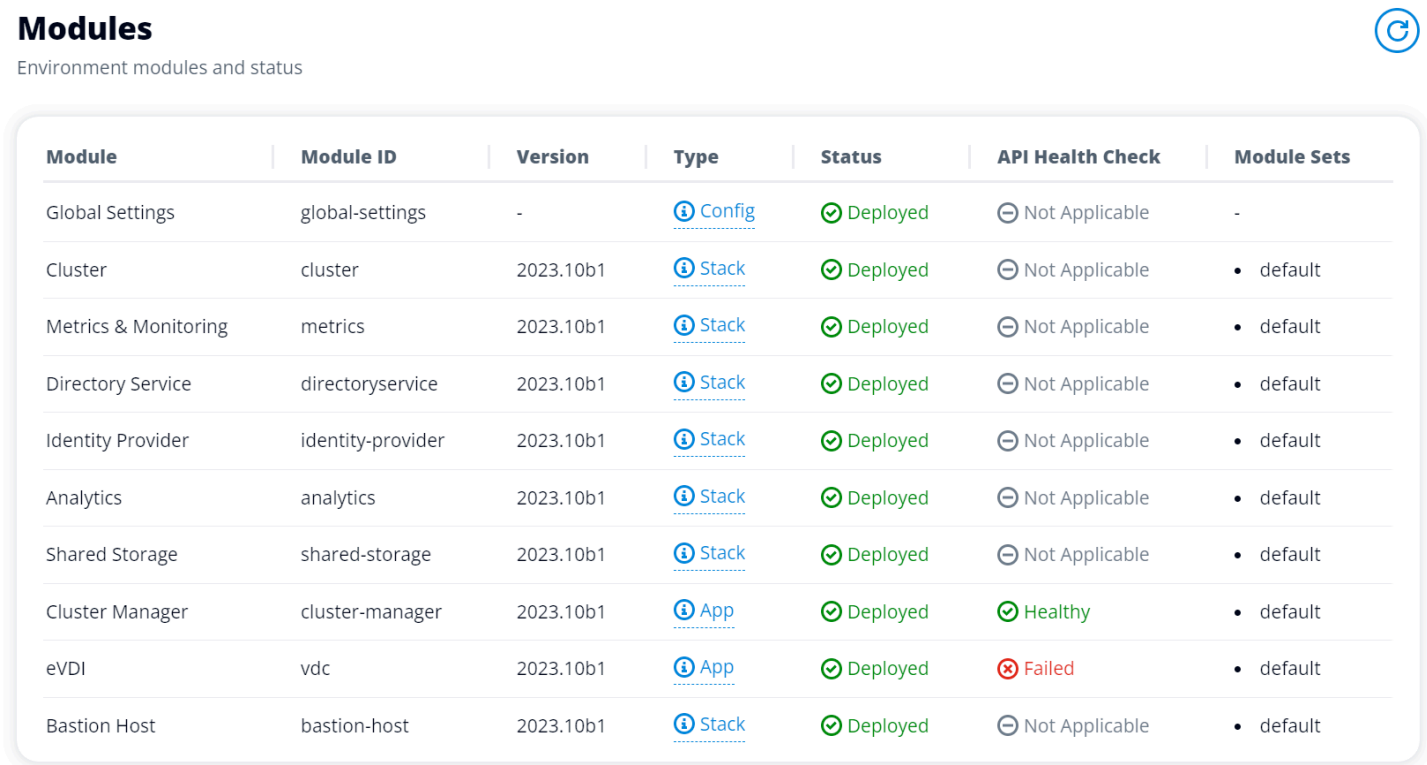
```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

Comprueba las etiquetas de la EC2 instancia de Amazon y confirma que coinciden con la lista anterior.

.....

La instancia de vdc-controller está en ciclo debido a que no se pudo unir al módulo AD/eVDI muestra un error en la comprobación de estado de la API

Si el módulo eVDI no pasa la comprobación de estado, mostrará lo siguiente en la sección Estado del entorno.



Modules

Environment modules and status

Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10b1	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10b1	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10b1	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	App	Deployed	Healthy	• default
eVDI	vdc	2023.10b1	App	Deployed	Failed	• default
Bastion Host	bastion-host	2023.10b1	Stack	Deployed	Not Applicable	• default

En este caso, la ruta general para la depuración consiste en consultar los registros del administrador del clúster CloudWatch. (Busque el nombre del grupo de registros). `<env-name>/cluster-manager`

Posibles problemas:

- Si los registros contienen el texto`Insufficient permissions`, asegúrese de que el ServiceAccount nombre de usuario indicado al crear la pila de resoluciones esté escrito correctamente.

  Ejemplo de línea de registro:

  ```
  Insufficient permissions to modify computer account:
   CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
   000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
   (CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
   request will be retried in 30 seconds
  ```

  - Puede acceder al ServiceAccount nombre de usuario proporcionado durante la implementación de RES desde la SecretsManager consola. Busque el secreto correspondiente en el administrador de secretos y seleccione Recuperar texto sin formato. Si el nombre de usuario es

incorrecto, selecciona Editar para actualizar el valor secreto. Finalice las instancias actuales de cluster-manager y vdc-controller. Las nuevas instancias aparecerán en un estado estable.

- El nombre de usuario debe ser ServiceAccount «» si utiliza los recursos creados por la pila de recursos externos proporcionada. Si el `DisableADJoin` parámetro se estableció en False durante la implementación de RES, asegúrese de que el usuario ServiceAccount «» tenga permisos para crear objetos informáticos en el AD.

- Si el nombre de usuario utilizado es correcto, pero los registros contienen el texto`Invalid credentials`, es posible que la contraseña que ingresó sea incorrecta o haya caducado.

  Ejemplo de línea de registro:

```
{'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
 'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
 data 532, v4563'}
```

  - Puede leer la contraseña que ingresó durante la creación del entorno accediendo al secreto que almacena la contraseña en la consola de Secrets Manager. Seleccione el secreto (por ejemplo,`<env_name>directoryserviceServiceAccountPassword`) y seleccione Recuperar texto sin formato.
  - Si la contraseña del secreto es incorrecta, selecciona Editar para actualizar su valor en el secreto. Finalice las instancias actuales de cluster-manager y vdc-controller. Las nuevas instancias usarán la contraseña actualizada y aparecerán en un estado estable.
  - Si la contraseña es correcta, es posible que haya caducado en el Active Directory conectado. Primero tendrá que restablecer la contraseña en Active Directory y, a continuación, actualizar el secreto. Puede restablecer la contraseña del usuario en Active Directory desde la consola de Directory Service:
    1. Elija el ID de directorio adecuado
    2. Seleccione Acciones, Restablecer la contraseña del usuario y, a continuación, rellene el formulario con el nombre de usuario (por ejemplo, "ServiceAccount«) y la nueva contraseña.
    3. Si la contraseña recién establecida es diferente de la contraseña anterior, actualice la contraseña en el secreto de Secret Manager correspondiente (por ejemplo,`<env_name>directoryserviceServiceAccountPassword`.
    4. Finalice las instancias actuales de cluster-manager y vdc-controller. Las nuevas instancias aparecerán en un estado estable.

.....

El proyecto no aparece en el menú desplegable al editar la pila de software para añadirla

Este problema puede estar relacionado con el siguiente problema relacionado con la sincronización de la cuenta de usuario con AD. Si aparece este problema, busca el error `<user-home-init> account not available yet. waiting for user to be synced` "" en el grupo de registros de CloudWatch Amazon, administrador del clúster, para determinar si la causa es la misma o está relacionada.

.....

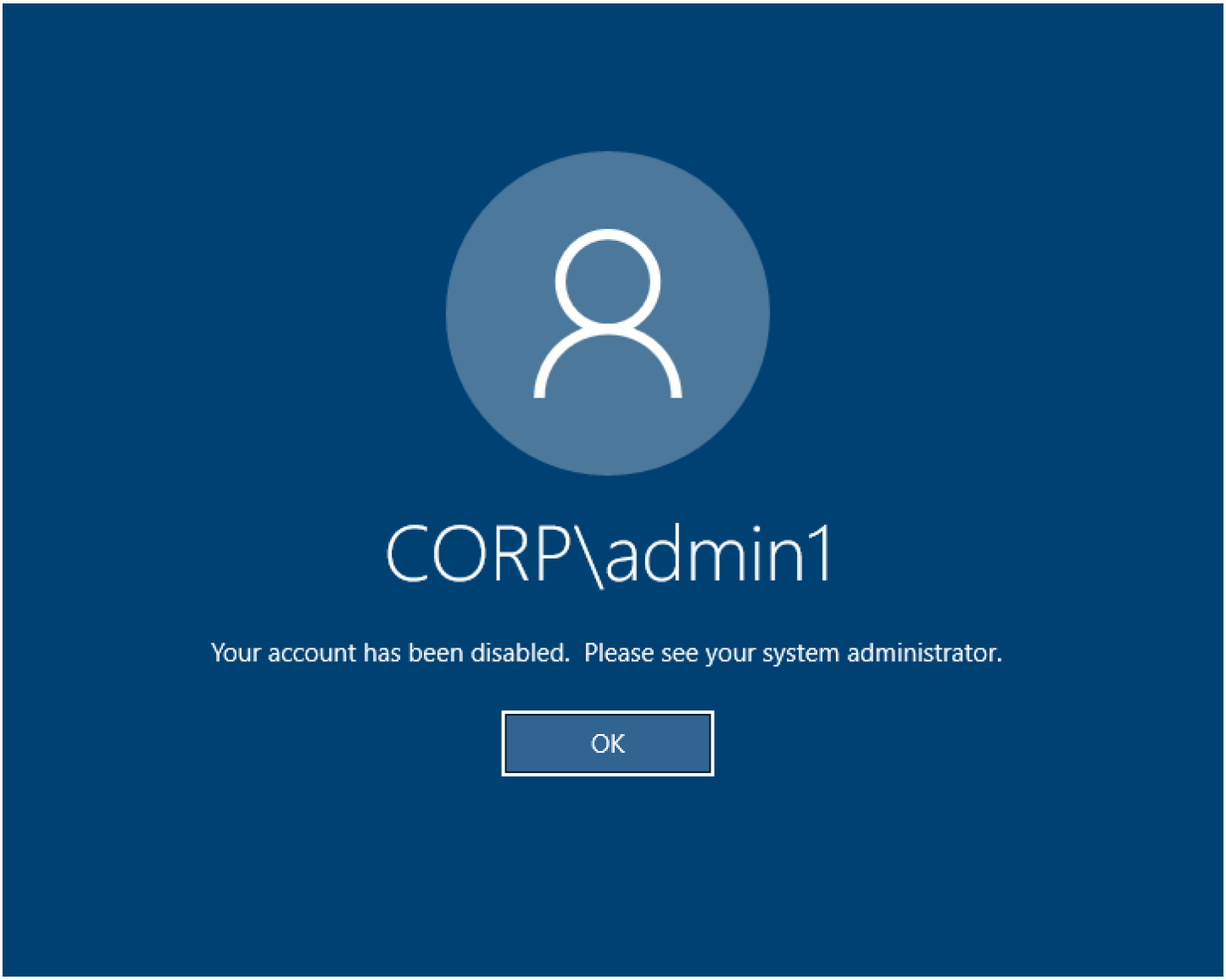
El registro de CloudWatch Amazon del administrador de clústeres muestra «user-home-init< > la cuenta aún no está disponible. En espera de que se sincronice el usuario» (donde la cuenta es un nombre de usuario)

El suscriptor de SQS está ocupado y atrapado en un bucle infinito porque no puede acceder a la cuenta de usuario. Este código se activa cuando se intenta crear un sistema de archivos doméstico para un usuario durante la sincronización del usuario.

La razón por la que no puede acceder a la cuenta de usuario puede deberse a que RES no se configuró correctamente para el AD en uso. Un ejemplo podría ser que el `ServiceAccountUsername` parámetro utilizado en la creación del BI/RES entorno no fuera el valor correcto, por ejemplo, utilizando «ServiceAccount» en lugar de «Admin».

.....

Al intentar iniciar sesión en el escritorio de Windows, aparece el mensaje «Tu cuenta ha sido deshabilitada». Consulte a su administrador»



Si el usuario no puede volver a iniciar sesión en una pantalla bloqueada, esto puede indicar que el usuario se ha desactivado en el AD configurado para RES tras haber iniciado sesión correctamente mediante el inicio de sesión único.

El inicio de sesión único debería fallar si la cuenta de usuario se ha desactivado en AD.

.....

Problemas de opciones de DHCP con external/customer la configuración de AD

Si encuentra un error relacionado "The connection has been closed. Transport error" con los escritorios virtuales de Windows al usar RES con su propio Active Directory, consulte el CloudWatch registro de dcv-connection-gateway Amazon para ver algo similar a lo siguiente:

```
Oct 28 00:12:30.626  INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
 error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
 lookup address information: Name or service not known" }

Oct 28 00:12:30.626  WARN HTTP:Splicer Connection{id=263}:
 Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
 connection: Server unreachable: Server error: IO error: failed to lookup address
 information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

Si utiliza un controlador de dominio de AD para las opciones de DHCP de su propia VPC, debe:

1. Agregue AmazonProvided DNS a los dos controladores de dominio. IPs
2. Establezca el nombre de dominio en ec2.internal.

Aquí se muestra un ejemplo. Sin esta configuración, el escritorio de Windows generará un error de transporte, ya que RES/DCV busca el nombre de host ip-10-0-x-xx.ec2.internal.

.....

Error de Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

Cuando utilizas el navegador web Firefox, es posible que aparezca el mensaje de error MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING cuando intentes conectarte a un escritorio virtual.

La causa es que el servidor web RES está configurado con TLS + Stapling activado, pero no responde con la validación de grapado (consulte https://support.mozilla). org/en-US/questions/1372483.

Para solucionarlo, sigue las instrucciones que se encuentran en: / mozilla_pkix_error_required_tls_feature_missing. https://really-simple-ssl.com

.....

Eliminación de Env

Temas

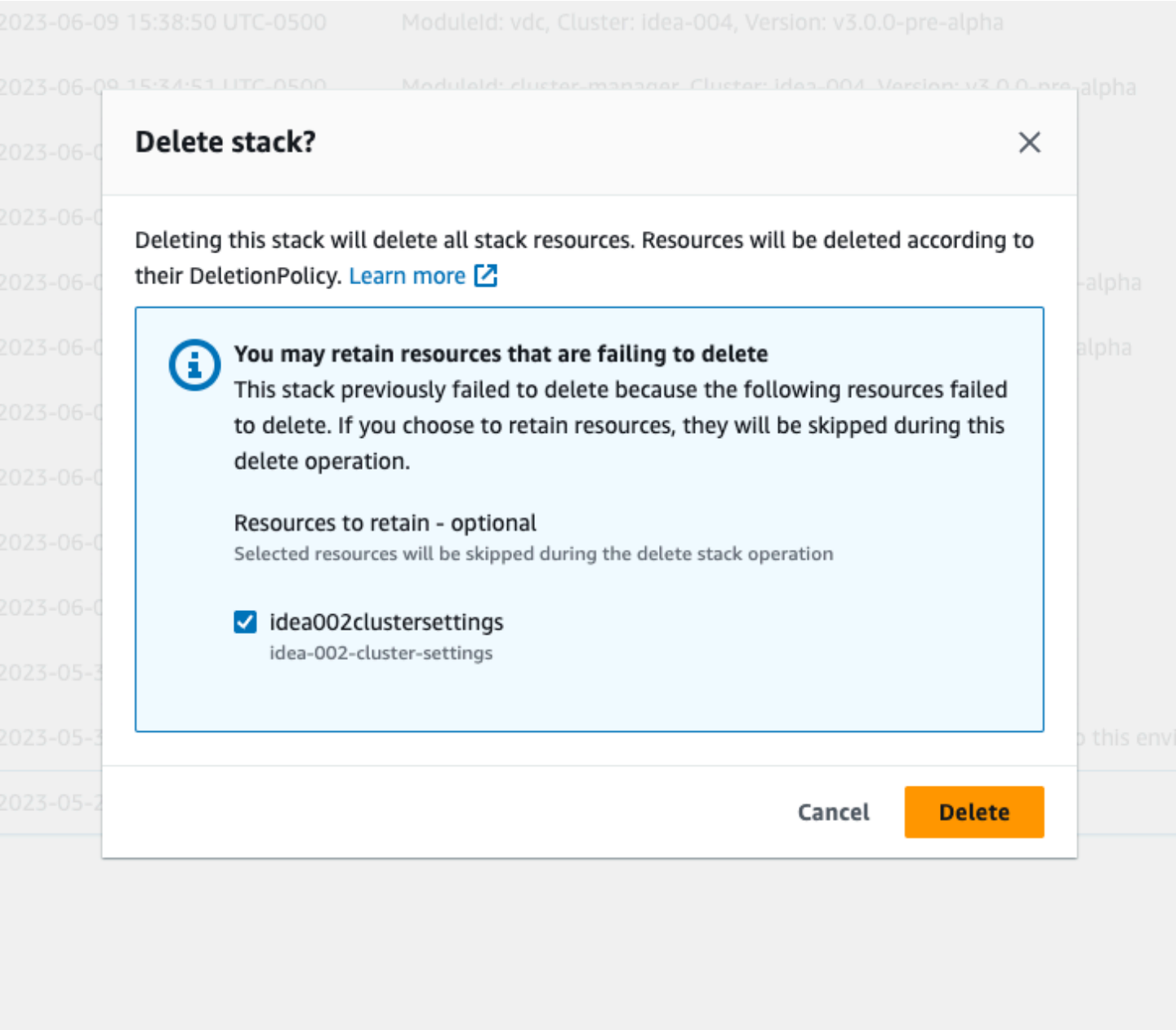
- res-xxx-cluster se apilan en el estado «DELETE_FAILED» y no se pueden eliminar manualmente debido al error «El rol no es válido o no se puede asumir»
- Recopilación de registros
- Descarga de registros de VDI
- Descarga de registros de instancias de Linux EC2
- Descargar registros de EC2 instancias de Windows
- Recopilación de registros de ECS para detectar el WaitCondition error

.....

res-xxx-cluster se apilan en el estado «DELETE_FAILED» y no se pueden eliminar manualmente debido al error «El rol no es válido o no se puede asumir»

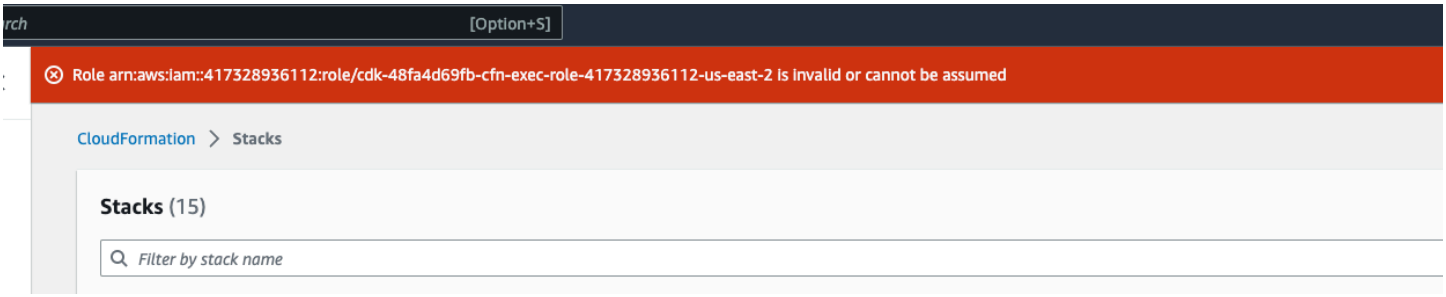
Si observa que la pila «res-xxx-cluster" está en el estado «DELETE_FAILED» y no se puede eliminar manualmente, puede realizar los siguientes pasos para eliminarla.

Si ves la pila en el estado «DELETE_FAILED», primero intenta eliminarla manualmente. Es posible que aparezca un cuadro de diálogo confirmando la opción Eliminar pila. Seleccione Eliminar.



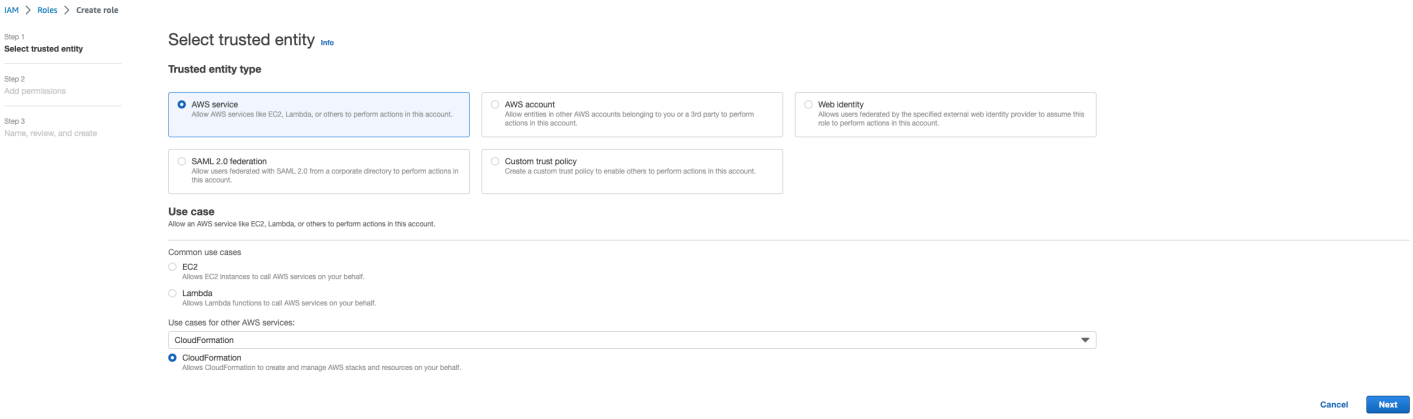
A veces, incluso si eliminas todos los recursos de la pila necesarios, es posible que sigas viendo el mensaje para seleccionar los recursos que deseas conservar. En ese caso, selecciona todos los recursos como «recursos a conservar» y selecciona Eliminar.

Es posible que veas un error parecido a `Role: arn:aws:iam::... is Invalid or cannot be assumed`

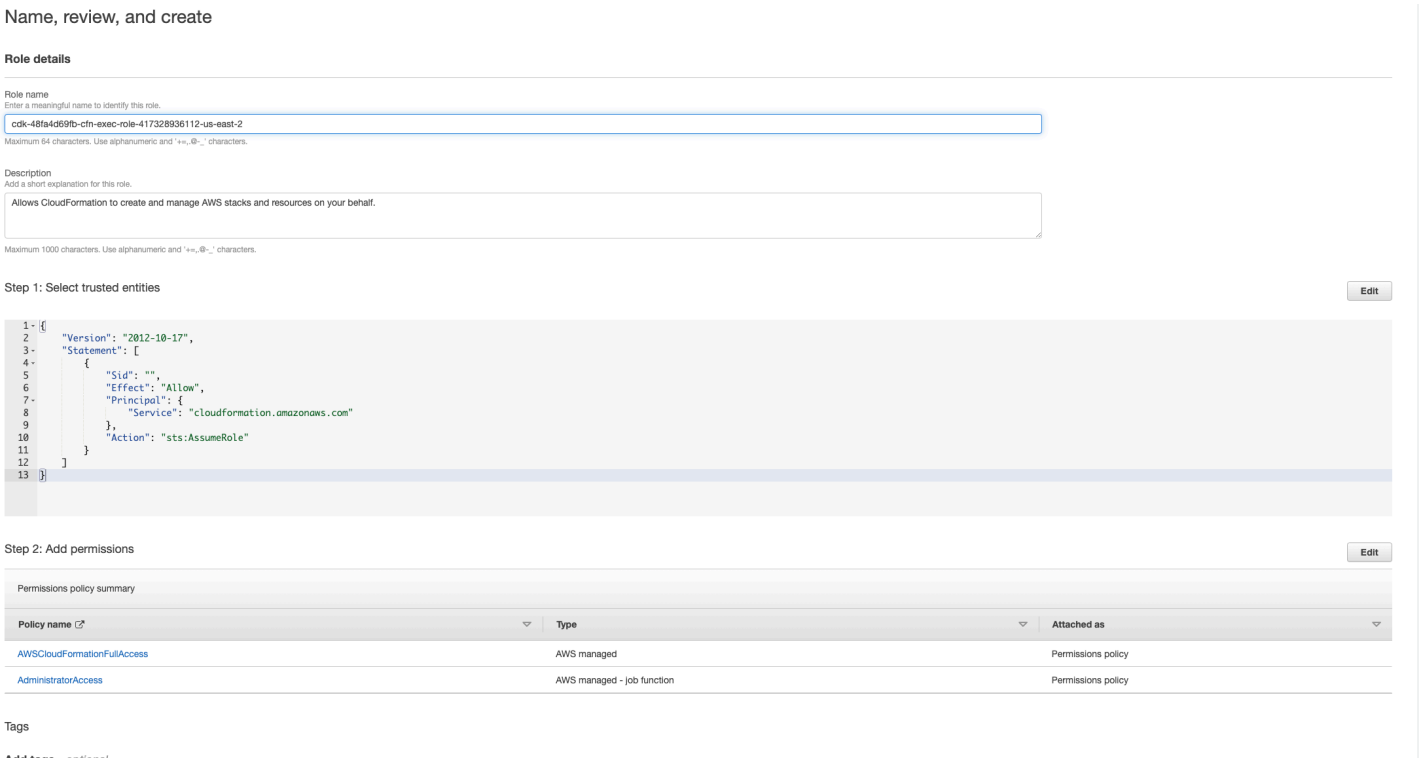


Esto significa que la función necesaria para eliminar la pila se eliminó primero antes que la pila. Para evitar esto, copia el nombre del rol. Vaya a la consola de IAM y cree un rol con ese nombre utilizando los parámetros que se muestran aquí, que son:

- Para el tipo de entidad de confianza, seleccione AWS servicio.
- En Caso de uso, `Use cases for other AWS services` seleccione`CloudFormation`.



Seleccione Siguiente. Asegúrese de conceder los permisos «» y `AWSCloudFormationFullAccess` «`AdministratorAccess`» al rol. Tu página de reseñas debería tener este aspecto:



A continuación, vuelva a la CloudFormation consola y elimine la pila. Ahora deberías poder eliminarlo desde que creaste el rol. Por último, vaya a la consola de IAM y elimine el rol que creó.

.....

Recopilación de registros

Iniciar sesión en una EC2 instancia desde la EC2 consola

- Sigue estas instrucciones para iniciar sesión en tu EC2 instancia de Linux.
- Sigue estas instrucciones para iniciar sesión en tu EC2 instancia de Windows. A continuación, abre Windows PowerShell para ejecutar cualquier comando.

Recopilación de registros del host de Infrastructure

1. Administrador de clústeres: obtenga los registros para el administrador de clústeres de los siguientes lugares y adjúntelos al ticket.
   a. Todos los registros del grupo de registros. CloudWatch `<env-name>/cluster-manager`
   b. Todos los registros del `/root/bootstrap/logs` directorio de la `<env-name>-cluster-manager` EC2 instancia. Sigue las instrucciones que aparecen en el enlace «Iniciar sesión en

una EC2 instancia desde la EC2 consola» al principio de esta sección para iniciar sesión en tu instancia.

2. Controlador de VDC: Obtenga los registros del controlador de VDC de los siguientes lugares y adjúntelos al ticket.
   a. Todos los registros del grupo de registros. CloudWatch `<env-name>/vdc-controller`
   b. Todos los registros del `/root/bootstrap/logs` directorio de la `<env-name>-vdc-controller` EC2 instancia. Sigue las instrucciones que aparecen en el enlace «Iniciar sesión en una EC2 instancia desde la EC2 consola» al principio de esta sección para iniciar sesión en tu instancia.

Una de las maneras de obtener los registros fácilmente es seguir las instrucciones de la Descarga de registros de instancias de Linux EC2 sección. El nombre del módulo sería el nombre de la instancia.

Recopilación de registros de VDI

Identifica la EC2 instancia de Amazon correspondiente

Si un usuario lanzara una VDI con un nombre de sesión`VDI1`, sería `<env-name>-VDI1-<user name>` el nombre correspondiente de la instancia en la EC2 consola de Amazon.

Recopile los registros de VDI de Linux

Inicia sesión en la EC2 instancia de Amazon correspondiente desde la EC2 consola de Amazon siguiendo las instrucciones que aparecen en «Iniciar sesión en una EC2 instancia desde la EC2 consola» al principio de esta sección. Obtenga todos los registros de los `/var/log/dcv/` directorios `/root/bootstrap/logs` y de la EC2 instancia de Amazon de VDI.

Una de las formas de obtener los registros sería subirlos a s3 y luego descargarlos desde allí. Para ello, puedes seguir estos pasos para obtener todos los registros de un directorio y luego subirlos:

1. Siga estos pasos para copiar los registros dcv del `/root/bootstrap/logs` directorio:

```
sudo su -
cd /root/bootstrap
mkdir -p logs/dcv_logs
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. Ahora, siga los pasos que se indican en la siguiente sección Descarga de registros de VDI para descargar los registros.

Recopile los registros de VDI de Windows

Inicia sesión en la EC2 instancia de Amazon correspondiente desde la EC2 consola de Amazon siguiendo las instrucciones que aparecen en «Iniciar sesión en una EC2 instancia desde la EC2 consola» al principio de esta sección. Coloca todos los registros en el `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` directorio de la EC2 instancia de VDI.

Una de las formas de obtener los registros sería subirlos a S3 y, a continuación, descargarlos desde allí. Para hacerlo, siga los pasos que se enumeran en la siguiente sección:Descarga de registros de VDI.

.....

Descarga de registros de VDI

1. Actualice la función de IAM de la EC2 instancia de VDI para permitir el acceso a S3.
2. Ve a la EC2 consola y selecciona tu instancia de VDI.
3. Seleccione el rol de IAM que está utilizando.
4. En la sección Políticas de permisos del menú desplegable Añadir permisos, seleccione Adjuntar políticas y, a continuación, elija la política de FullAccessAmazonS3.
5. Seleccione Añadir permisos para adjuntar esa política.
6. Después, siga los pasos que se indican a continuación en función del tipo de VDI para descargar los registros. El nombre del módulo sería el nombre de la instancia.
   a. Descarga de registros de instancias de Linux EC2 para Linux.
   b. Descargar registros de EC2 instancias de Windowspara Windows.
7. Por último, edite el rol para eliminar la `AmazonS3FullAccess` política.

> **Note**
>
> Todos VDIs utilizan el mismo rol de IAM, que es `<env-name>-vdc-host-role-<region>`

.....

Descarga de registros de instancias de Linux EC2

Inicia sesión en la EC2 instancia desde la que quieres descargar los registros y ejecuta los siguientes comandos para cargar todos los registros en un bucket de s3:

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

Después, vaya a la consola S3, seleccione el bucket con su nombre `<environment_name>-cluster-<region>-<aws_account_number>` y descargue el `<module_name>_logs.tar.gz` archivo cargado anteriormente.

.....

Descargar registros de EC2 instancias de Windows

Inicie sesión en la EC2 instancia desde la que desee descargar los registros y ejecute los siguientes comandos para cargar todos los registros en un bucket de S3:

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

Después, vaya a la consola S3, seleccione el bucket con su nombre `<environment_name>-cluster-<region>-<aws_account_number>` y descargue el `<module_name>_logs.zip` archivo cargado anteriormente.

.....

Recopilación de registros de ECS para detectar el WaitCondition error

1. Ve a la pila implementada y selecciona la pestaña Recursos.
2. Expanda Implementar ResearchAndEngineeringStudio→ Instalador → Tareas CreateTaskDef→ CreateContainer→ → LogGroupy seleccione el grupo de registros para abrir CloudWatch los registros.
3. Obtenga el registro más reciente de este grupo de registros.

.....

Entorno de demostración

Temas

- Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad

.....

Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad

Problema

Si intentas iniciar sesión y aparece un «error inesperado al tramitar la solicitud de autenticación al proveedor de identidad», es posible que tus contraseñas estén caducadas. Puede ser la contraseña del usuario con el que intenta iniciar sesión o su cuenta de Active Directory Service.

Mitigación

1. Restablezca las contraseñas de usuario y cuenta de servicio en la consola de servicio de Directory.

2. Actualice las contraseñas de las cuentas de servicio en Secrets Manager para que coincidan con la nueva contraseña que ingresó anteriormente:
   - para la pila Keycloak: -... PasswordSecret - -... RESExternal - DirectoryService-... con descripción: Contraseña para Microsoft Active Directory
   - para RES: res- ServiceAccountPassword -... con descripción: contraseña de la cuenta de Active Directory Service
3. Vaya a la EC2 consola y finalice la instancia del administrador de clústeres. Las reglas de Auto Scaling activarán automáticamente el despliegue de una nueva instancia.

.....

Problemas conocidos

- Problemas conocidos de la versión 2024.x
  - (2024.06) La aplicación de la instantánea falla cuando el nombre del grupo de AD contiene espacios
  - (2024.04-2024.04.02) Siempre que el límite de permisos de IAM no esté asociado a la función de las instancias de VDI
  - (2024.04.02 y versiones anteriores) Las instancias de Windows NVIDIA en ap-southeast-2 (Sídney) no se inician
  - (2024.04 y 2024.04.01) Error al eliminar RES en GovCloud
  - (2024.04 - 2024.04.02) Es posible que el escritorio virtual Linux quede atrapado en el estado «REANUDANDO» al reiniciarse
  - (04.02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo atributo de SAMAccount nombre incluye letras mayúsculas o caracteres especiales
  - (02 de abril de 2020 y versiones anteriores) La clave privada para acceder al host del bastión no es válida
  - (2024.06 y versiones anteriores) Los miembros del grupo no se sincronizaron con RES durante la sincronización de AD
  - (2024.06 y versiones anteriores) CVE-2024-6387, Regre, vulnerabilidad de seguridad en Ubuntu SSHion RHEL9 VDIs

Problemas conocidos de la versión 2024.x

.....

(2024.06) La aplicación de la instantánea falla cuando el nombre del grupo de AD contiene espacios

Problema

El RES 2024.06 no aplica las instantáneas de versiones anteriores si los grupos de AD contienen espacios en sus nombres.

Los registros del administrador de clústeres (del grupo de CloudWatch registros) incluirán el `<environment-name>/cluster-manager` siguiente error durante la sincronización de AD:

```
[apply-snapshot] authz.role-assignments/<Group name with
 spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key
 doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_.-]{1,20}:(user|group)$
```

El error se debe a que RES solo acepta nombres de grupos que cumplan los siguientes requisitos:

- Solo puede contener letras ASCII mayúsculas y minúsculas, dígitos, guiones (-), puntos (.) y caracteres de subrayado (_)
- No se permite usar un guión (-) como primer carácter
- No puede contener espacios.

Versiones afectadas

2024.06

Mitigación

1. Para descargar el script y el archivo del parche (patch.py y groupname_regex.patch), ejecute el siguiente comando y `<output-directory>` sustitúyalos por el directorio en el que desee colocar los archivos y `<environment-name>` por el nombre del entorno RES:
   a. El parche solo se aplica a la RES 2024.06
   b. El script del parche requiere AWS CLI v2, Python 3.9.16 o superior y Boto3.

c. Configure la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de S3 para escribir en el bucket creado por RES:

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
 ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. Navegue hasta el directorio donde se descargaron el script y el archivo del parche. Ejecute el siguiente comando de parche:

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. Para reiniciar la instancia de Cluster Manager para su entorno, ejecute los siguientes comandos: También puede finalizar la instancia desde Amazon EC2 Management Console.

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> El parche permite que los nombres de los grupos de AD contengan letras ASCII minúsculas y mayúsculas, dígitos, guiones (-), puntos (.), caracteres de subrayado (_) y espacios con una longitud total de entre 1 y 30, ambos inclusive.

.....

(2024.04-2024.04.02) Siempre que el límite de permisos de IAM no esté asociado a la función de las instancias de VDI

¿El problema

Las sesiones de escritorios virtuales no heredan correctamente la configuración de límites de permisos de su proyecto. Esto se debe a que el límite de permisos definido por el parámetro IAMPermission Límite no se asignó correctamente a un proyecto durante su creación.

Versiones afectadas

2024.04 - 2024.04.02

Mitigación

Siga estos pasos para poder heredar correctamente VDIs el límite de permisos asignado a un proyecto:

1. Para descargar el script y el archivo del parche (patch.py y vdi_host_role_permission_boundary.patch), ejecute el siguiente comando y sustitúyalos por el directorio local en el que desee colocar los archivos: `<output-directory>`

   a. El parche solo se aplica a la RES 2024.04.02. Si tiene la versión 2024.04 o 2024.04.01, puede seguir los pasos que se indican en el documento público para las actualizaciones de las versiones menores a fin de actualizar su entorno a la versión 2024.04.02.

   b. El script del parche requiere AWS CLI (v2), Python 3.9.16 o superior y Boto3.

   c. Configure la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de S3 para escribir en el bucket creado por RES.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
 --output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. Navegue hasta el directorio donde se descargaron el script y el archivo del parche. Ejecute el siguiente comando patch y `<environment-name>` sustitúyalo por el nombre de su entorno RES:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. Reinicie la instancia del administrador de clústeres en su entorno ejecutando este comando, sustituyéndolo `<environment-name>` por el nombre de su entorno RES. También puede cancelar la instancia desde Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 y versiones anteriores) Las instancias de Windows NVIDIA en ap-southeast-2 (Sídney) no se inician

¿El problema

Amazon Machine Images (AMIs) se utilizan para activar escritorios virtuales (VDIs) en RES con configuraciones específicas. Cada AMI tiene un identificador asociado que varía según la región. El ID de AMI configurado en RES para lanzar instancias de Windows Nvidia en ap-southeast-2 (Sídney) es incorrecto actualmente.

El AMI-ID `ami-0e190f8939a996caf` para este tipo de configuración de instancia aparece incorrectamente en ap-southeast-2 (Sídney). En su lugar, se `ami-027cf6e71e2e442f4` debe usar el ID de AMI.

Los usuarios recibirán el siguiente error al intentar lanzar una instancia con la `ami-0e190f8939a996caf` AMI predeterminada.

```
An error occured (InvalidAMIID.NotFound) when calling the RunInstances operation: The
 image id '[ami-0e190f8939a996caf]' does not exist
```

Pasos para reproducir el error, incluido un ejemplo de archivo de configuración:

- Implemente RES en la región ap-southeast-2.
- Lanza una instancia con la pila de software predeterminada de Windows-NVIDIA (ID de AMI)`ami-0e190f8939a996caf`.

Versiones afectadas

Todas las versiones 2024.04.02 o anteriores de RES se ven afectadas

Mitigación

La siguiente mitigación se probó en la versión 2024.01.01 de RES:

- Registre una nueva pila de software con la siguiente configuración
  - ID de AMI: `ami-027cf6e71e2e442f4`
  - Sistema operativo: Windows
  - Fabricante de GPU: NVIDIA
  - Mín. Tamaño de almacenamiento (GB): 30
  - Mín. RAM (GB): 4
- Utilice esta pila de software para lanzar instancias de Windows-NVIDIA

.....

(2024.04 y 2024.04.01) Error al eliminar RES en GovCloud

¿El problema

Durante el flujo de trabajo de eliminación de RES, `UnprotectCognitoUserPool` Lambda desactiva la protección contra eliminación para los grupos de usuarios de Cognito que se eliminarán más adelante. La ejecución de Lambda se inicia con. `InstallerStateMachine`

Debido a las diferencias de versión de AWS CLI predeterminadas entre la versión comercial y GovCloud las regiones, la `update_user_pool` llamada en la Lambda fallará en GovCloud las regiones.

Los clientes recibirán el siguiente error al intentar eliminar RES en GovCloud las regiones:

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
 VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
 DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
 AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

Pasos para reproducir el error:

- Implemente RES en una GovCloud región
- Elimine la pila RES

Versiones afectadas

RES versiones 2024.04 y 2024.04.01

Mitigación

La siguiente mitigación se probó en la versión 2024.04 de RES:

- Abra la `UnprotectCognitoUserPool` Lambda
  - Convención de nomenclatura: *`<env-name>`*`-InstallerTasksUnprotectCognitoUserPool-...`
- Configuración del tiempo de ejecución -> Editar -> Seleccionar tiempo de ejecución `Python 3.11` -> Guardar.
- Abrir CloudFormation.
- Elimine la pila RES -> deje sin marcar Retain Installer Resource -> Eliminar.

.....

(2024.04 - 2024.04.02) Es posible que el escritorio virtual Linux quede atrapado en el estado «REANUDANDO» al reiniciarse

¿El problema

Los escritorios virtuales Linux pueden quedarse atascados en el estado «REANUDANDO» al reiniciarse después de una parada manual o programada.

Una vez reiniciada la instancia, el AWS Systems Manager no ejecuta ningún comando remoto para crear una nueva sesión de DCV y falta el siguiente mensaje de registro en los registros del controlador de vdc (en el grupo de CloudWatch registros): `<environment-name>/vdc/controller` CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

Versiones afectadas

2024.04 - 2024.04.02

Mitigación

Para recuperar los escritorios virtuales que están atrapados en el estado «REANUDANDO»:

1. Acceda mediante SSH a la instancia problemática desde la consola. EC2
2. Ejecuta los siguientes comandos en la instancia:

   ```
   sudo su -
   /bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
   configure_post_reboot.sh
   sudo reboot
   ```
3. Espera a que la instancia se reinicie.

Para evitar que los nuevos escritorios virtuales sufran el mismo problema, sigue estos pasos:

1. Para descargar el script y el archivo del parche (patch.py y vdi_stuck_in_resuming_status.patch), ejecute el siguiente comando y reemplácelo por el directorio en el que desee colocar los archivos: `<output-directory>`

   > **Note**
   >
   > - El parche solo se aplica a la RES 2024.04.02.
   > - El script del parche requiere AWS CLI v2, Python 3.9.16 o superior y Boto3.
   > - Configure la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de S3 para escribir en el bucket creado por RES.

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. Navegue hasta el directorio donde se descargaron el script y el archivo del parche. Ejecute el siguiente comando de parche y `<environment-name>` sustitúyalo por el nombre de su entorno RES y `<aws-region>` por la región en la que se implementa RES:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
 --module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. Para reiniciar la instancia del controlador VDC de su entorno, ejecute los siguientes comandos y `<environment-name>` sustitúyalos por el nombre de su entorno RES:

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(04.02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo atributo de SAMAccount nombre incluye letras mayúsculas o caracteres especiales

¿El problema

RES no sincroniza a los usuarios de AD después de configurar el SSO durante al menos dos horas (dos ciclos de sincronización de AD). Los registros del administrador de clústeres (del grupo de CloudWatch registros) incluyen el `<environment-name>/cluster-manager` siguiente error durante la sincronización de AD:

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

El error se debe a que RES solo acepta un SAMAccount nombre de usuario que cumpla los siguientes requisitos:

- Solo puede contener letras ASCII minúsculas, dígitos, puntos (.) y caracteres de subrayado (_).
- No se permite un punto o un guión bajo como primer o último carácter.
- No puede contener dos puntos o guiones bajos continuos (por ejemplo,.., __, ._, _.).

Versiones afectadas

2024.04.02 y versiones anteriores

Mitigación

1. Para descargar el script y el archivo del parche (patch.py y samaccountname_regex.patch), ejecute el siguiente comando y reemplácelo por el directorio en el que desee colocar los archivos: `<output-directory>`

   > **Note**
   >
   > - El parche solo se aplica al RES 2024.04.02.
   > - El script del parche requiere AWS CLI v2, Python 3.9.16 o superior y Boto3.
   > - Configure la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de S3 para escribir en el bucket creado por RES.

   ```
   OUTPUT_DIRECTORY=<output-directory>

   curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
   releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
   ```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
 ${OUTPUT_DIRECTORY}/samaccountname_regex.patch
```

2. Navegue hasta el directorio donde se descargaron el script y el archivo del parche. Ejecute el siguiente comando patch y `<environment-name>` sustitúyalo por el nombre de su entorno RES:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. Para reiniciar la instancia de Cluster Manager para su entorno, ejecute los siguientes comandos y `<environment-name>` sustitúyalos por el nombre de su entorno RES. También puede cancelar la instancia desde Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(02 de abril de 2020 y versiones anteriores) La clave privada para acceder al host del bastión no es válida

¿El problema

Cuando un usuario descarga la clave privada para acceder al servidor del bastión desde el portal web de RES, la clave no está bien formateada: se descargan varias líneas en una sola línea, lo que invalida la clave. El usuario recibirá el siguiente error cuando intente acceder al host del bastión con la clave descargada:

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
```

```
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)
```

Versiones afectadas

2024.04.02 y versiones anteriores

Mitigación

Recomendamos usar Chrome para descargar las claves, ya que este navegador no se ve afectado.

Como alternativa, se puede volver a formatear el archivo clave creando una nueva línea después `-----BEGIN PRIVATE KEY-----` y otra línea nueva justo antes. `-----END PRIVATE KEY-----`

.....

(2024.06 y versiones anteriores) Los miembros del grupo no se sincronizaron con RES durante la sincronización de AD

Descripción del error

Los miembros del grupo no se sincronizarán correctamente con RES si el GroupOU es diferente del UserOU.

RES crea un filtro ldapsearch cuando intenta sincronizar usuarios de un grupo de AD. El filtro actual utiliza incorrectamente el parámetro UserOU en lugar del parámetro GroupOU. El resultado es que la búsqueda no devuelve ningún usuario. Este comportamiento solo se produce en los casos en que UserSou y GroupU son diferentes.

Versiones afectadas

Este problema afecta a todas las versiones 2024.06 o anteriores de RES

Mitigación

Siga estos pasos para resolver el problema:

1. Para descargar el script patch.py y el archivo group_member_sync_bug_fix.patch, ejecute los siguientes comandos y `<output-directory>` sustitúyalos por el directorio local en el que

desee descargar los archivos y <res_version> por la versión de RES a la que desee aplicar el parche:

> **Note**
>
> - El script del parche requiere AWS CLI v2, Python 3.9.16 o superior y Boto3.
> - Configure la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de S3 para escribir en el bucket creado por RES.
> - El parche solo es compatible con las versiones 2024.04.02 y 2024.06 de RES. Si utiliza la 2024.04 o la 2024.04.01, puede seguir los pasos que se indican para actualizar primero su entorno Actualizaciones de versiones menores a la versión 2024.04.02 antes de aplicar el parche.
>   - Versión RES: RES 2024.04.02
>
>   Enlace de descarga del parche: 2024.04.02_group_member_sync_bug_fix.patch
>   - Versión RES: RES 2024.06
>
>   Enlace de descarga del parche: 2024.06_group_member_sync_bug_fix.patch

```
OUTPUT_DIRECTORY=<output-directory>
RES_VERSION=<res_version>
mkdir -p ${OUTPUT_DIRECTORY}

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch
 --output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando patch y <environment-name> sustitúyalo por el nombre de su entorno RES:

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>
```

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. Para reiniciar la instancia del administrador de clústeres de su entorno, ejecute los siguientes comandos:

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.06 y versiones anteriores) CVE-2024-6387, Regre, vulnerabilidad de seguridad en Ubuntu SSHion RHEL9 VDIs

Descripción del error

El CVE-2024-6387, denominado regreSSHion, ha sido identificado en el servidor OpenSSH. Esta vulnerabilidad permite a los atacantes remotos y no autenticados ejecutar código arbitrario en el servidor de destino, lo que representa un grave riesgo para los sistemas que utilizan OpenSSH para comunicaciones seguras.

En el caso de RES, la configuración estándar consiste en pasar por el host bastión para acceder mediante SSH a los escritorios virtuales, y el host bastión no se ve afectado por esta vulnerabilidad. Sin embargo, la AMI (Amazon Machine Image) predeterminada que proporcionamos RHEL9 y Ubuntu 2024 VDIs (infraestructura de escritorio virtual) en TODAS las versiones de RES utilizan una versión OpenSSH que es vulnerable a la amenaza de seguridad.

Esto significa que la versión existente RHEL9 y Ubuntu2024 VDIs podrían ser explotables, pero el atacante necesitaría acceder al servidor bastión.

Puedes encontrar más detalles sobre el problema aquí.

Versiones afectadas

Este problema afecta a todas las versiones 2024.06 o anteriores de RES.

Mitigación

RHEL9 Tanto Ubuntu como Ubuntu han lanzado parches para OpenSSH que corrigen la vulnerabilidad de seguridad. Estos se pueden obtener utilizando el administrador de paquetes respectivo de la plataforma.

Si tienes Ubuntu existente RHEL9 o Ubuntu VDIs, te recomendamos que sigas las VDIs instrucciones de PATCH EXISTING que aparecen a continuación. Para parchear el futuro VDIs, recomendamos seguir las VDIs instrucciones de PATCH FUTURE. Estas instrucciones describen cómo ejecutar un script para aplicar la actualización de la plataforma en su VDIs.

PARCHE EXISTENTE VDIs

1. Ejecute el siguiente comando que parcheará todos los Ubuntu existentes y RHEL9 VDIs:

   a. El script del parche requiere AWS CLI v2.

   b. Configure la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de administrador de AWS sistemas para enviar un comando de ejecución de Systems Manager.

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \
    --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
patch_scripts/scripts/patch_openssh.sh\"}"],"commandLine":["bash
 patch_openssh.sh"]}'
```

2. Puede comprobar que el script se ha ejecutado correctamente en la página Ejecutar comandos. Haga clic en la pestaña Historial de comandos, seleccione el ID de comando más reciente y compruebe que todas las instancias IDs tienen un mensaje de éxito.

PARCHE EL FUTURO VDIs

1. Para descargar el script y el archivo del parche (patch.py y update_openssh.patch) ejecute los siguientes comandos y sustitúyalos por `<output-directory>` el directorio en el que desea descargar los archivos y por el nombre de su entorno `<environment-name>` RES:

> **Note**
>
> - El parche solo se aplica a la RES 2024.06.
> - El script del parche requiere AWS CLI (v2), Python 3.9.16 o superior y Boto3.
> - Configure su copia de la AWS CLI para la cuenta y la región donde se implementa RES y asegúrese de tener permisos de S3 para escribir en el bucket creado por RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
 ${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. Ejecute el siguiente comando de parche:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. Reinicie la instancia de la controladora VDC de su entorno con los siguientes comandos:

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Important**
>
> La aplicación de parches en el futuro solo VDIs se admite en las versiones 2024.06 y posteriores de RES. Para parchear el futuro VDIs en entornos RES con versiones anteriores a la 2024.06, primero actualice el entorno RES a la 2024.06 siguiendo las instrucciones de:. Actualizaciones de versiones principales

.....

Avisos

Cada EC2 instancia de Amazon incluye dos licencias de Servicios de Escritorio Remoto (Terminal Services) para fines de administración. Esta información está disponible para ayudarle a aprovisionar estas licencias a sus administradores. También puede usarlo AWS Systems Manager Session Manager, lo que permite el acceso remoto a las EC2 instancias de Amazon sin RDP y sin necesidad de licencias de RDP. Si se necesitan licencias adicionales de Remote Desktop Services, el usuario de Remote Desktop CALs debe adquirirse en Microsoft o en un distribuidor de licencias de Microsoft. Los usuarios de escritorios remotos CALs con Software Assurance activo tienen las ventajas de la movilidad de licencias y pueden trasladarse a entornos de inquilinos AWS predeterminados (compartidos). Para obtener información sobre cómo adquirir licencias sin las ventajas de Software Assurance o License Mobility, consulte esta sección de las preguntas frecuentes.

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas de productos AWS actuales, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS sus filiales, proveedores o licenciantes. AWS los productos o servicios se proporcionan «tal cual» sin garantías, representaciones o condiciones de ningún tipo, ya sean expresas o implícitas. AWS Las responsabilidades y obligaciones con sus clientes están reguladas por AWS acuerdos, y este documento no forma parte de ningún acuerdo entre sus clientes AWS y sus clientes ni lo modifica.

La licencia de Research and Engineering Studio on AWS se rige por los términos de la versión 2.0 de la licencia Apache, disponible en The Apache Software Foundation.

Revisiones

Para obtener más información, consulte el archivo ChangeLog.md del repositorio. GitHub

Date	Cambio

Agosto de 2024	• Versión de lanzamiento 2024.08 —
	  • Se agregó soporte para montar buckets de Amazon S3 en instancias de infraestr uctura de escritorio virtual (VDI) de Linux. Consulte Buckets de Amazon S3.
	  • Se agregó soporte para permisos de proyectos personalizados, un modelo de permisos mejorado que permite personali zar los roles existentes y agregar roles personalizados. Consulte Perfiles de permisos.
	• Guía del usuario: se amplió la Solución de problemas sección.

Junio de 2024	• Versión de lanzamiento 2024.06: compatibi lidad con Ubuntu, permisos de propietario del proyecto. • Guía del usuario: añadida Cree un entorno de demostración
Abril de 2024	Versión de lanzamiento 2024.04: plantilla s listas para RES y para el lanzamiento de proyectos AMIs
Marzo de 2024	Temas adicionales de solución de problemas , conservación de CloudWatch registros y desinstalación de versiones secundarias
Febrero de 2024	Versión de lanzamiento 2024.01.01: plantilla de despliegue actualizada

Date	Cambio
Enero de 2024	Versión de lanzamiento 2024.01
Diciembre de 2023	GovCloud instrucciones y plantillas añadidas
Noviembre de 2023	Versión inicial

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.