aws

Guía del usuario de

Estudio de investigación e ingeniería

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Estudio de investigación e ingeniería: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas registradas y la imagen comercial de Amazon no se pueden utilizar en ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Descripción general de

> **Important**
>
> Esta guía del usuario cubre la versión actual (2026.03) de Research and Engineering Studio en adelante. AWS Para ver las versiones anteriores, consulte la. Archivo de versiones anteriores

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 proporciona un portal unificado para que los usuarios lancen escritorios virtuales seguros para realizar investigaciones científicas, diseños de 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 propias pilas de software de aplicaciones (mediante Amazon Machine Images o AMI) y permitir a los usuarios de RES lanzar escritorios virtuales de Windows o Linux y 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, también puede personalizar la experiencia de usuario del portal RES para que se adapte a sus propias necesidades.

RES está disponible sin costo adicional y solo paga 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:

Web-based interfaz de usuario

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

Project-based configuración

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. Los miembros invitados pueden iniciar sesión en RES para conectarse a los escritorios compartidos.

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 en RES. Los servicios de almacenamiento compatibles incluyen Amazon Elastic File System para escritorios Linux y Amazon FSx NetApp para 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 Research and Engineering Studio sobre AWS:

Explorador de archivos

Un explorador de archivos es una parte de la interfaz de usuario de RES donde los usuarios que están conectados actualmente 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 distinto para los recursos de datos y cómputo. Esto garantiza la gobernanza del flujo de datos y evita compartir datos y hosts de VDI entre proyectos.

Project-based permisos

Project-based los permisos 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 ni a los VDI 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

Delegado administrativo con acceso a un proyecto específico y propietario del mismo. 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 RES-specific metadatos 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 AWS términos, consulte el glosario.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.

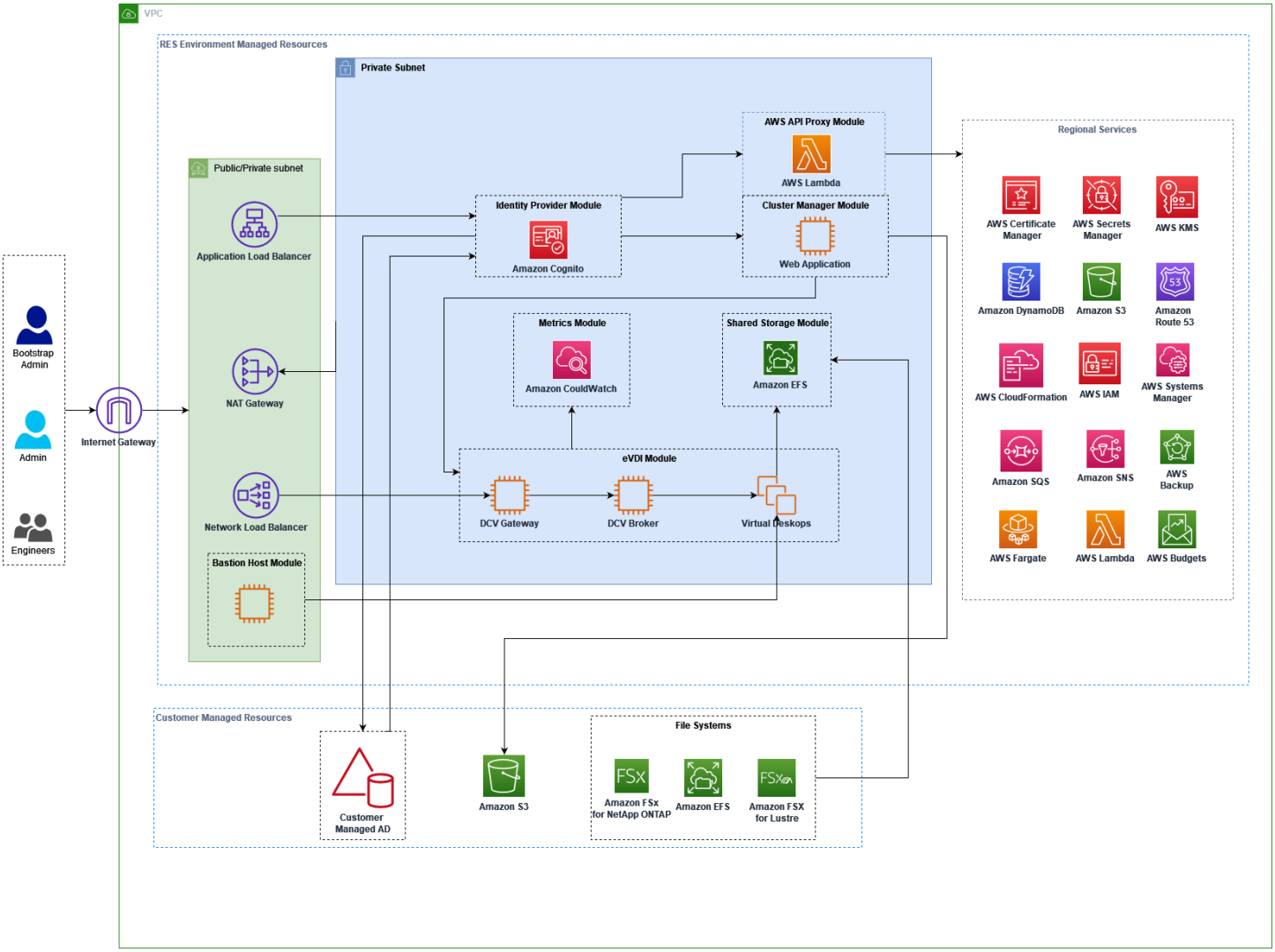


Figura 1: Estudio de investigación e ingeniería sobre AWS arquitectura

> **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 usar SSH para conectarse al componente de host Bastion y 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 «clusteradmin» debe cambiar la contraseña la primera vez que inicie sesión.

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	Tipo	Description (Descripción)
Amazon Elastic Compute Cloud	Core	Proporciona los servicios informáticos subyacentes para crear escritorios virtuales con el sistema operativo y la pila de software que elijan.
Elastic Load Balancing	Core	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	Core	Todos los componentes principales del producto se crean en su VPC.
Amazon Cognito	Core	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	Core	Proporciona el sistema de `/home` archivos para el

AWS servicio	Tipo	Description (Descripción)
		explorador de archivos y los hosts de VDI, así como para los sistemas de archivos externos compartidos.
Amazon DynamoDB	Core	Almacena datos de configuración, como usuarios, grupos, proyectos, sistemas de archivos y ajustes de componentes.
AWS Systems Manager	Core	Almacena documentos para ejecutar comandos para la administración de sesiones de VDI.
AWS Lambda	Core	Admite funcionalidades del producto, como la actualización de la configuración de la 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	Compatible	Proporciona métricas y registros de actividad para todos los hosts de Amazon EC2 y las funciones de Lambda.
Amazon Simple Storage Service	Apoyando	Almacena los archivos binarios de las aplicaciones para el arranque y la configuración del host.

AWS servicio	Tipo	Description (Descripción)
AWS Key Management Service	Apoyando	Se utiliza para el cifrado en reposo con colas de Amazon SQS, tablas de DynamoDB y temas de Amazon SNS.
AWS Secrets Manager	Apoyando	Almacena las credenciales de las cuentas de servicio en Active Directory y los certifica dos autofirmados para los VDI.
AWS CloudFormation	Compatible	Proporciona un mecanismo de despliegue para el producto.
AWS Identity and Access Management	Apoyando	Restringe el nivel de acceso de los hosts.
Amazon Route 53	Apoyando	Crea una zona alojada privada para resolver el balancead or de cargas interno y el nombre de dominio del host del bastión.
Amazon Simple Queue Service	Apoyando	Crea colas de tareas para respaldar las ejecuciones asíncronas.
Amazon Simple Notification Service	Apoyando	Admite el modelo de publicaci ón-suscriptor entre los componentes de la VDI, como el controlador y los hosts.
AWS Fargate	Apoyando	Instala, actualiza y elimina entornos mediante las tareas de Fargate.

AWS servicio	Tipo	Description (Descripción)
Pasarela de archivos Amazon FSx	Opcional	Proporciona un sistema de archivos compartidos externo.
Amazon FSx para ONTAP NetApp	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 capacidades de respaldo para hosts, sistemas de archivos y DynamoDB de Amazon EC2.

Cree un entorno de demostración

> **Note**
>
> Este entorno de demostración no es compatible con AWS GovCloud (US).

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 las instrucciones que Pasos posteriores a la implementación se indican a continuación para configurar los usuarios en el entorno antes de iniciar sesión.

Cree una pila de demostración con un solo clic

Esta 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
- Cree un par de claves SSH de Amazon EC2
- 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. Abra https://portal.aws.amazon.com/billing/signup.
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.

Cree un par de claves SSH de Amazon EC2

Si no tiene un par de claves SSH de Amazon EC2, tendrá que crear uno. Para obtener más información, consulte Crear un par de claves mediante Amazon EC2 en la Guía del usuario de Amazon EC2.

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 las IP EC2-VPC elásticas 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 Region-specific. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar. Para obtener más información, consulte the section called “Cuotas para AWS los servicios de este producto”.

Cree recursos e introduzca parámetros

1. Inicie sesión en Consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation.

> **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	Description (Descripción)
EnvironmentName	`<res-demo>`	Un nombre exclusivo asignado a su entorno RES que comienza con res-, no más de 11 caracteres y sin letras mayúsculas.
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.
IPCIdR del cliente	<0.0.0. 0/0>	Filtro de direcciones IP que limita la conexión al sistema. Puede actualizarlo ClientIpC idr después de la implement ación.

Parámetro	Predeterminado	Description (Descripción)
InboundPrefixList		(Opcional) Proporcione una lista de prefijos gestionad a para las IP que pueden acceder directamente a la interfaz de usuario web y a SSH desde el host bastión.

4. Seleccione Creación de pila.

Pasos posteriores a la implementación

1. Ahora puede iniciar sesión en el entorno de demostración con el usuario clusteradmin y la contraseña temporal enviada al correo electrónico del administrador que ingresó durante la configuración. Se le solicitará que cree una nueva contraseña la primera vez que inicie sesión.
2. Si quieres utilizar la función «Iniciar sesión con el inicio de sesión único de la organización», primero debes restablecer las contraseñas de cada usuario con el que quieras iniciar sesión. Puede restablecer las contraseñas de los usuarios desde AWS Directory Service. La pila de demostración crea cuatro usuarios con nombres de usuario que puede utilizar: admin1, user1, admin2 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, introduce el nombre de usuario, escribe la nueva contraseña que desees y, a continuación, selecciona Restablecer contraseña.
3. Una vez que haya restablecido las contraseñas de los usuarios, vaya a la página de inicio de sesión con inicio de sesión único para acceder al entorno.

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

Esta sección contiene información sobre el coste, la seguridad, las regiones admitidas y las cuotas que pueden ayudarle a planificar el despliegue de Research and Engineering Studio en AWS

Costo

Research and Engineering Studio on AWS está disponible sin coste adicional y solo se paga por los AWS recursos necesarios para ejecutar las 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.
> Como práctica recomendada, cree un presupuesto AWS Cost Explorerpara ayudar a administrar los costos. 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

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted.

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento de los programas de . Para obtener más información sobre los programas de cumplimiento que se aplican a Research and Engineering Studio on AWS, consulte AWS Servicios dentro del alcance por programa de cumplimiento AWS .

- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Para saber cómo aplicar el modelo de responsabilidad compartida a los AWS servicios utilizados por Research and Engineering Studio, consulteConsideraciones de seguridad para los servicios de este producto. 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 instancias de Amazon EC2 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 de Lambda, las instancias de Amazon EC2, los sistemas de archivos y los puntos de enlace VPN remotos. Revise los grupos de seguridad y restrinja aún más el acceso según sea necesario después de implementar 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 RES-owned clave. 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. Se requiere TLS 1.2, pero se recomienda TLS 1.3.

Consideraciones de seguridad para los servicios de este producto

Para obtener información más detallada sobre las consideraciones de seguridad de los servicios utilizados por Research and Engineering Studio, siga los enlaces de esta tabla:

AWS información de seguridad del servicio	tipo de servicio	Cómo se usa el servicio en RES
Amazon Elastic Compute Cloud	Core	Proporciona los servicios informáticos subyacentes para crear escritorios virtuales con el sistema operativo y la pila de software que elijan.
Elastic Load Balancing	Core	Los hosts Bastion, cluster-manager y VDI se crean en grupos de Auto Scaling detrás del balanceador de cargas. Elastic Load Balancing equilibra el tráfico del portal web entre los hosts de RES.
Amazon Virtual Private Cloud	Core	Todos los componentes principales del producto se crean en su VPC.
Amazon Cognito	Core	Administra las identidades y la autenticación de los usuarios. Los usuarios de Active Directory se asignan a usuarios y grupos de Amazon

AWS información de seguridad del servicio	tipo de servicio	Cómo se usa el servicio en RES
		Cognito para autenticar los niveles de acceso.
Amazon Elastic File System	Core	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	Core	Almacena datos de configura ción, como usuarios, grupos, proyectos, sistemas de archivos y ajustes de componentes.
AWS Systems Manager	Core	Almacena documentos para ejecutar comandos para la administración de sesiones de VDI.
AWS Lambda	Core	Admite funcionalidades del producto, como la actualiza ción de la configuración de la 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	Compatible	Proporciona métricas y registros de actividad para todos los hosts de Amazon EC2 y las funciones de Lambda.

AWS información de seguridad del servicio	tipo de servicio	Cómo se usa el servicio en RES
Amazon Simple Storage Service	Apoyando	Almacena los archivos binarios de las aplicaciones para el arranque y la configura ción del host.
AWS Key Management Service	Apoyando	Se utiliza para el cifrado en reposo con colas de Amazon SQS, tablas de DynamoDB y temas de Amazon SNS.
AWS Secrets Manager	Apoyando	Almacena las credenciales de las cuentas de servicio en Active Directory y los certifica dos autofirmados para los VDI.
AWS CloudFormation	Compatible	Proporciona un mecanismo de despliegue para el producto.
AWS Identity and Access Management	Apoyando	Restringe el nivel de acceso de los hosts.
Amazon Route 53	Apoyando	Crea una zona alojada privada para resolver el balancead or de cargas interno y el nombre de dominio del host del bastión.
Amazon Simple Queue Service	Apoyando	Crea colas de tareas para respaldar las ejecuciones asíncronas.

AWS información de seguridad del servicio	tipo de servicio	Cómo se usa el servicio en RES
Amazon Simple Notification Service	Apoyando	Admite el modelo de publicación y suscripción entre los componentes de la VDI, como el controlador y los hosts.
AWS Fargate	Apoyando	Instala, actualiza y elimina entornos mediante las tareas de Fargate.
Pasarela de archivos Amazon FSx	Opcional	Proporciona un sistema de archivos compartidos externo.
Amazon FSx para ONTAP NetApp	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 capacidades de respaldo para hosts, sistemas de archivos y DynamoDB de Amazon EC2.

Cuotas

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

Cuotas de 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.

Como práctica recomendada, aumente 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 las cuotas de AWS CloudFormation en la Guía del usuario de AWS CloudFormation .

Planificar la resiliencia

El producto implementa una infraestructura predeterminada con el número y el tamaño mínimos de instancias de Amazon EC2 para operar el sistema. Para mejorar la resiliencia en entornos de producción a gran escala, como práctica recomendada, aumente la configuración de capacidad mínima predeterminada dentro de los grupos de Auto Scaling (ASG) de la infraestructura. Al aumentar el valor de una instancia a dos instancias, se obtienen las ventajas de disponer de varias zonas de disponibilidad (AZ) y se reduce el tiempo necesario para restaurar la funcionalidad del sistema en caso de una pérdida inesperada de datos.

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

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	Region	Versiones anteriores	Última versión (2025.12)
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 (Osaka)	ap-northeast-3	yes	sí
Asia-Pacífico (Mumbai)	ap-south-1	yes	sí
Asia-Pacífico (Singapur)	ap-southeast-1	yes	sí
Asia-Pacífico (Sídney)	ap-southeast-2	yes	sí
Asia-Pacífico (Yakarta)	ap-southeast-3	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

Nombre de la región	Region	Versiones anteriores	Última versión (2025.12)
Europa (Londres)	eu-west-2	yes	sí
Europa (París)	eu-west-3	yes	sí
Europa (Estocolmo)	eu-north-1	yes	sí
Israel (Tel Aviv)	il-central-1	yes	sí
Medio Oriente (EAU)	me-central-1	yes	sí
América del Sur (São Paulo)	sa-east-1	yes	sí
AWS GovCloud (US-East)	us-gov-east-1	yes	sí
AWS GovCloud (US-West)	us-gov-west-1	yes	sí

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

Temas

Cree una Cuenta de AWS con un usuario administrativo

Debe tener una Cuenta de AWS con un usuario administrativo:

1. Abra https://portal.aws.amazon.com/billing/signup.
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.

   Al suscribirse a 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.

Cree un par de claves SSH de Amazon EC2

Si no tiene un par de claves SSH de Amazon EC2, debe crear uno. Para obtener más información, consulte Crear un par de claves mediante Amazon EC2 en la Guía del usuario de Amazon EC2.

Aumentar las cuotas de servicio

Como práctica recomendada, aumente 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 las IP EC2-VPC elásticas de cinco a diez.

Su AWS cuenta tiene cuotas predeterminadas para cada AWS servicio. A menos que se indique lo contrario, cada cuota es Region-specific. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar. Para obtener más información, consulte Cuotas de los AWS servicios de este producto.

Crear un grupo de usuarios de Cognito (opcional)

Tiene la opción de importar un grupo de usuarios de Cognito existente para la autenticación de usuarios y clientes al instalar RES. De lo contrario, RES creará automáticamente un nuevo grupo de usuarios de Cognito. El grupo de usuarios preexistente debe tener los siguientes atributos personalizados de registro:

Name	Tipo	Mínimo value/length	Max value/length	Mutable
personalizado:aws_region	Cadena			TRUE
personalizado:cluster_name	Cadena			TRUE
personalizado:password_last_set	Número			TRUE
personalizado:password_max_age	Número			TRUE
personalizado:uid	Número	2000200001	4294967294	TRUE

Crea un dominio personalizado (opcional)

Como práctica recomendada, usa un dominio personalizado para el producto a fin de crear una URL fácil de usar. Puede proporcionar un dominio personalizado y, si lo desea, proporcionarle un certificado.

Hay un proceso en la pila de recursos externos para crear un certificado para un dominio personalizado que usted proporcione. Puede omitir estos pasos si tiene un dominio y desea utilizar las capacidades de generación de certificados de la pila de recursos externos.

O bien, siga estos pasos para registrar un dominio mediante Amazon Route 53 e importar un certificado para el dominio mediante AWS Certificate Manager.

1. Siga las instrucciones para registrar un dominio en Route 53. Deberías recibir un correo electrónico de confirmación.
2. Recupera la zona alojada de tu dominio. Route 53 lo crea automáticamente.
    a. Abra la consola Route 53.
    b. Seleccione 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 Route 53. La solicitud tardará aproximadamente diez minutos en procesarse.
7. Una vez emitido el certificado, copie el ARN de la sección de estado del certificado.

Cree un dominio (GovCloud únicamente)

Si va a realizar el despliegue en una AWS GovCloud región y utiliza un dominio personalizado para Research and Engineering Studio, debe completar estos pasos previos.

1. Implemente la 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 = controlador de escritorio virtual
    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 = controlador de escritorio virtual

   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 instancias EC2 que se utilizan 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 el nombre de usuario y la contraseña de la cuenta del servicio de Active Directory formateados como un par clave-valor (nombre de usuario y contraseña)

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

> **Warning**
>
> Debe proporcionar una dirección de correo electrónico válida para todos los usuarios de Active Directory (AD) que desee sincronizar.

> **Tip**
>
> Si está implementando un entorno de demostración y no dispone de estos recursos externos, puede utilizar recetas 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 una AWS GovCloud región, debe completar los pasos previos que se indican. Cree un dominio (GovCloud únicamente)

Configure LDAPS en su entorno (opcional)

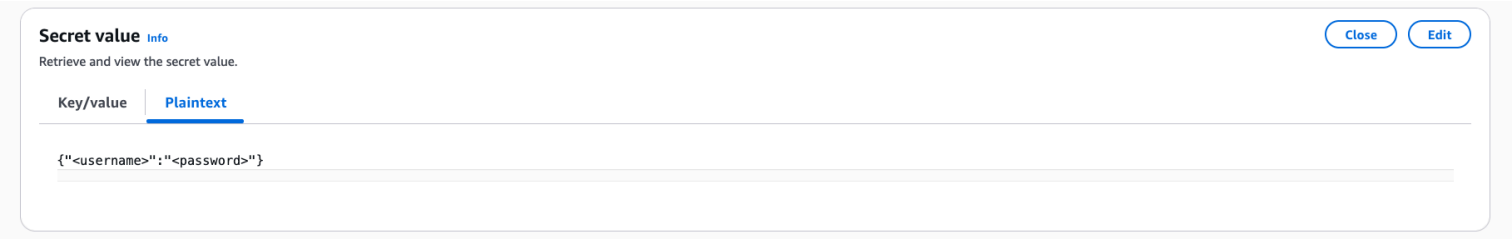
Si planea utilizar la comunicación LDAPS en su entorno, debe completar estos pasos para crear y adjuntar certificados al controlador de dominio AWS Managed Microsoft AD (AD) a fin de proporcionar comunicación entre AD y RES.

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. Selecciona Base-64 codificado X.509 (.CER) y selecciona 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. Paso 1: lanzar el producto

Configurar una cuenta de servicio para Microsoft Active Directory

Si elige Microsoft Active Directory (AD) como fuente de identidad para RES, dispondrá de una cuenta de servicio en su AD que le permitirá el acceso mediante programación. Debe transmitir un secreto con las credenciales de la cuenta de servicio como parte de la instalación de RES. El secreto debe tener el formato que se muestra aquí.



Tenga en cuenta también que el `username` campo no admite nombres de NT-style inicio de sesión con este formato`DOMAIN\username`.

La cuenta de servicio es responsable de las siguientes funciones:

- Sincronizar usuarios desde el AD: RES debe sincronizar los usuarios del AD para que puedan iniciar sesión en el portal web. El proceso de sincronización utiliza la cuenta de servicio para consultar el AD mediante LDAP y determinar qué usuarios y grupos están disponibles.
- Unirse al dominio de AD: esta es una operación opcional para los escritorios virtuales y los hosts de infraestructura de Linux en los que la instancia se une al dominio de AD. En RES, esto se controla con el `DisableADJoin` parámetro. Este parámetro está establecido en False de forma predeterminada, lo que significa que los escritorios virtuales Linux intentarán unirse al dominio AD en la configuración predeterminada.
- Conectarse al AD: los escritorios virtuales y los hosts de infraestructura de Linux se conectarán al dominio de AD si no se unen a él (`DisableADJoin`= True). Para que esta funcionalidad funcione, la cuenta de servicio también necesita acceso de lectura para los usuarios y grupos que se encuentren dentro y fuera del sistema`UsersOU`. `GroupsOU`

La cuenta de servicio requiere los siguientes permisos:

- Para sincronizar los usuarios y conectarse a AD → Acceso de lectura para los usuarios `UsersOU` y grupos locales`GroupsOU`.
- Para unirse al dominio AD → cree `Computer` objetos en`ComputersOU`.

El script de aquí https://github.com/aws-samples/aws-hpc-recipes/blob/main/recipes/res/res_demo_env/assets/service_account.ps1proporciona un ejemplo de cómo conceder los permisos adecuados a una cuenta de servicio. Puede modificarlo en función de su propio AD.

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

- Preparar imágenes de máquinas de Amazon (AMI)
- Configurar puntos finales de VPC
- Conéctese a servicios sin puntos finales de VPC
- Defina los parámetros de despliegue de una VPC privada

Preparar imágenes de máquinas de Amazon (AMI)

1. Descargue las dependencias en https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/latest/res-installation-scripts.tar.gz. Para implementarse en una VPC aislada, la infraestructura RES requiere la disponibilidad de dependencias sin tener acceso público a Internet.

   > **Important**
   >
   > Sustituya **`latest`** el URI de descarga por el número de versión exacto (por ejemplo**`2025.06`**) si la versión de su entorno RES no es la más reciente.

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, elija EC2 y elija Siguiente.

d. En Agregar permisos, seleccione las siguientes políticas de permisos y, a continuación, elija Siguiente:

- AmazonS3ReadOnlyAccess
- AmazonSSMManagedInstanceCore
- EC2InstanceProfileForImageBuilder

e. Agregue un nombre y una descripción del rol y, a continuación, elija Crear rol.

3. Cree el componente generador de imágenes de EC2:

a. Abra la consola https://console.aws.amazon.com//imagebuilder EC2 Image Builder en.

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, Amazon Linux 2023, RHEL8, RHEL 9 o Windows 10 y 11
Nombre del componente	Introduzca un nombre como: *<research-and-engineering-studio-infrastructure>*
Versión del componente	Recomendamos empezar con la versión 1.0.0.
Description (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:
  - 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-installation-scripts/res-
installation-scripts.tar.gz'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd /root/bootstrap/res-installation-scripts'
                - 'tar -xf res-installation-scripts.tar.gz'
                - 'cd scripts/infrastructure-host'
                - '/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,ecs.
{{ AWSRegion }}.amazonaws.com,.execute-api.{{ AWSRegion }}.amazonaws.com
                  " >> /etc/environment launch template
```

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 o Red Hat Enterprise Linux (RHEL)
	Origen de la imagen	Inicio rápido (Amazon-managed)
	Nombre de la imagen	Amazon Linux 2 x86, Amazon Linux 2023 x86, Red Hat Enterprise Linux 8 x86 o Red Hat Enterprise Linux 9 x86

Sección	Parámetro	Entrada de usuario
	Auto-versioning options	Utilice la última versión del sistema operativo disponibl e.
Configuración de instancias	–	Mantén todo en la configuración predeterm inada y asegúrate de que no esté seleccionada la opción Eliminar el agente SSM tras la ejecución de la canalización.
Directorio de trabajo	Ruta del directorio de trabajo	/root/bootstrap/res-install ation-scripts
Componentes	Construya componentes	Busque y seleccione lo siguiente: • Amazon-managed: aws-cli-version-2-linux • Amazon-managed: amazon-cloudwatch-agent-linux • De su propiedad: componente de Amazon EC2 creado anteriorm ente. Coloque su AWS región actual en el campo.
	Pruebe los componentes	Busque y seleccione: • Amazon-managed: 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 adecuado, como res-infra-linux-x86.
	Descripción	Añada una descripción opcional.
	Rol de IAM	Seleccione el rol de IAM creado anteriormente.
AWS infraestructura	Tipo de instancia	Elija t3.medium.

Sección	Parámetro	Entrada de usuario

	VPC, subred y grupos de seguridad	Seleccione una opción que permita el acceso a Internet y al bucket de Amazon S3. Si necesita crear un grupo de seguridad, puede crear uno desde la consola Amazon EC2 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
		  • Origen: personalizado
		  • Bloque CIDR: 0.0.0. 0/0

d. Elija Crear configuración de infraestructura.

6. Cree una nueva canalización de EC2 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 Image Builder de EC2.
- Si desea implementar RES en varias regiones, puede elegir Crear una nueva configuración de distribución y añadir allí más regiones.

g. Revisa tus selecciones y selecciona Crear canalización.

7. Ejecute la canalización de EC2 Image Builder:

a. En Image Pipelines, busque y seleccione la canalización que ha creado.

b. Elige 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
Application Auto Scaling	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
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams
AWS Lambda	com.amazonaws. *region*.lambda
Amazon S3	com.amazonaws. *region*.s3 (requiere un punto final de puerta de enlace que se crea de forma predeterminada en RES). Se requieren puntos de enlace de interfaz Amazon S3 adicionales para el montaje cruzado de los buckets en un

Servicio de AWS	Nombre del servicio
	entorno aislado. Consulte Acceder a los puntos finales de la interfaz de Amazon Simple Storage Service.
AWS Secrets Manager	com.amazonaws. *region*.administrador de secretos
Servicio Amazon Elastic Container	com.amazonaws. *region*.ecs
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 integrarse 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. Niegue 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. Infrastructure/VDIs

4. Modifique el grupo de seguridad de la instancia EC2 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 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 “Preparar imágenes de máquinas de Amazon (AMI)”.
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.
HttpProxy	Ejemplo: `http://10.1.2.3:123`
HttpsProxy	Ejemplo: `http://10.1.2.3:123`
NoProxy	Ejemplo:

```
127.0.0.1,169.254.169.254,169.254.17
0.2,localhost,us-east-1.res,us-east-
1.vpce.amazonaws.com,us-east-1.elb.a
mazonaws.com,s3.us-east-1.amazonaws.
com,s3.dualstack.us-east-1.amazonaws
.com,ec2.us-east-1.amazonaws.com,ec2
.us-east-1.api.aws,ec2messages.us-ea
st-1.amazonaws.com,ssm.us-east-1.ama
zonaws.com,ssmmessages.us-east-1.ama
zonaws.com,kms.us-east-1.amazonaws.c
om,secretsmanager.us-east-1.amazonaw
s.com,sqs.us-east-1.amazonaws.com,el
asticloadbalancing.us-east-1.amazona
ws.com,sns.us-east-1.amazonaws.com,l
ogs.us-east-1.amazonaws.com,logs.us-
east-1.api.aws,elasticfilesystem.us-
east-1.amazonaws.com,fsx.us-east-1.a
mazonaws.com,dynamodb.us-east-1.amaz
onaws.com,api.ecr.us-east-1.amazonaw
```

Parámetro	Input
	`s.com,.dkr.ecr.us-east-1.amazonaws.com,kinesis.us-east-1.amazonaws.com,.data-kinesis.us-east-1.amazonaws.com,.control-kinesis.us-east-1.amazonaws.com,events.us-east-1.amazonaws.com,cloudformation.us-east-1.amazonaws.com,sts.us-east-1.amazonaws.com,application-autoscaling.us-east-1.amazonaws.com,monitoring.us-east-1.amazonaws.com,ecs.us-east-1.amazonaws.com,.execute-api.us-east-1.amazonaws.com`

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 Consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation.

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

2. Inicie la plantilla en la consola.

   Si va a realizar la implementación en una AWS GovCloud región, inicie la plantilla en su cuenta de GovCloud partición (por ejemplo, aquí para la región AWS GovCloud (US-West)).

3. Introduzca los parámetros de la plantilla:

> **Important**
>
> Utilice valores diferentes para estas cuentas `AdminPassword` y `ServiceAccountPassword` para mantenerlas dentro de los límites de seguridad adecuados.

Parámetro	Predeterminado	Description (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.

Parámetro	Predeterminado	Description (Descripción)
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	Description (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	Description (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":"somepassword"}` 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	Description (Descripción)
Ruta LDIFS3	`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	Description (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	Description (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 instrucciones paso a paso 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 la implementación en AWS GovCloud (US-West), 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. Inicie sesión en Consola de administración de AWS y abra la CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. Abre la plantilla.

   Para implementar en AWS GovCloud (US-West), lanza esta plantilla.
3. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar el producto en otro sitio 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	Description (Descripción)
EnvironmentName	`<res-demo>`	Un nombre exclusivo asignado a su entorno RES que comienza con res-, no más de 11 caracteres y sin letras mayúsculas.

Parámetro	Predeterminado	Description (Descripción)
AdministratorEmail		La dirección de correo electrónico del usuario que completa la configuración del producto. Este usuario también funciona como un usuario con acceso de emergencia 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 ID de AMI personalizado para usarlo en todos los hosts de la infraestructura. Los sistemas operativos compatibles actualmente son Amazon Linux 2, Amazon Linux 2023, RHEL8, RHEL9, Windows Server 2019 y 2022 (x86) y Windows 10 y 11. Para obtener más información, consulte Preparar imágenes de máquinas de Amazon (AMI).
SSHKeyPair		El key pair que se utiliza para conectarse a los hosts de la infraestructura.

Parámetro	Predeterminado	Description (Descripción)
ClientIP	*x.x.x*. 0/24 o*x.x.x*. 0/32	Filtro de direcciones IP que limita las conexiones al sistema. Puede actualizarlo ClientIpCidr después de la implementación.
ClientPrefixList		(Opcional) Proporcione una lista de prefijos gestionad a para las IP que pueden acceder directamente a la interfaz de usuario web y a SSH desde el host bastión.
IAMPermissionBoundary		(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.
IAMResourcePrefix		(Opcional) Un prefijo aplicado a los recursos de IAM implementados por el entorno RES que no - supere los 12 caracteres.
IAMResourcePath	/	(Opcional) Una ruta aplicada a los recursos de IAM implementados por el entorno RES que comienza y termina con. /

Parámetro	Predeterminado	Description (Descripción)
VpcId		ID de la VPC en la que se lanzarán las instancias.
IsLoadBalancerInternetFacing		Seleccione true para implementar un balanceador de cargas orientado a Internet (se requieren subredes públicas para el balanceador de cargas). Para las implementaciones que necesitan acceso restringido a Internet, selecciona false.
LoadBalancerSubnets		Seleccione al menos dos subredes en distintas zonas de disponibilidad donde se lanzarán los balanceadores de carga. Para las implementaciones que necesitan acceso restringido a Internet, selecciona subredes privadas. Para las implementaciones que necesitan acceso a Internet, seleccione subredes públicas. Si la pila de redes externas creó más de dos, seleccione todas las que se crearon.

Parámetro	Predeterminado	Description (Descripción)
InfrastructureHostSubnets		Seleccione al menos dos subredes privadas en distintas zonas de disponibilidad donde se lanzarán los hosts de infraestructura. Si la pila de redes externas creó más de dos, seleccione todas las que se hayan creado.
VdiSubnets		Seleccione al menos dos subredes privadas en distintas zonas de disponibilidad donde se lanzarán las instancias de VDI. Si la pila de redes externas creó más de dos, seleccione todas las que se hayan creado.
ActiveDirectoryName	*corp.res.com*	Dominio para Active Directory. No es necesario que coincida con el nombre de dominio del portal.
ADShortName	*corp*	Nombre abreviado de Active Directory. 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.

Parámetro	Predeterminado	Description (Descripción)
URI de conexión LDAP		Una única ruta ldap://qu e apunta al servidor host de Active Directory. Si implementó los recursos externos automatizados con el dominio AD predeterm inado, puede usar ldap: // corp.res.com.
ServiceAccountCred entialsSecretArn		Proporcione un ARN secreto que contenga el nombre de usuario y la contraseña del usuario de la cuenta de servicio de Active Directory , con el formato de un par de nombre de usuario y contraseña. key/value
SOU del usuario		Unidad organizativa dentro de AD para los usuarios que se sincronizarán.
Grupo SOU		Unidad organizativa dentro de AD para los grupos que se sincronizarán.
SudoersGroupName	Administradores de RES	Nombre de grupo que contiene a todos los usuarios con acceso sudo 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.

Parámetro	Predeterminado	Description (Descripción)
DomainTLSCertificateSecretARN		(Necesario para LDAPS) Proporcione un ARN secreto de certificado TLS de dominio para habilitar la comunicación TLS con AD. Déjelo en blanco si no utiliza LDAPS.
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.
Deshabilita Adjoin	False	Para evitar que los hosts Linux se unan al dominio del directorio, cambie a True. De lo contrario, deje la configuración predeterminada de False.
ServiceAccountUserDN		Proporcione el nombre distintivo (DN) del usuario de la cuenta de servicio en el Directorio.

Parámetro	Predeterminado	Description (Descripción)
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.
CustomDomainNameforVDI		(Opcional) Subdominio utilizado por el portal web para proporcionar enlaces a la parte de VDI del sistema.
ACMCertificateARNf orWebApp		(Opcional) Si se utiliza la configuración predeterm inada, 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 aplicació n web, consulte. Guía de configuración

Parámetro	Predeterminado	Description (Descripción)
CertificateSecretARNforVDI		(Opcional) Este secreto de ARN almacena el certifica do público del certificado público de su portal web. Si establece un nombre de dominio de portal para sus recursos externos automatiz ados, puede encontrar este valor en la pestaña Resultados de la pila res-bi.
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.
CognitoUserPoolId		Grupo de usuarios de Cognito para la autentica ción de usuarios y clientes. RES creará uno de forma predeterminada si no se especifica ningún grupo de usuarios de Cognito.

Parámetro	Predeterminado	Description (Descripción)
CognitoUserPoolDomainUrl		Dominio del grupo de usuarios de Cognito para el inicio de sesión gestionado. Este parámetro debe proporcionarse cuando `CognitoUserPoolId` se especifique.

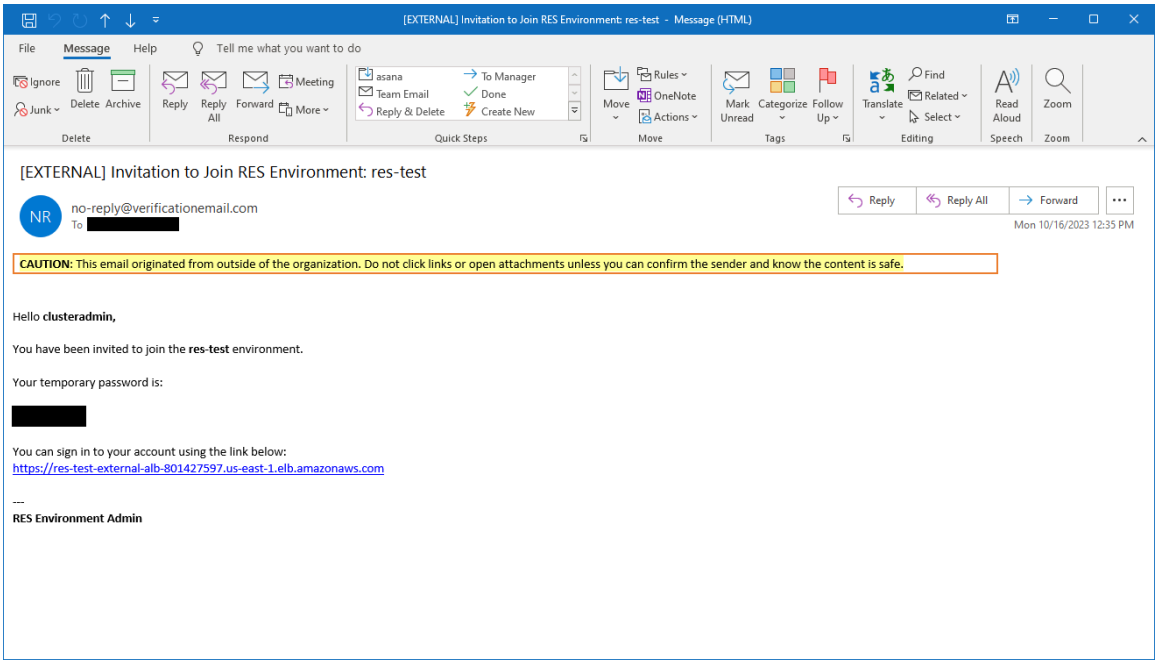
5. En Configurar opciones de pila → Etiquetas: opcional, añada las etiquetas (pares clave-valor) que desee aplicar a los recursos desplegados en RES. RES conserva la clave `Name` de etiqueta y no se pueden usar como claves de etiqueta. `res:*`
6. Elija Create stack (Crear pila) para implementar la pila.

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

> **Important**
>
> Usted es responsable de aplicar los parches a sus infrastructure/VDI hosts después de la implementación.

Paso 2: inicie sesión por primera vez

Una vez que la gama de productos se despliegue 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.



Después de iniciar sesión por primera vez, puede 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` se trata de una cuenta única: puede utilizarla 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.

Actualizar 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 última versión 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

> **Warning**
>
> La actualización de la versión 2025.06 de RES a la 2025.06.01 requiere utilizar este proceso. Actualizaciones de versiones principales

Para las actualizaciones de versiones menores de RES, no es necesaria una nueva instalación. Puede actualizar la pila RES existente actualizando su CloudFormation plantilla. Compruebe la versión de su entorno RES actual 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 CloudFormation plantilla más reciente enthe section called “Paso 1: lanza el producto”.
2. Abre la 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 Consola de administración de AWS 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 para conservarlos.

Uso del Consola de administración de AWS

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 grupo de seguridad de almacenamiento compartido

> **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 Consola de administración de AWS 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. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. https://console.aws.amazon.com/ec2/
4. Elimine la `<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 Consola de administración de AWS 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 AWS producto con Research and Engineering Studio.

Temas

Administración de identidades

Research and Engineering Studio puede utilizar cualquier proveedor de identidad compatible con SAML 2.0. Para utilizar Amazon Cognito como un directorio de usuarios nativo que permite a los usuarios iniciar sesión en el portal web y en los VDI basados en Linux con identidades de usuario de Cognito, consulte. Configuración de los usuarios de Amazon Cognito Si implementó RES con recursos externos o planea usar el centro de identidades de IAM, consulte. Configuración del inicio de sesión único (SSO) con el Centro de identidad de IAM 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)

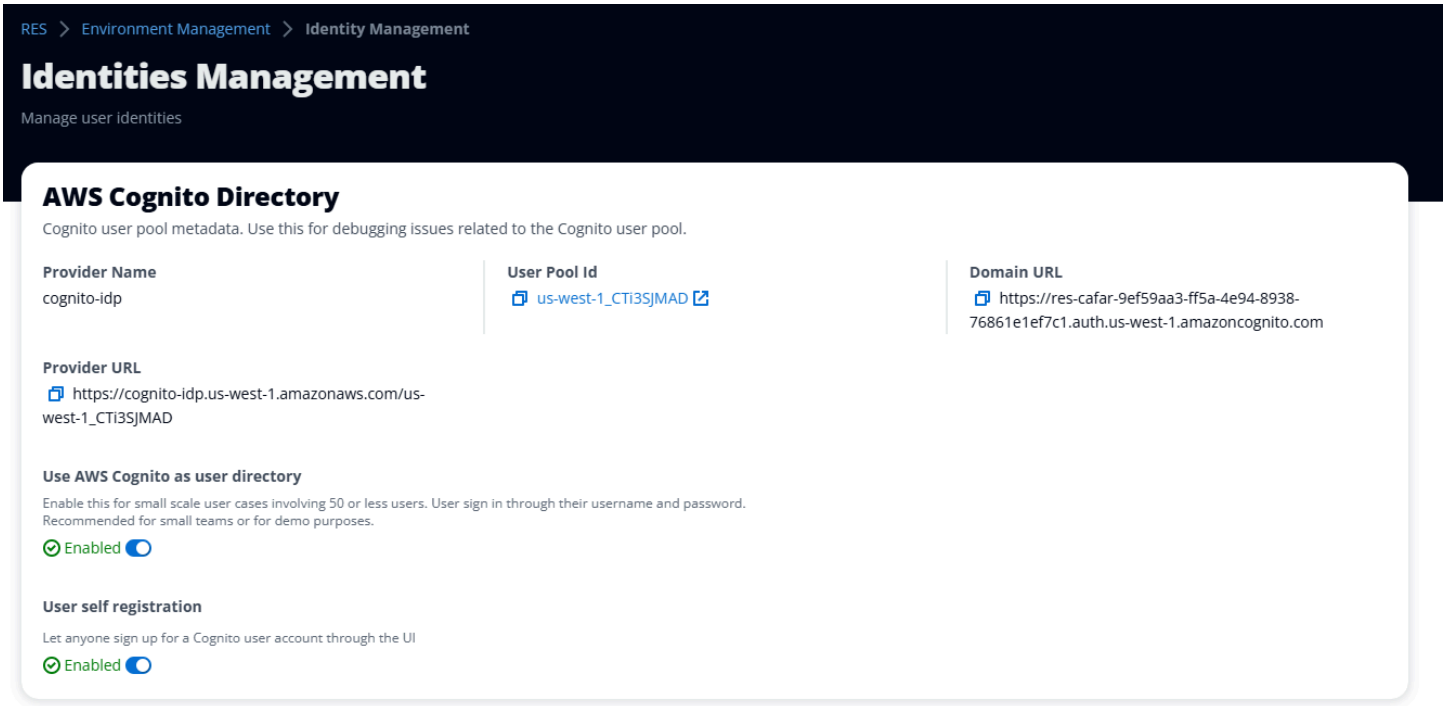
Temas

Configuración de los usuarios de Amazon Cognito

Research and Engineering Studio (RES) le permite configurar Amazon Cognito como un directorio de usuarios nativo. Esto permite a los usuarios iniciar sesión en el portal web y en los Linux-based VDI con las identidades de usuario de Amazon Cognito. Los administradores pueden importar varios usuarios al grupo de usuarios mediante un archivo csv de la AWS consola. Para obtener más información sobre la importación masiva de usuarios, consulte Importación de usuarios a grupos de usuarios desde un archivo CSV en la Guía para desarrolladores de Amazon Cognito. RES admite el uso conjunto de un directorio de usuarios Cognito-based nativo de Amazon y un SSO.

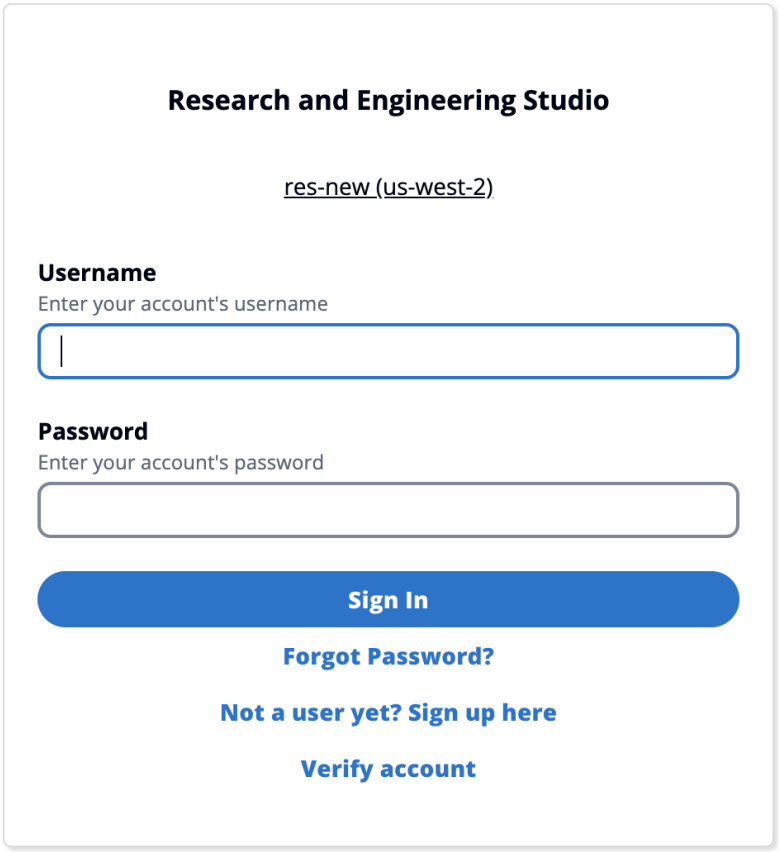
Configuración administrativa

Como administrador de RES, para configurar el entorno RES para usar Amazon Cognito como directorio de usuarios, active el botón Usar Amazon Cognito como directorio de usuarios en la página de administración de identidades, a la que se puede acceder desde la página de administración del entorno. Para permitir que los usuarios se registren automáticamente, active el botón de registro automático de usuarios en esa misma página.



Flujo de inicio de sesión de up/sign los usuarios

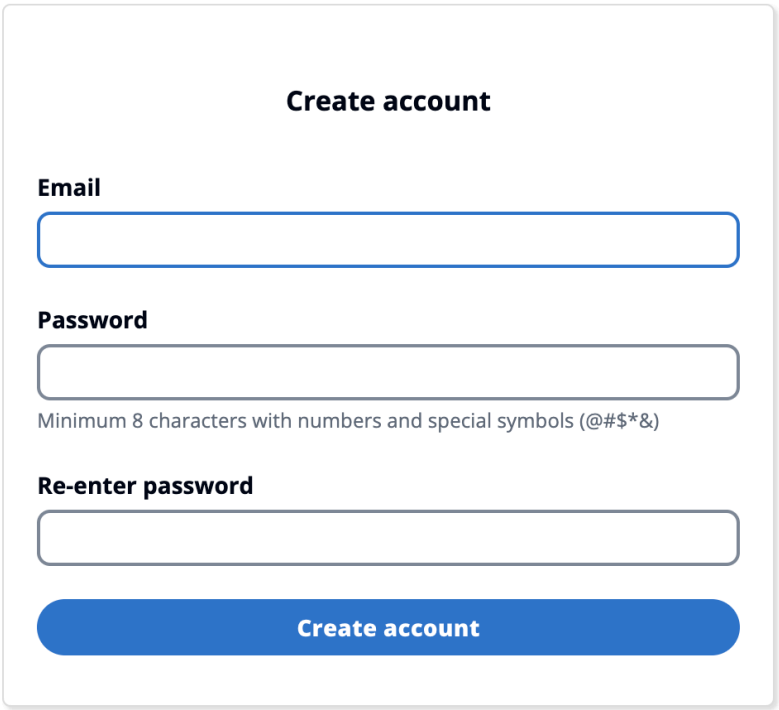
Si el registro automático de usuarios está activado, puede proporcionar a sus usuarios la URL de su aplicación web. Allí, los usuarios encontrarán una opción que dice ¿Aún no eres usuario? Inscríbase aquí.



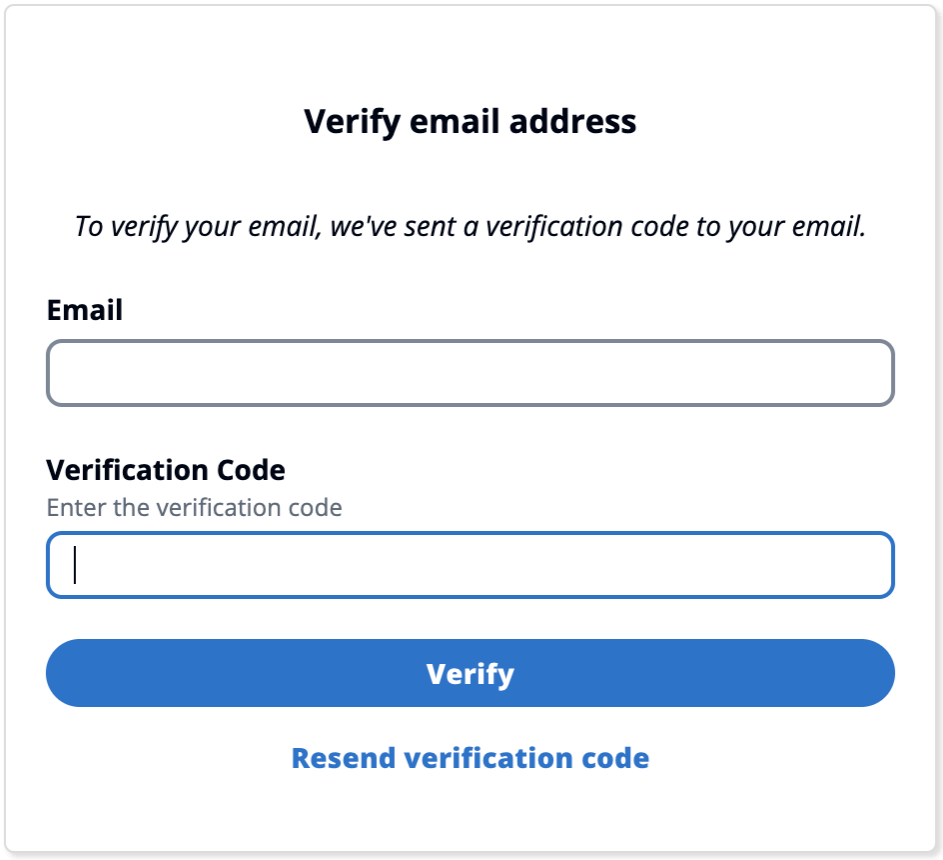
Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

Flujo de registro

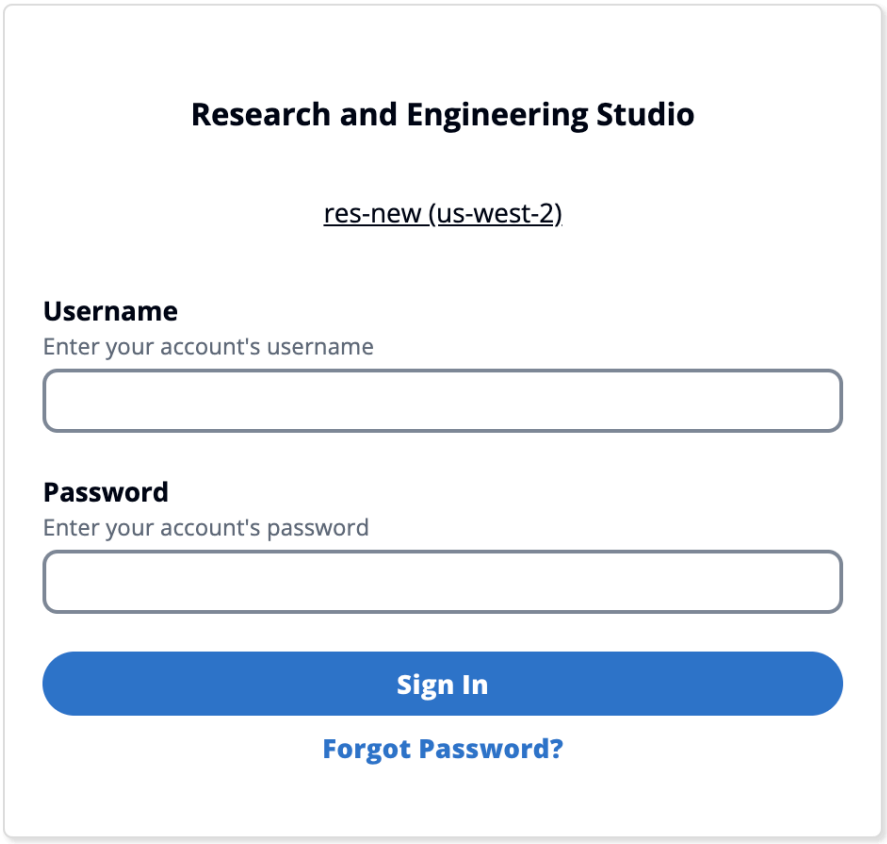
Usuarios que elijan ¿Aún no eres usuario? Si se registran aquí, se les pedirá que introduzcan su correo electrónico y contraseña para crear una cuenta.



Como parte del proceso de registro, se les pedirá a los usuarios que introduzcan el código de verificación recibido en su correo electrónico para completar el proceso de registro.

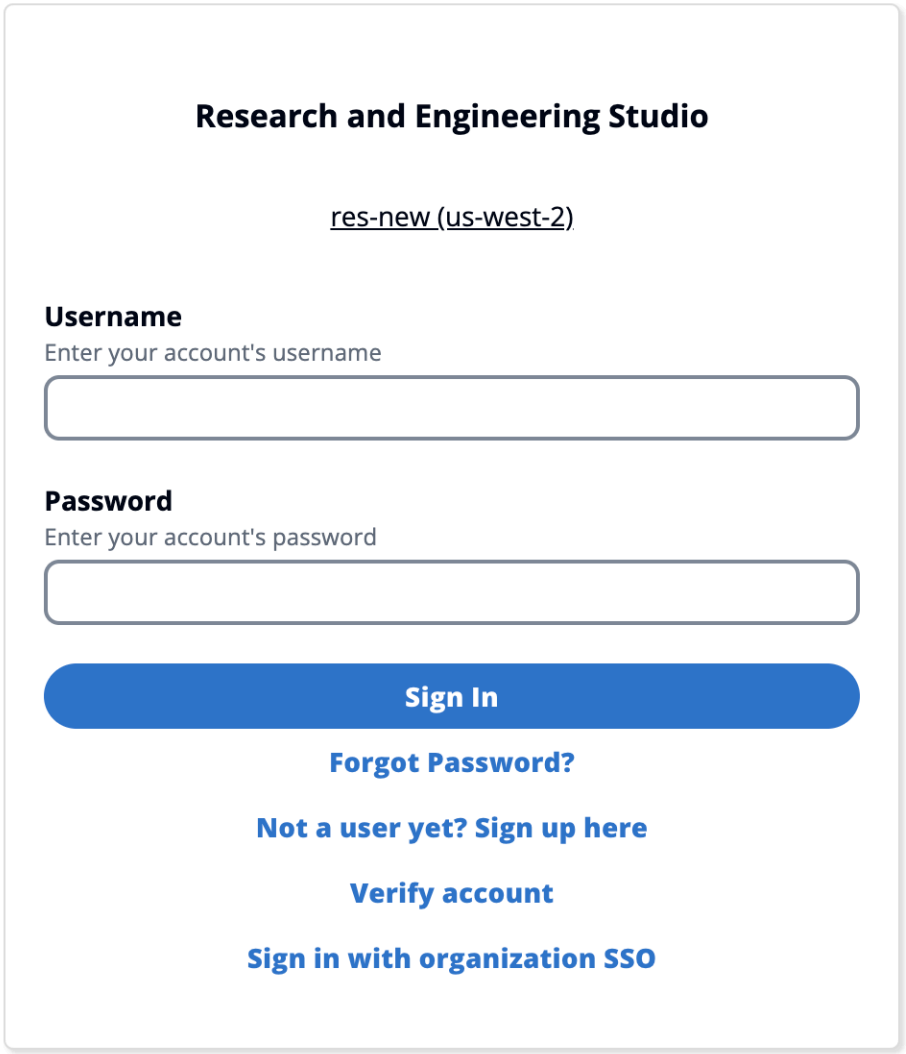


Si el registro automático está desactivado, los usuarios no verán el enlace de registro. Los administradores deben configurar los usuarios en Amazon Cognito fuera de RES. (Consulte Creación de cuentas de usuario como administrador en la Guía para desarrolladores de Amazon Cognito).



Opciones de página de inicio de sesión

Si tanto el SSO como Amazon Cognito están habilitados, aparecerá la opción Iniciar sesión con el SSO de la organización. Cuando los usuarios hagan clic en esa opción, se les redirigirá a su página de inicio de sesión única. De forma predeterminada, los usuarios se autenticarán con Amazon Cognito si está activado.



Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

Restricciones

- El nombre de su grupo de Amazon Cognito puede tener un máximo de seis letras; solo se aceptan letras minúsculas.
- El registro en Amazon Cognito no permitirá dos direcciones de correo electrónico con el mismo nombre de usuario pero con una dirección de dominio diferente.
- Si Active Directory y Amazon Cognito están habilitados y el sistema detecta un nombre de usuario duplicado, solo los usuarios de Active Directory podrán autenticarse. Los administradores deben tomar medidas para no configurar nombres de usuario duplicados entre Amazon Cognito y su Active Directory.

- Los usuarios de Cognito no podrán lanzar Windows-based VDI, ya que RES no admite la Cognito-based autenticación de Amazon para instancias de Windows.

Grupo de administradores para usuarios de Amazon Cognito

De forma predeterminada, RES concede a los usuarios de Cognito el privilegio de administrador del `admins` grupo. Para añadir usuarios al grupo de Cognito`admins`:

1. Navegue hasta la consola de Amazon Cognito y elija el grupo de usuarios existente utilizado para RES.
2. Vaya a Grupos en Administración de usuarios y, a continuación, seleccione Crear un grupo.
3. En la página Crear un grupo, en Nombre del grupo, introduzca`admins`.
4. Seleccione el `admins` grupo que ha creado y elija Añadir usuario al grupo para añadir usuarios de Cognito.
5. Inicie la sincronización de Cognito manualmente de la siguiente manera. Sincronización

Tras una sincronización correcta de Amazon Cognito, los usuarios añadidos al `admins` grupo recibirán privilegios de administrador.

Sincronización

RES sincroniza su base de datos con la información de usuarios y grupos de Amazon Cognito cada hora. A todos los usuarios que pertenezcan al grupo «administradores» se les otorgará el privilegio de sudo en sus VDI.

También puede iniciar la sincronización manualmente desde la consola Lambda.

Inicie el proceso de sincronización manualmente:

1. Abra la consola de Lambda.
2. Busca la Lambda de sincronización de Cognito. Esta Lambda sigue esta convención de nomenclatura:. *`{RES_ENVIRONMENT_NAME}`*`_cognito-sync-lambda`
3. Seleccione Probar.
4. En la sección Evento de prueba, selecciona el botón de prueba en la parte superior derecha. No importa el formato del cuerpo del evento.

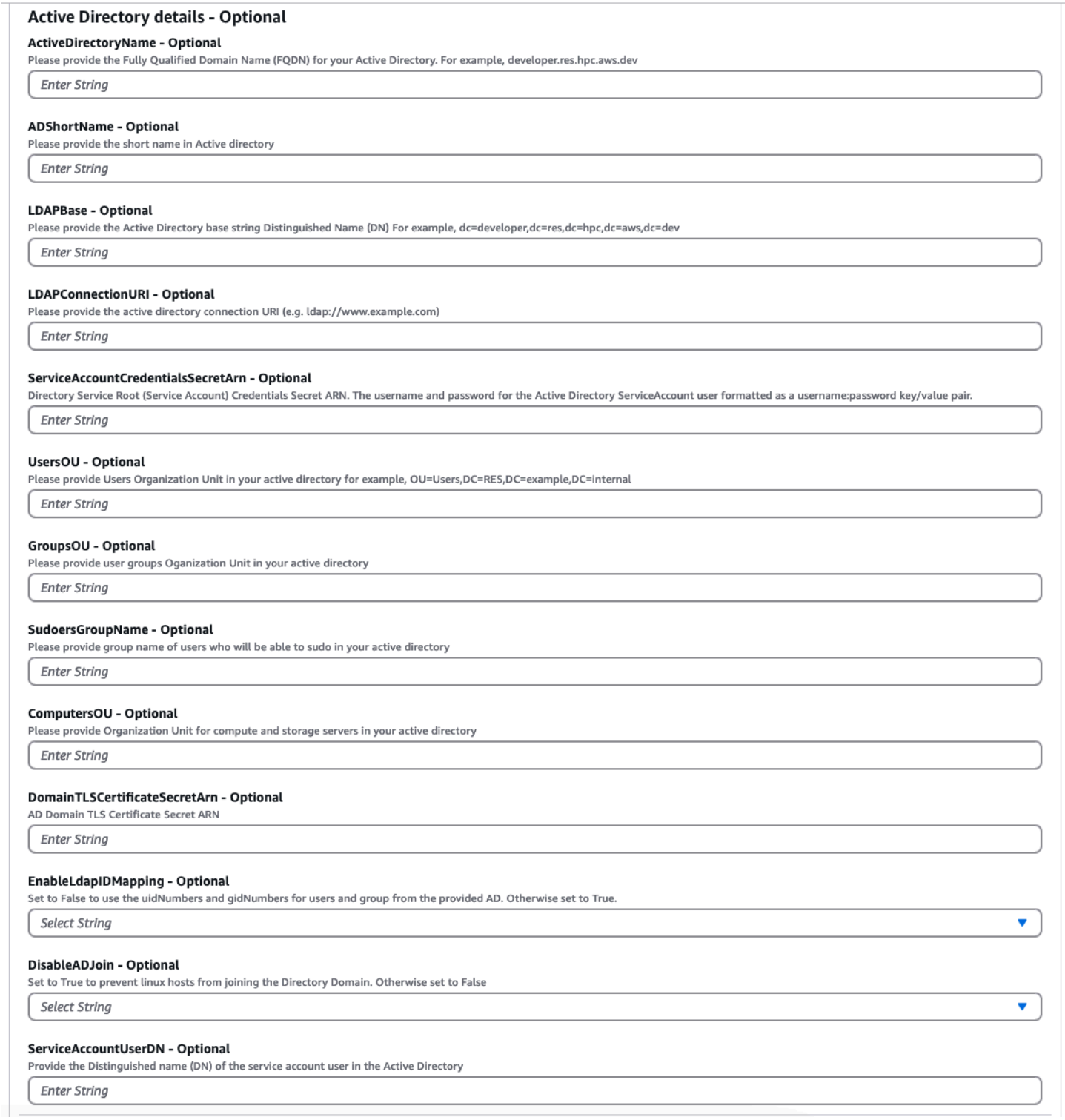
Consideraciones de seguridad para Cognito

Antes de la versión 2024.12, el registro de actividad de los usuarios, que forma parte de la función del plan Amazon Cognito Plus, estaba habilitado de forma predeterminada. Esta función se eliminó de la implementación básica para ahorrar costos a los clientes que desean probar RES. Puede volver a activar esta función según sea necesario para ajustarla a la configuración de seguridad en la nube de su organización.

Sincronización de Active Directory

Configuración de tiempo de ejecución

Todos los AWS CloudFormation parámetros relacionados con Active Directory (AD) son opcionales durante la instalación.

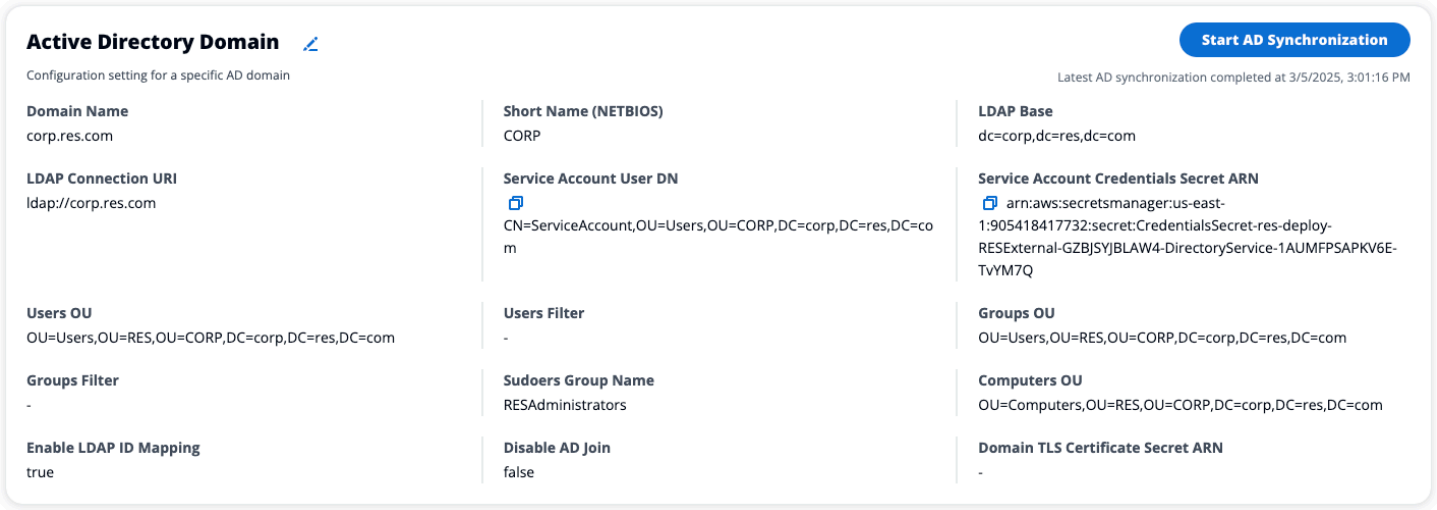


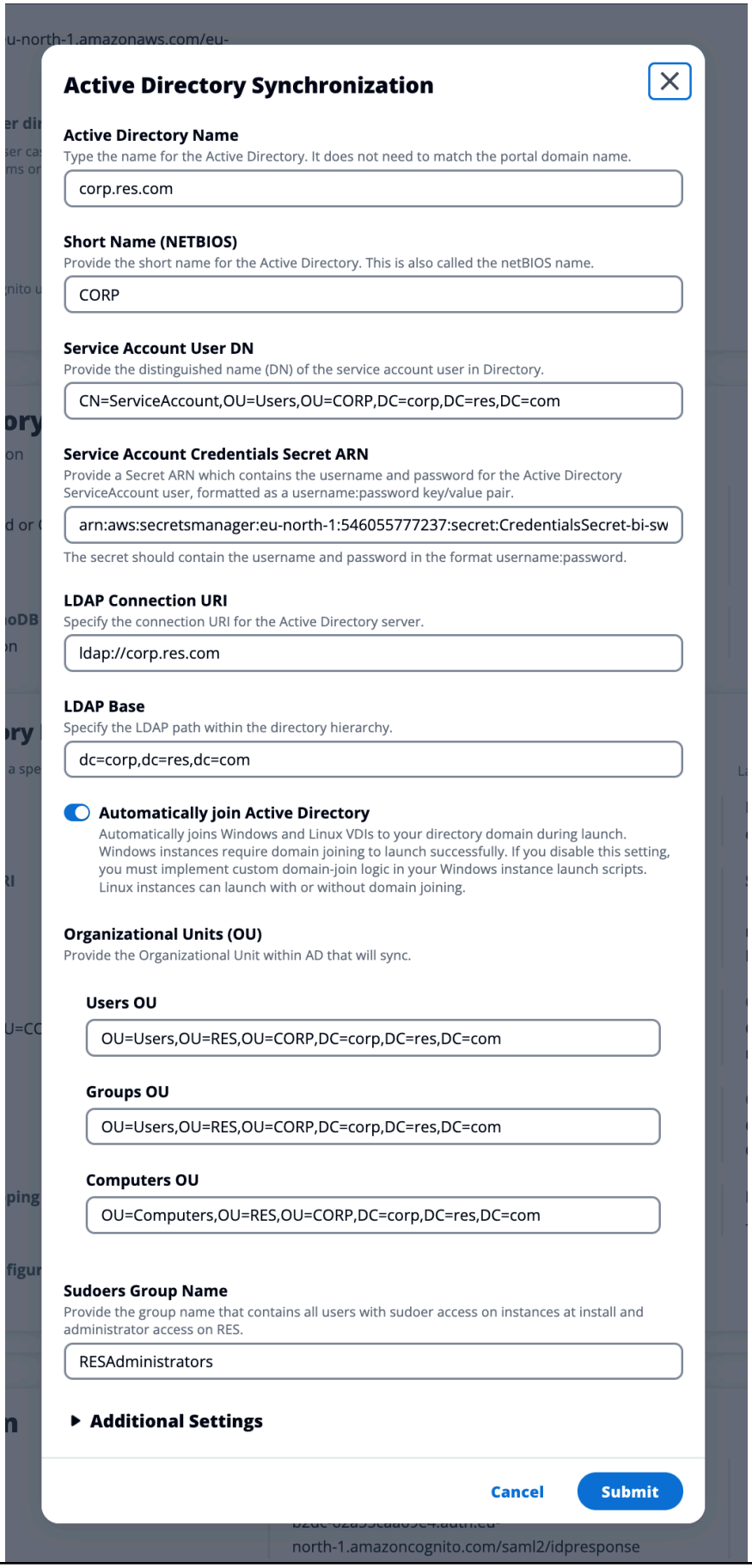
Para cualquier ARN secreto proporcionado en tiempo de ejecución (por ejemplo, `ServiceAccountCredentialsSecretArn` o`DomainTLSCertificateSecretArn`), asegúrese de añadir las siguientes etiquetas al secreto para que RES obtenga permisos para leer el valor secreto:

- clave: `res:EnvironmentName`, valor: *`<your RES environment name>`*
- clave: `res:ModuleName`, valor: `directoryservice`

Cualquier actualización de la configuración de AD en el portal web se recogerá automáticamente durante la próxima sincronización de AD programada (cada hora). Es posible que los usuarios tengan que volver a configurar el SSO después de cambiar la configuración de AD (por ejemplo, si cambian a un AD diferente).

Tras la instalación inicial, los administradores pueden ver o editar la configuración de AD en el portal web de RES, en la página de administración de identidades:




Active Directory Synchronization
Active Directory Name
Type the name for the Active Directory. It does not need to match the portal domain name.
corp.res.com
Short Name (NETBIOS)
Provide the short name for the Active Directory. This is also called the netBIOS name.
CORP
Service Account User DN
Provide the distinguished name (DN) of the service account user in Directory.
CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com
Service Account Credentials Secret ARN
Provide a Secret ARN which contains the username and password for the Active Directory ServiceAccount user, formatted as a username:password key/value pair.
arn:aws:secretsmanager:eu-north-1:546055777237:secret:CredentialsSecret-bi-sw
The secret should contain the username and password in the format username:password.
LDAP Connection URI
Specify the connection URI for the Active Directory server.
ldap://corp.res.com
LDAP Base
Specify the LDAP path within the directory hierarchy.
dc=corp,dc=res,dc=com
Automatically join Active Directory
Automatically joins Windows and Linux VDIs to your directory domain during launch. Windows instances require domain joining to launch successfully. If you disable this setting, you must implement custom domain-join logic in your Windows instance launch scripts. Linux instances can launch with or without domain joining.
Organizational Units (OU)
Provide the Organizational Unit within AD that will sync.
Users OU
OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
Groups OU
OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
Computers OU
OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com
Sudoers Group Name
Provide the group name that contains all users with sudoer access on instances at install and administrator access on RES.
RESAdministrators
Additional Settings
Cancel
Submit

Únase automáticamente a Active Directory

Los administradores pueden configurar la opción Unirse automáticamente a Active Directory para controlar el comportamiento de unión al dominio del directorio durante el lanzamiento de la VDI.

Opciones de configuración:

- Habilitado: une automáticamente los VDI de Windows y Linux al dominio del directorio durante el lanzamiento.
- Desactivado: desactiva la unión automática a un dominio. Las instancias de Linux se pueden lanzar con o sin la unión de un dominio. Las instancias de Windows requieren la unión de dominios para lanzarse correctamente, por lo que los administradores deben incluir la lógica de unión de dominios en sus scripts de lanzamiento personalizados.

> **Important**
>
> Si deshabilita esta configuración, compruebe que los scripts de lanzamiento personalizados de las instancias de Windows incluyan la lógica de unión a dominios necesaria.

Ajustes adicionales

Filtros

Los administradores pueden filtrar los usuarios o grupos para sincronizarlos mediante las opciones Filtro de usuarios y Filtro de grupos. Los filtros deben seguir la sintaxis del filtro LDAP. Un filtro de ejemplo es:

```
(sAMAccountname=<user>)
```

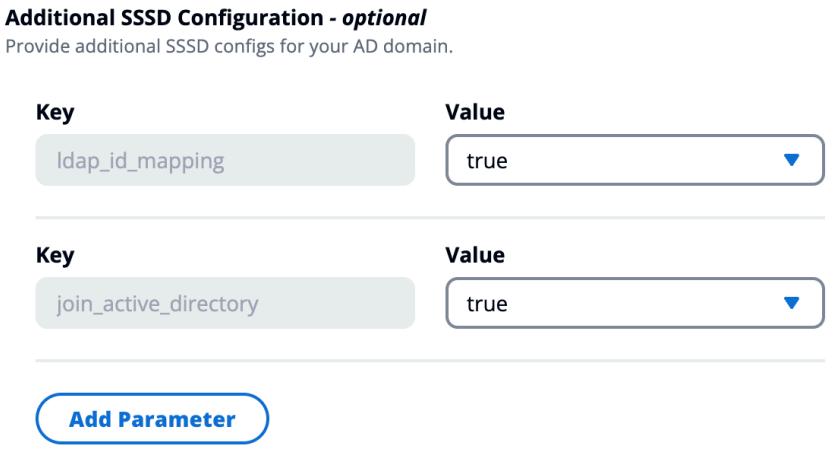
Parámetros SSSD personalizados

Los administradores pueden proporcionar un diccionario de pares clave-valor que contenga parámetros y valores de SSSD para escribirlos en la `[domain_type/DOMAIN_NAME]` sección del archivo de configuración de SSSD de las instancias de clúster. RES aplica las actualizaciones de SSSD automáticamente: reinicia el servicio SSSD en las instancias del clúster y activa el proceso de sincronización de AD.

Algunas de las configuraciones de SSSD personalizadas más comunes son:

- `enumerate`- Configúrelo en «true» para almacenar en caché todas las entradas de usuarios y grupos del servicio de directorio. Si se desactiva, se podría retrasar un poco el primer inicio de sesión de los usuarios.
- `ldap_id_mapping`- Configúrelo en «true» para asignar los ID de LDAP/AD usuario y grupo a los UID y GID locales del sistema Linux. Habilitar esto puede mejorar la compatibilidad con los scripts y aplicaciones POSIX existentes.

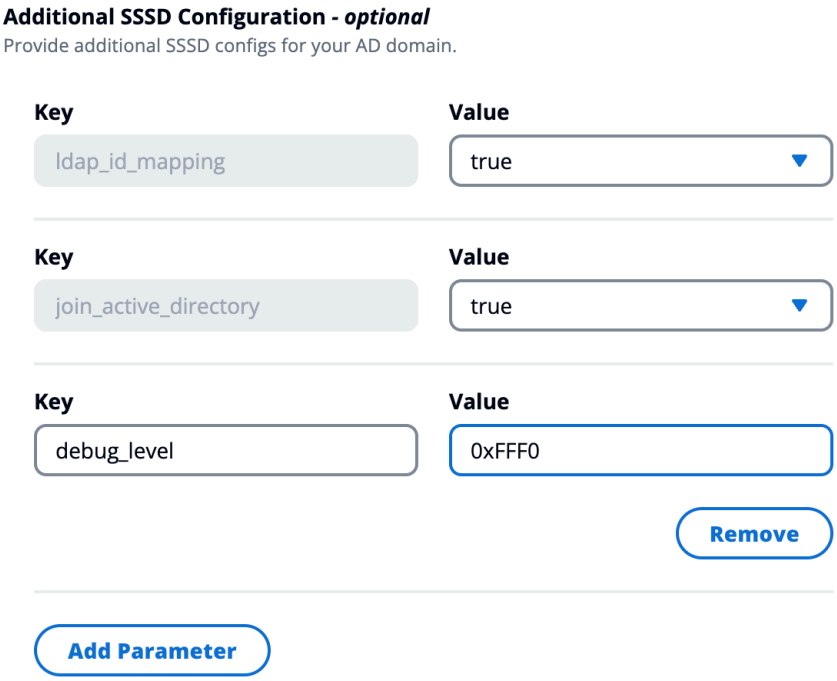
Para obtener una descripción completa del archivo de configuración SSSD, consulte las páginas de manual de Linux de. `SSSD`



Los parámetros y valores del SSSD deben ser compatibles con la configuración del RES SSSD, tal como se describe aquí:

- `id_provider`está configurado internamente por RES y no debe modificarse.
- Las configuraciones relacionadas con AD`ldap_uri`, incluidas`ldap_search_base`, `ldap_default_bind_dn` `ldap_default_authtok` se establecen en función de las demás configuraciones de AD proporcionadas y no deben modificarse.

El siguiente ejemplo habilita el nivel de depuración de los registros SSSD:

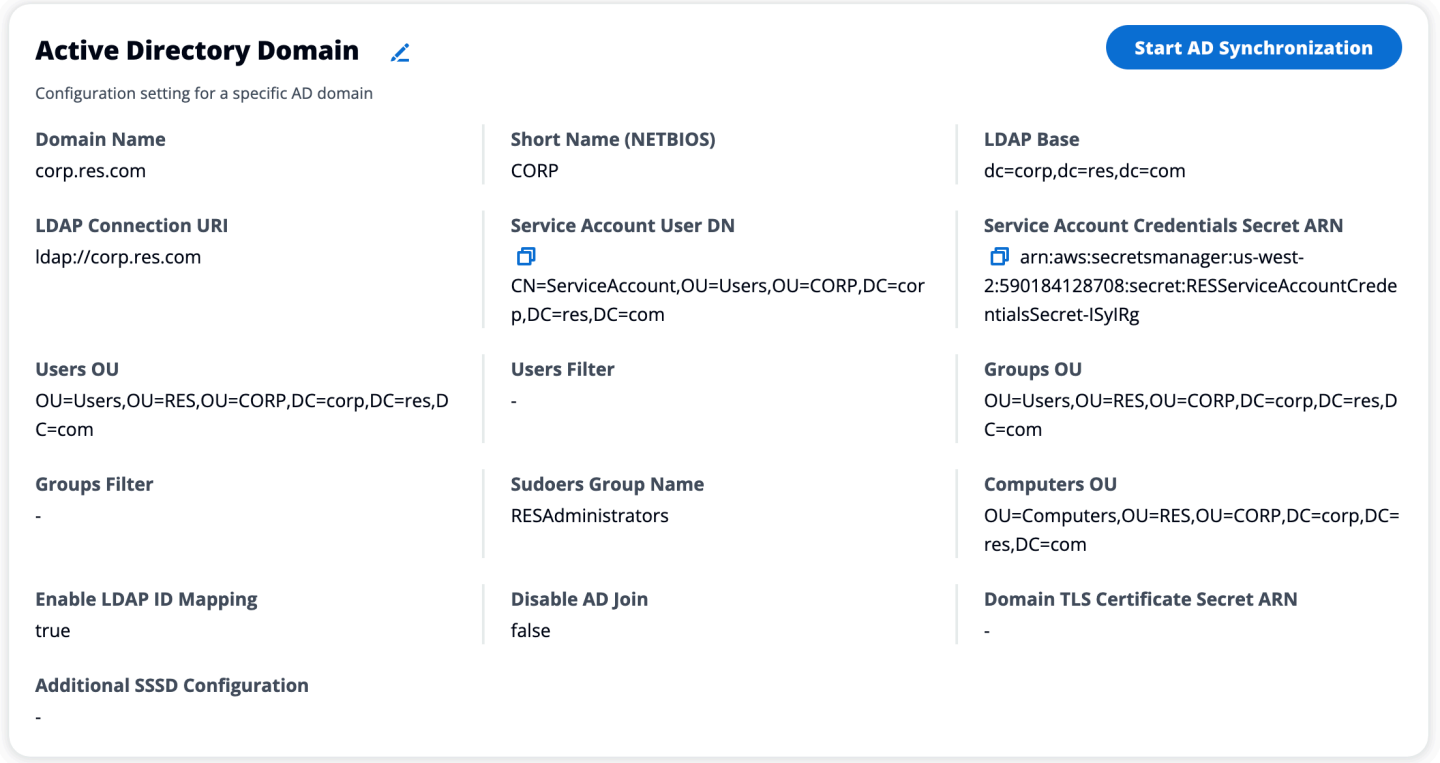


Actualización del correo electrónico tras la sincronización inicial de AD (versión 2025.09 y versiones posteriores)

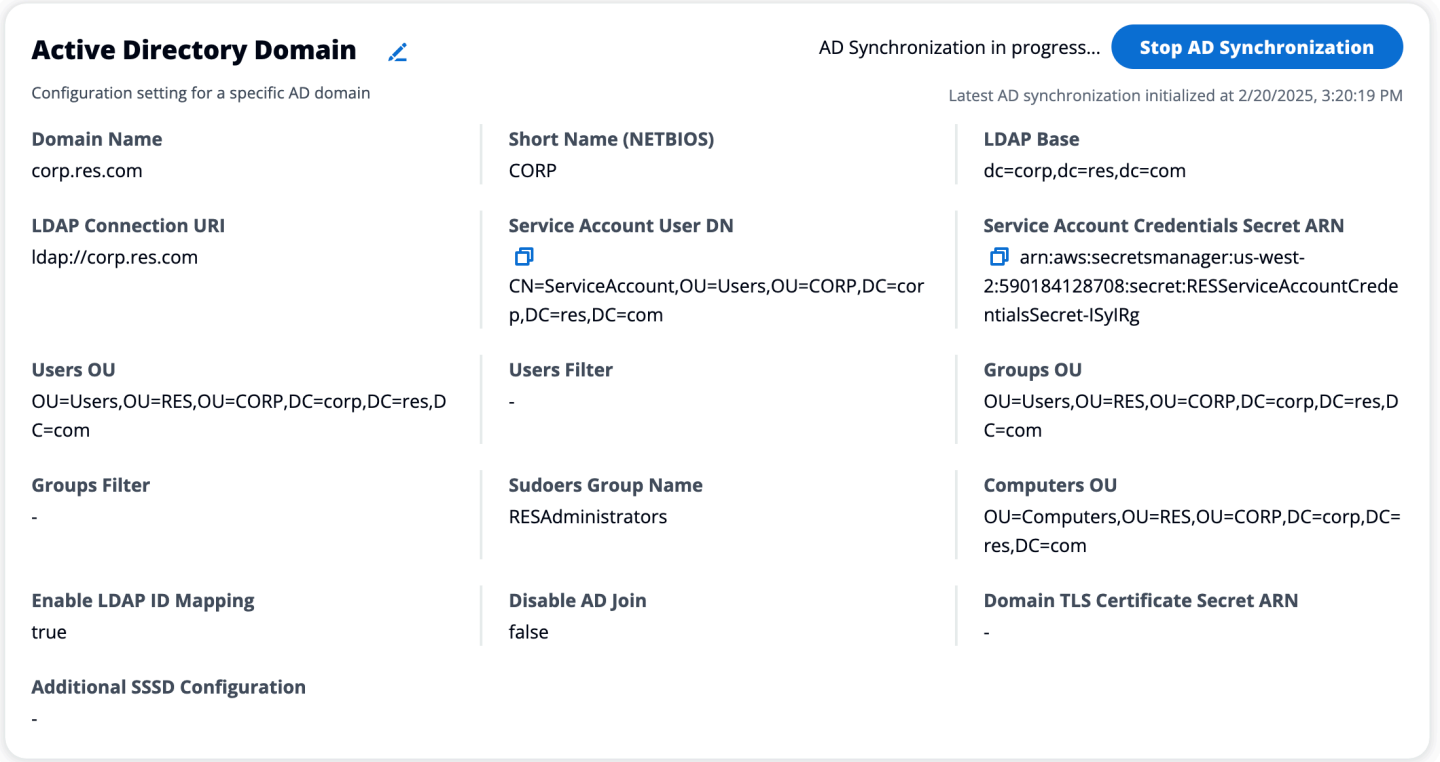
Si la dirección de correo electrónico de un usuario de Active Directory ha cambiado, los administradores pueden iniciar la sincronización de AD manualmente o esperar a que se recoja el cambio y se sincronice con RES en la siguiente sincronización de AD programada.

Cómo iniciar o detener la sincronización manualmente (versión 2025.03 y versiones posteriores)

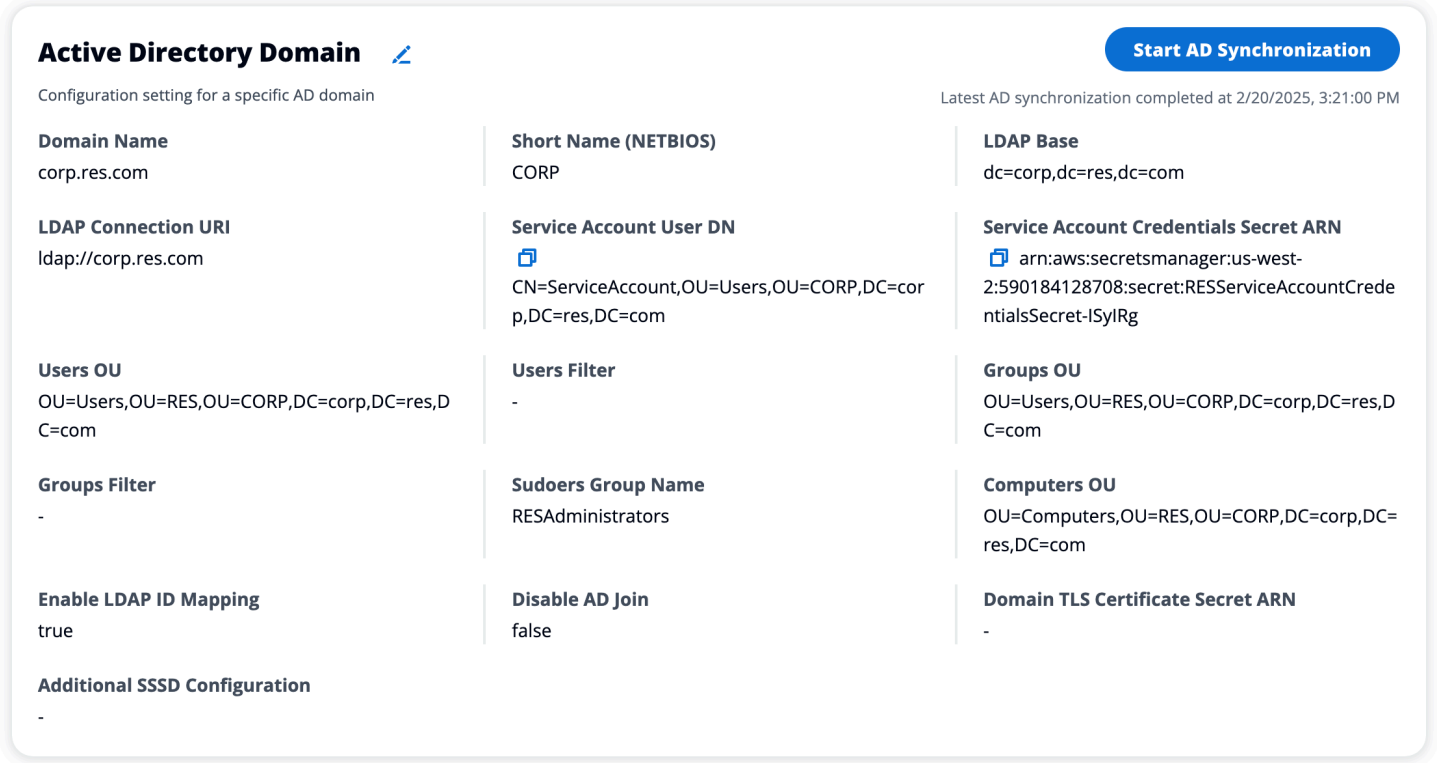
Vaya a la página de administración de identidades y pulse el botón Iniciar la sincronización de AD en el contenedor de dominios de Active Directory para activar una sincronización de AD bajo demanda.



Para detener una sincronización de AD en curso, seleccione el botón Detener la sincronización de AD en el contenedor de dominios de Active Directory.



También puede comprobar el estado de la sincronización de AD y la última hora de sincronización en el contenedor de dominios de Active Directory.



Cómo ejecutar la sincronización manualmente (versiones 2024.12 y 2024.12.01)

El proceso de sincronización de Active Directory se ha trasladado del host de infraestructura de Cluster Manager a una tarea única de Amazon Elastic Container Service (ECS) en segundo plano. El proceso está programado para ejecutarse cada hora y puede encontrar una tarea de ECS en ejecución en la consola de Amazon ECS, en el `<res-environment-name>-ad-sync-cluster` clúster, mientras está en curso.

Para lanzarla manualmente:

1. Navegue hasta la consola de Lambda y busque la lambda llamada. `<res-environment>-scheduled-ad-sync`
2. Abra la función Lambda y vaya a Probar
3. En el JSON de eventos, introduzca lo siguiente:

```
{
    "detail-type": "Scheduled Event"
}
```

4. Seleccione Probar
5. Observe los registros de la tarea de sincronización de AD en ejecución en CloudWatch→ Grupos de registros →/`<environment-name>`/`ad-sync`. Verás los registros de cada una de las tareas de ECS en ejecución. Seleccione la más reciente para ver los registros.

> **Note**
>
> - Si cambias los parámetros de AD o añades filtros de AD, RES añadirá los nuevos usuarios según los parámetros recién especificados y eliminará los usuarios que se hayan sincronizado previamente y que ya no estén incluidos en el espacio de búsqueda de LDAP.
> - RES no puede eliminar un usuario o grupo que esté asignado activamente a un proyecto. Debe eliminar usuarios de los proyectos para que RES los elimine del entorno.

Configuración del SSO

Una vez proporcionada la configuración de AD, los usuarios deben configurar el modo Single Sign-On (SSO) para poder iniciar sesión en el portal web de RES como usuarios de AD. La configuración del SSO se trasladó de la página de configuración general a la nueva página de administración de identidades. Para obtener más información sobre la configuración del SSO, consulte. Administración de identidades

Configuración del inicio de sesión único (SSO) con el Centro de identidad de IAM

Si aún no tiene un centro de identidad conectado al Active Directory administrado, comience conPaso 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 una GovCloud región, 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. Elija Activar con AWS Organizations.
5. Elija Continuar.

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

Conexión del Centro de Identidad de IAM 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, elija Acciones y elija Cambiar fuente de identidad.
3. En Directorios existentes, selecciona tu directorio.
4. Elija Siguiente.
5. Revise los cambios e **`ACCEPT`** introdúzcalos en el cuadro de confirmación.
6. Elija Cambiar fuente de identidad.

Sincronizar usuarios y grupos con el centro de identidad

Una vez que se hayan completado Conexión del Centro de Identidad de IAM 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. Elija 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. Seleccione los usuarios para los que desea habilitar el acceso.
3. Elija Habilitar el acceso de los usuarios.

Paso 2: Conectarse a un centro de identidad

Configuración de la aplicación en el Centro de Identidad de IAM

1. Abra la consola de IAM Identity Center.
2. Elija Aplicaciones.
3. Elija Añadir aplicación.
4. En las preferencias de configuración, elija Tengo una aplicación que quiero configurar.
5. En Tipo de aplicación, seleccione SAML 2.0.
6. Elija 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. Seleccione la pestaña Proveedor de identidades.
    c. En Single Sign-On, 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 identidades, abra los detalles de la aplicación que ha creado.
2. Elija Acciones y, a continuación, elija Editar asignaciones de atributos.
3. En Asunto, introduzca **`${user:email}`**.
4. En Formato, selecciona Dirección de correo electrónico.
5. Seleccione Agregar nueva asignación de atributos.
6. En el campo Atributo de usuario de la aplicación, introduce «correo electrónico».
7. En Asignar a este valor de cadena o atributo de usuario del Centro de Identidad de IAM, introduzca. **`${user:email}`**
8. En Formato, escriba «sin especificar».
9. Seleccione Save changes (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. Seleccione los usuarios a los que desee asignar el acceso a la aplicación.
3. Elija Assign users (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 Individual Sign-On, 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. Introduzca la URL que copió durante el proceso[Configuración de la aplicación en el Centro de Identidad de IAM](#).
    e. En el atributo de correo electrónico del proveedor, introduce «correo electrónico».
    f. Seleccione 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 identidad 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. [Configuración del inicio de sesión único (SSO) con el Centro de identidad de IAM](#)

> **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](#)
- [Configure RES para usar su proveedor de identidad](#)
- [Configurar el proveedor de identidades en un entorno que no sea de producción](#)
- [Depuración de problemas de IdP de SAML](#)

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="https://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

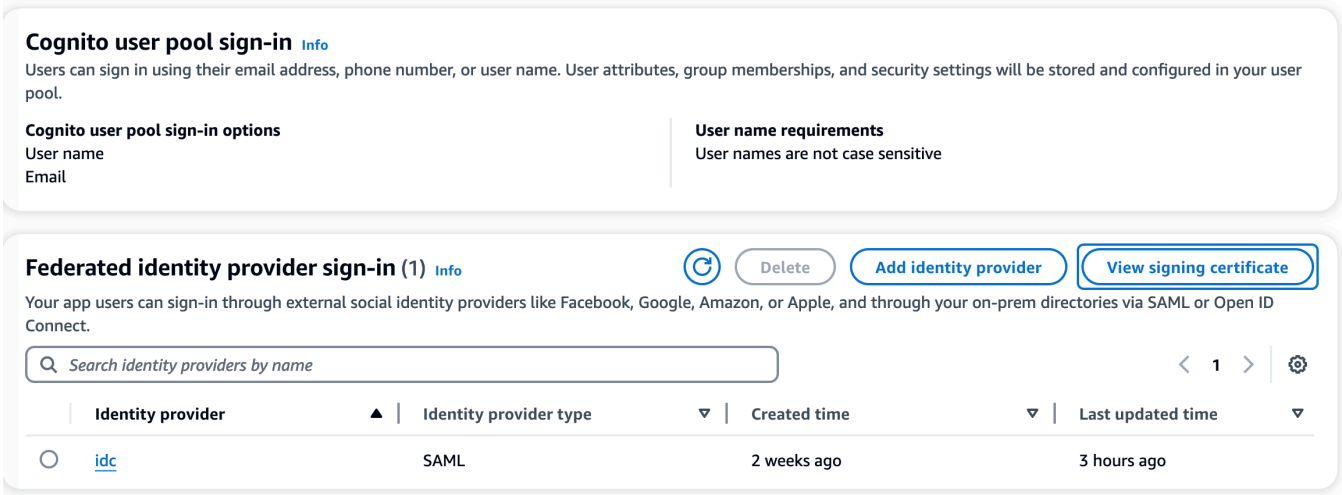
   1. Inicie sesión en RES como administrador o administrador de clústeres.
   2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.
   3. Elija la URL del dominio.

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.

2. Seleccione su grupo de usuarios. Su grupo de usuarios debería serlo`res-<environment name>-user-pool`.
3. Seleccione la pestaña de Sign-in experiencia.
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.

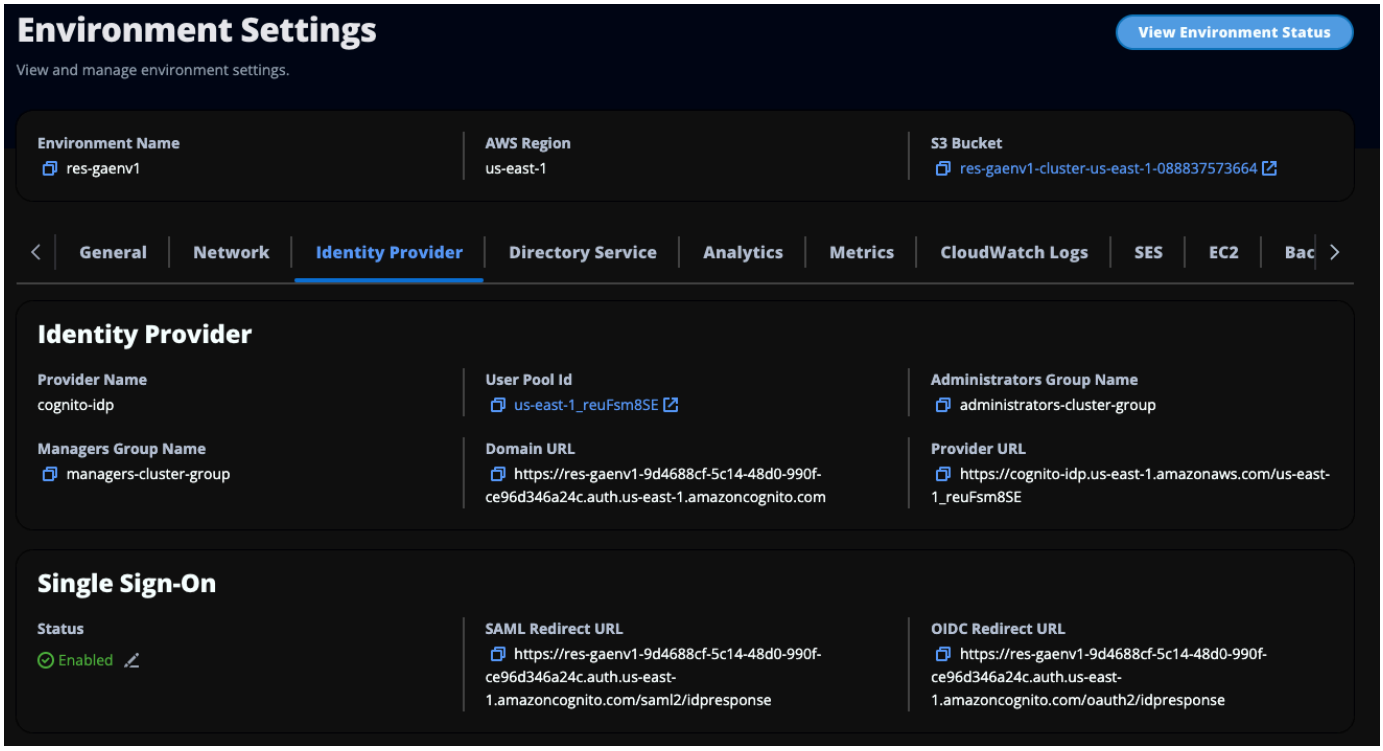
> **Note**
>
> Esto no se aplica a Keycloak ni a IDC.

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.

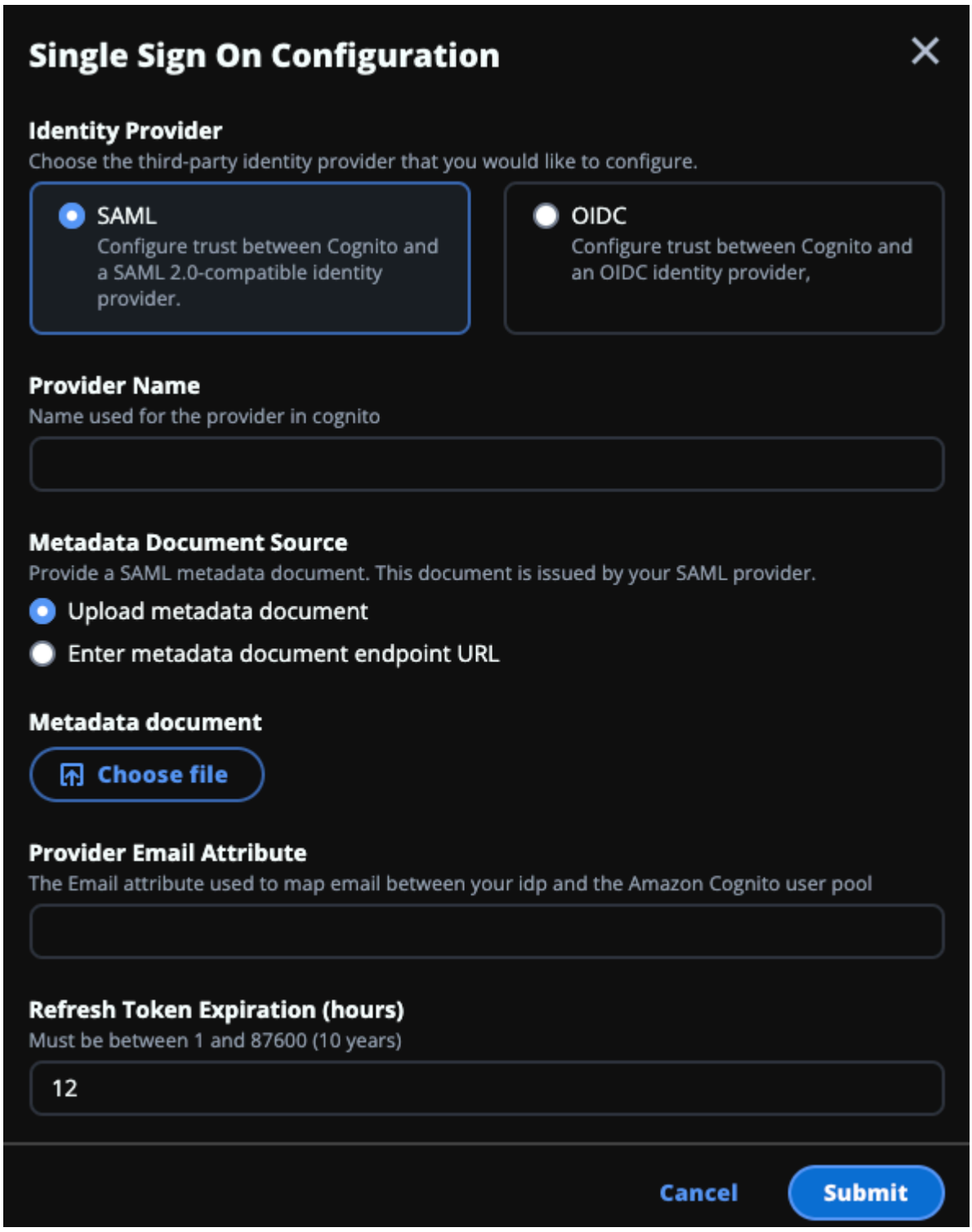
Configure RES para usar su proveedor de identidad

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 Single Sign-On, 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. Seleccione 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

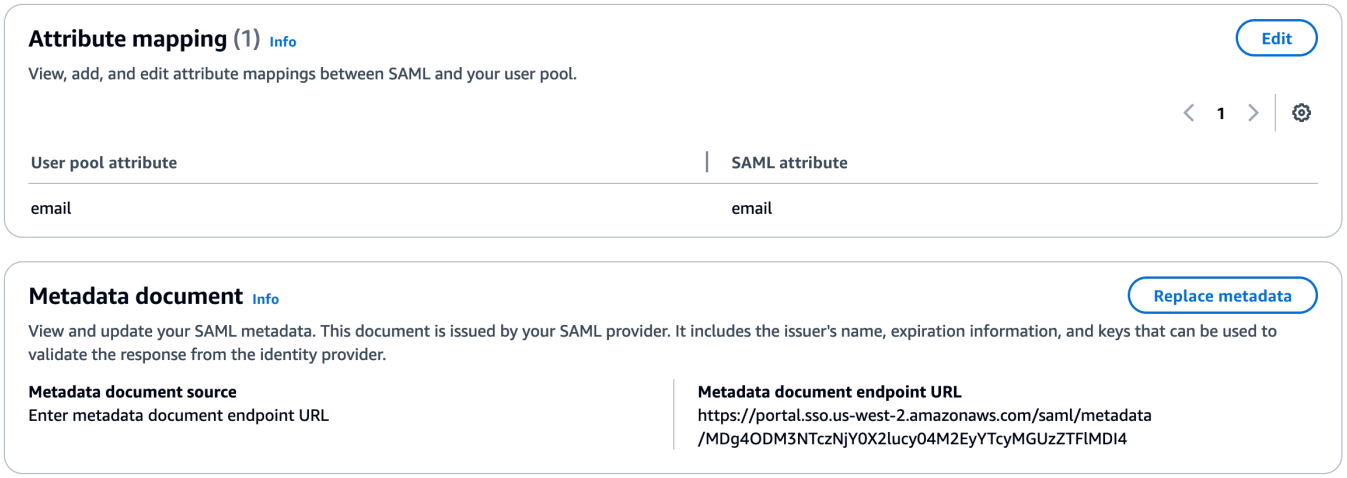
Si utilizó los recursos externos proporcionados para crear un entorno RES que no fuera de producción y configuró IAM Identity Center como su proveedor de identidades, puede que desee configurar un proveedor de identidades diferente, como Okta. El formulario de activación del SSO de RES solicita tres 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. Seleccione su grupo de usuarios para ver la descripción general del grupo de usuarios.
4. En la pestaña de Sign-in experiencia, vaya al inicio de sesión con el proveedor de identidad federado y abra el proveedor de identidades 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.

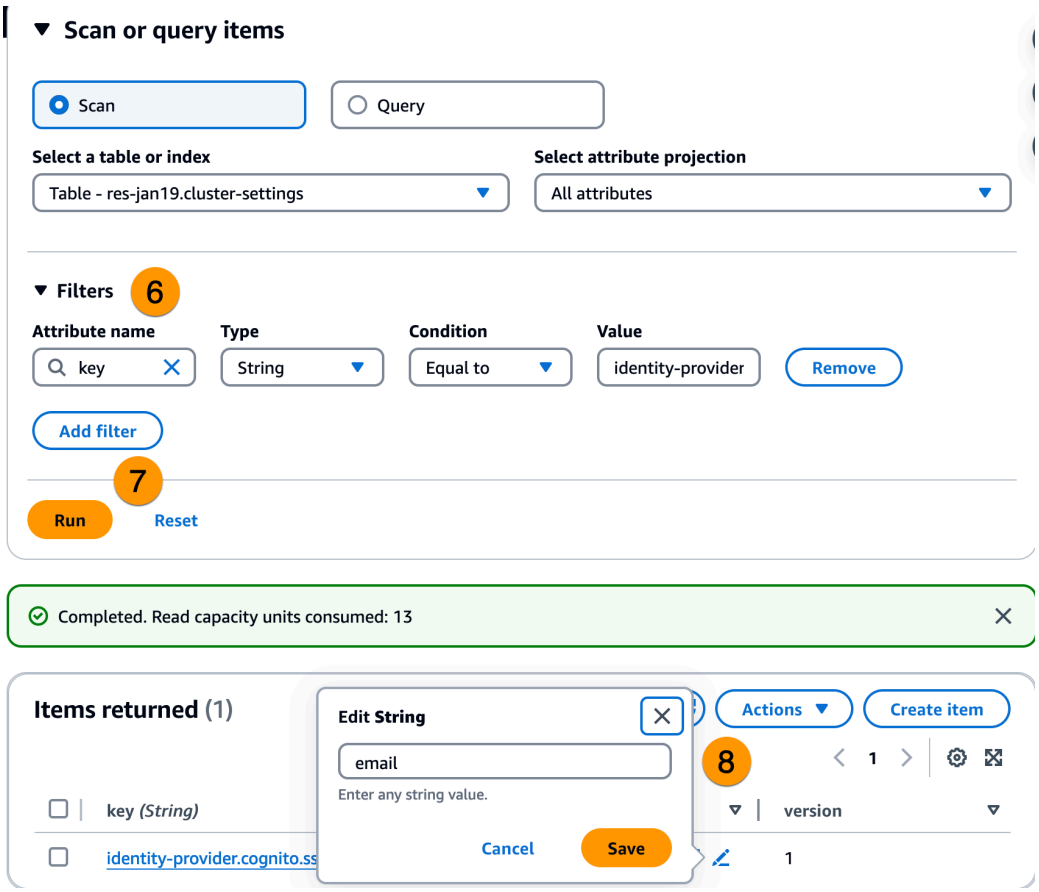
   b. Busque y seleccione la `<environment name>.cluster-settings` tabla y, en el menú Acciones, seleccione Explorar elementos.

   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 que el navegador Chrome realice un seguimiento de las solicitudes de SAML y compruebe los valores de las aserciones de SAML. Para obtener más información, consulta la tienda SAML-tracerweb 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 Directory Service consola, selecciona el directorio de la pila creada.
2. En el menú Acciones, selecciona Restablecer la contraseña del usuario.
3. Seleccione el usuario e introduzca una contraseña nueva.
4. Seleccione 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 una GovCloud región, configure la aplicación web y los subdominios de VDI en la cuenta de partición comercial que aloja la zona alojada pública 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. Seleccione 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 una GovCloud región, 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 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 vas a realizar el despliegue en una GovCloud región, copia 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/ <installation-stack-name>-cluster-endpoints`	Nunca caducan
`/aws/lambda/ <installation-stack-name>-cluster-manager-scheduled-ad-sync`	Nunca caducan
`/aws/lambda/ <installation-stack-name>-cluster-settings`	Nunca caducan
`/aws/lambda/ <installation-stack-name>-oauth-credentials`	Nunca caducan
`/aws/lambda/ <installation-stack-name>-self-signed-certificate`	Nunca caducan

CloudWatch Grupos de registros	Retención
/aws/lambda/ *<installation-stack-name>*-update-cluster-prefix-list	Nunca caducan
/aws/lambda/ *<installation-stack-name>*-vdc-scheduled-event-transformer	Nunca caducan
/aws/lambda/ *<installation-stack-name>*-vdc-update-cluster-manager-client-scope	Nunca caducan
/*<installation-stack-name>* /cluster-manager	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, vaya a la CloudWatch consola y siga las instrucciones que se indican en la sección Cambiar la retención de datos de registro en CloudWatch los registros.

Establecer límites de permisos personalizados

A partir del 24 de abril de 2020, puede modificar opcionalmente las funciones creadas por RES adjuntando límites de permisos personalizados. Se puede definir un límite de permiso personalizado como parte de la CloudFormation instalación de RES proporcionando el ARN del límite de permiso como parte del IAMPermissionBoundary parámetro. 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:*",
            "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 las RES-ready AMI

Con RES-ready Amazon Machine Images (AMI), puede preinstalar dependencias de RES para instancias de escritorios virtuales (VDI) en sus AMI personalizadas. El uso de las RES-ready AMI mejora los tiempos de arranque de las instancias de VDI mediante las imágenes preconfiguradas.

Con EC2 Image Builder, puede crear y registrar sus AMI como 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.

> **Important**
>
> RES-ready Las AMI creadas antes de la RES 2025.06.01 son incompatibles con la RES 2025.06.01 y todas las versiones posteriores. Al actualizar el entorno RES de una versión anterior a la 2025.06.01 a la más reciente, debe reconstruir todas las AMI. RES-ready

Temas

Prepare una 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:

- Relaciones de confianza que incluyen el servicio Amazon EC2.
- AmazonS3ReadOnlyAccess AmazonSSMManagedInstanceCore y EC2InstanceProfileForImageBuilder políticas.

Crear el componente Image Builder de EC2

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.

```
key : value
```

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.

> **Important**
>
> En el archivo de definición, sustituya **`latest`** el URI de descarga (`- source: 's3://research-engineering-studio-us-east-1/releases/latest/res-installation-scripts.tar.gz'`) por el número de versión exacto (por ejemplo,**`2025.06`**) si la versión del entorno RES no es la más reciente.

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:
  - GPUFamily:
      type: string
      description: GPU family (NONE, NVIDIA, or AMD)
      default: NONE
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://research-engineering-studio-us-east-1/releases/latest/
res-installation-scripts.tar.gz"
            destination: "/root/bootstrap/res-installation-scripts/res-
installation-scripts.tar.gz"
      - name: RunInstallScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - "cd /root/bootstrap/res-installation-scripts"
            - "tar -xf res-installation-scripts.tar.gz"
            - "cd scripts/virtual-desktop-host/linux"
            - "/bin/bash install.sh -g {{ GPUFamily }}"
      - name: RebootAfterInstall
        action: Reboot
```

```
        onFailure: Abort
        maxAttempts: 3
        inputs:
            delaySeconds: 0
      - name: RunInstallPostRebootScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - "cd /root/bootstrap/res-installation-scripts/scripts/virtual-
desktop-host/linux"
            - 'sed -i ''/^export AWS_DEFAULT_PROFILE="bootstrap_profile"$/d''
 install_post_reboot.sh'
            - "/bin/bash install_post_reboot.sh -g {{ GPUFamily }}"
      - name: PreventAL2023FromUninstallingCronie
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - "rm -f /tmp/imagebuilder_service/crontab_installed"
```

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
```

```
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://research-engineering-studio-us-east-1/releases/
latest/res-installation-scripts.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res-installation-
scripts.tar.gz'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'tar -xf res-installation-scripts.tar.gz'
                - 'Import-Module .\scripts\virtual-desktop-host\windows
\Install.ps1'
                - 'Install-WindowsEC2Instance -PrebakeAMI'
```

6. Cree cualquier etiqueta opcional y elija Crear componente.

Prepare su receta de EC2 Image Builder

Una receta de Generador de Imágenes de EC2 define la imagen base que se utilizará como punto de partida para crear una nueva imagen, junto con el conjunto de componentes que añade para personalizar la imagen y comprobar que todo funciona según lo previsto. 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)
- Amazon Linux 2023 (x86 y ARM64)
- RHEL 8 (x86) y 9 (x86)
- Rocky Linux 9 (x86)
- Ubuntu 22.04.3 (x86)
- Ubuntu 24.04.3 (x86)
- Windows Server 2019, 2022 (x86)
- Windows 10, 11 (x86)

> **Note**
>
> A partir de la versión 2026.03, Amazon Linux 2 y RHEL 8 ya no se incluyen como paquetes de software predeterminados. Si es necesario, se pueden seguir registrando paquetes de software personalizados con estos sistemas operativos.

Create a new recipe

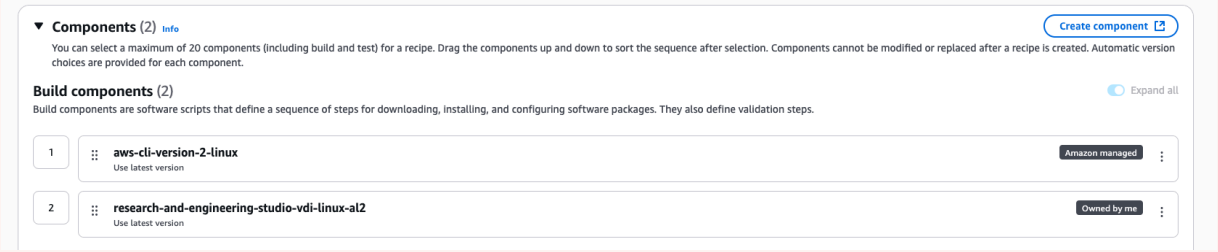
1. Abra la consola https://console.aws.amazon.com/imagebuilder EC2 Image Builder en.
2. En Recursos guardados, elija Recetas de imágenes.
3. Seleccione Crear receta de imagen.
4. Introduce un nombre único y un número de versión.
5. Seleccione una imagen base compatible con RES.
6. En Configuración de 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 instancias EC2 para Linux.

- Instalación y desinstalación manual del agente SSM en las instancias EC2 para Windows Server.

7. Para las recetas basadas en Linux, añada el componente de Amazon-managed `aws-cli-version-2-linux` compilación a la receta. Para recetas basadas en Windows, añada el componente de Amazon-managed `aws-cli-version-2-windows` compilación 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.
8. Añada el componente EC2 Image Builder creado para su entorno Linux o Windows.

> **Important**
>
> Debe agregar estos componentes en orden y agregar primero el componente de compilación `aws-cli-version-2-linux` `aws-cli-version-2-windows` (para Linux) o (para Windows).



9. (Recomendado) Añada el componente de Amazon-managed `simple-boot-test-<linux-or-windows>` prueba para comprobar que se puede iniciar 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

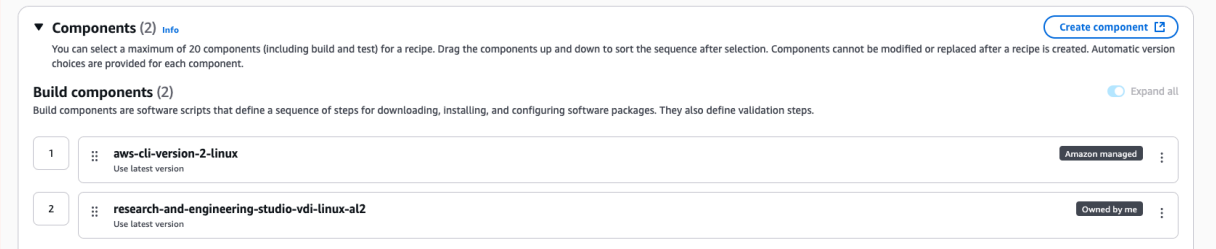
Si ya tiene una receta de EC2 Image Builder, puede utilizarla añadiendo los siguientes componentes:

1. Para las recetas basadas en Linux, añada el componente de Amazon-managed `aws-cli-version-2-linux` compilación a la receta. Para recetas basadas en Windows, añada el componente de Amazon-managed `aws-cli-version-2-windows` compilación 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.

2. Añada el componente EC2 Image Builder creado para su entorno Linux o Windows.

> **Important**
>
> Debe agregar estos componentes en orden y agregar primero el componente de compilación `aws-cli-version-2-linux` `aws-cli-version-2-windows` (para Linux) o (para Windows).



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

Configuración de la infraestructura de EC2 Image Builder

Puede utilizar las configuraciones de infraestructura para especificar la infraestructura de Amazon EC2 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. Prepare una 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 básica que haya elegido. Consulte los tipos de instancias de Amazon EC2.

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 las RES-ready AMI, 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 el panel de navegación, elija Image Pipelines.
3. Seleccione 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 enPrepare su receta de EC2 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 la infraestructura, elija Elegir la configuración de infraestructura existente y seleccione la configuración de infraestructura creada enConfiguración de la infraestructura de EC2 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 enPrepare su receta de EC2 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 enConfigurar 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 (AMI)” para registrar una pila de software.
2. Para el ID de AMI, introduzca el ID de AMI de la imagen de salida integradaEjecute la canalización de imágenes de Image Builder.

Umbrales de validación de sesiones de DCV configurables

Cuando se reanuda o se inicia una sesión de VDI, RES comprueba repetidamente si la sesión de DCV ha alcanzado el estado READY. Si la sesión no está lista tras un número determinado de reintentos, se marca como ERROR.

Estos umbrales de reintentos se pueden configurar mediante la tabla de DynamoDB`<env-name>.cluster-settings`, lo que permite a los administradores ajustarlos en función de su entorno. Esto resulta especialmente útil para entornos con tiempos de arranque más prolongados debido a configuraciones de AMI personalizadas, instalaciones de software adicionales u otra lógica de configuración de VDI.

Key	Description (Descripción)	Predeterminado
`vdc.validation_request_threshold`	Número máximo de reintentos antes de marcar una sesión no lista como ERROR	50
`vdc.session_deleted_threshold`	Número máximo de reintentos antes de marcar una sesión ELIMINADA como ERROR	15

Configure dominios personalizados después de la instalación de RES

> **Note**
>
> Requisitos previos: Debe almacenar el certificado y el PrivateKey contenido en un secreto de Secrets Manager antes de realizar estos pasos.

Agregue certificados al cliente web

1. Actualiza el certificado adjunto al detector del balanceador de cargas external-alb:
   a. Navegue hasta el balanceador de cargas externo RES en la AWS consola, en EC2 > Equilibrio de carga > Equilibradores de carga.
   b. Busque el balanceador de cargas que siga la convención de nomenclatura. *<env-name>*-`external-alb`
   c. Comprueba los oyentes conectados al balanceador de cargas.
   d. Actualice el listener que tiene un SSL/TLS certificado predeterminado adjunto con los detalles del nuevo certificado.
   e. Guarde los cambios.
2. En la tabla de configuración del clúster:
   a. Busque la tabla de configuración del clúster en DynamoDB -> Tablas ->. *<env-name>*`.cluster-settings`

b. Vaya a Explorar elementos y filtre por atributo: nombre «clave», tipo «cadena», condición «contiene» y valor «external_alb».

c. Establézcalo en True. `cluster.load_balancers.external_alb.certificates.provided`

d. Actualice el valor `decluster.load_balancers.external_alb.certificates.custom_dns_name`. Este es el nombre de dominio personalizado para la interfaz de usuario web.

e. Actualice el valor `decluster.load_balancers.external_alb.certificates.acm_certificate_arn`. Es el nombre de recurso de Amazon (ARN) del certificado correspondiente almacenado en Amazon Certificate Manager (ACM).

3. Actualice el registro de subdominio de Route53 correspondiente que creó para su cliente web para que apunte al nombre DNS del balanceador de cargas de laboratorio externo. `<env-name>-external-alb`

4. Si el SSO ya está configurado en el entorno, vuelva a configurarlo con las mismas entradas que utilizó inicialmente en el botón Administración del entorno > Administración de identidades > Único > Estado Sign-On > Editar del portal web de RES.

Agregue certificados a los VDI o rote los certificados

1. Conceda permiso a la aplicación RES para realizar una GetSecret operación en el secreto añadiendo las siguientes etiquetas al secreto:

   - `res:EnvironmentName` : *`<env-name>`*
   - `res:ModuleName` : `virtual-desktop-controller`

2. En la tabla de configuración del clúster:

   a. Busque la tabla de configuración del clúster en DynamoDB -> Tablas ->. *`<env-name>`*`.cluster-settings`

   b. Vaya a Explorar elementos y filtre por atributo: nombre «clave», tipo «cadena», condición «contiene» y valor «dcv_connection_gateway».

   c. Establézcalo en True. `vdc.dcv_connection_gateway.certificate.provided`

   d. Actualice el valor `devdc.dcv_connection_gateway.certificate.custom_dns_name`. Este es el nombre de dominio personalizado para el acceso a la VDI.

e. Actualice el valor de. `vdc.dcv_connection_gateway.certificate.certificate_secret_arn` Este es el ARN del secreto que contiene el contenido del certificado.

f. Actualice el valor de. `vdc.dcv_connection_gateway.certificate.private_key_secret_arn` Este es el ARN del secreto que contiene el contenido de la clave privada.

3. Actualice la plantilla de lanzamiento utilizada para la instancia de puerta de enlace:

   a. Abra el grupo Auto Scaling en la AWS consola, en EC2 > Auto Scaling > Auto Scaling Groups.

   b. Seleccione el grupo de escalado automático de la puerta de enlace que corresponda al entorno RES. El nombre sigue la convención de nomenclatura*<env-name>*`-vdc-gateway-asg`.

   c. Busque y abra la plantilla de lanzamiento en la sección de detalles.

   d. En Detalles > Acciones > selecciona Modificar plantilla (Crear nueva versión).

   e. Desplázate hacia abajo hasta Detalles avanzados.

   f. Desplázate hasta el final, hasta Datos de usuario.

   g. Busca las palabras `CERTIFICATE_SECRET_ARN` y`PRIVATE_KEY_SECRET_ARN`. Actualice estos valores con los ARN proporcionados a los secretos que contienen el contenido del certificado (consulte el paso 2.c) y la clave privada (consulte el paso 2.d).

   h. Asegúrese de que el grupo Auto Scaling esté configurado para usar la versión recientemente creada de la plantilla de lanzamiento (de la página del grupo Auto Scaling).

4. Actualice el registro de subdominio de Route53 correspondiente que creó para sus escritorios virtuales para que apunte al nombre DNS del balanceador de cargas nlb externo:. *<env-name>*`-external-nlb`

5. Termina la instancia dcv-gateway existente *<env-name>*`-vdc-gateway` y espera a que se active una nueva. La instancia dcv-gateway comprueba todos los días a las 12:00 a.m. (medianoche) UTC si hay cambios en los valores del certificado y la clave privada almacenados en Secrets Manager, y recupera y aplica automáticamente los nuevos valores si se actualizan.

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 secretos

Research and Engineering Studio mantiene los siguientes secretos al usar 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	Description (Descripción)	RES generado	Ingresó el administrador
`<envname> -sso-client-secret`	Secreto de cliente Sign-On OAuth2 único para el entorno	✓	
`<envname> -vdc-client-secret`	VDC ClientSecret	✓	
`<envname> -vdc-client-id`	VDC ClientId	✓	
`<envname> -vdc-gateway-certificate-private-key`	Self-Signed certificado de clave privada para el dominio	✓	

Nombre del secreto	Description (Descripción)	RES generado	Ingresó el administrador
`<envname> -vdc-gateway-certificate-certificate`	Self-Signed certificado de dominio	✓	
`<envname> -cluster-manager-client-secret`	administrador de clústeres ClientSecret	✓	
`<envname> -cluster-manager-client-id`	administrador de clústeres ClientId	✓	
`<envname> -external-private-key`	Self-Signed certificado, clave privada para el dominio	✓	
`<envname> -external-certificate`	Self-Signed certificado de dominio	✓	
`<envname> -internal-private-key`	Self-Signed certificado, clave privada para el dominio	✓	
`<envname> -internal-certificate`	Self-Signed certificado de dominio	✓	

Nombre del secreto	Description (Descripción)	RES generado	Ingresó el administrador
<envname> -directoryservice-ServiceAccountUserDN	El atributo de nombre distintivo (DN) del ServiceAccount usuario.	✓	

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

Key	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
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	pila
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	

Key	origen
`cluster.load_balancers.external_alb.certificates.private_key_secret_arn`	pila
`cluster-manager.client_secret`	

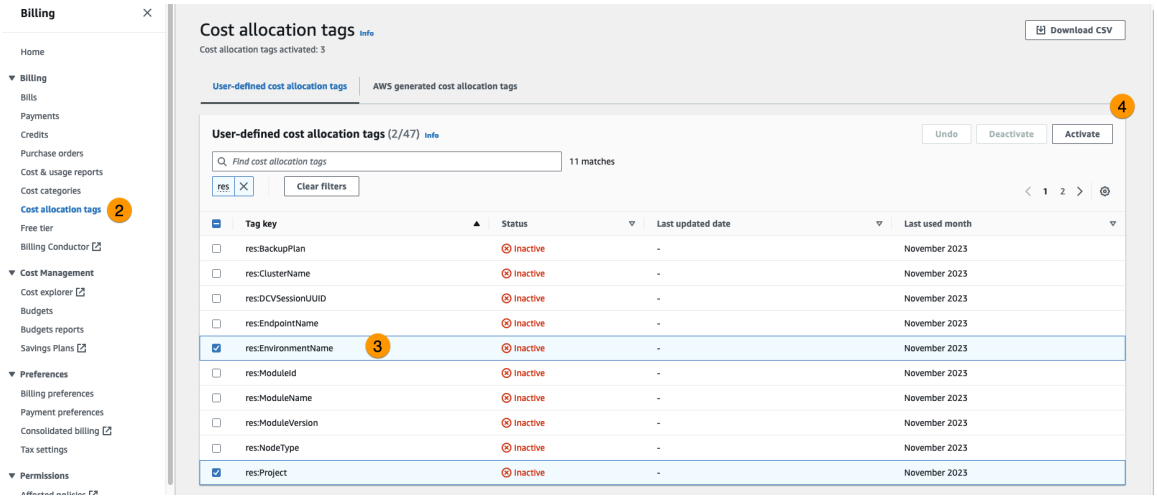
Supervisión y control de costes

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

Cree 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.

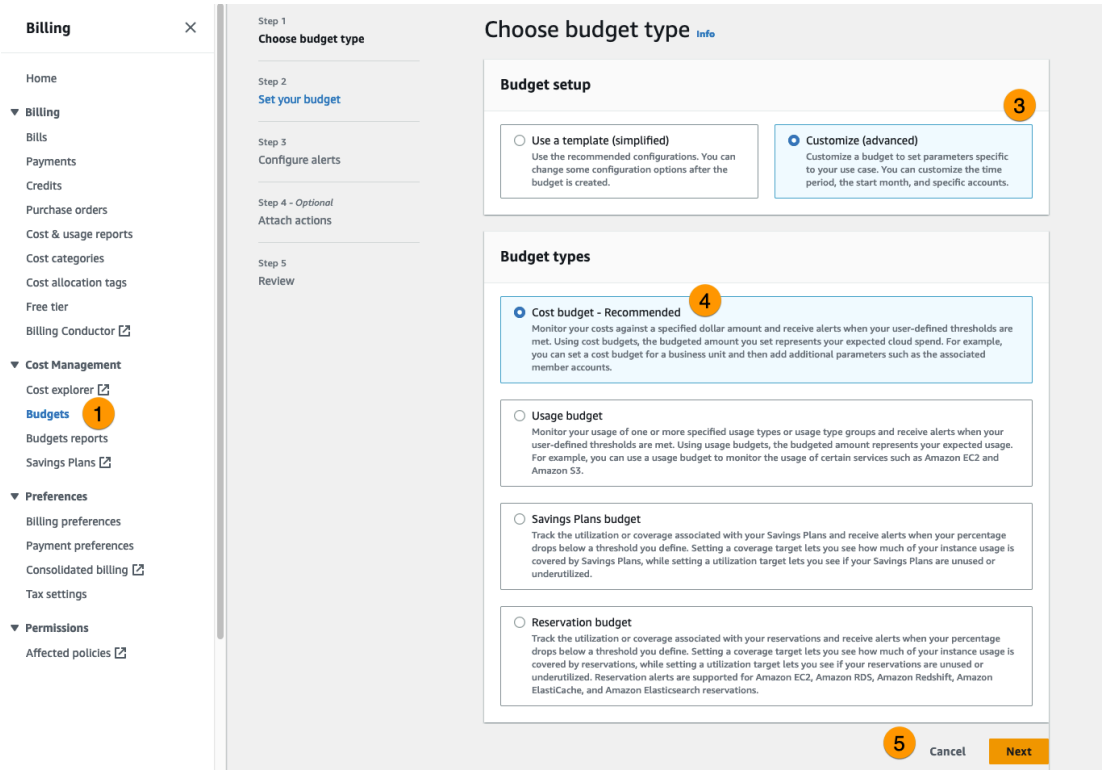
1. Inicie sesión en la consola AWS de administración y abra la consola AWS Billing and Cost Management.
2. Elija las etiquetas de asignación de costes.
3. Busque y seleccione las `res:EnvironmentName` etiquetas `res:Project` y.
4. Seleccione Activar.



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

Para crear un presupuesto para los recursos de RES:

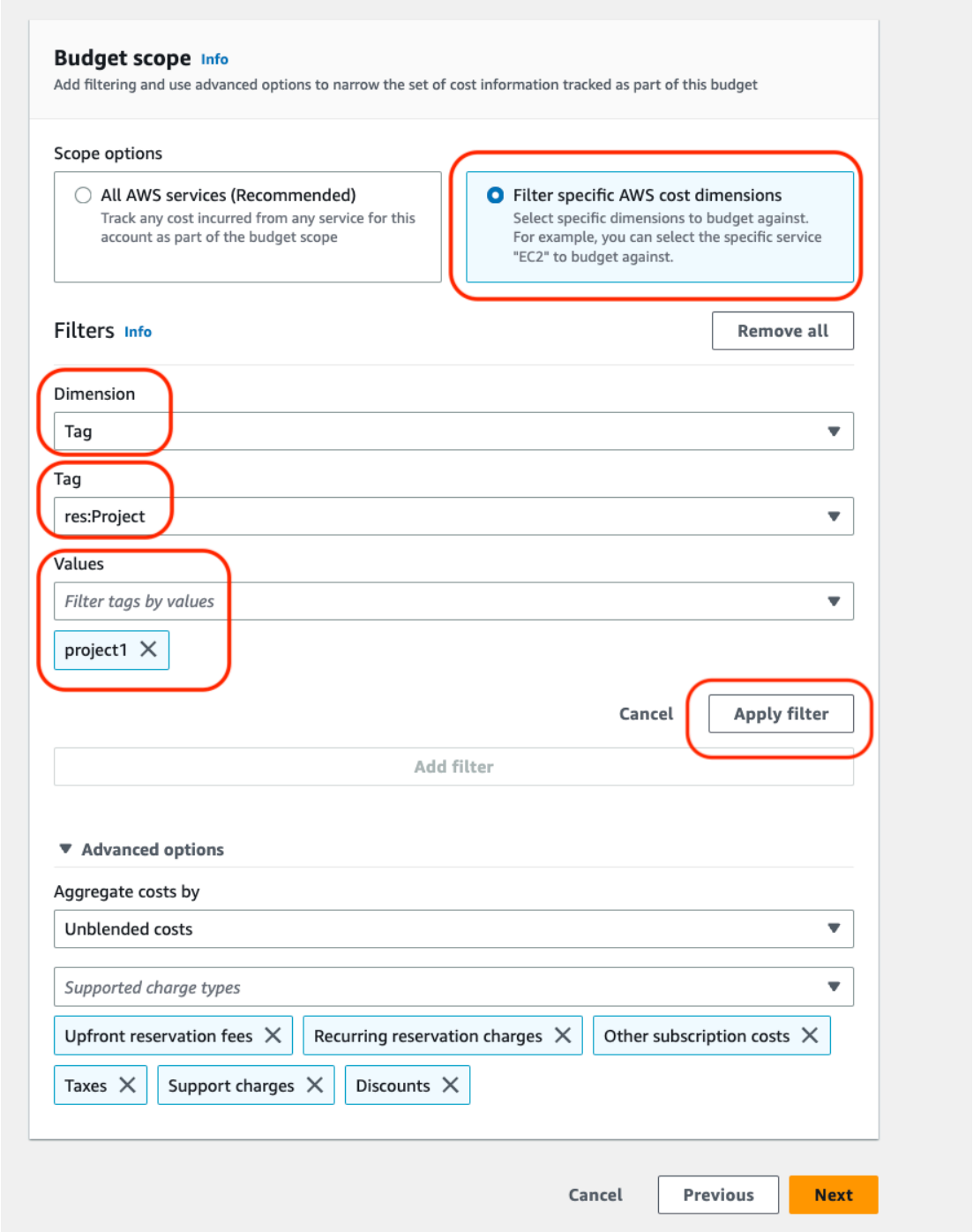
1. En la consola de facturación, selecciona Presupuestos.
2. Selecciona Crear un presupuesto.
3. En Configuración del presupuesto, seleccione Personalización (avanzada).
4. En Tipos de presupuesto, selecciona Presupuesto de costes: recomendado.
5. Elija Siguiente.



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.

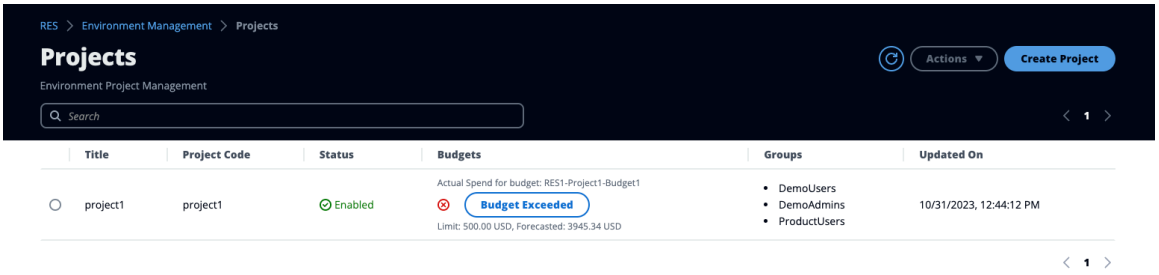
12. En Valores, seleccione el nombre del proyecto.
13. Elija Aplicar filtro para adjuntar el filtro del proyecto al presupuesto.
14. Elija Siguiente.



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.

Panel de análisis de costos

El panel de análisis de costos permite a los administradores de RES monitorear los presupuestos y los costos del proyecto a lo largo del tiempo desde el portal de RES. Los costos se pueden filtrar a nivel de proyecto.

Temas

- Requisitos previos
- Gráfica de proyectos con presupuesto asignado
- Gráfico de análisis de costes a lo largo del tiempo
- Descargar CSV

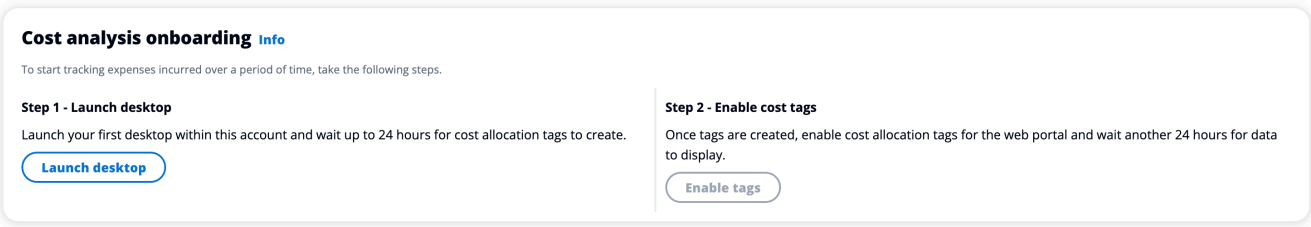
Requisitos previos

Para utilizar el panel de costes de Research and Engineering Studio, primero debe:

- Crear un proyecto.

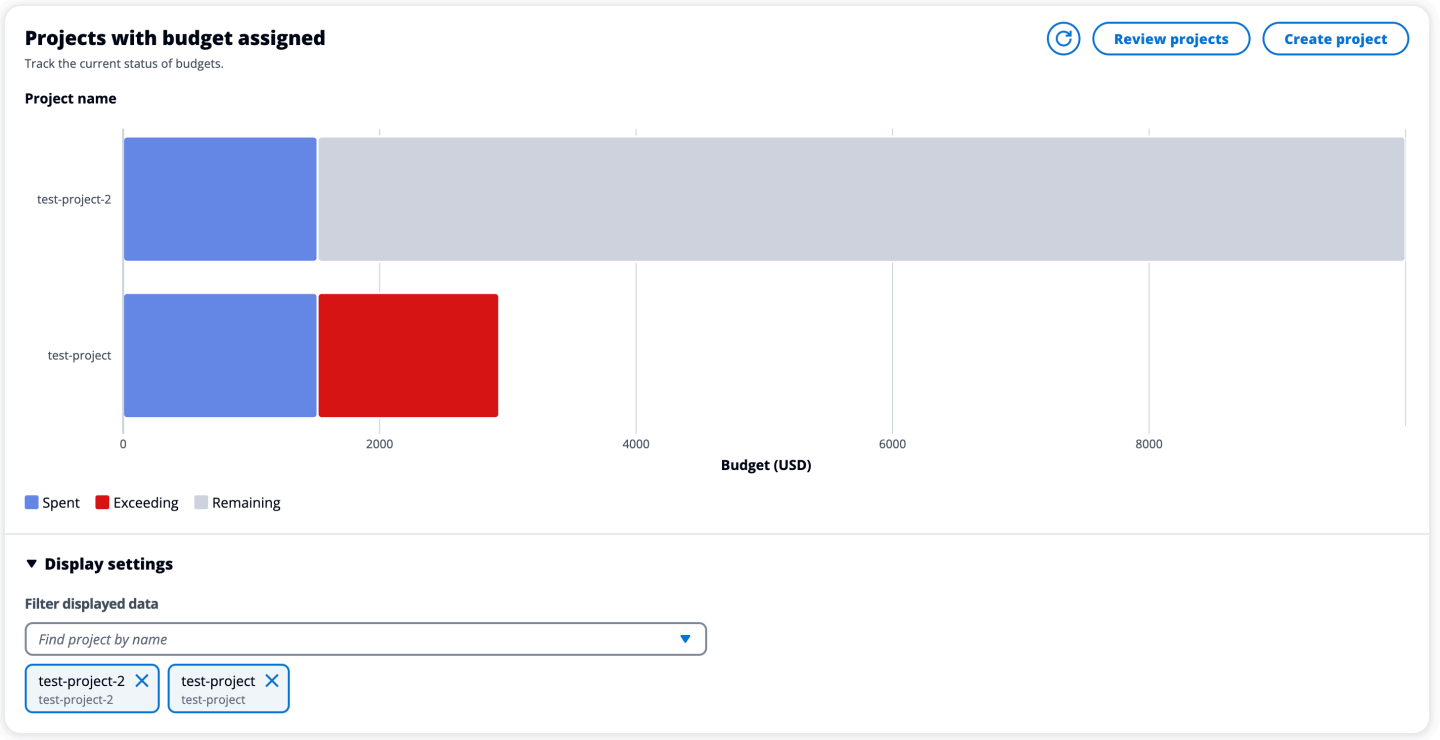
- Cree un presupuesto en la consola AWS Billing and Cost Management.
- Adjunte el presupuesto al proyecto (consulteEdita un proyecto).
- Active el cuadro de análisis de costes para las cuentas con nuevas implementaciones de RES. Para ello, sigue estos pasos:

  1. Implemente una VDI para el proyecto que creó. Esto aprovisiona la `res:Project` etiqueta en el AWS Cost Explorer, lo que puede tardar hasta 24 horas.
  2. Una vez creada la etiqueta, se activa el botón Activar etiquetas. Pulse el botón para activar las etiquetas en Cost Explorer. Este proceso puede tardar 24 horas adicionales.



Gráfica de proyectos con presupuesto asignado

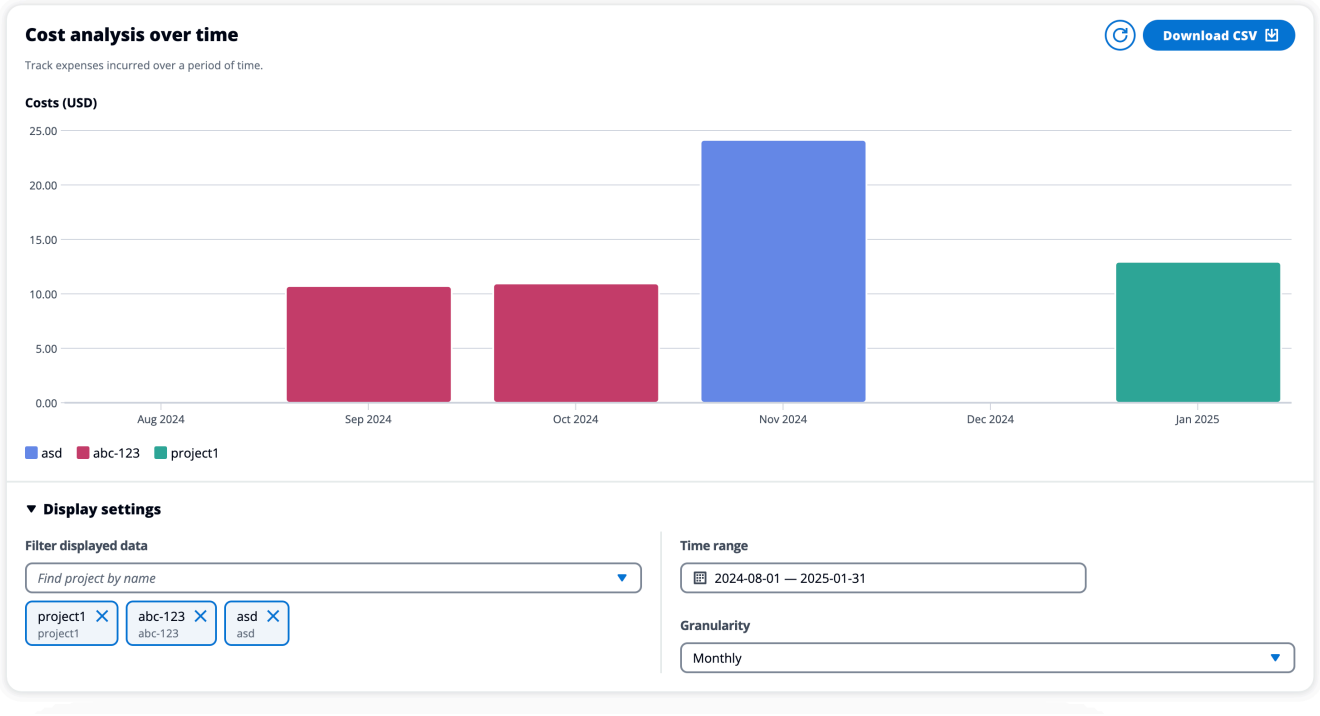
El gráfico de proyectos con presupuesto asignado muestra el estado presupuestario de los proyectos en el entorno de energías renovables a los que se les han asignado presupuestos. De forma predeterminada, el gráfico muestra los 5 proyectos principales por importe presupuestario. Puede seleccionar proyectos específicos en el menú desplegable Filtrar los datos mostrados, que carga la lista completa de proyectos asignados al presupuesto.



El gráfico muestra los importes gastados, restantes y superiores de cada presupuesto en USD. Pase el ratón sobre una barra para ver los importes exactos en USD de cada categoría. También puedes abrir las páginas Proyectos y Crear proyecto pulsando los botones Revisar proyectos y Crear proyecto en la esquina superior derecha, respectivamente.

Gráfico de análisis de costes a lo largo del tiempo

El gráfico del análisis de costos a lo largo del tiempo muestra el desglose de los costos por proyecto durante un período de tiempo específico. De forma predeterminada, el gráfico muestra los datos de cada uno de los últimos 6 meses. Muestra los 5 proyectos principales por costo total en el rango de tiempo seleccionado con la granularidad que seleccione. Todos los demás proyectos seleccionados, además de los 5 principales, se agrupan en la categoría Otros.

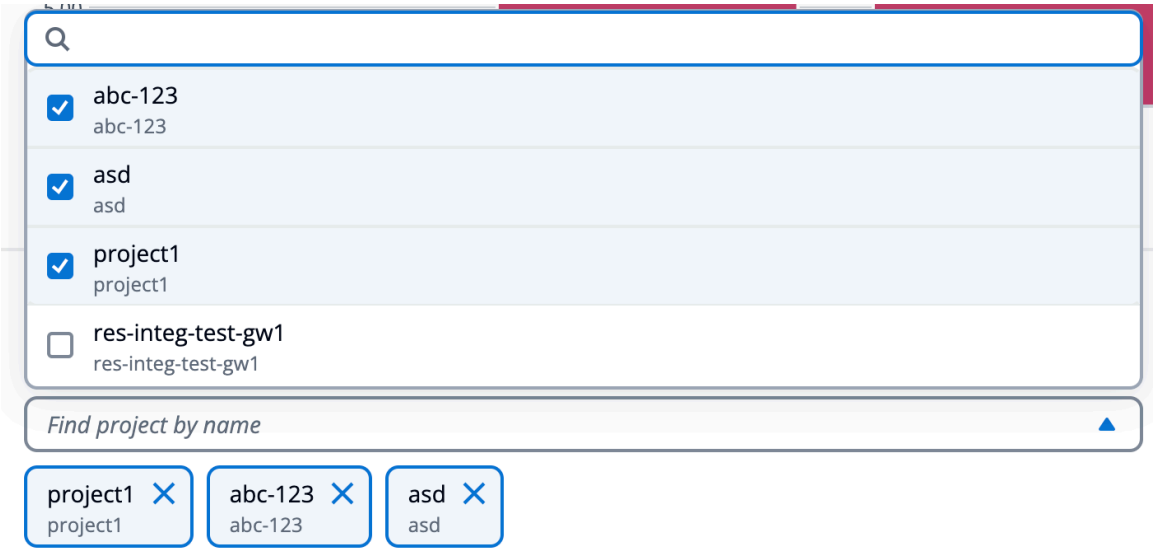


Filtros

Puede filtrar por proyecto, rango de tiempo y granularidad para personalizar la vista del gráfico del análisis de costos a lo largo del tiempo. Si selecciona alguna combinación de filtros no válida, aparecerá una ventana modal en la que podrá volver a la configuración anterior o aceptar una sugerencia para la combinación de filtros actualizada.

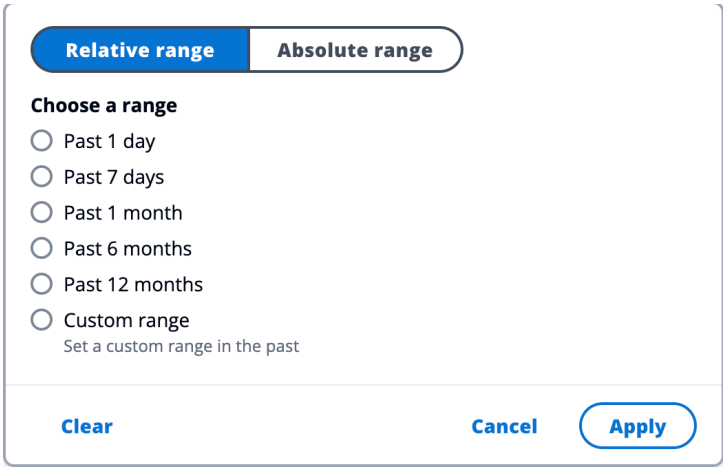
Proyecto

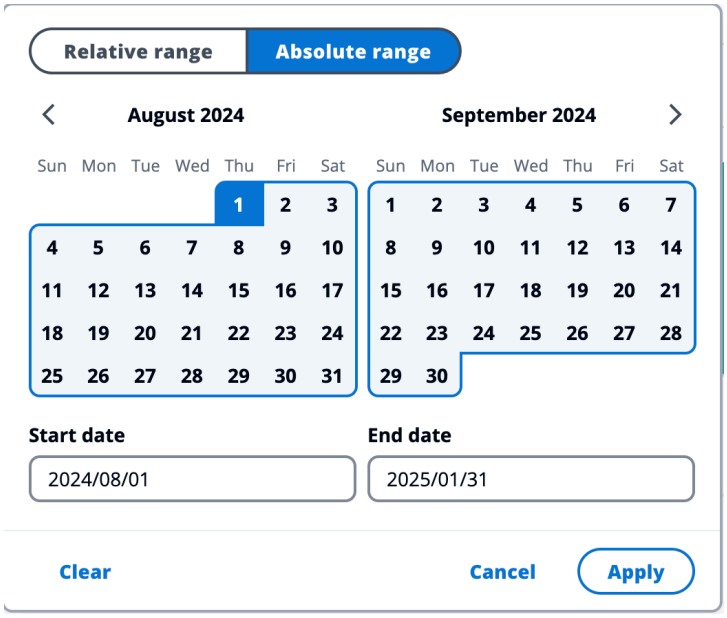
Al elegir el menú desplegable Filtrar los datos mostrados, verá una lista completa de los proyectos de su entorno RES actual. Aparece el nombre del proyecto y, debajo, el código del proyecto.



Especificar el intervalo de tiempo

Puede elegir usar un rango absoluto o un rango relativo al especificar un rango de fechas. Al seleccionar un rango relativo, las fechas se calculan utilizando unidades de tiempo completas. Por ejemplo, si selecciona la opción de los últimos 6 meses en febrero de 2025, tendrá como resultado un intervalo de tiempo comprendido entre 8/1 /24 y /25. 1/31



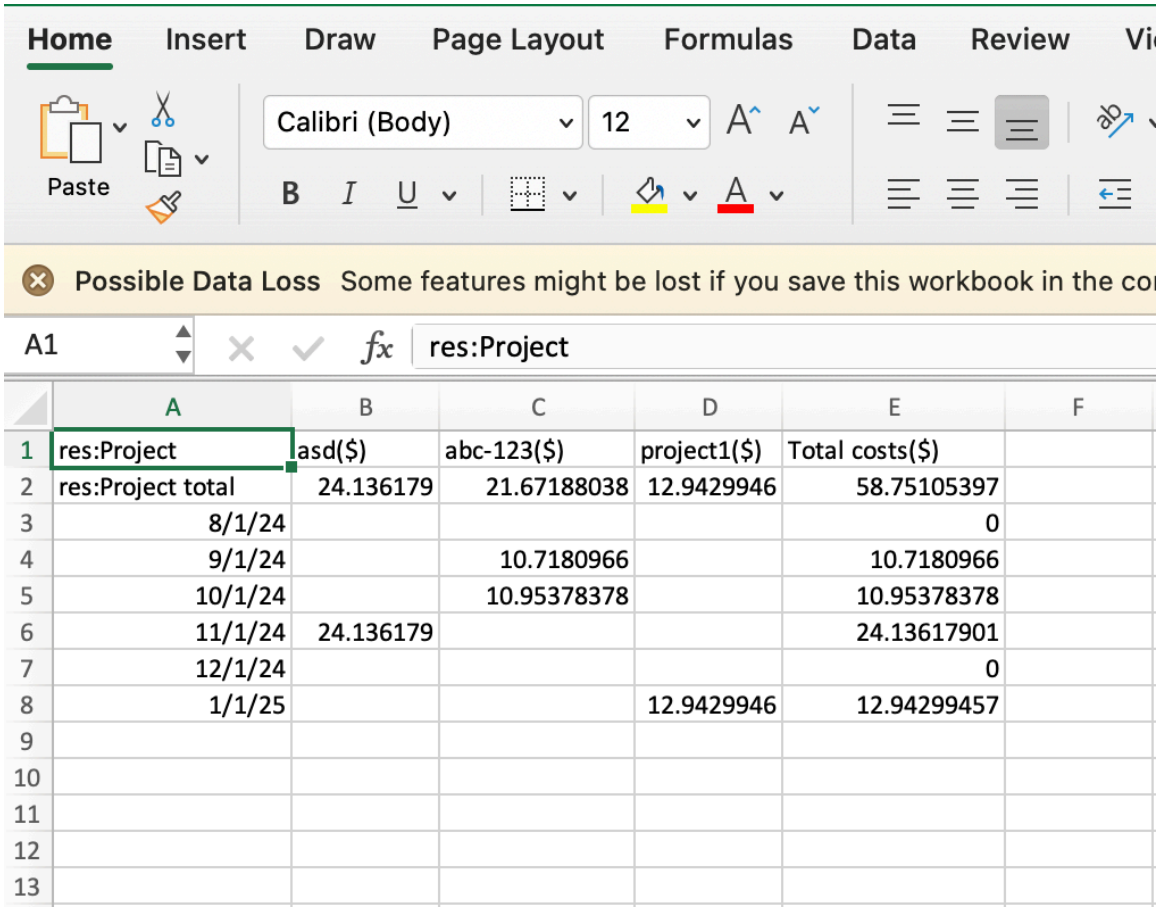


Granularity (Grado de detalle)

Puede elegir ver los datos con una granularidad mensual, diaria o horaria. La granularidad horaria solo admite un intervalo de fechas de hasta 14 días. La granularidad diaria solo admite un intervalo de fechas de hasta 14 meses.

Descargar CSV

Para exportar la vista de análisis de costes actual, seleccione Descargar CSV en la parte superior derecha del gráfico Análisis de costes a lo largo del tiempo. El CSV descargado contiene la información de costos de cada proyecto seleccionado para el período de tiempo especificado, así como los costos totales por proyecto y por período de tiempo.



	A	B	C	D	E	F
1	res:Project	asd($)	abc-123($)	project1($)	Total costs($)	
2	res:Project total	24.136179	21.67188038	12.9429946	58.75105397	
3	8/1/24				0	
4	9/1/24		10.7180966		10.7180966	
5	10/1/24		10.95378378		10.95378378	
6	11/1/24	24.136179			24.13617901	
7	12/1/24				0	
8	1/1/25			12.9429946	12.94299457	
9						
10						
11						
12						
13						

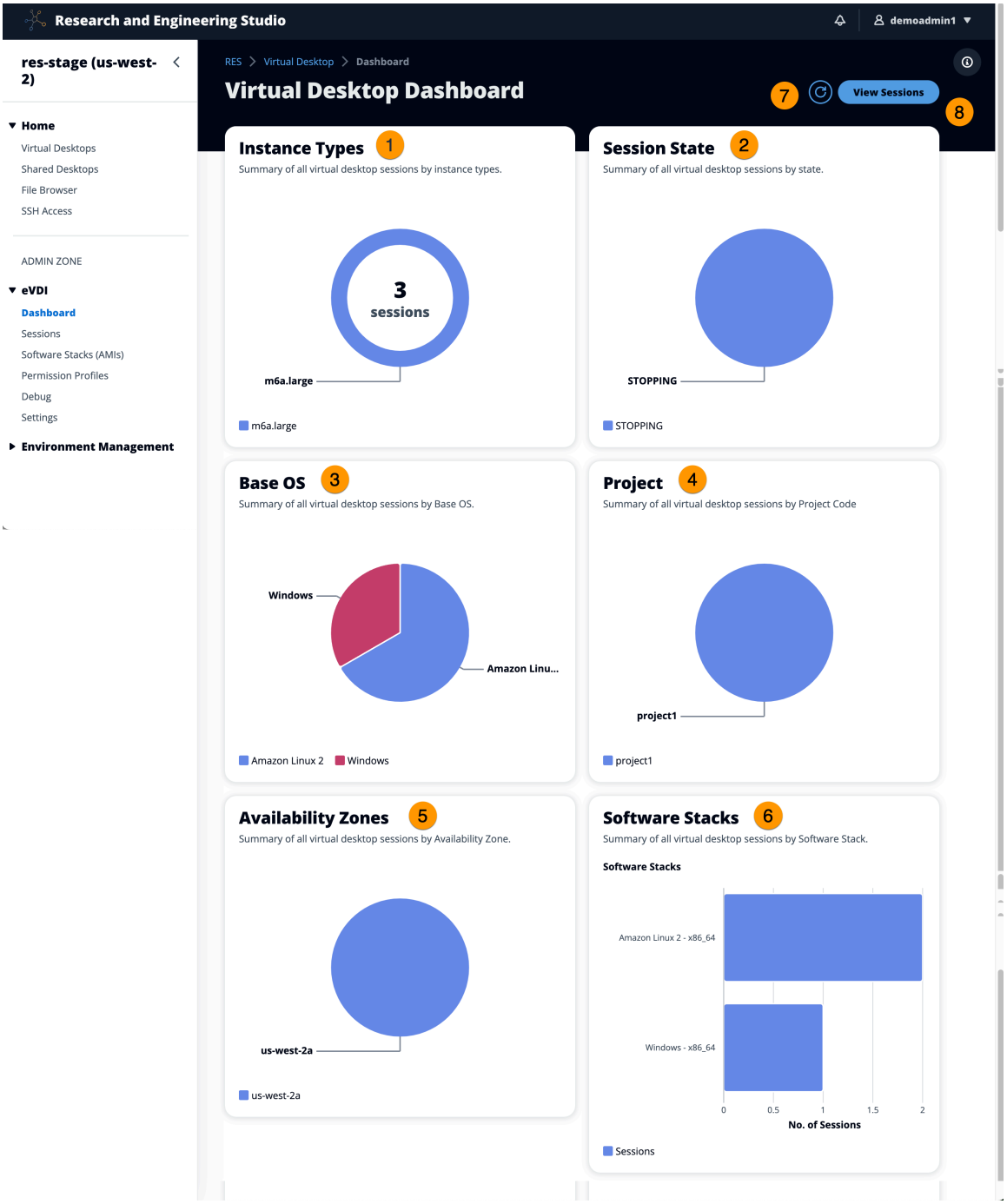
Administración de sesiones

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
- Sesiones
- Pilas de software (AMI)
- Debugging
- Configuración de escritorio

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

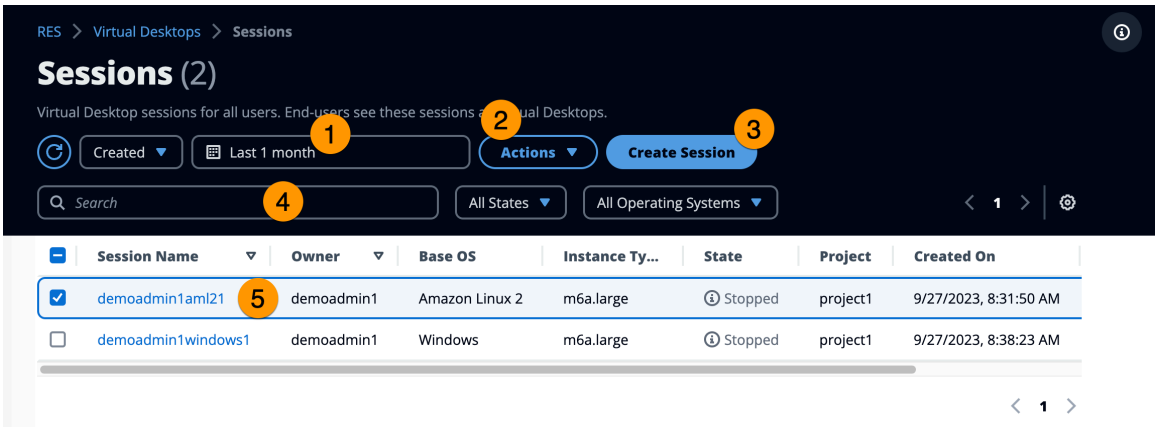
4. Proyectos
5. Zonas de disponibilidad
6. Pilas de software

Además, los administradores pueden:

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

Sesiones

Las sesiones muestran 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. Usa 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. Reiniciar sesión (s): reinicia las sesiones seleccionadas. Esta acción también está disponible para las sesiones en estado ERROR, lo que permite a los administradores recuperar los VDI erróneos.
   e. Finalizar sesión (s)
   f. Forzar la finalización de la (s) sesión (s)

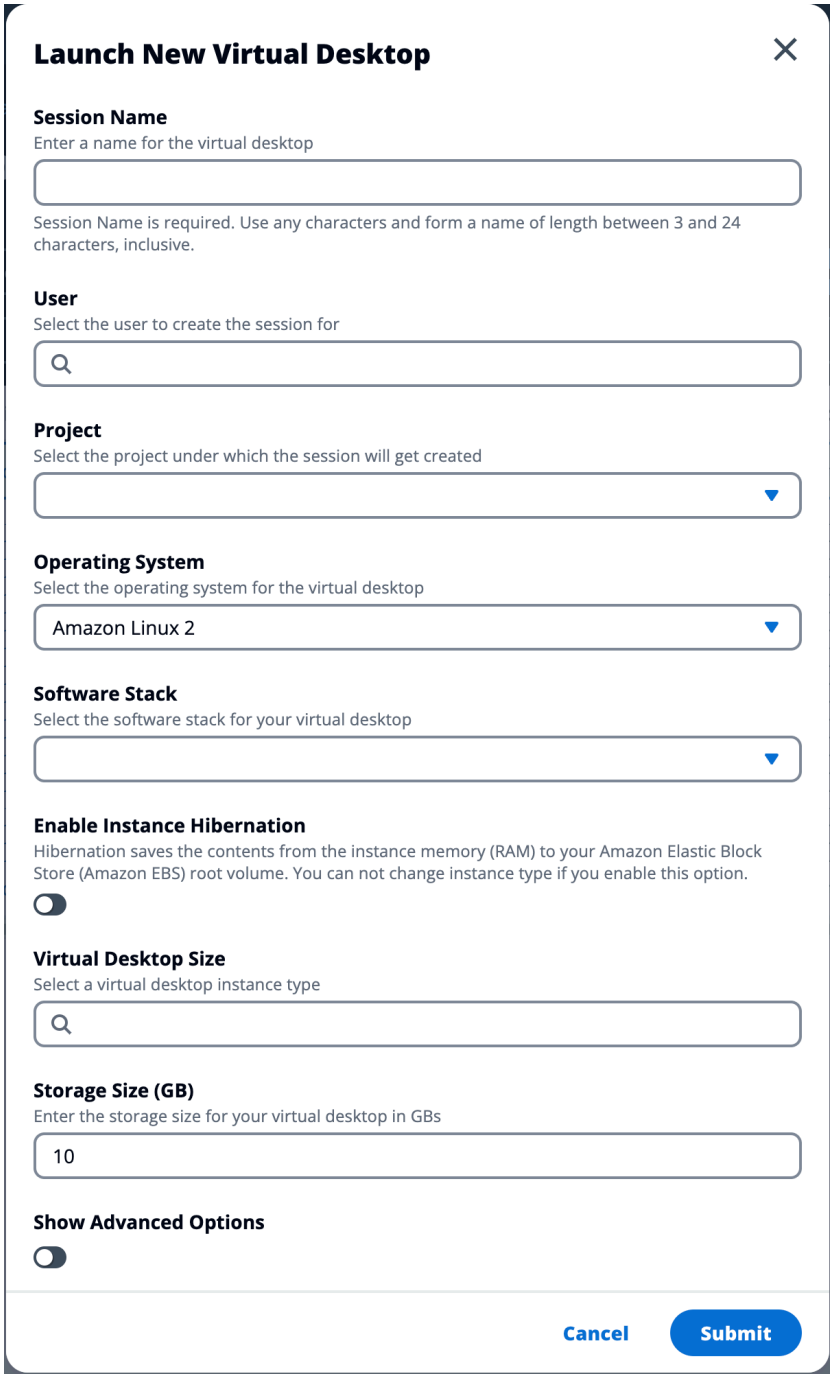
g. Salud de la (s) sesión (s)

h. 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. Seleccione el nombre de la sesión para ver más detalles.

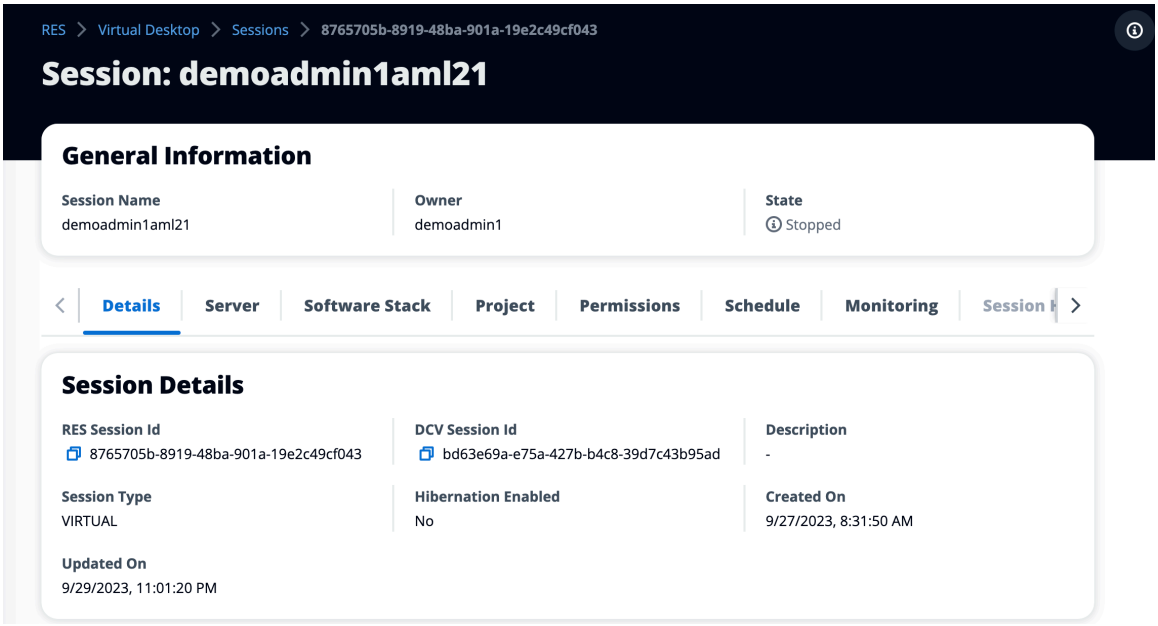
Crear una sesión

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. Seleccione Enviar.



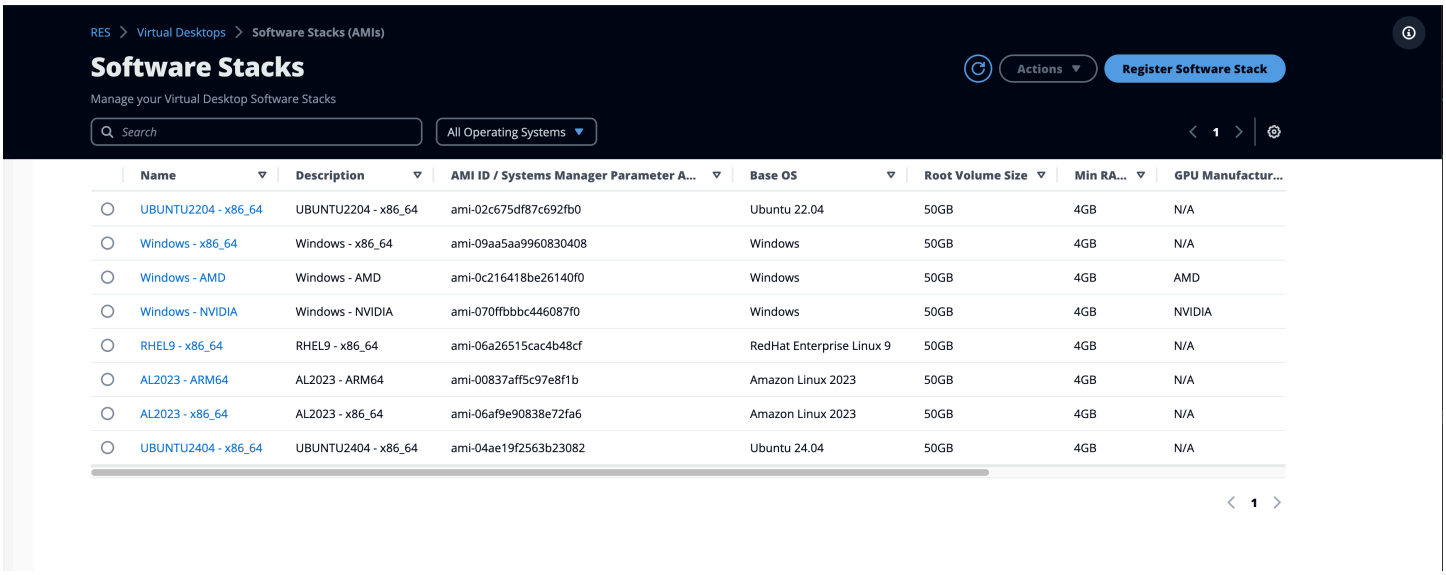
Detalles de la sesión

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



Pilas de software (AMI)

En la página Software Stacks, puede configurar Amazon Machine Images (AMI) o gestionar las existentes.



1. Para buscar una pila de software existente, usa el menú desplegable del sistema operativo para filtrar por sistema operativo.
2. Seleccione el nombre de una pila de software para ver los detalles de la pila.
3. Seleccione el botón de opción situado junto a una pila de software y, a continuación, utilice el menú Acciones para editar la pila y asignarla a un proyecto.

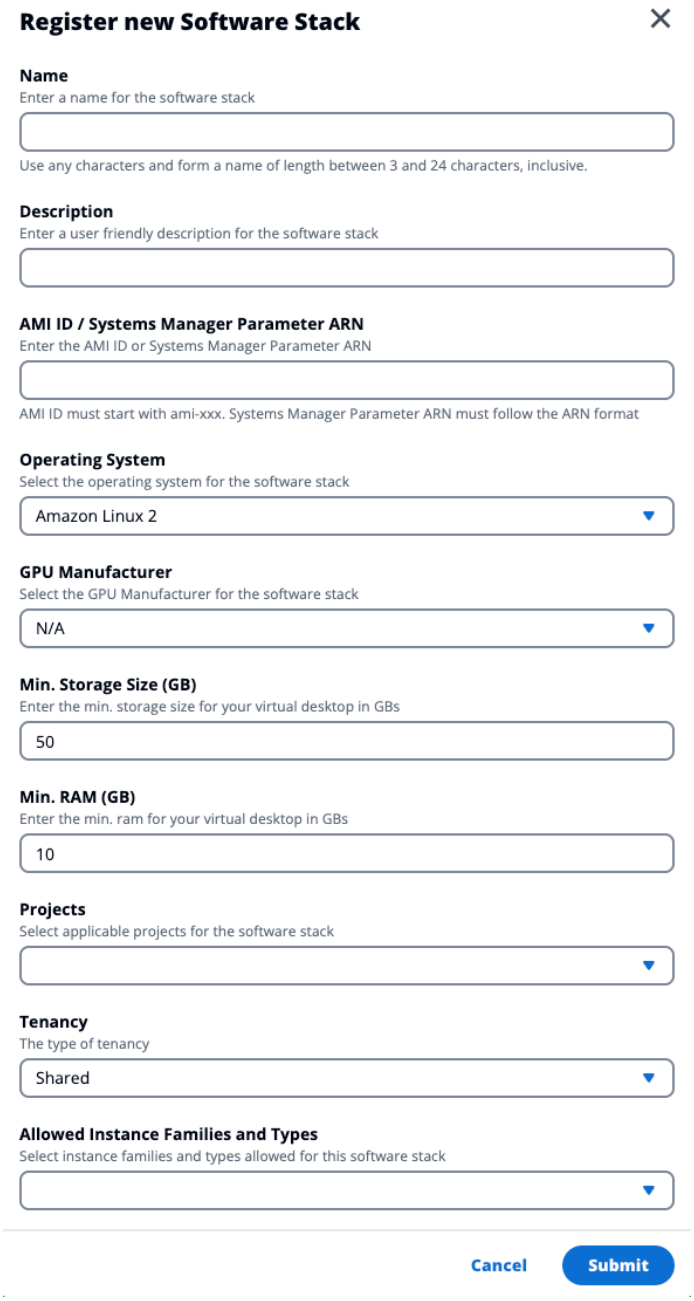
4. Pulse el botón Registrar pila de software para crear una pila nueva.

Registre una nueva pila de software

El botón Registrar pila de software le permite crear una nueva pila:

> **Note**
>
> Puede utilizar un parámetro de Systems Manager no cifrado como alias para el ID de la pila de software.
> El parámetro Systems Manager requerirá las siguientes etiquetas para que RES pueda acceder a ellos:
>
> - clave: `res:EnvironmentName`, valor: *`<your RES environment name>`*
> - clave: `res:ModuleName`, valor: `virtual-desktop-controller`

1. Seleccione Registrar pila de software.
2. Introduzca los detalles de la nueva pila de software, incluidos el nombre, la descripción, el ID de AMI y el sistema operativo.
3. (Opcional) Utilice el campo Tipos de instancias permitidos para especificar las familias o los tipos de instancias permitidos para esta pila de software. Puedes introducir familias de instancias (por ejemplo`t3`) o tamaños de instancia específicos (por ejemplo,`t3.xlarge`).
4. Seleccione Enviar.



Asigne una pila de software a un proyecto

Al crear una nueva pila de software, puede asignarla a los proyectos. Sin embargo, si necesitas añadir la pila a un proyecto después de la creación inicial, haz lo siguiente:

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

1. En la página Software Stacks, seleccione el botón de radio correspondiente a la pila de software que desee añadir a un proyecto.
2. Elija Acciones.
3. Elija Edit (Edición de).
4. Utilice el menú desplegable Proyectos para seleccionar el proyecto.

Update Software Stack: AL2023 - x86_64

Stack Name
Enter a name for the Software Stack.
AL2023 - x86_64
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
AL2023 - x86_64

AMI ID / Systems Manager Parameter ARN
Enter the AMI ID or Systems Manager Parameter ARN
ami-08a6efd148b1f7504
AMI ID must start with ami-xxx. Systems Manager Parameter ARN must follow the ARN format

Operating System
Select the operating system for the software stack
Amazon Linux 2023

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
50

Min. RAM (GB)
Enter the min. ram for your virtual desktop in GBs
4

Projects
Select applicable projects for the software stack

Tenancy
The type of tenancy
Shared

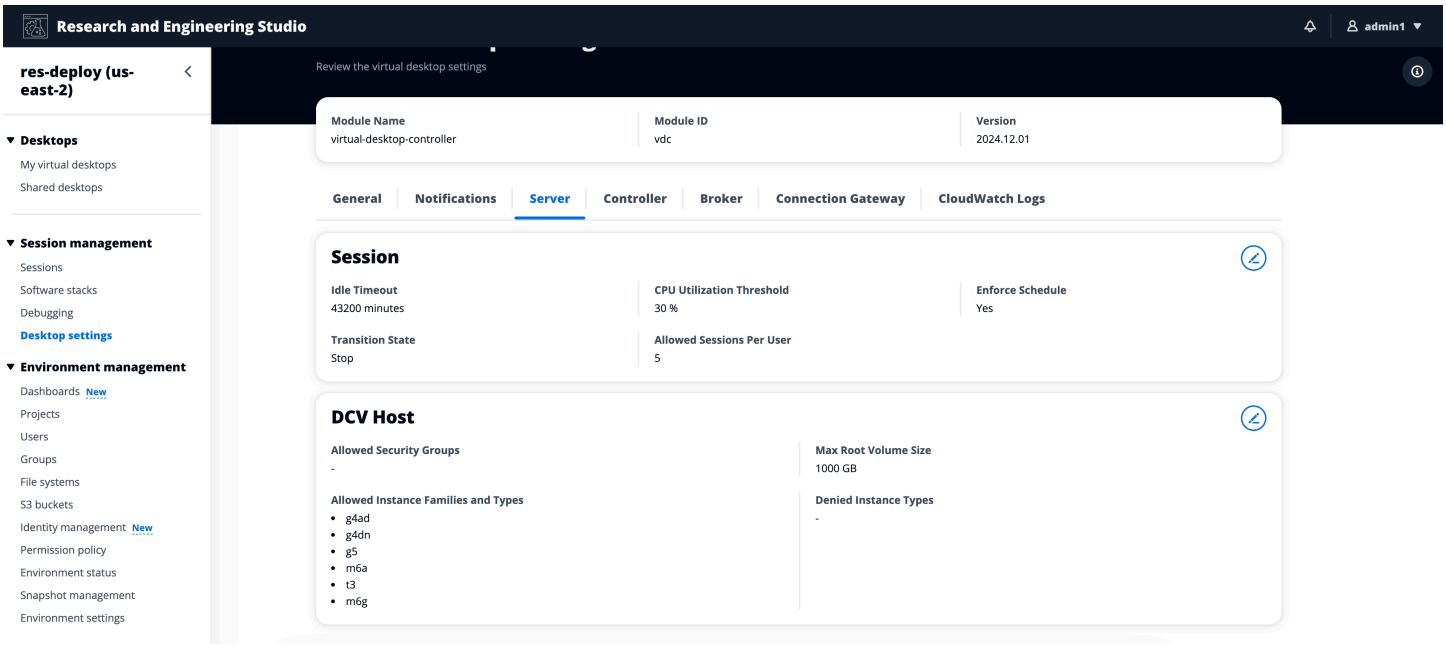
Allowed Instance Families and Types
Select instance families and types allowed for this software stack
m6a t3

5. Seleccione Enviar.

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

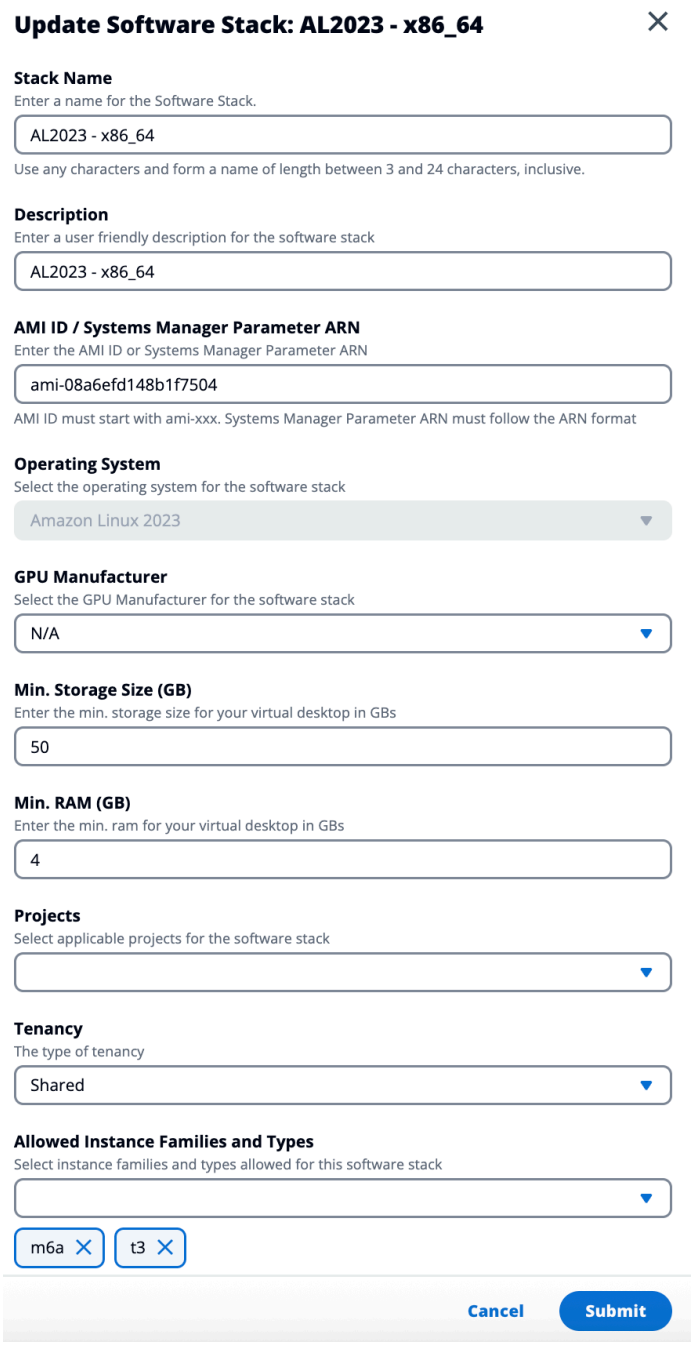
Modifique la lista de instancias de VDI de la pila de software

Para cada pila de software registrada, puedes elegir las familias y los tipos de instancias permitidos. La lista de opciones para cada pila de software se filtra según las opciones definidas en la configuración del escritorio. Allí puede buscar y modificar los tipos y familias de instancias permitidos a nivel mundial.



Para editar el atributo de familias y tipos de instancias permitidos de una pila de software:

1. En la página Pilas de software, seleccione el botón de radio de la pila de software.
2. Elija Acciones y, a continuación, seleccione Editar pila.
3. Elige las familias y los tipos de instancias que desees en la lista desplegable de Tipos y familias de instancias permitidos.



4. Seleccione Enviar.

> **Note**
>
> Si el conjunto global de familias y tipos de instancias permitidos incluye una familia de instancias y un tipo de instancia dentro de esa familia (por ejemplo, `t3` `yt3.large`), las

opciones disponibles para el atributo de familias y tipos de instancias permitidos de una pila de software solo incluirán la familia de instancias.

⚠ Important

- Cuando type/family se elimina una instancia de la lista de permitidos en el nivel del entorno, debe eliminarse automáticamente de todas las pilas de software.
- Las instancias types/families que se agregan a nivel de entorno no se agregan automáticamente a las pilas de software.

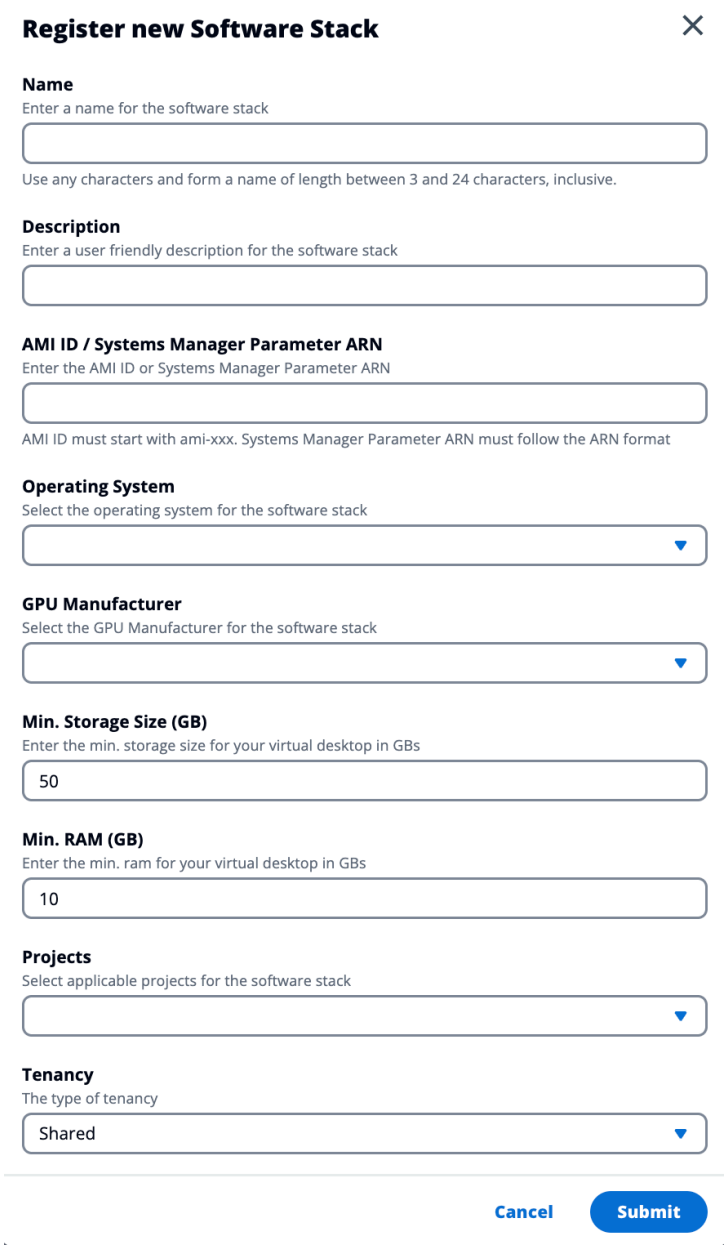
Vea los detalles de la pila de software

En la página Pilas de software, seleccione el nombre de la pila de software para ver sus detalles. También puede seleccionar el botón de radio de una pila de software, elegir Acciones y seleccionar Editar para editar la pila de software.

Soporte de arrendamiento de VDI

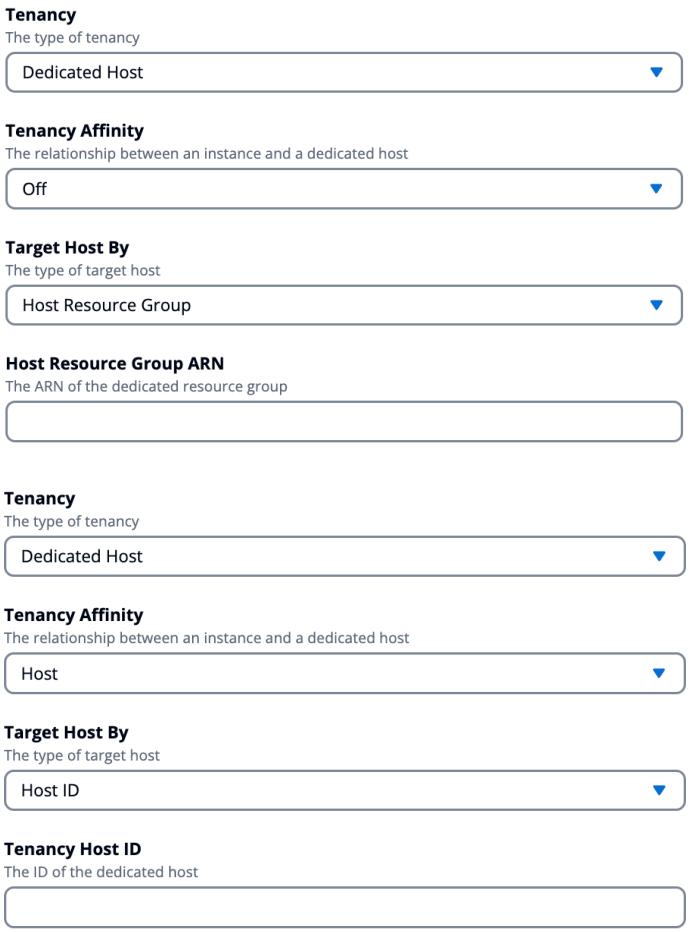
Al registrar una nueva pila de software o editar una pila de software existente, puede seleccionar el arrendamiento de los VDI lanzados desde esta pila de software. Se admiten los tres arrendamientos siguientes:

- Compartido (predeterminado): ejecute VDI con instancias de hardware compartidas
- Instancia dedicada: ejecute VDI con instancias dedicadas
- Host dedicado: ejecute VDI con un host dedicado



Al seleccionar el tipo de arrendamiento de host dedicado, también debe seleccionar la afinidad de arrendamiento y el tipo de host de destino. Se admiten los siguientes tipos de host de destino:

- Grupo de recursos de host: grupo de recursos de host creado en AWS License Manager
- ID de host: un ID de host específico



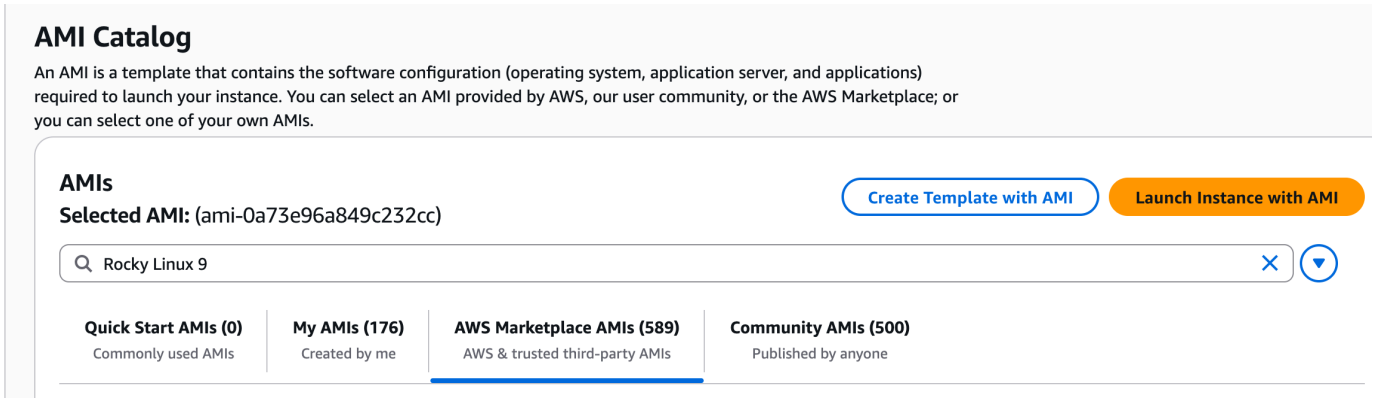
Para especificar las licencias autogestionadas que necesiten sus VDI al lanzarlas con la tenencia de host dedicada, asocie las licencias a su AMI siguiendo el procedimiento Asociar licencias autogestionadas y AMI de la Guía del usuario de License Manager AWS .

Añadir una pila de software de Rocky Linux 9

RES no tiene una pila de software predeterminada para Rocky Linux 9, por lo que esta sección ofrece una recomendación sobre qué AMI de Rocky usar y cómo usarla.

1. Inicie sesión en la consola AWS de administración y vaya a la página del catálogo de AMI en la consola EC2.
2. Busque las AMI en la pestaña AWS Marketplace con el nombre Rocky Linux 9.
3. Seleccione la AMI denominada Rocky Linux 9 (Official) - x86_64 de Rocky Linux.

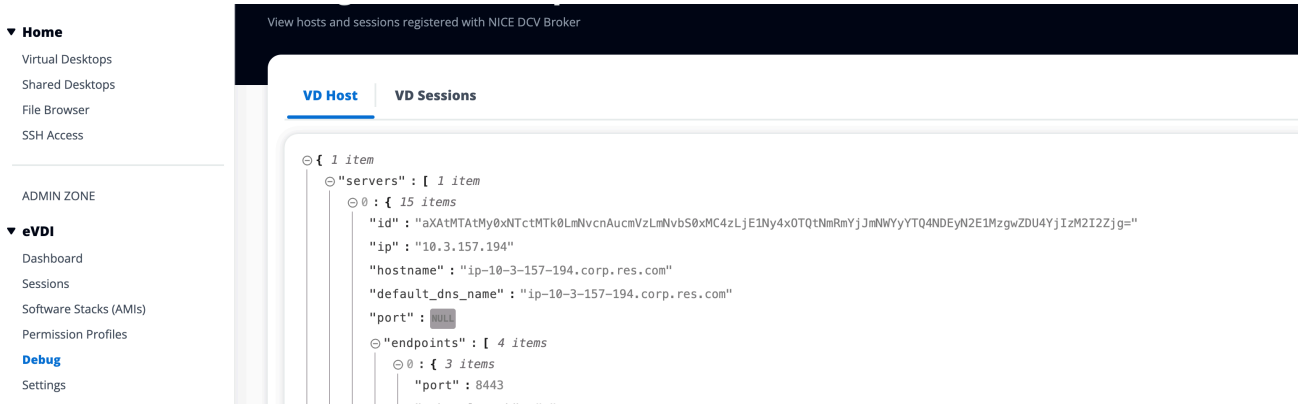
4. Una vez seleccionado, elija Suscríbase ahora.
5. Desplázate hacia arriba y copia el ID de la AMI seleccionada.



6. Vaya al portal RES y registre una nueva pila de software en la página Pilas de software mediante esta AMI.

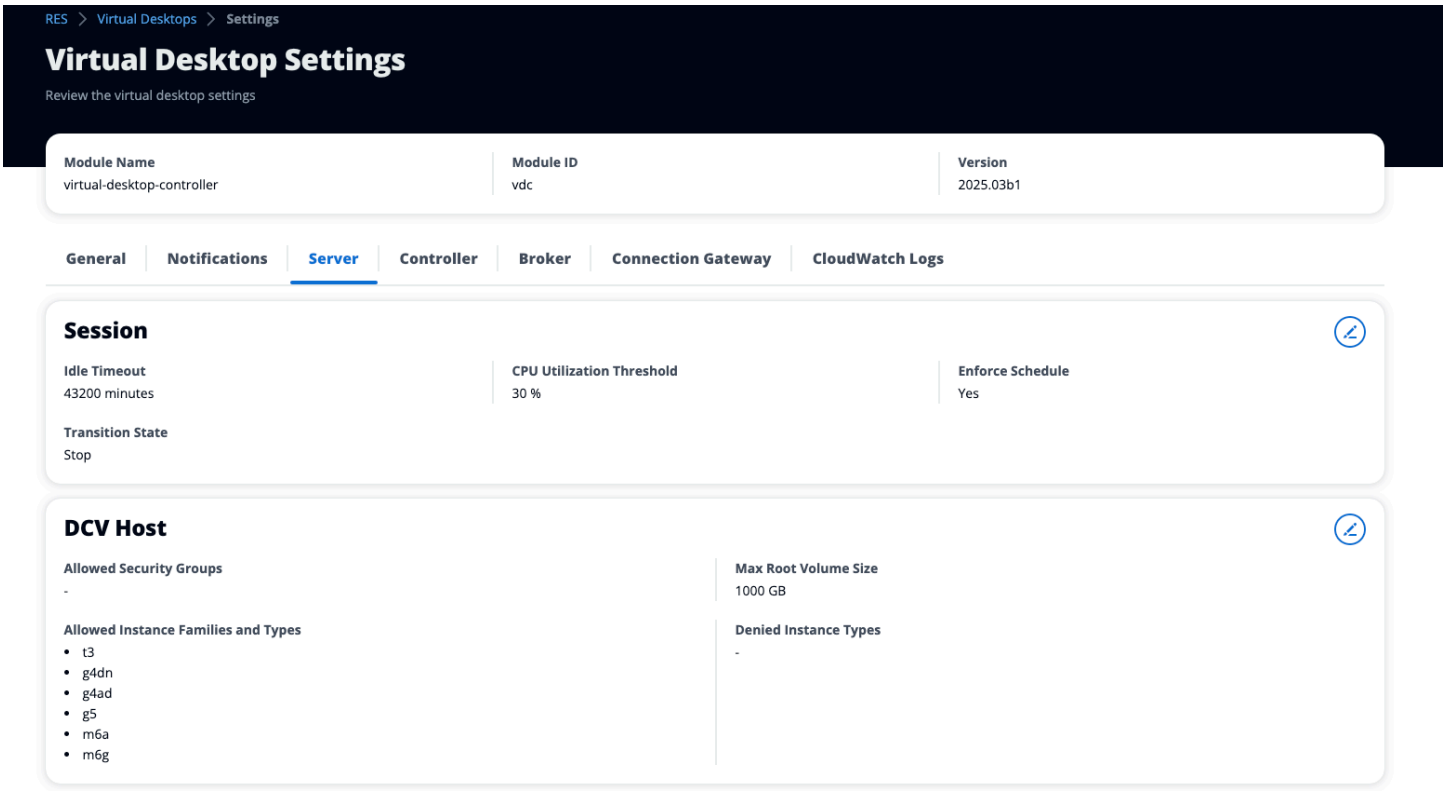
Debugging

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 Host de escritorio virtual muestra la actividad específica de la instancia y la pestaña Sesiones de escritorio virtual 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.



General

La pestaña General proporciona acceso a ajustes como:

QUIC

Activa QUIC en lugar de TCP como protocolo de transmisión predeterminado para todos sus escritorios virtuales.

Tipo de sesión DCV predeterminado

El tipo de sesión DCV predeterminado que se utiliza para todos los escritorios virtuales. Esta configuración no se aplicará a los escritorios creados anteriormente. Esto solo se aplicará en los casos en que el tipo de instancia y el sistema operativo admitan los tipos de sesión virtual o de consola.

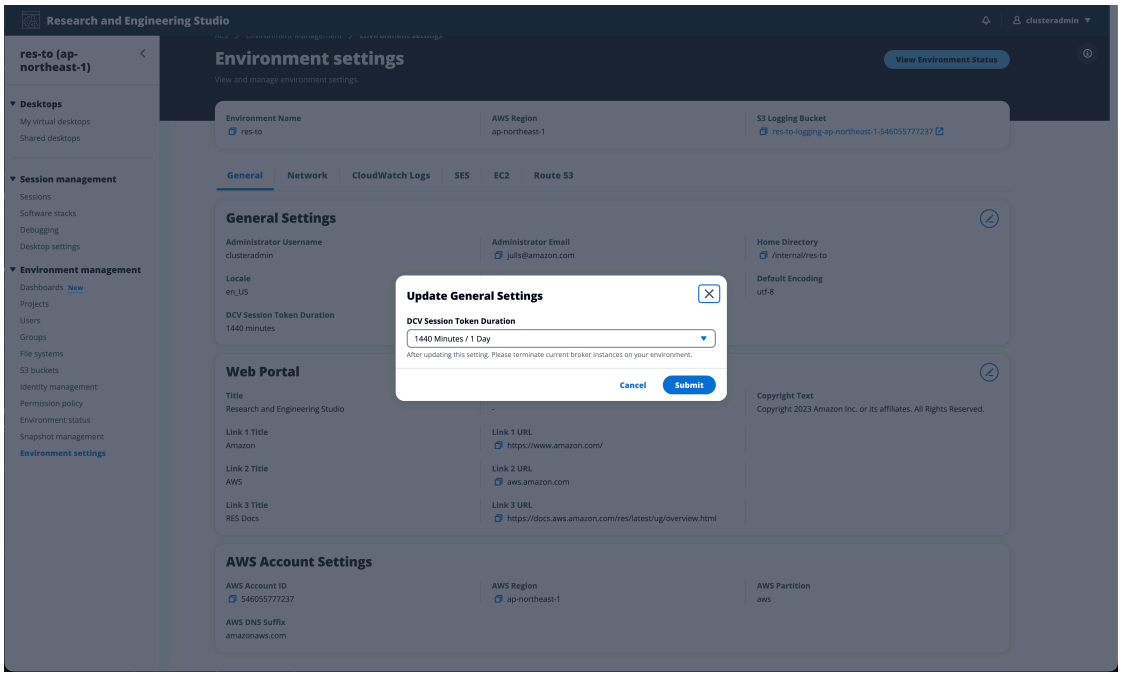
Sesiones permitidas de forma predeterminada por usuario y proyecto

El valor predeterminado para el número permitido de sesiones de VDI por usuario y proyecto.

Expiración del token de sesión de DCV

El tiempo durante el cual un token de sesión DCV sigue siendo válido. Cuando un token caduca, los usuarios deben volver a descargar el archivo de conexión DCV del portal web para seguir accediendo a su sesión de escritorio virtual. Las opciones disponibles son:

- 1440 minutos (1 día)
- 10.080 minutos (7 días)
- 43.200 minutos (30 días)



Servidor

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

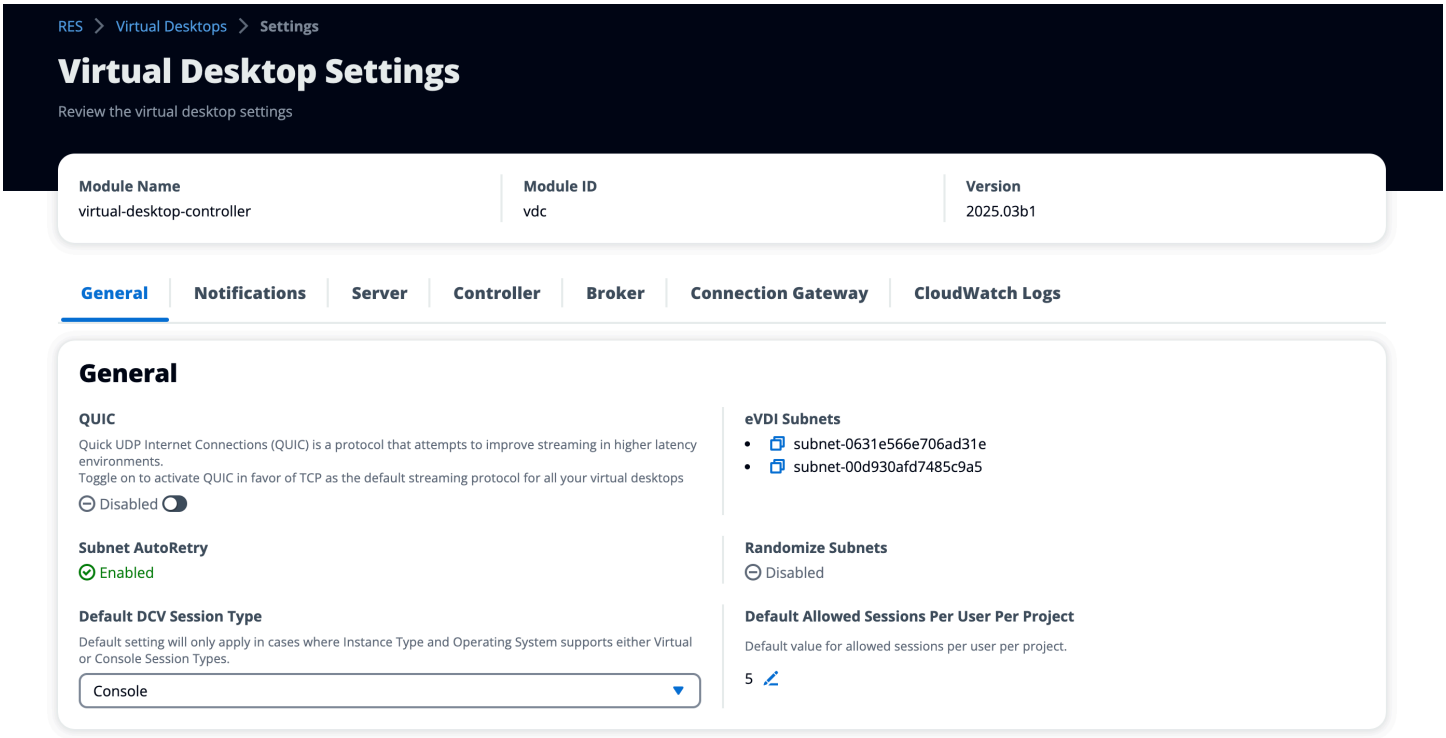
: El uso de la CPU debe considerarse inactivo.

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

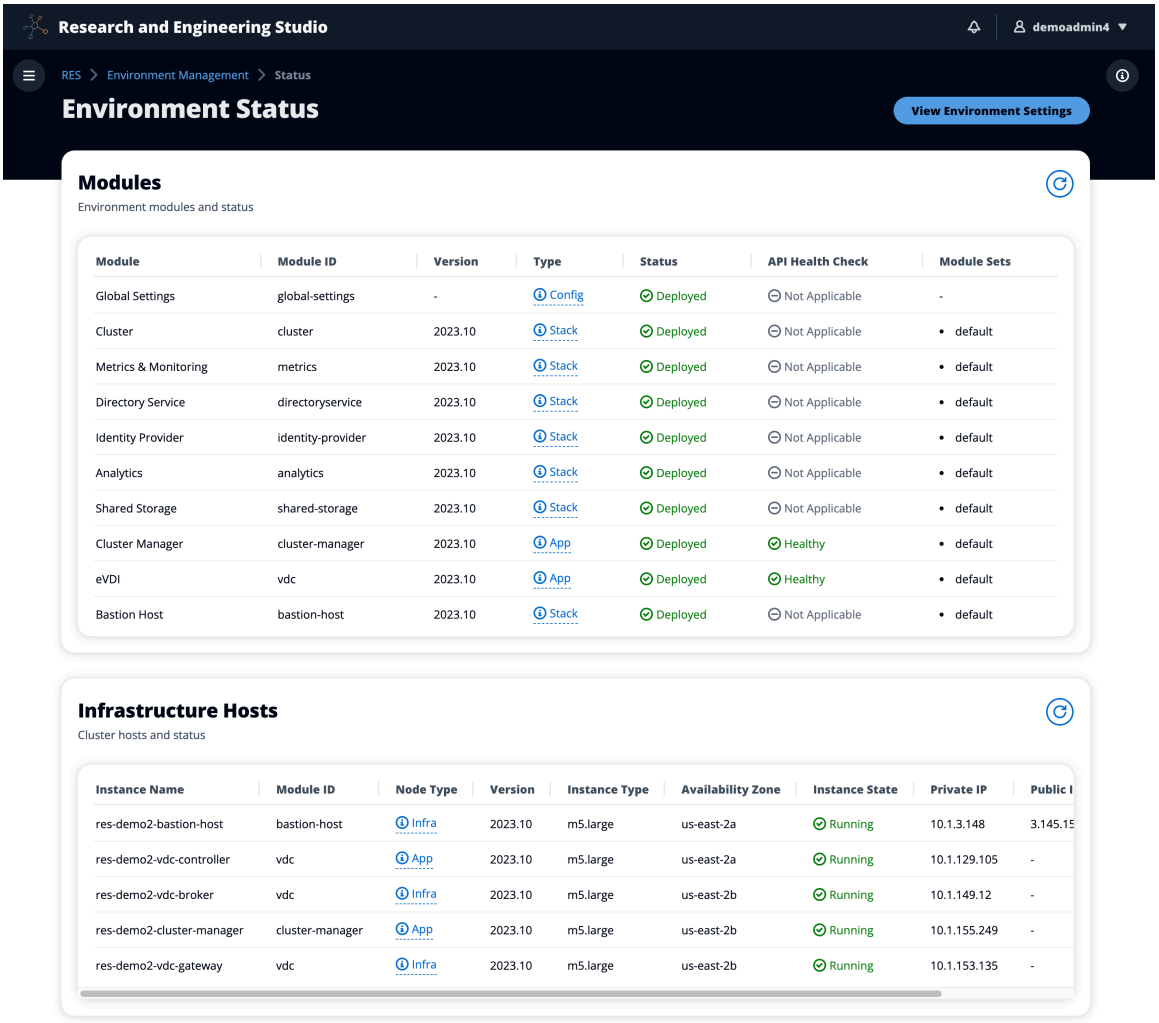
Desde la sección de gestión medioambiental de Research and Engineering Studio, los usuarios administrativos pueden crear y gestionar entornos aislados para sus proyectos de investigación e ingeniería. Estos entornos pueden incluir recursos informáticos, almacenamiento y otros componentes necesarios, 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

- Administración de instantáneas
- Buckets de Amazon S3

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.



Configuración del entorno

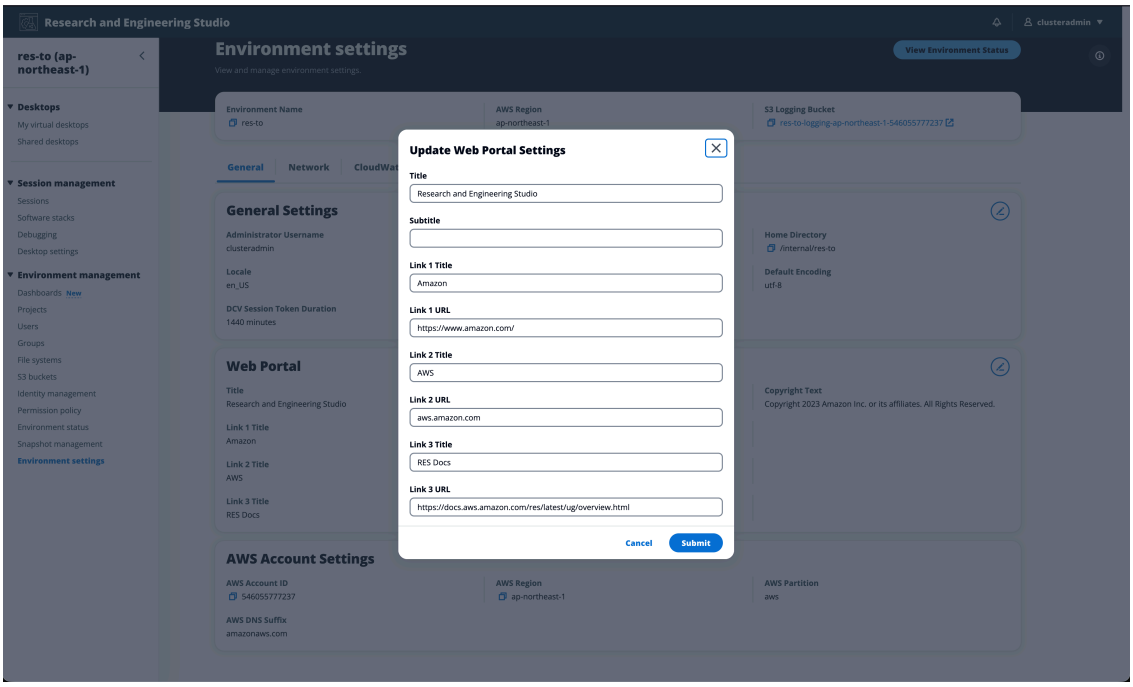
La página de configuración del entorno muestra los detalles de configuración del producto, como:

- General

Puede editar el título y los subtítulos del portal web y añadir enlaces personalizados a la página de inicio de sesión del portal web. Para configurar los enlaces personalizados:

1. Vaya a Administración del entorno > Configuración del entorno.
2. En la pestaña General, elija Editar.
3. En la sección Enlaces personalizados, selecciona Añadir enlace.
4. Introduce un título y una URL para cada enlace que quieras mostrar en la página de inicio de sesión.
5. Elija Enviar para guardar los cambios.

Los enlaces personalizados aparecen en la página de inicio de sesión del portal web, lo que permite a los administradores dirigir a los usuarios a recursos como la documentación interna, las páginas de soporte o las políticas de uso aceptable.



- Proveedor de identidades

  Muestra información como el Sign-On estado único.

- Network

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

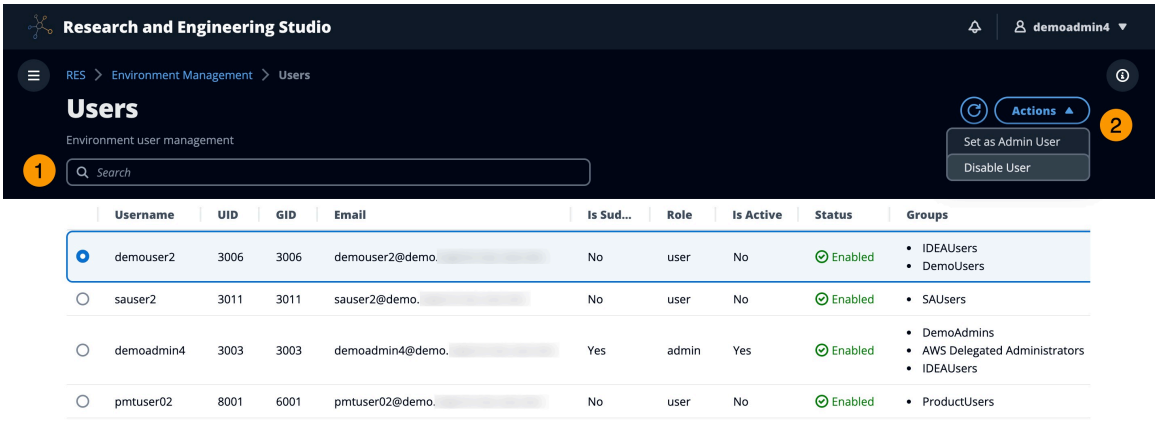
- Directory Service

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.

Users

Todos los usuarios sincronizados desde su directorio activo 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.

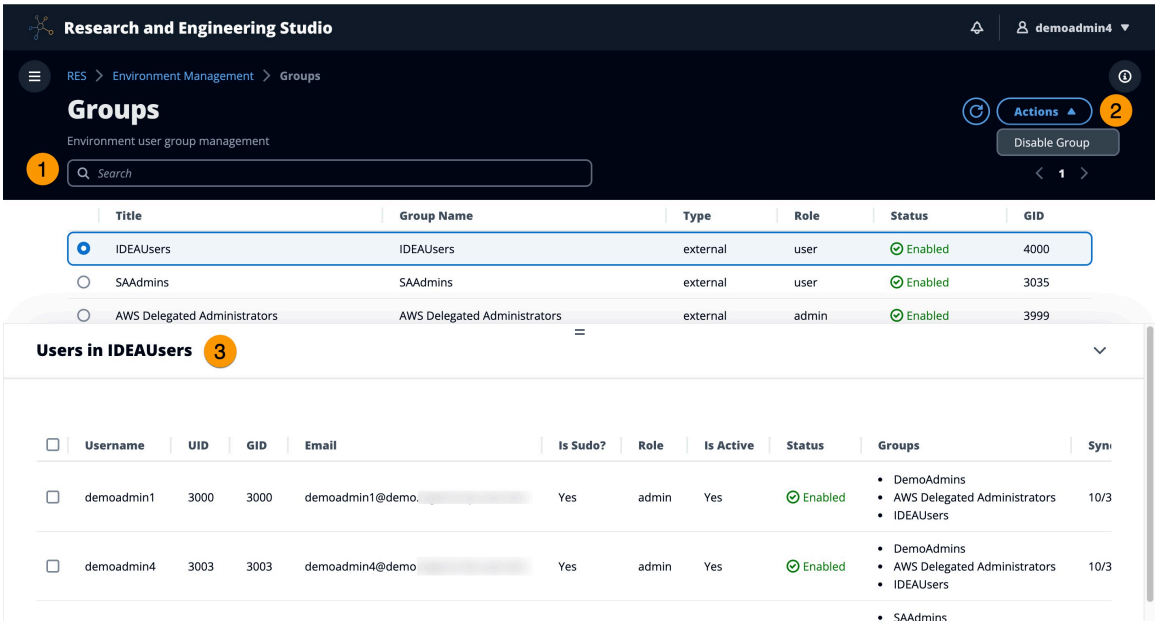


Desde la página de usuarios, puedes:

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

Groups

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.

Proyectos

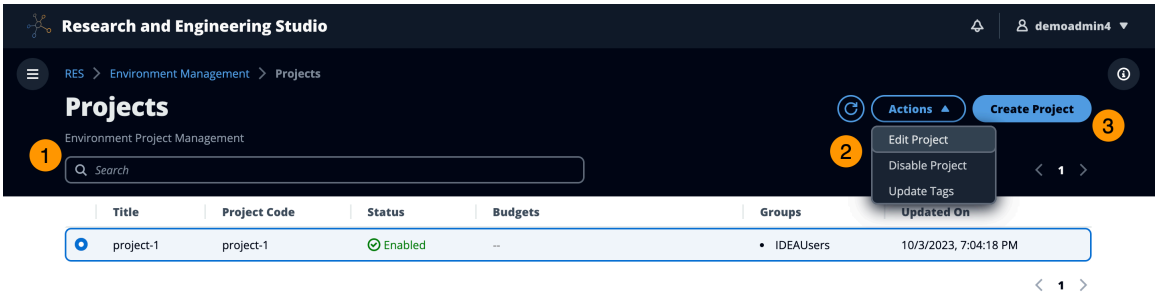
Los proyectos constituyen un límite para los escritorios, los equipos y los presupuestos virtuales. Al crear un proyecto, se definen sus ajustes, como el nombre, la descripción y la configuración del entorno. Los proyectos suelen incluir uno o más entornos, que se pueden personalizar para cumplir con 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
- Desactivar un proyecto
- Eliminación de 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
   d. Eliminación de un proyecto
3. Puede elegir Crear proyecto para crear un proyecto nuevo.

Crear un proyecto

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

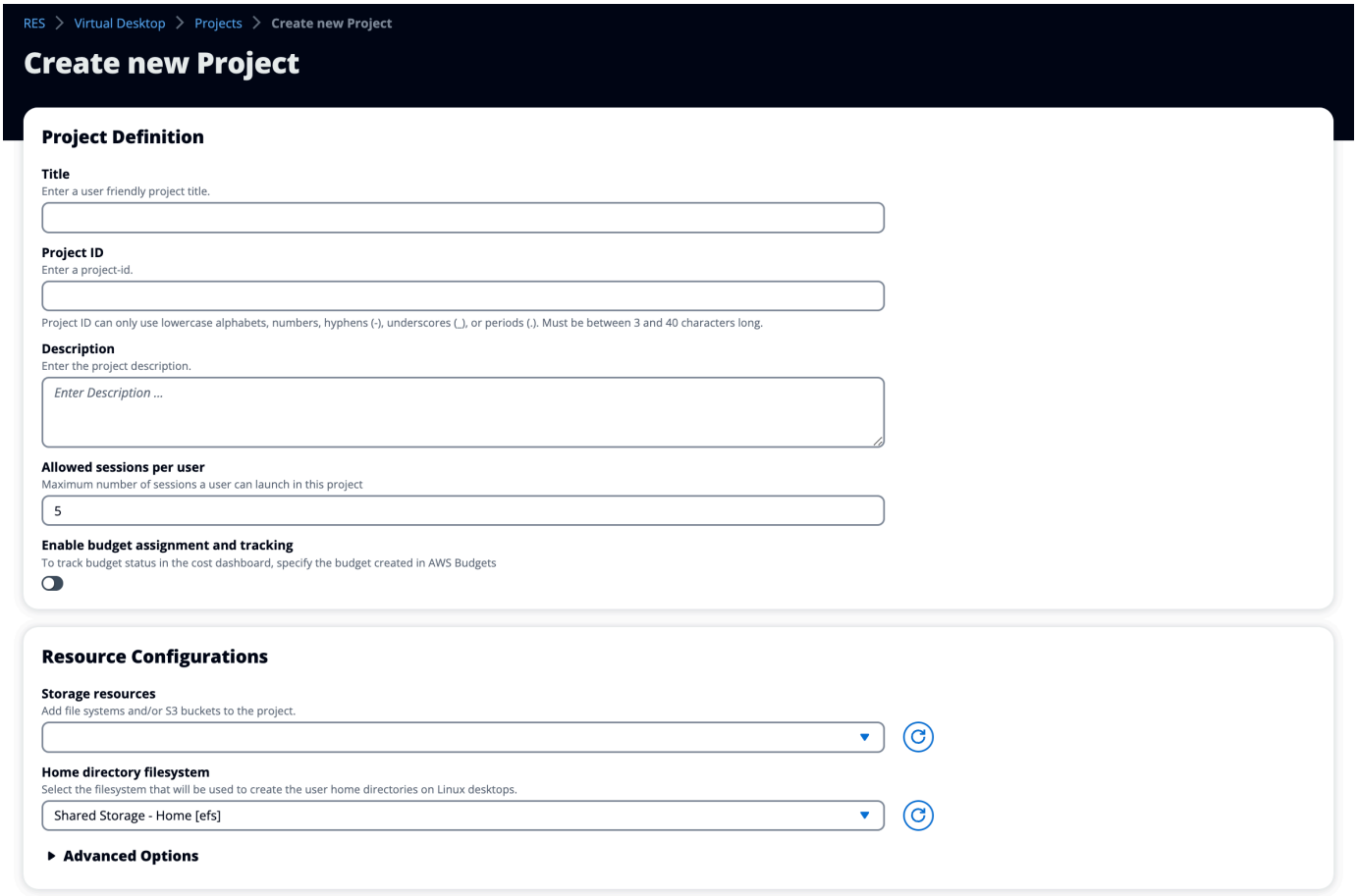
El identificador del proyecto es una etiqueta de recursos que se puede utilizar para realizar un seguimiento de la asignación de costes AWS Cost Explorer Service. Para obtener más información, consulte Activación de etiquetas de asignación de costes definidas por el usuario.

> **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. El sistema de archivos del directorio principal puede utilizar el sistema de archivos principal compartido (predeterminado), EFS, FSx for Lustre, NetApp FSx ONTAP o EBS.

   El sistema de archivos doméstico compartido, EFS, FSx for Lustre y NetApp FSx ONTAP se pueden compartir en varios proyectos y VDI. Sin embargo, la opción de almacenamiento por volumen de EBS requerirá que cada VDI de ese proyecto tenga su propio directorio principal que no esté compartido entre otros VDI o proyectos. También puede incorporar varios volúmenes desde un único sistema de archivos FSx NetApp ONTAP.



5. Asigne a los usuarios, grupos o a ambos el rol apropiado («miembro del proyecto» o «propietario del proyecto»). Consulta Perfiles de permisos predeterminados las acciones que puede realizar cada rol.
6. Seleccione Enviar.

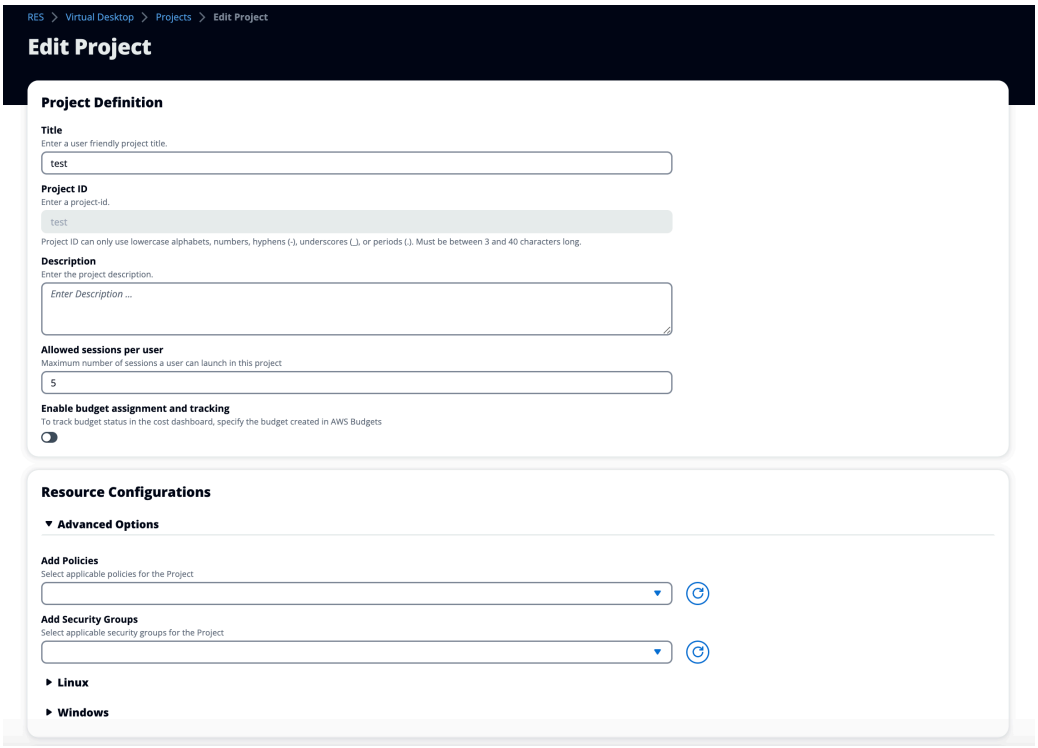
Edita un proyecto

1. Elija un proyecto de la lista de proyectos.
2. En el menú Acciones, selecciona Editar proyecto.
3. Introduce tus actualizaciones.

   Si tiene intención de activar los presupuestos, consulte Supervisión y control de costes para obtener más información. Al elegir un presupuesto para el proyecto, es posible que las opciones del menú desplegable del presupuesto tarden unos segundos en cargarse. Si no ve el presupuesto que acaba de crear, pulse el botón de actualización situado junto al menú desplegable.

Para obtener información sobre las opciones avanzadas, consulte. Añadir una plantilla de lanzamiento

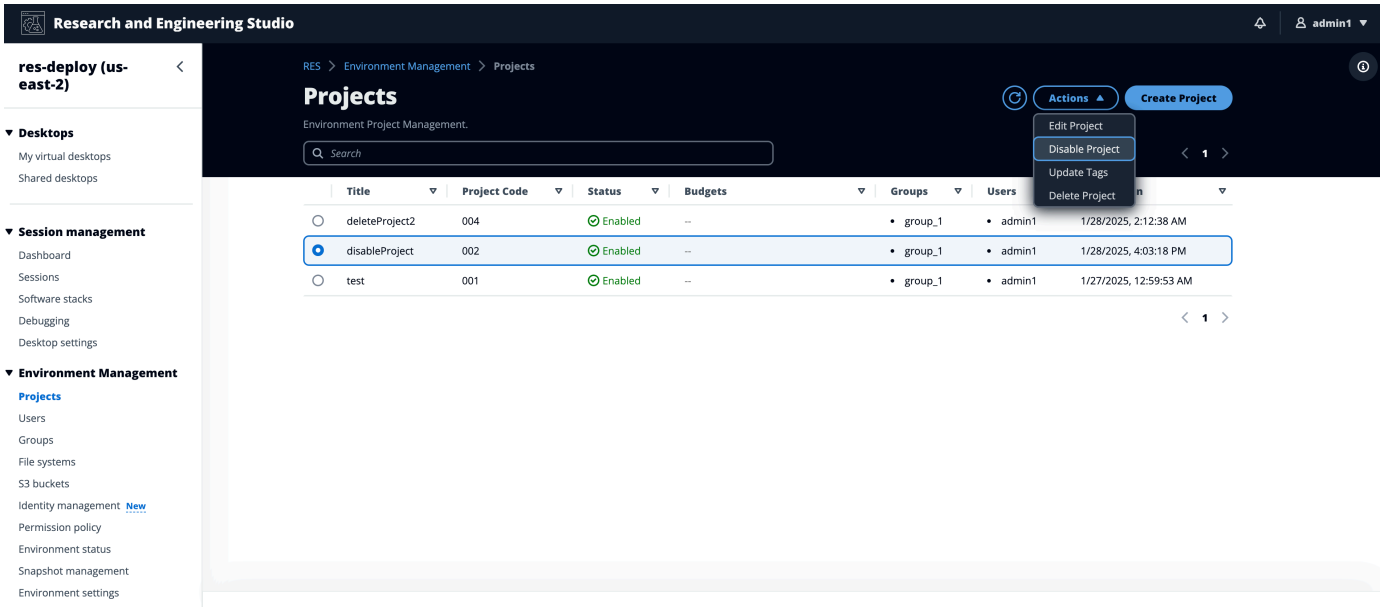
4. Seleccione Enviar.



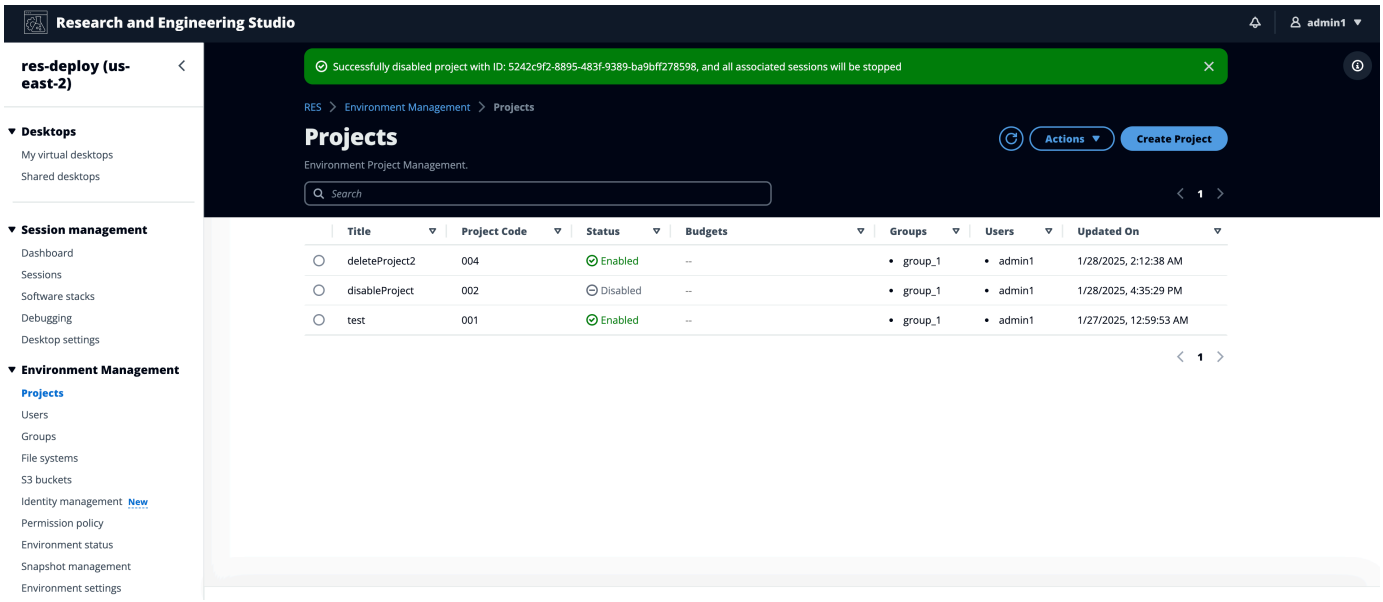
Desactivar un proyecto

Para deshabilitar un proyecto:

1. Seleccione un proyecto de la lista de proyectos.
2. En el menú Acciones, selecciona Desactivar proyecto.



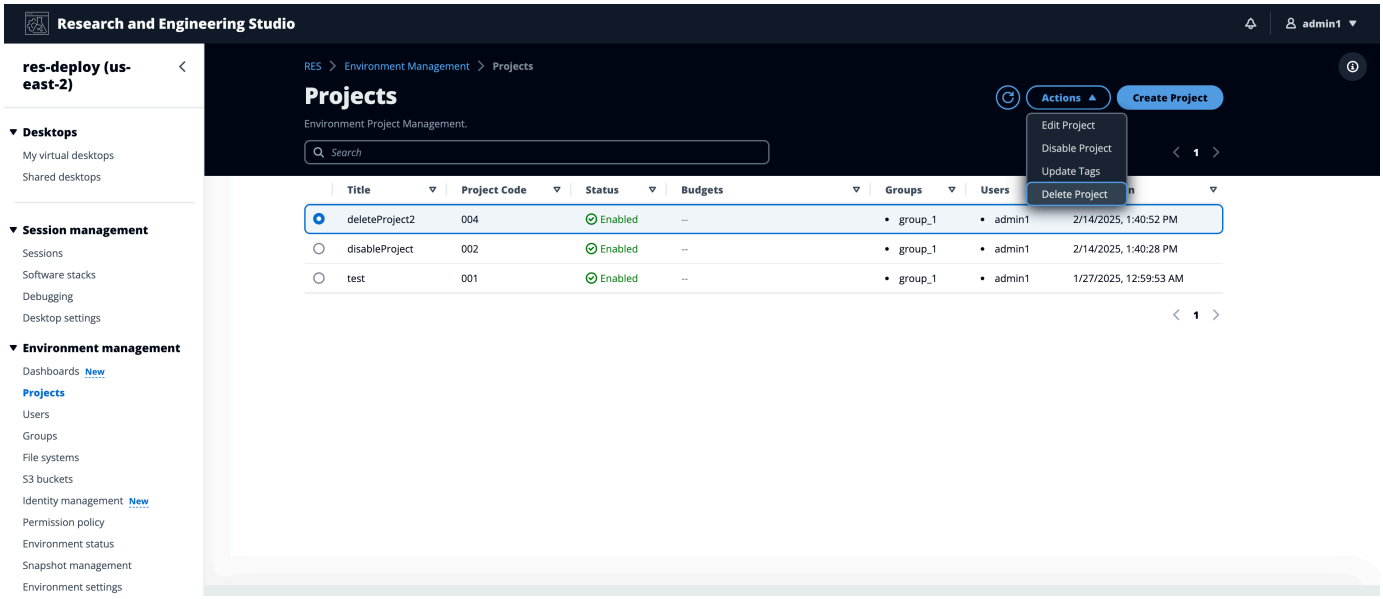
3. Si un proyecto está deshabilitado, se detienen todas las sesiones de VDI asociadas a ese proyecto. Esas sesiones no se pueden reiniciar mientras el proyecto esté desactivado.



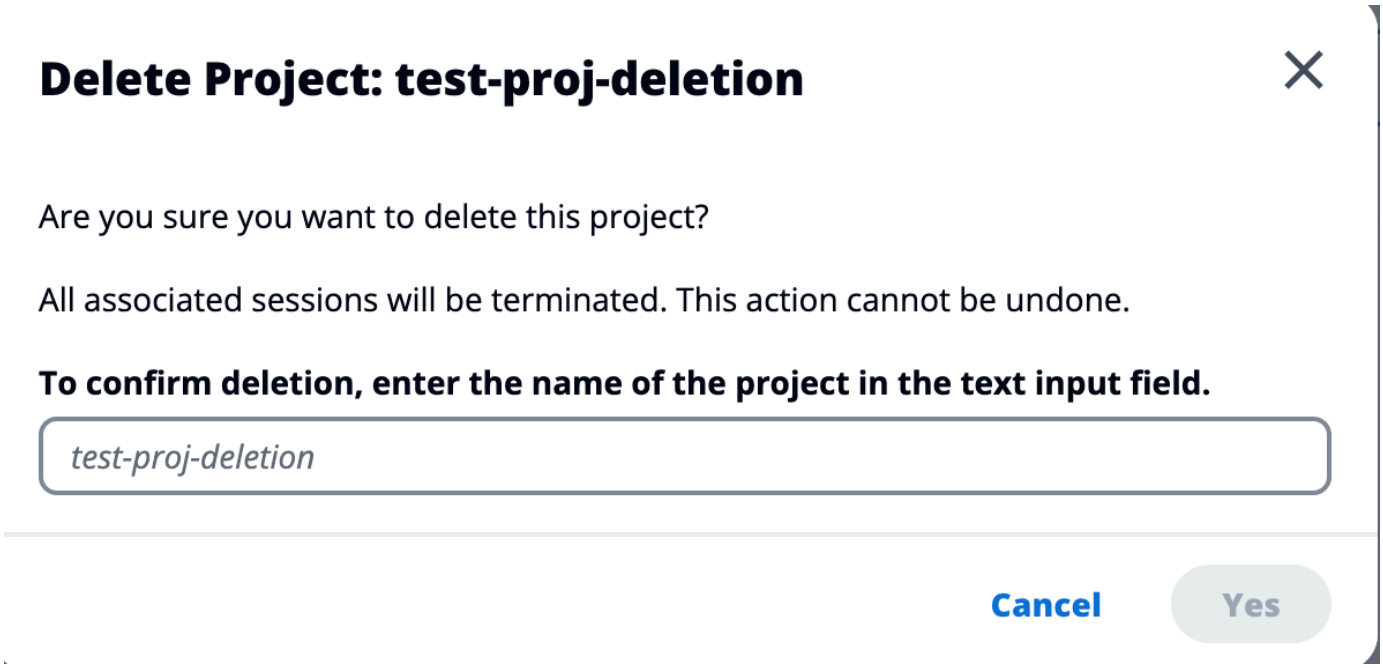
Eliminación de un proyecto

Para eliminar un proyecto:

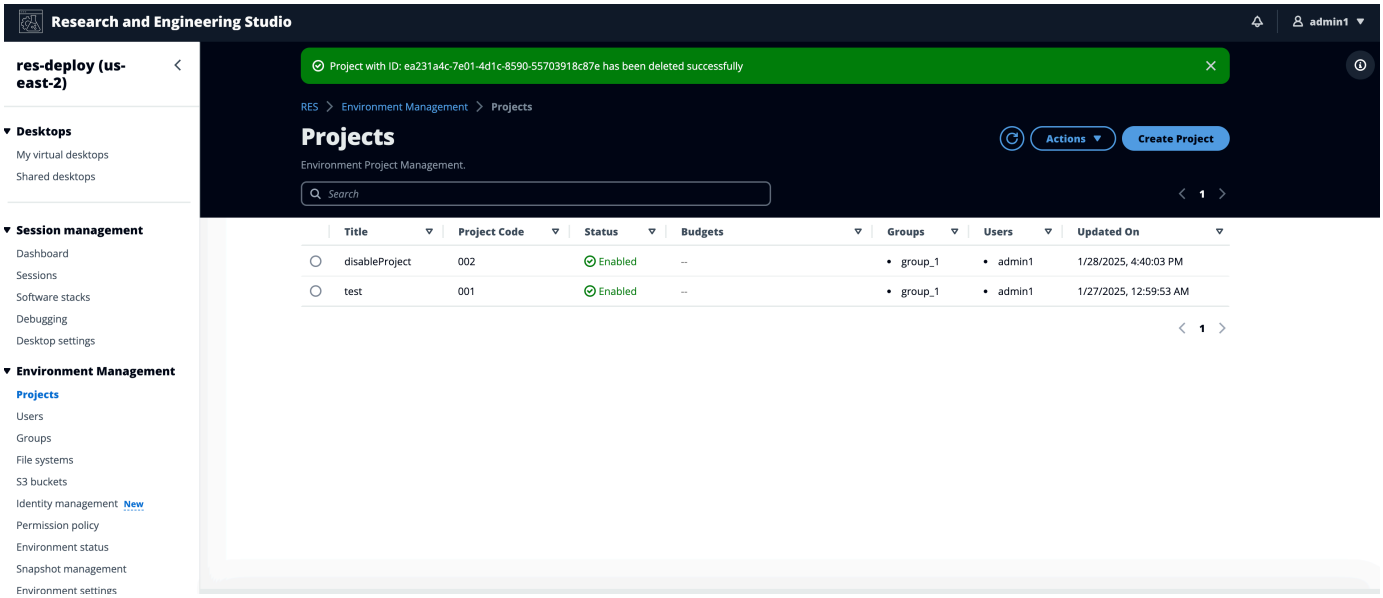
1. Seleccione un proyecto de la lista de proyectos.
2. En el menú Acciones, selecciona Eliminar proyecto.



3. Aparece una ventana emergente de confirmación. Introduzca el nombre del proyecto y, a continuación, seleccione Sí para eliminarlo.



4. Si se elimina un proyecto, se cancelan todas las sesiones de VDI asociadas a ese proyecto.



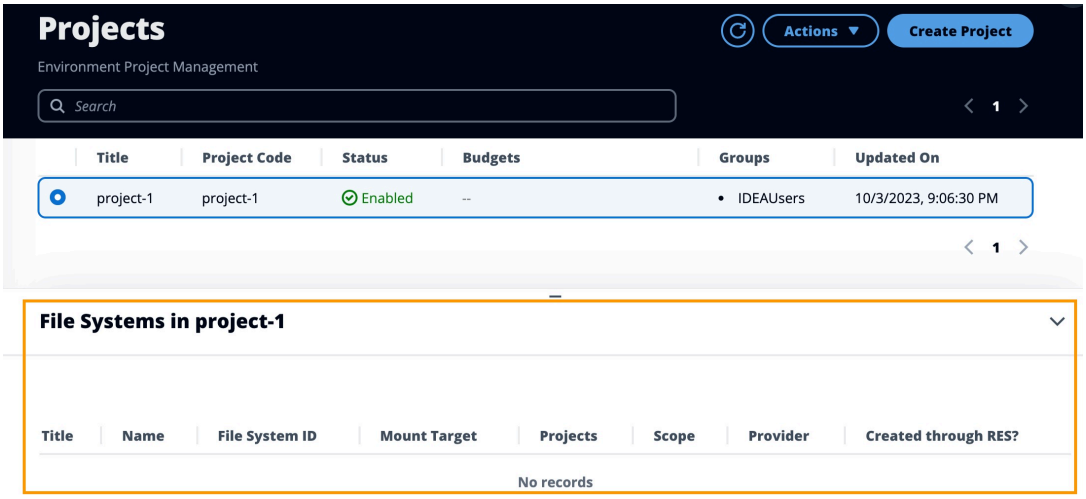
Añadir o eliminar etiquetas de un proyecto

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

1. Elija un proyecto de la lista de proyectos.
2. En el menú Acciones, selecciona 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.

Añada 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.

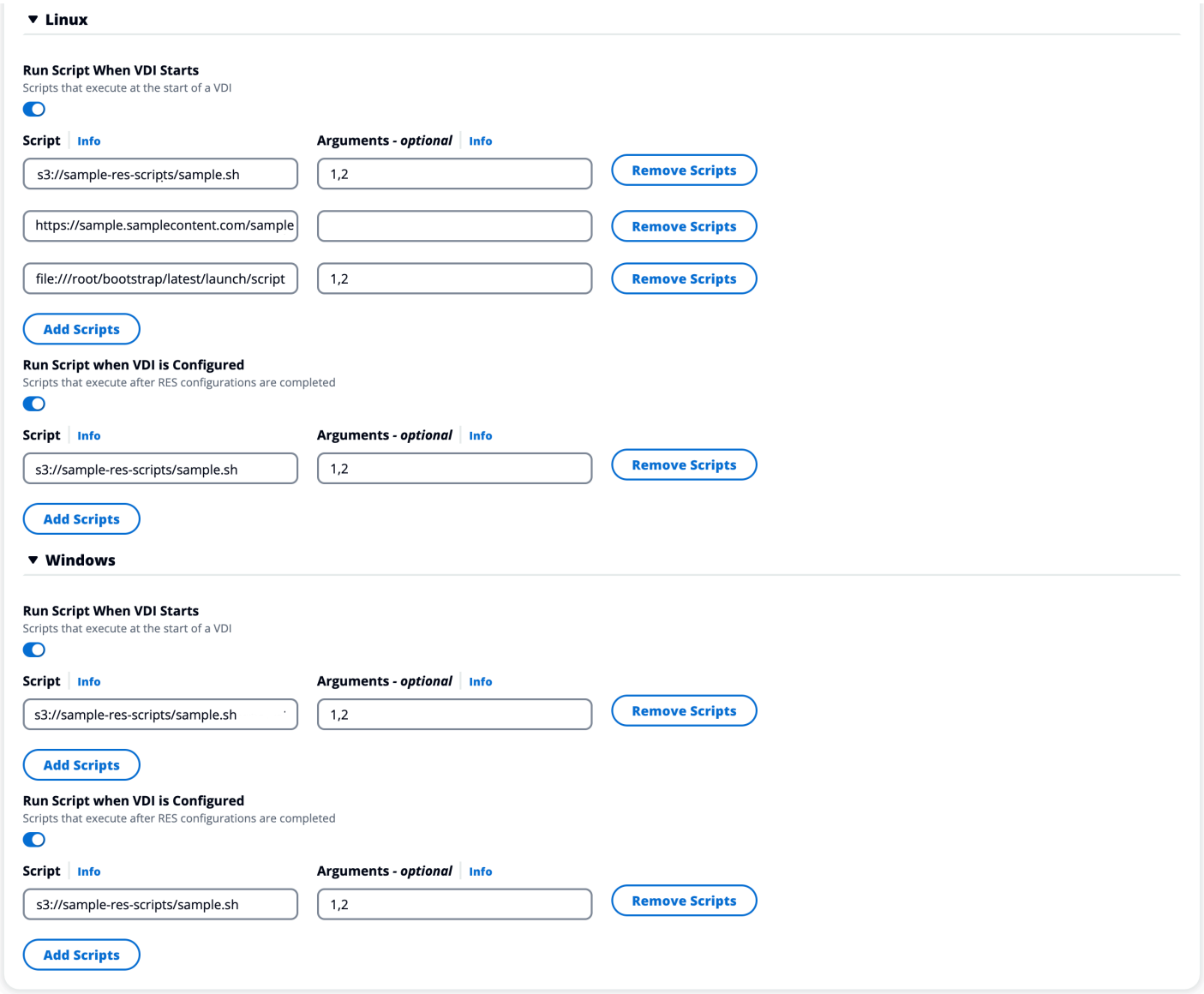
Los scripts admiten las siguientes opciones:

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

Todos los scripts personalizados que se alojan en buckets de S3 deben aprovisionarse con la siguiente etiqueta:

```
res:EnvironmentName/<res-environment>
```

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



Ejemplo de configuración de un proyecto

Ejemplos de plantillas para scripts de lanzamiento.

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.

#!/bin/bash

echo "start_script.sh running" >> /test_scripts
echo "All arguments: $@" >> /test_scripts
echo "Argument count: $#" >> /test_scripts
echo "Argument 1, $1" >> /test_scripts
echo "Argument 2, $2" >> /test_scripts
echo "end of start_script.sh" >> /test_scripts
```

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.

#!pwsh

Write-Output "configure_script.ps1 running" | Out-File -Append -FilePath "/
test_scripts"
Write-Output "All arguments: $args" | Out-File -Append -FilePath "/test_scripts"
Write-Output "Argument count: $($args.Count)" | Out-File -Append -FilePath "/
test_scripts"
Write-Output "Argument 1, $($args[0])" | Out-File -Append -FilePath "/test_scripts"
Write-Output "Argument 2, $($args[1])" | Out-File -Append -FilePath "/test_scripts"
Write-Output "end of configure_script.ps1" | Out-File -Append -FilePath "/
test_scripts"
```

Política de permisos

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 gestión 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 «sesión de Create/Terminate otro usuario», que permite a un usuario designado crear o finalizar las sesiones de otros usuarios de un proyecto.

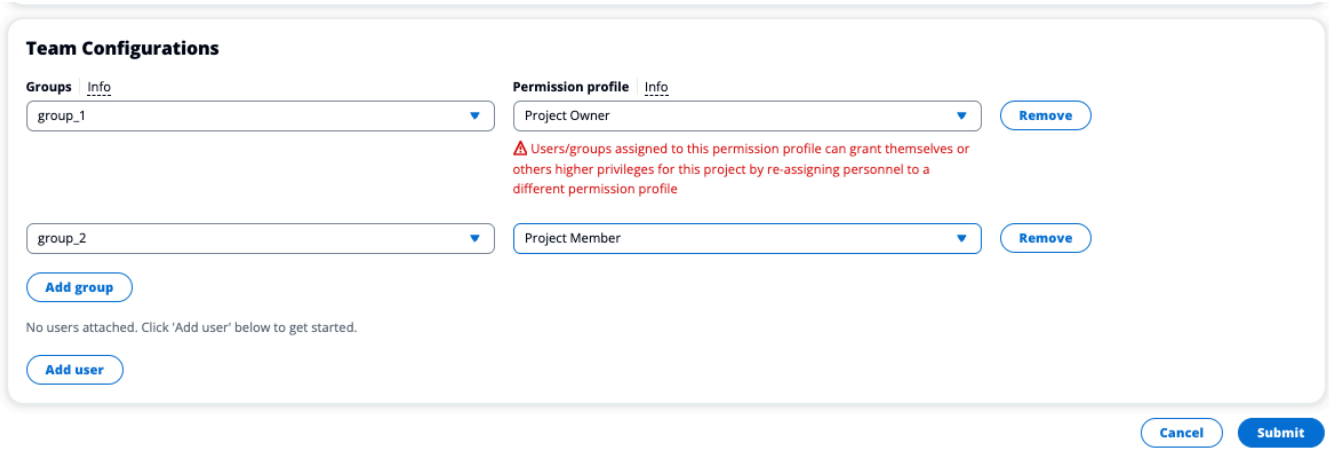
De esta forma, los administradores pueden delegar los permisos basados en el proyecto a personas de su entorno que no sean administradores.

Temas

Permisos de gestión de proyectos

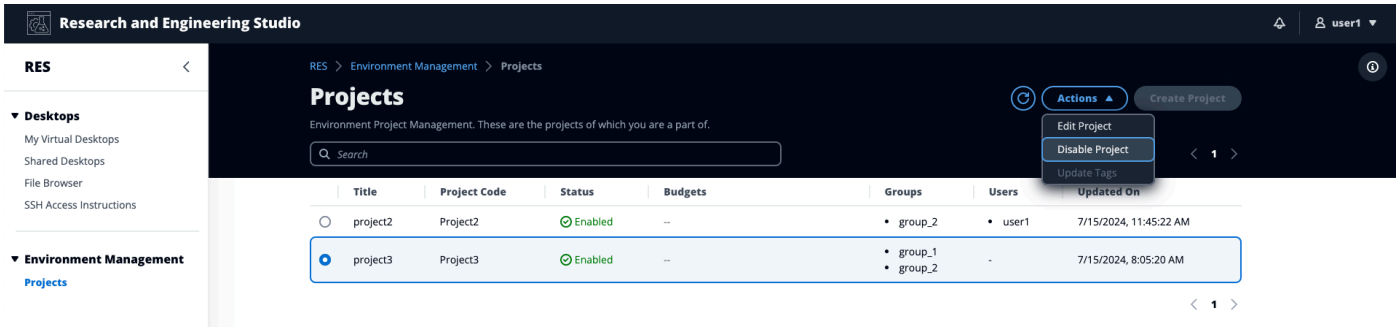
Actualizar la membresía del proyecto

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.

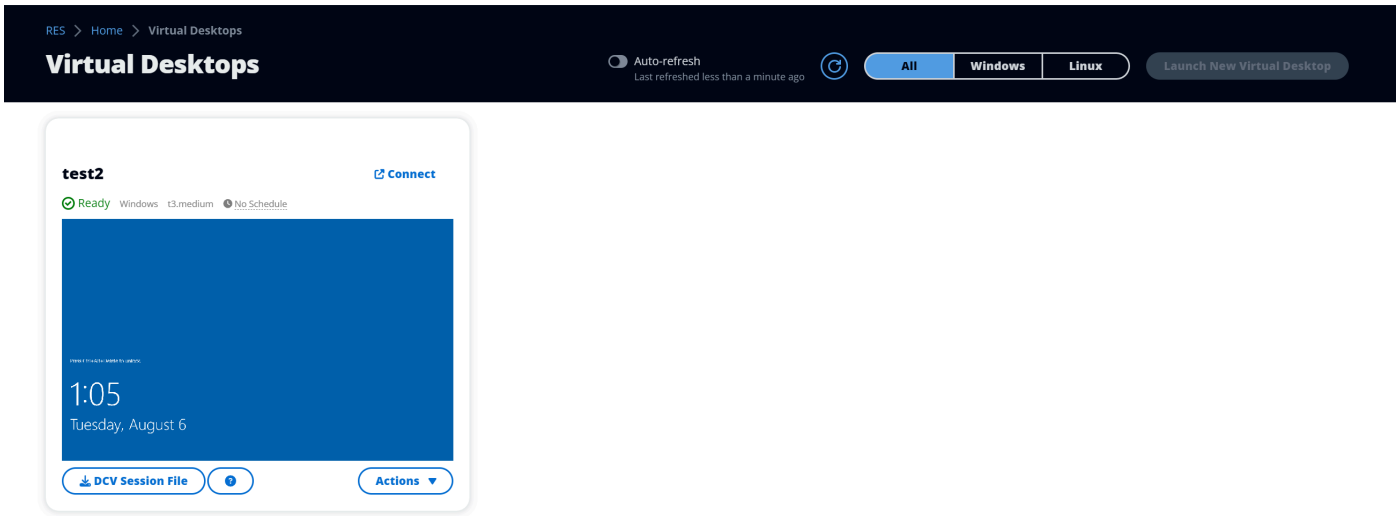


Permisos de administración de sesiones de VDI

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.

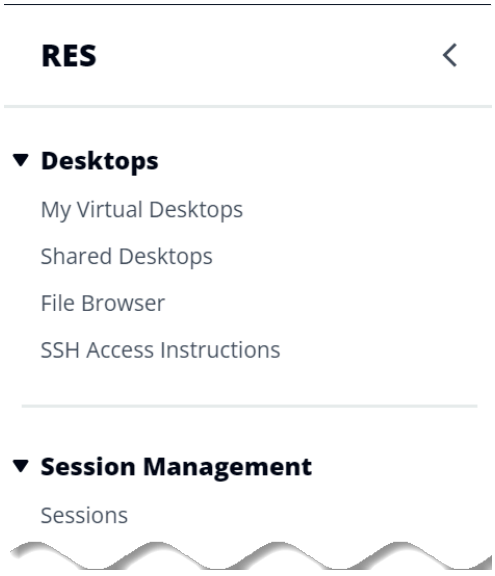
Si un usuario que no es administrador no tiene permisos para crear una sesión, se le deshabilitará el botón Iniciar un nuevo escritorio virtual, tal y como se muestra a continuación:



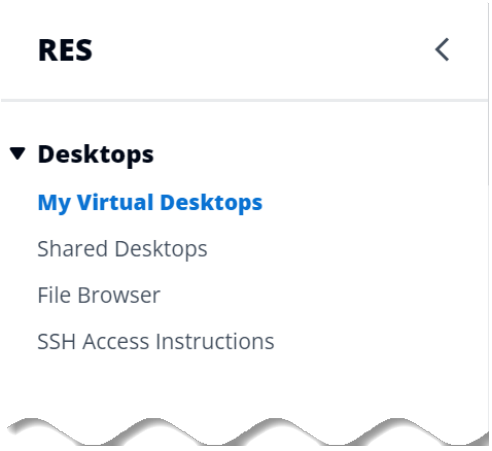
Cree o finalice las sesiones de otros

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 a continuación:

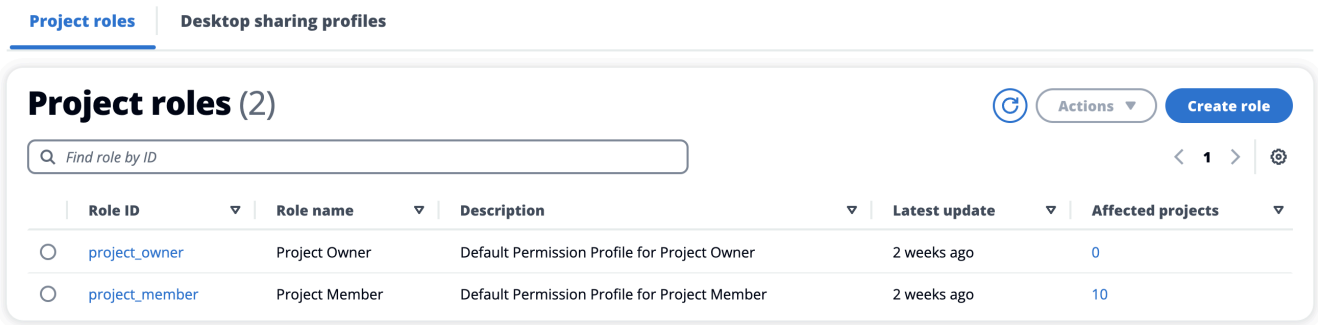


Administrar los perfiles de permisos

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

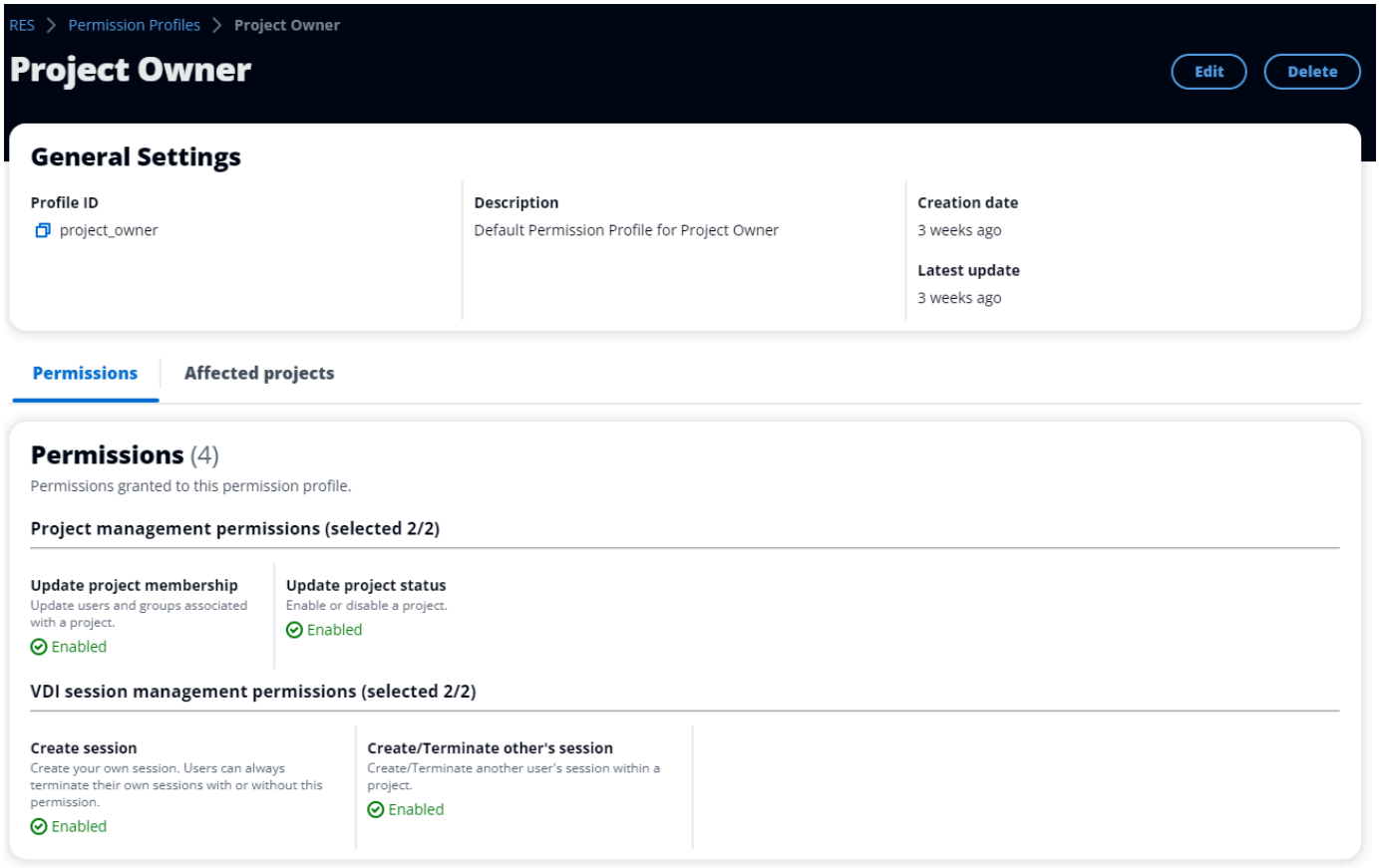
Enumere los perfiles de permisos

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

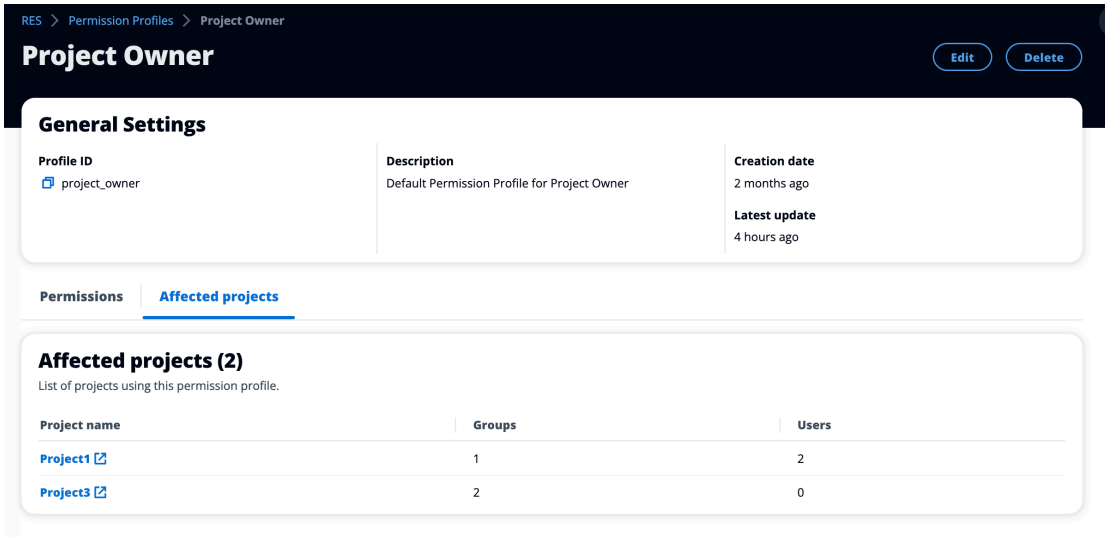


Ver los perfiles de permisos

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.



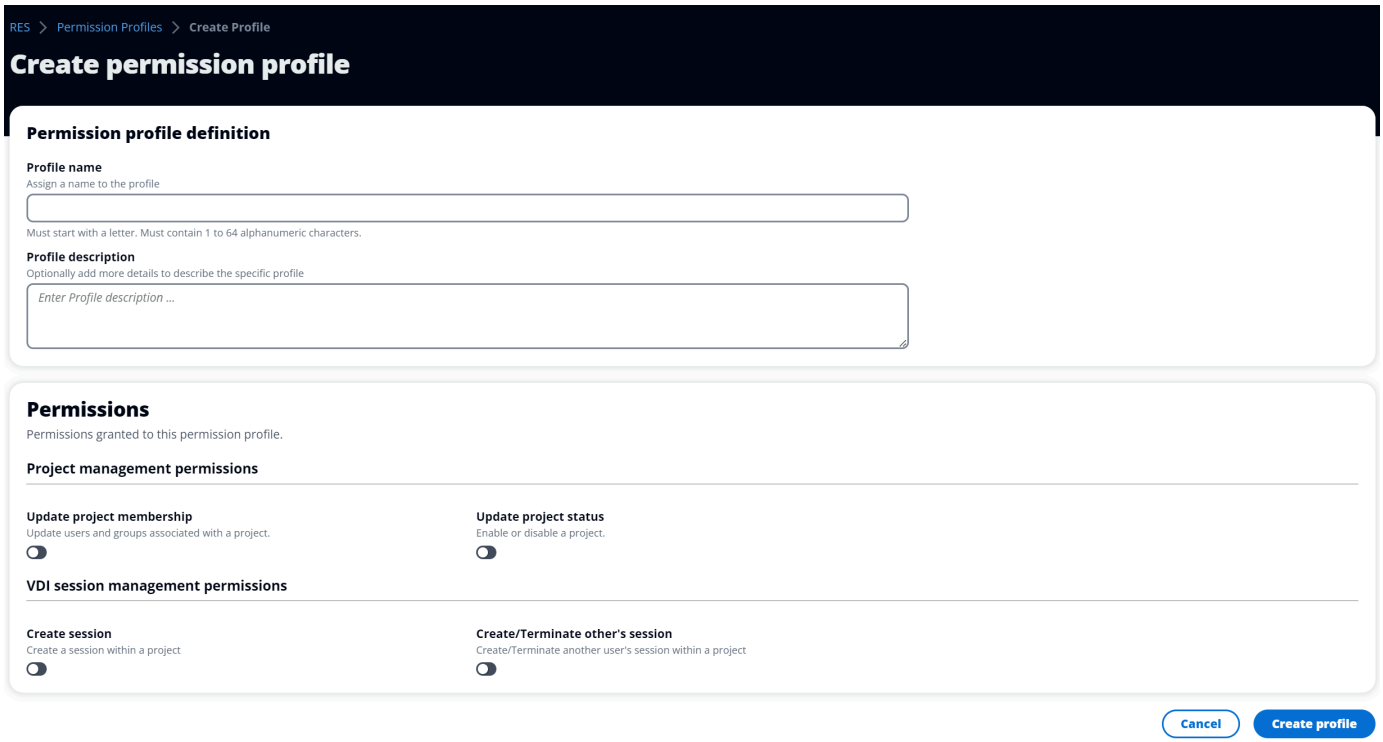
2. Seleccione la pestaña Proyectos afectados para ver los proyectos que utilizan actualmente el perfil de permisos.



Cree perfiles de permisos

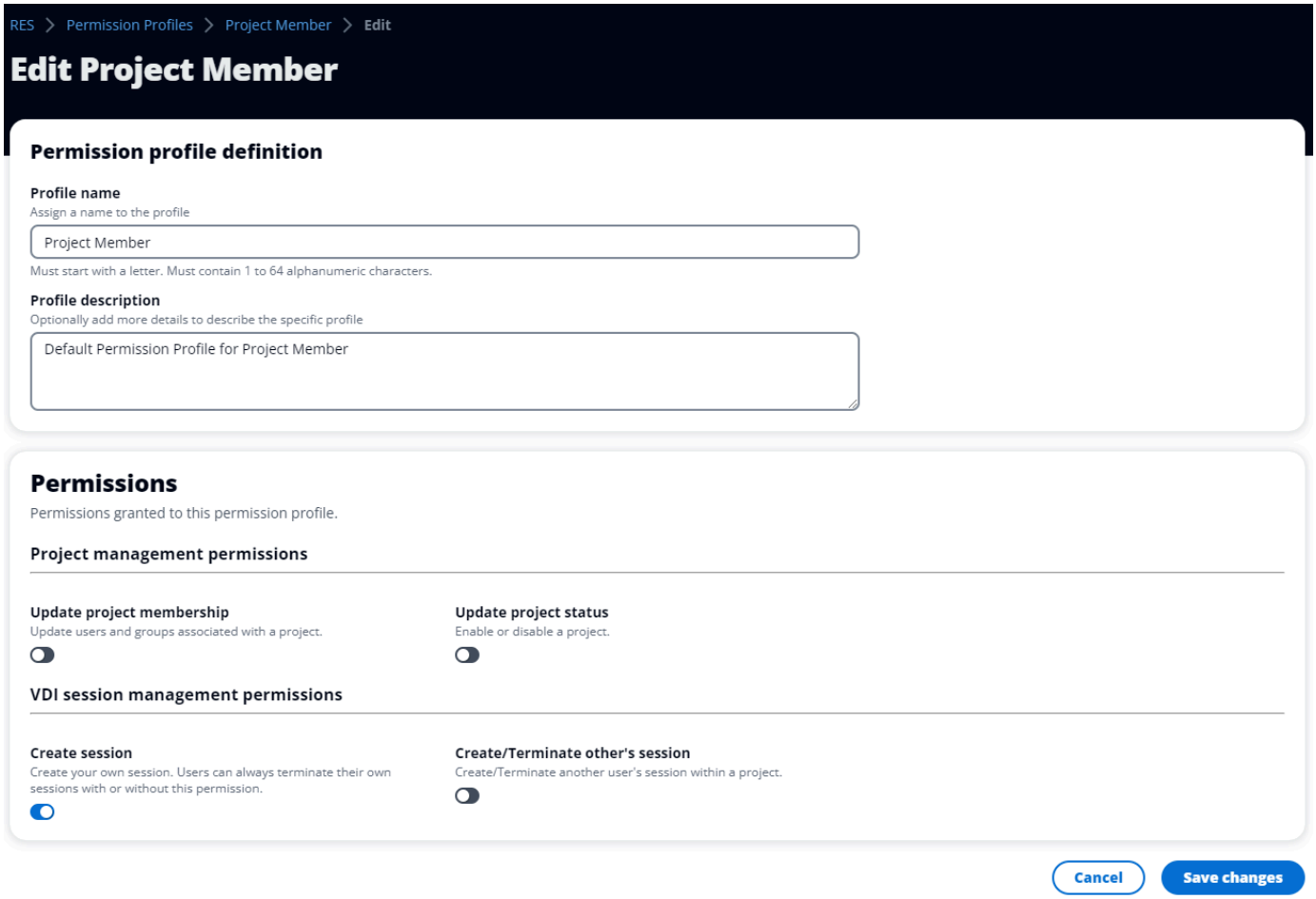
1. En la página principal de perfiles de permisos, elija Crear perfil para crear un perfil de permisos.

2. Introduzca un nombre y una descripción del perfil de permisos y, a continuación, seleccione los permisos que desee conceder a los usuarios o grupos que asigne a este perfil.



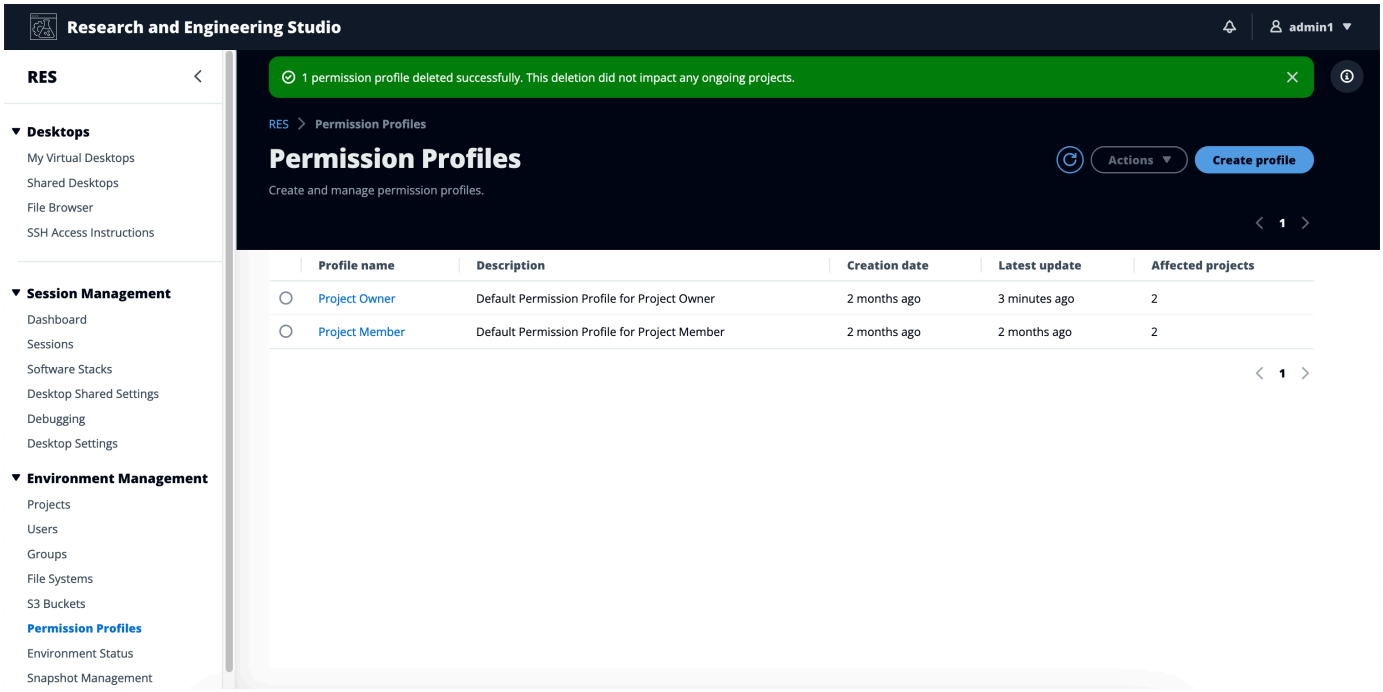
Editar perfiles de permisos

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



Perfiles de permisos predeterminados

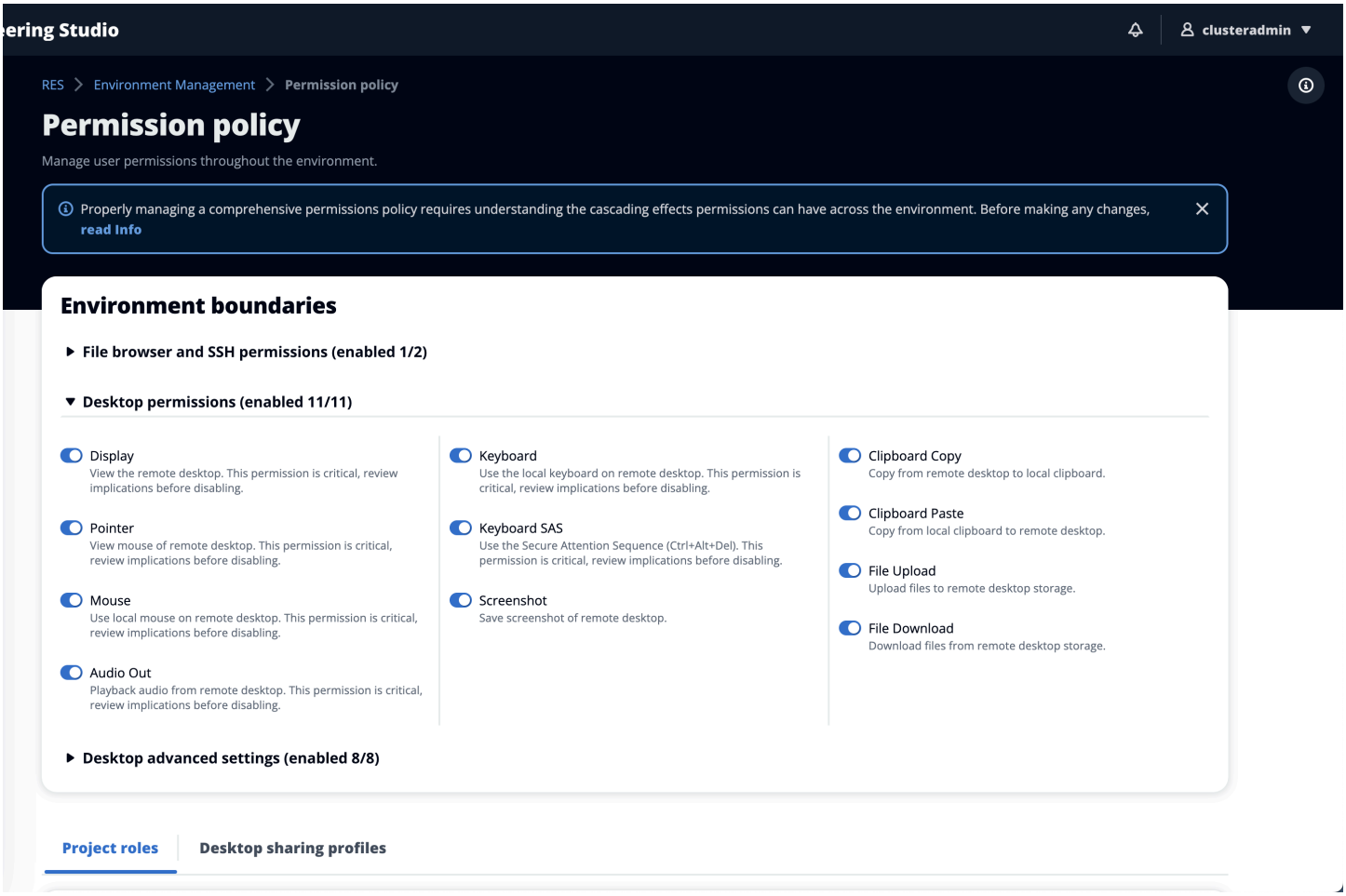
Cada proyecto de RES incluye dos perfiles de permisos predeterminados que los administradores globales pueden configurar. (Además, los administradores globales pueden crear y modificar nuevos perfiles de permisos para un proyecto). En la siguiente tabla se muestran los permisos permitidos para los perfiles 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	Description (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	Description (Descripción)	Miembro del proyecto	Dueño del proyecto	
	con o sin este permiso.			
Create/terminate sesiones de otros	Crear o terminar 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	

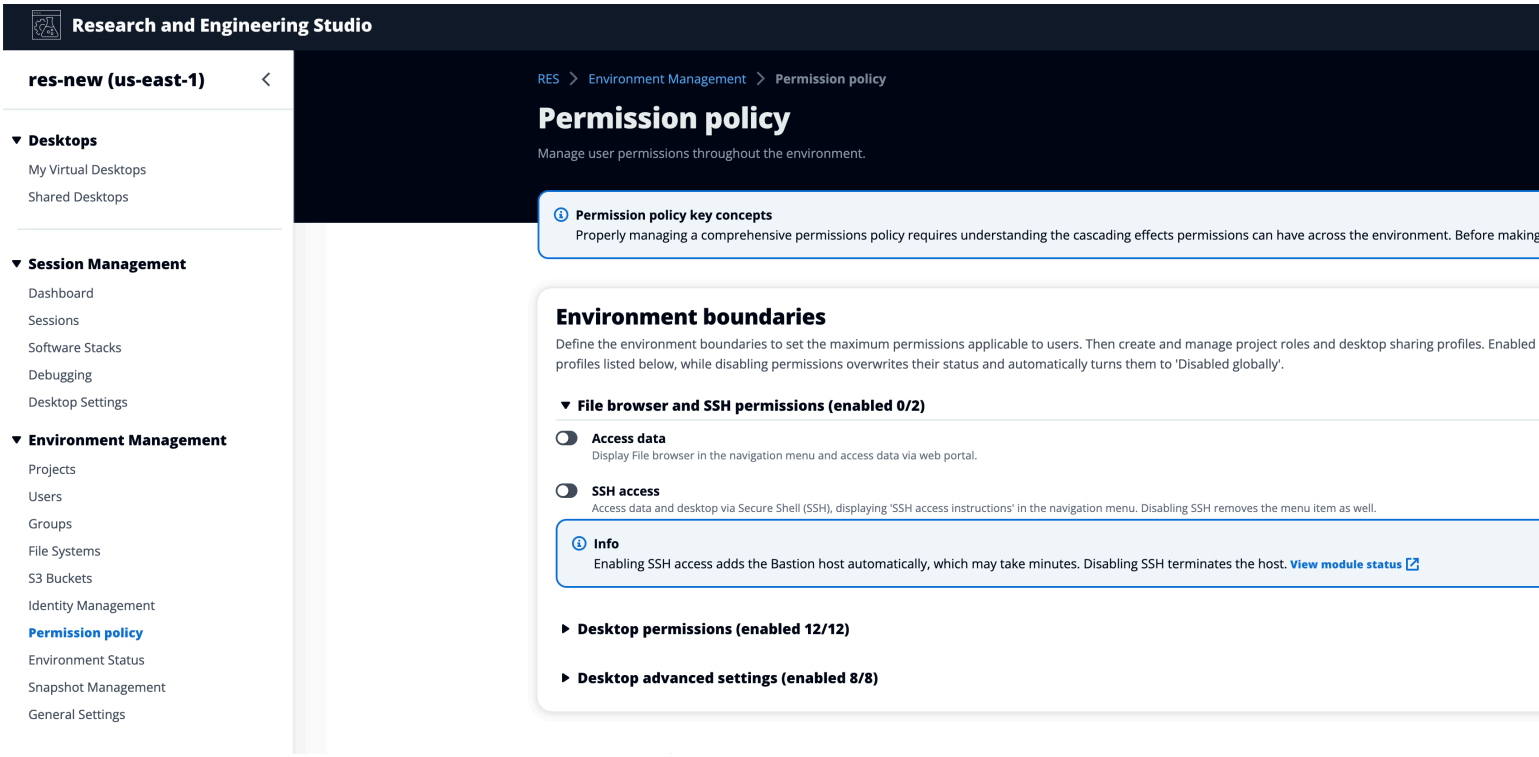
Límites del entorno

Los límites del entorno permiten a los administradores de Research and Engineering Studio (RES) configurar los permisos que se aplicarán a nivel mundial para todos los usuarios. Esto incluye permisos como los permisos del explorador de archivos y SSH, los permisos de escritorio y la configuración avanzada del escritorio.



Configuración del acceso al explorador de archivos

Los administradores de RES pueden activar o desactivar el acceso a los datos en los permisos del explorador de archivos. Si los datos de acceso están desactivados, los usuarios no verán la navegación por el explorador de archivos en su portal web y no podrán cargar ni descargar los datos adjuntos a su sistema de archivos global. Cuando los datos de acceso están habilitados, los usuarios tienen acceso a la navegación del explorador de archivos en su portal web, lo que les permite cargar o descargar los datos adjuntos a su sistema de archivos global.



Cuando la función de acceso a los datos esté activada y, posteriormente, desactivada, los usuarios que ya hayan iniciado sesión en el portal web no podrán cargar ni descargar archivos, aunque estén en la página correspondiente. Además, el menú de navegación desaparecerá cuando actualicen la página.

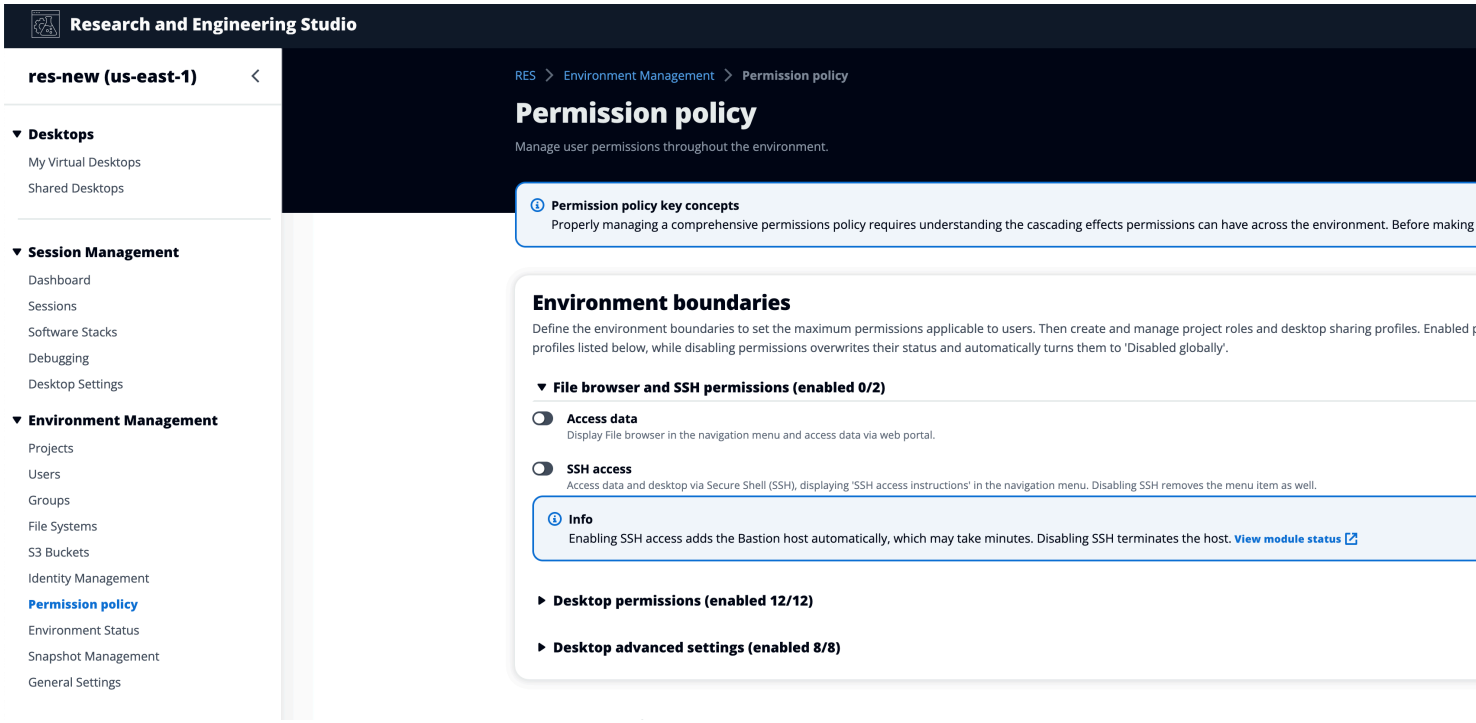
Configurar el acceso SSH

Los administradores pueden habilitar o deshabilitar SSH para el entorno RES desde la sección Límites del entorno. El acceso mediante SSH a los VDI se facilita a través de un host bastión. Al activar esta opción, RES despliega un host bastión y hace que la página de instrucciones de acceso a SSH esté visible para los usuarios. Al desactivar la opción, RES deshabilita el acceso a SSH, cierra el host bastión y elimina la página de instrucciones de acceso a SSH para los usuarios. Esta opción está desactivada de forma predeterminada.

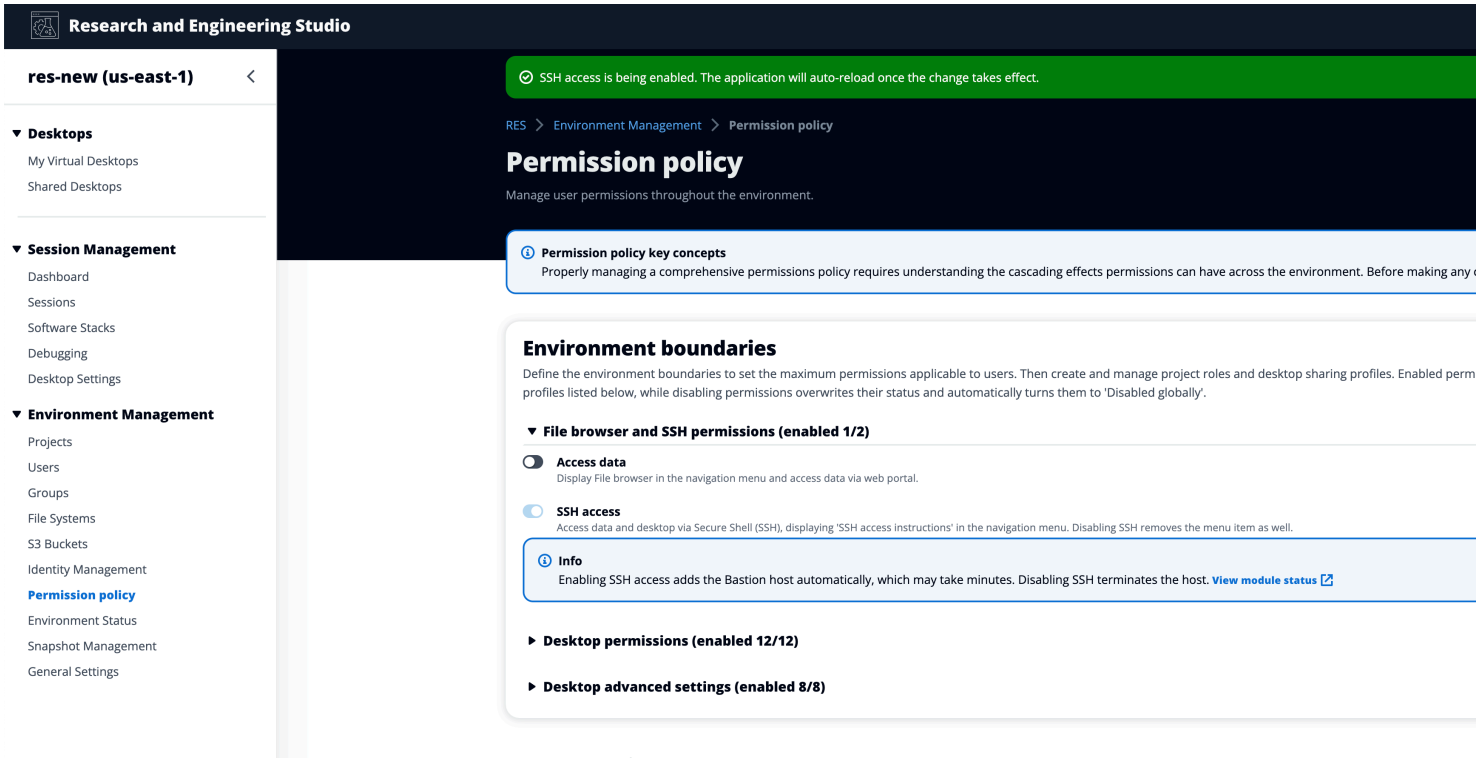
> **Note**
>
> Cuando RES implementa un host bastión, añade una instancia de Amazon `t3.medium` EC2 a su cuenta. AWS Usted es responsable de todos los cargos asociados a esta instancia. Consulte la página de precios de Amazon EC2 para obtener más información.

Para habilitar el acceso SSH

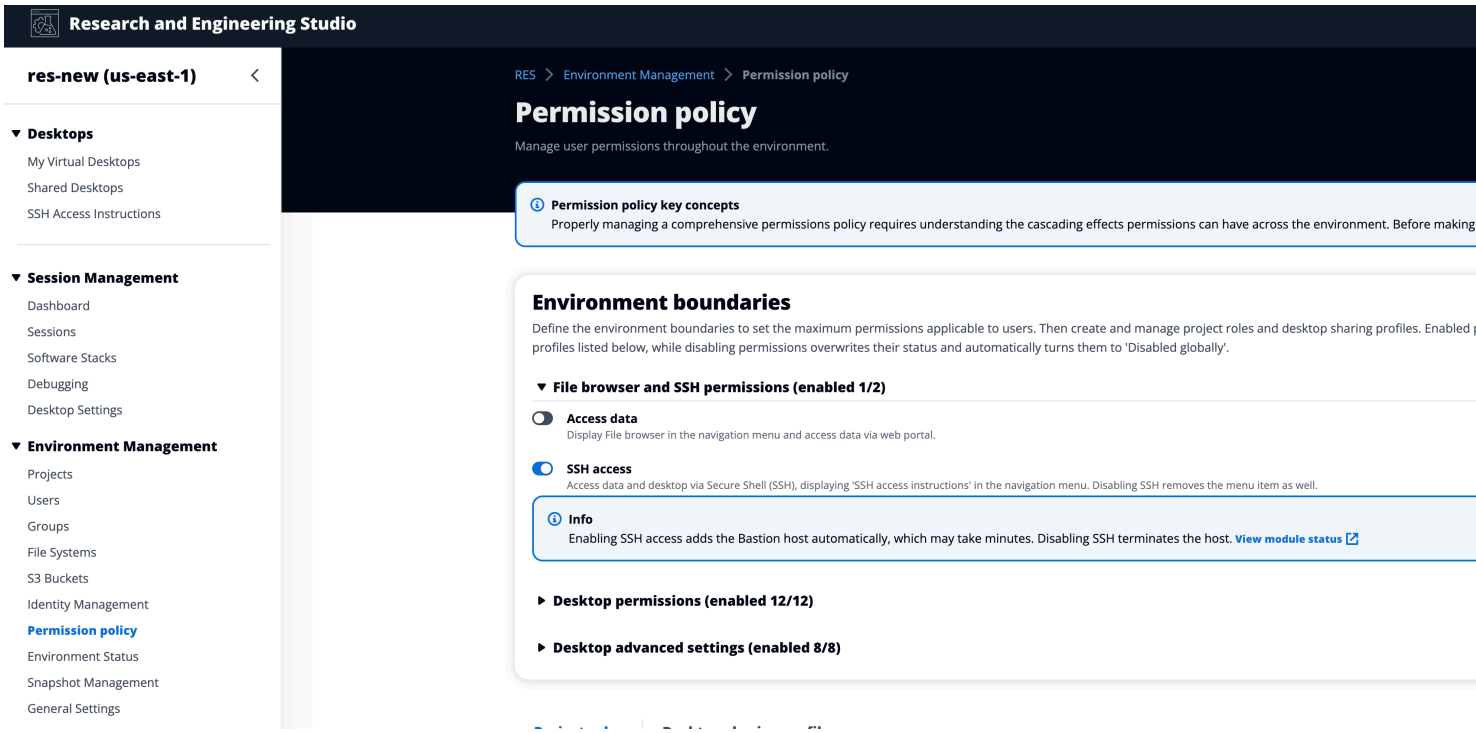
1. En la consola RES, en el panel de navegación izquierdo, selecciona Administración del entorno y, a continuación, Política de permisos. En Límites del entorno, seleccione el conmutador de acceso SSH.



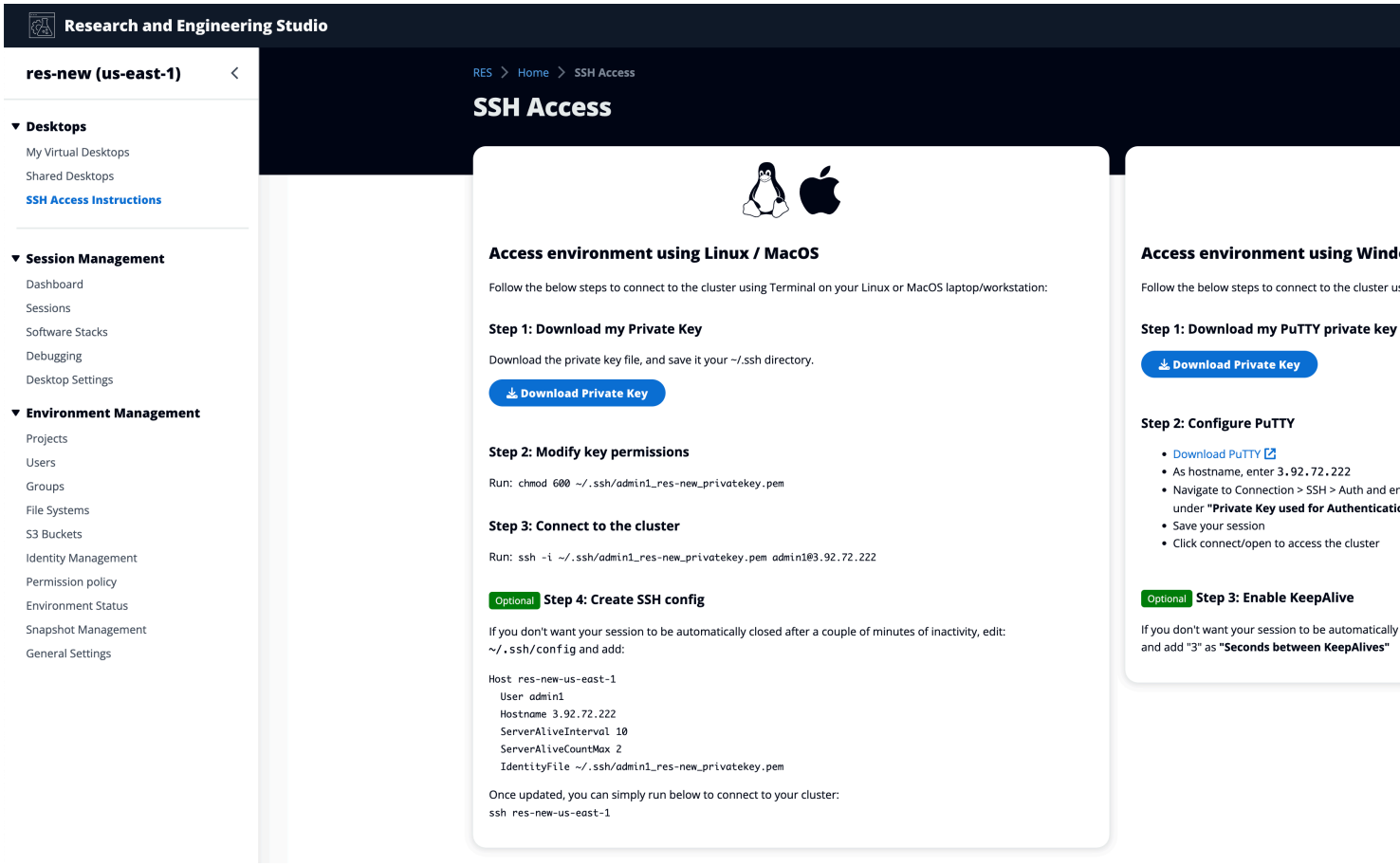
2. Espera a que se habilite el acceso SSH.



3. Una vez agregado el host Bastion, se habilita el acceso SSH.

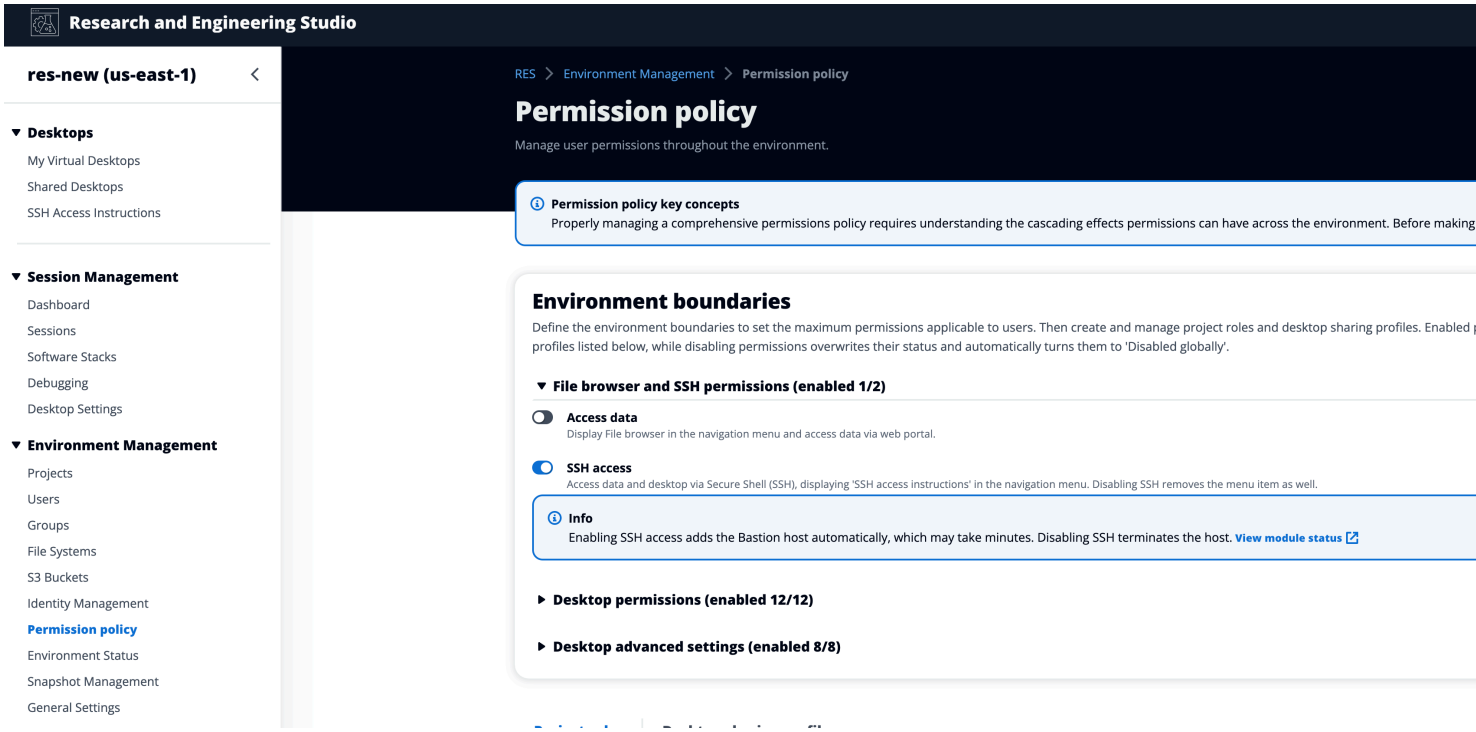


Los usuarios pueden ver la página de instrucciones de acceso a SSH desde el panel de navegación izquierdo.

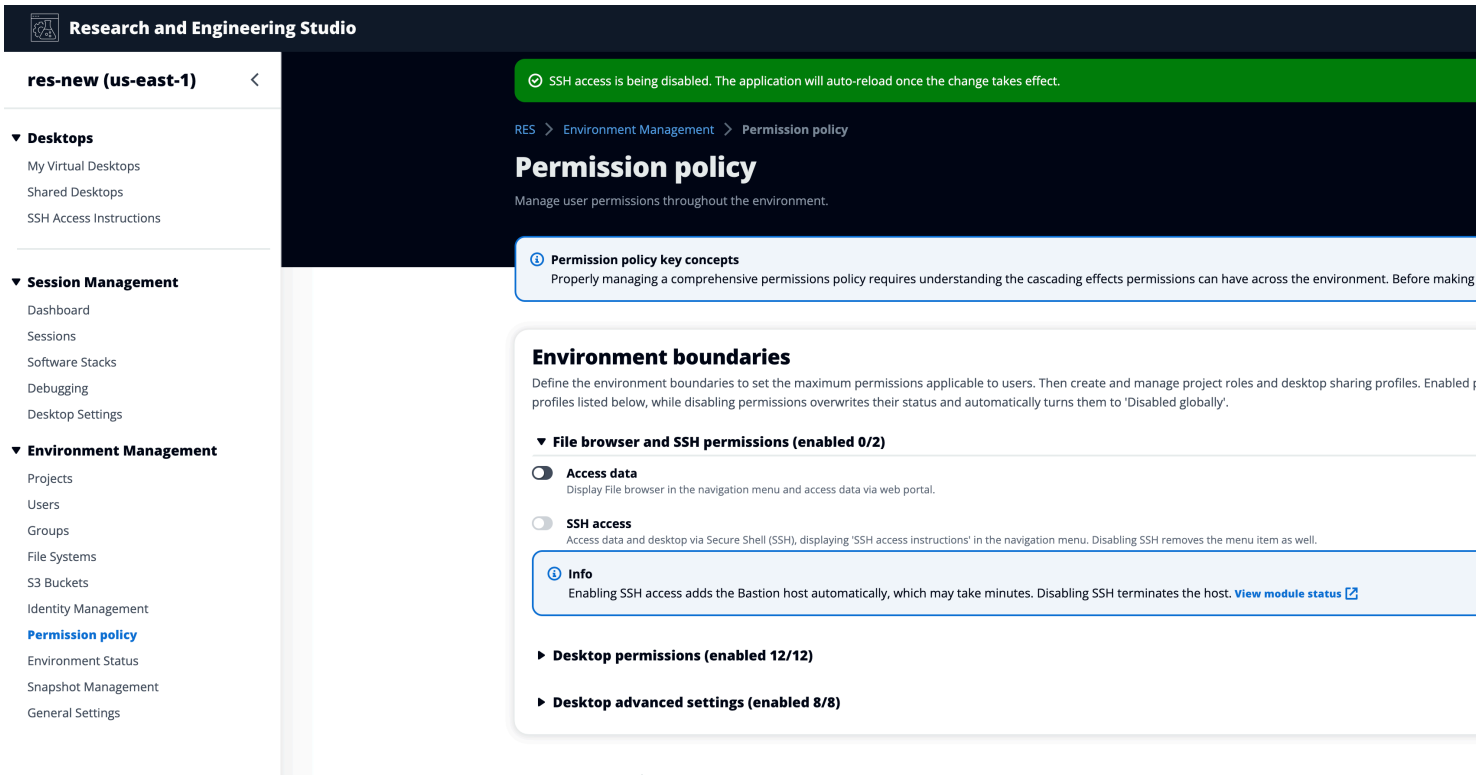


Para deshabilitar el acceso SSH

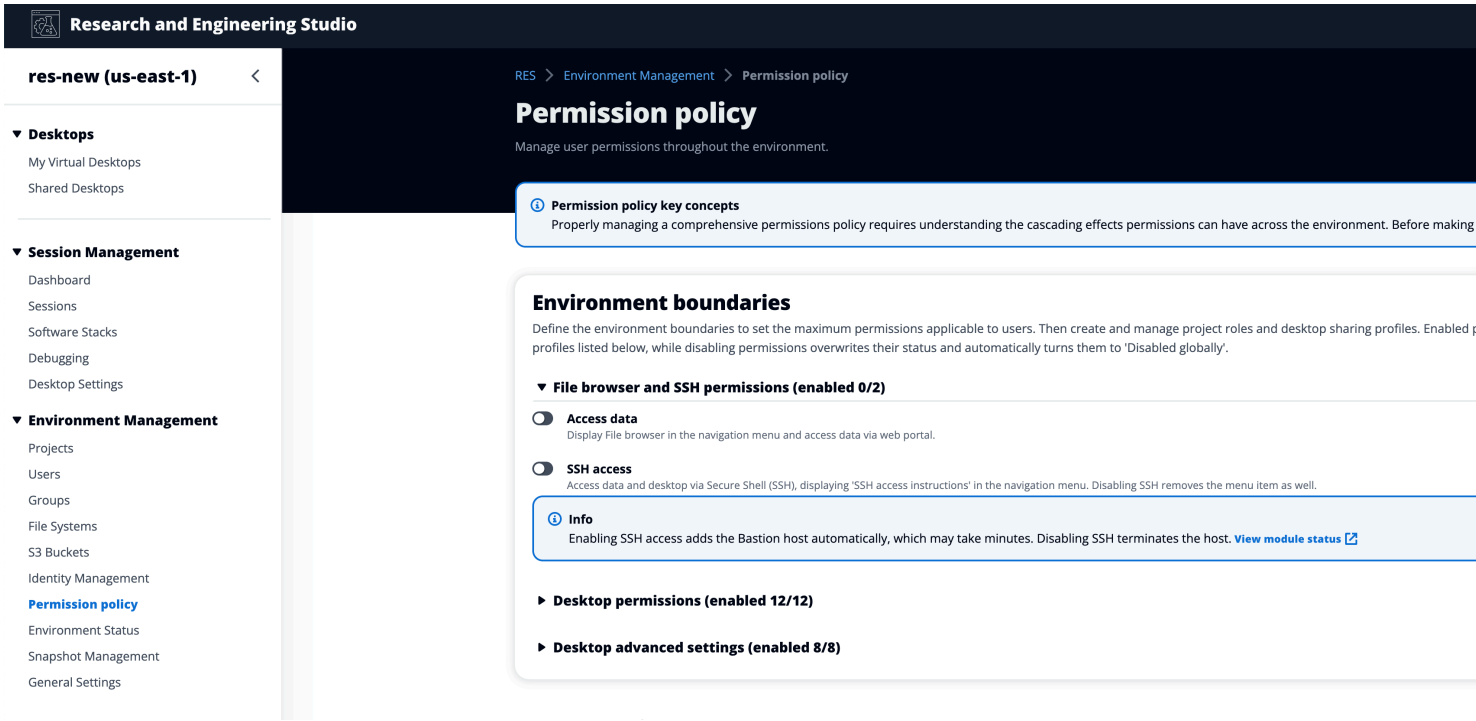
1. En la consola RES, en el panel de navegación izquierdo, selecciona Administración del entorno y, a continuación, Política de permisos. En Límites del entorno, seleccione el conmutador de acceso SSH.



2. Espera a que se desactive el acceso a SSH.

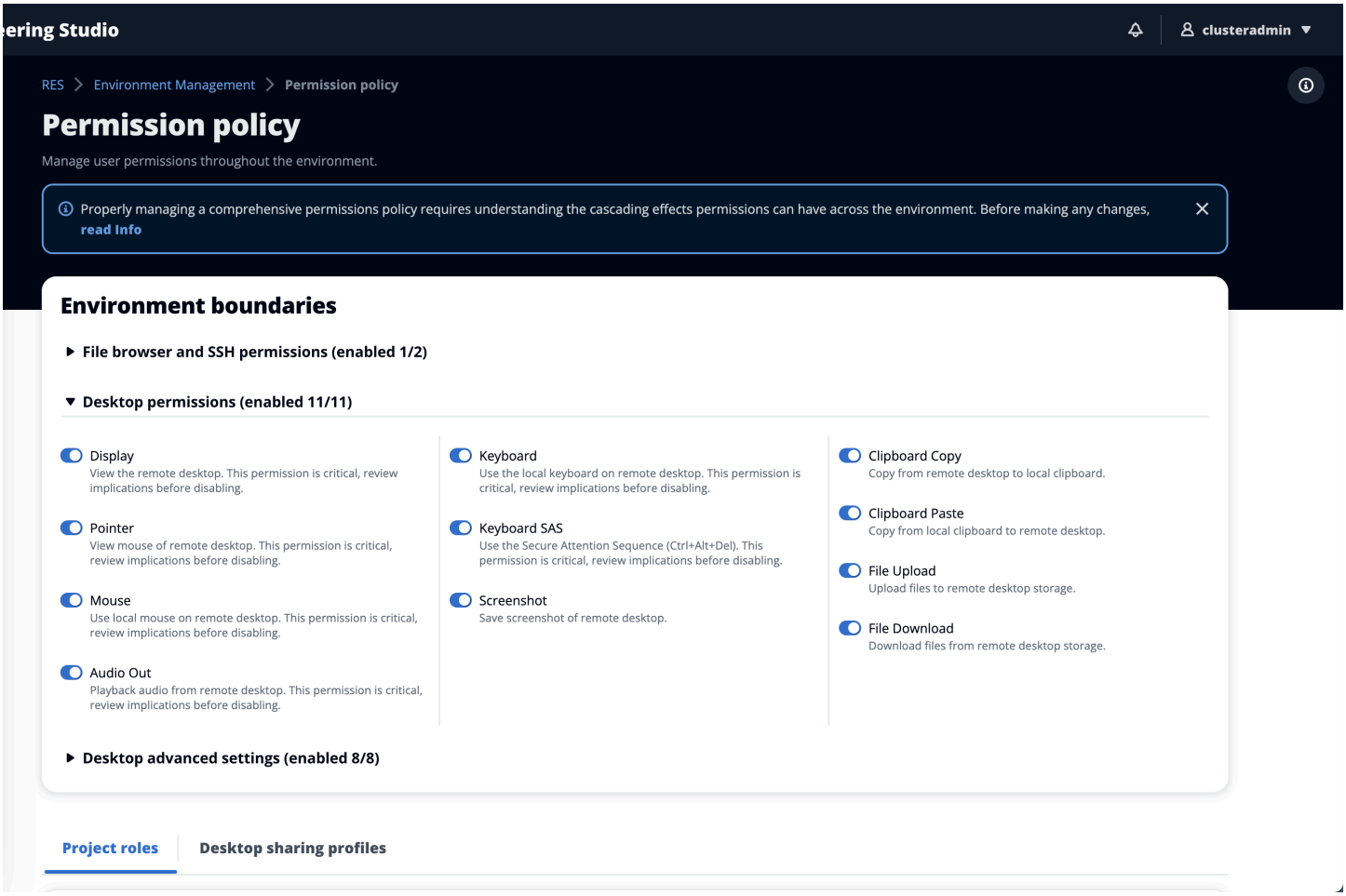


3. Una vez finalizado el proceso, se deshabilita el acceso a SSH.



Configuración de los permisos de escritorio

Los administradores pueden activar o desactivar los permisos de escritorio para administrar globalmente la funcionalidad de VDI de todos los propietarios de sesiones. Todos estos permisos, o un subconjunto, se pueden usar para crear perfiles de uso compartido de escritorios que determinen qué acciones pueden realizar los usuarios con los que se comparte un escritorio. Si se deshabilita algún permiso de escritorio, se deshabilitarán automáticamente los permisos correspondientes en los perfiles de uso compartido del escritorio. Estos permisos se etiquetarán como «Deshabilitados globalmente». Incluso si el administrador vuelve a habilitar este permiso de escritorio, el permiso del perfil de uso compartido del escritorio permanecerá deshabilitado hasta que el administrador lo habilite manualmente.

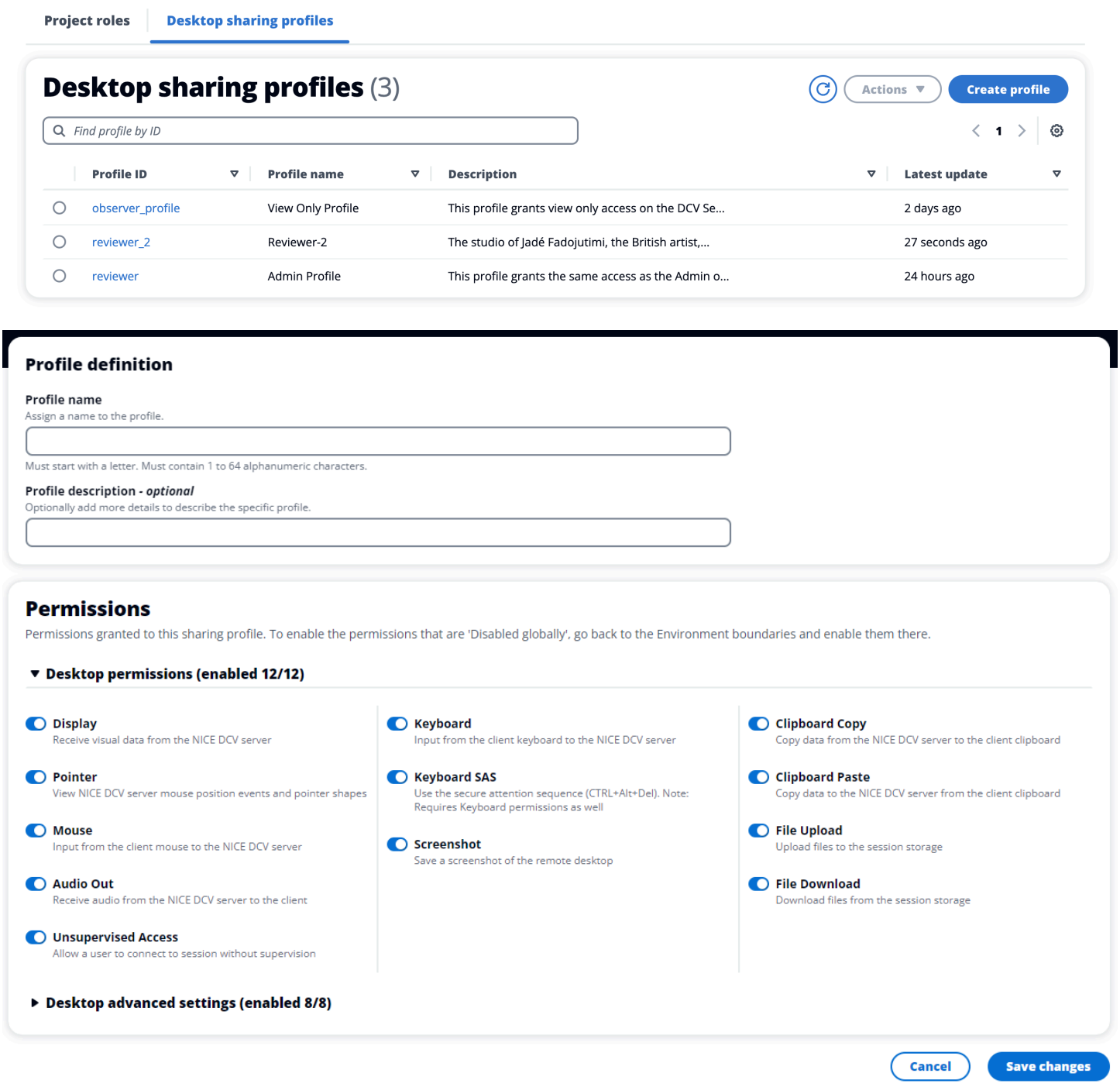


Perfiles para compartir escritorios

Los administradores pueden crear nuevos perfiles y personalizarlos. Todos los usuarios pueden acceder a estos perfiles y se utilizan al compartir una sesión con otros usuarios. El número máximo de permisos que se conceden en estos perfiles no puede superar los permisos de escritorio permitidos en todo el mundo.

Crear perfil

Los administradores pueden elegir Crear perfil para crear un perfil nuevo. A continuación, pueden introducir un nombre de perfil, una descripción del perfil, establecer los permisos deseados y guardar los cambios.



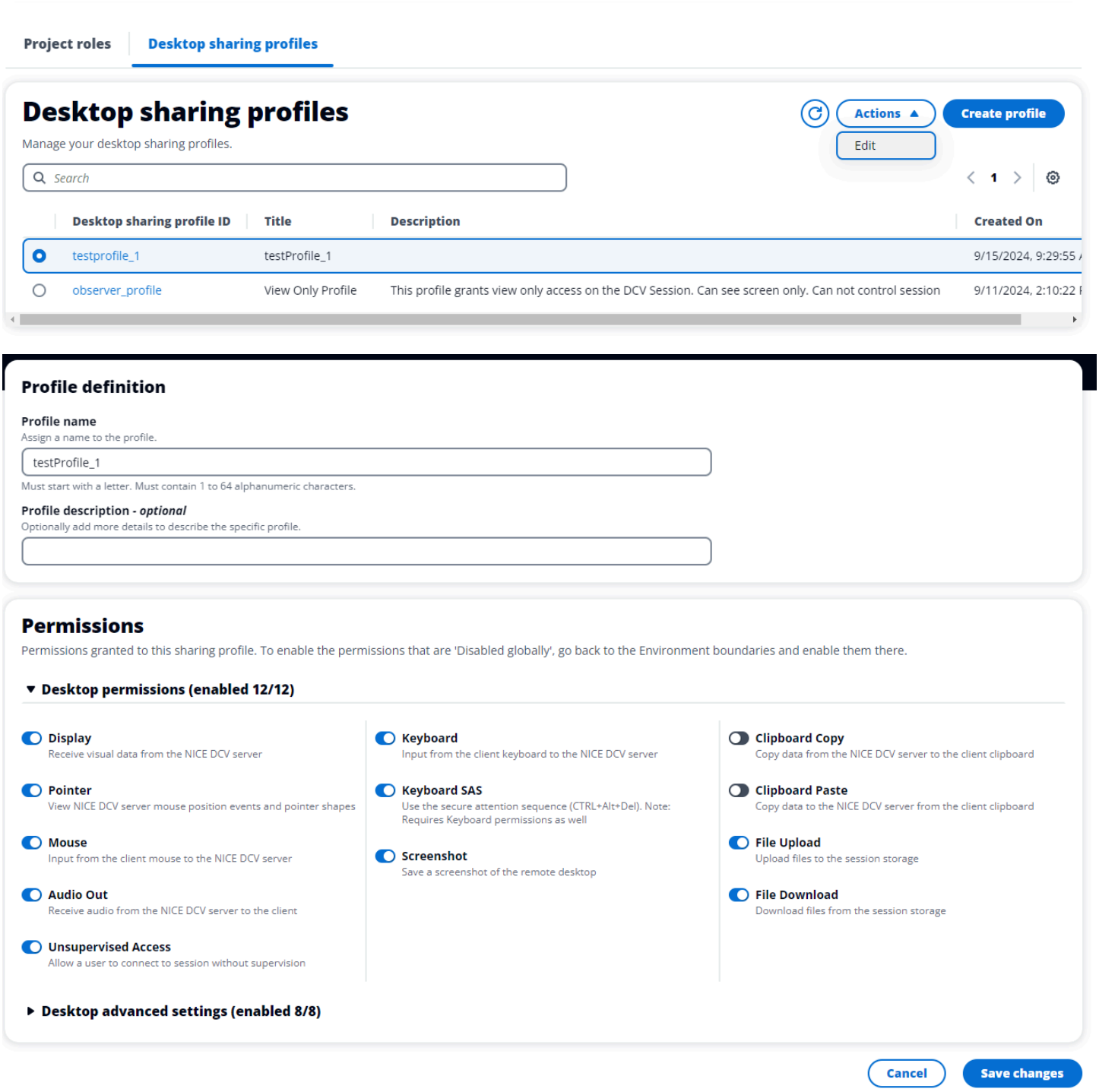
Editar perfil

Para editar un perfil:

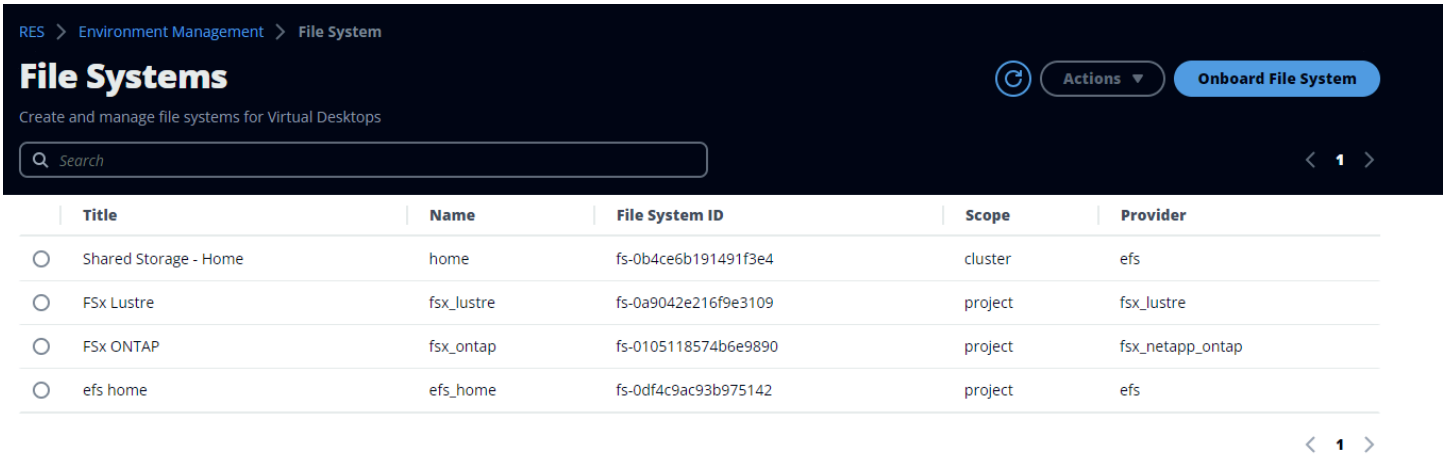
1. Seleccione el perfil deseado.
2. Elija Acciones y, a continuación, seleccione Editar para modificar el perfil.

3. Ajuste los permisos según sea necesario.
4. Seleccione Save changes (Guardar cambios).

Cualquier cambio realizado en el perfil se aplicará inmediatamente a las sesiones abiertas actuales.



Sistemas de archivos



Desde la página de 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. 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.

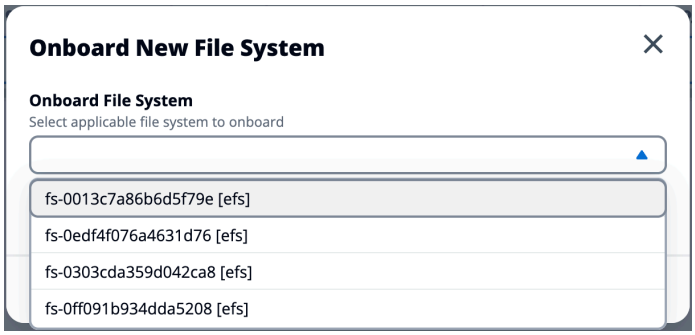
Temas

- Incorpore un sistema de archivos

Incorpore un sistema de archivos

> **Note**
>
> Para integrar correctamente un sistema de archivos, este debe compartir la misma VPC y al menos una de las subredes de RES. También debe asegurarse de tener el grupo de seguridad configurado correctamente para que sus VDI tengan acceso al contenido del sistema de archivos.

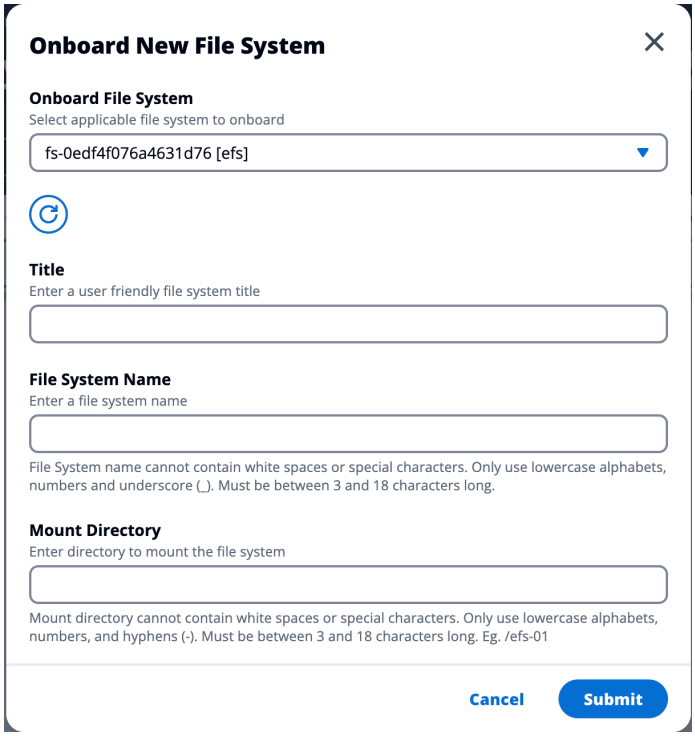
1. Elija Sistema de archivos integrado.
2. Seleccione un sistema de archivos en el menú desplegable. El modal se ampliará con entradas de detalles adicionales.



3. Introduzca los detalles del sistema de archivos.

> **Note**
>
> De forma predeterminada, los administradores y propietarios de proyectos tienen la posibilidad de elegir un sistema de archivos principal al crear un nuevo proyecto, que no se puede editar posteriormente.
> Los sistemas de archivos destinados a usarse como directorios principales en los proyectos deben incorporarse configurando su ruta de Mount Directory en. `/home` Esto rellenará el sistema de archivos incorporado en las opciones desplegables del sistema de archivos del directorio principal. Esta función ayuda a mantener los datos aislados en todos los proyectos, ya que solo los usuarios asociados al proyecto tendrán acceso al sistema de archivos a través de sus VDI. Los VDI montarán el sistema de archivos en el punto de montaje seleccionado durante la incorporación de un sistema de archivos.

4. Seleccione Enviar.



Varios volúmenes desde un único sistema de archivos ONTAP

RES permite la incorporación de varios volúmenes desde un único sistema de archivos para NetApp ONTAP. Esto permite a los administradores organizar los datos en volúmenes separados dentro del mismo sistema de archivos ONTAP y, al mismo tiempo, poner cada volumen a disposición de los proyectos de forma independiente.

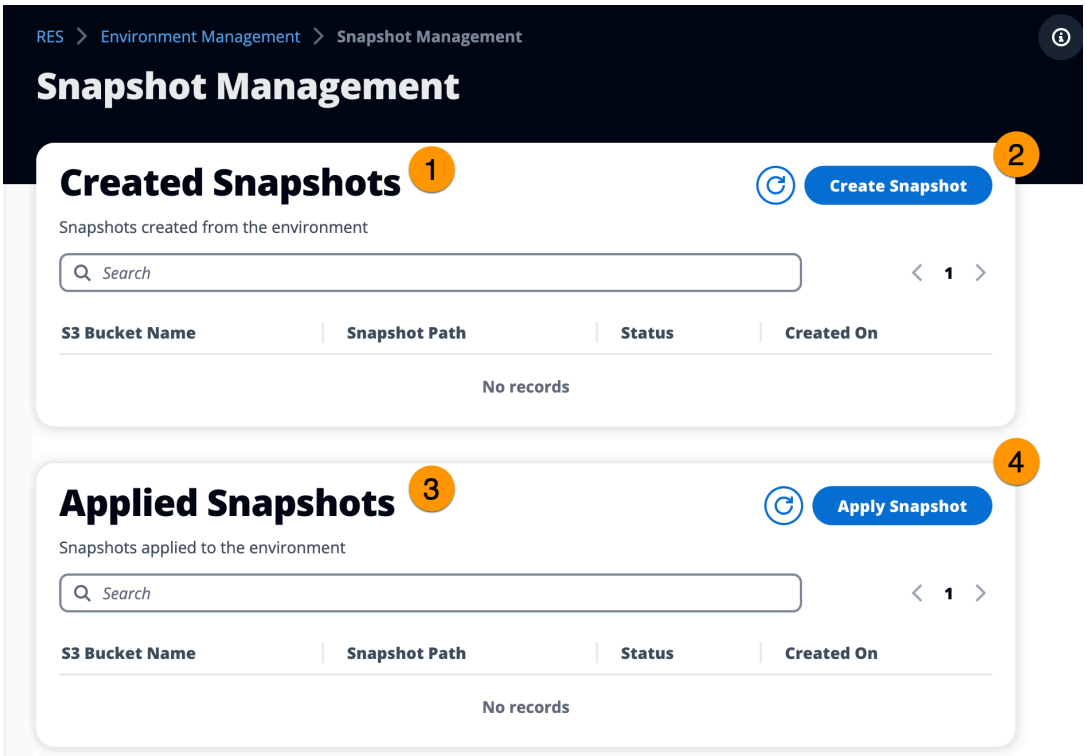
Para incorporar volúmenes adicionales desde un sistema de archivos de ONTAP que ya está incorporado:

1. Elija un sistema de archivos integrado.
2. Seleccione el mismo sistema de archivos ONTAP en el menú desplegable.
3. En el campo Volumen, seleccione un volumen diferente del sistema de archivos.
4. Especifique un directorio de montaje único para este volumen.
5. Seleccione Enviar.

> **Note**
>
> Cada volumen del mismo sistema de archivos ONTAP debe estar integrado con un directorio de montaje único. Los volúmenes se pueden asignar de forma independiente a diferentes proyectos.

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.

Temas

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. Habilite 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. Selecciona el depósito que has creado en la lista de depósitos.
2. Seleccione 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:
   - *111122223333*-> tu ID AWS de cuenta
   - *{RES_ENVIRONMENT_NAME}*-> el nombre de su entorno RES
   - *amzn-s3-demo-bucket*-> el nombre de su bucket de S3

> **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.

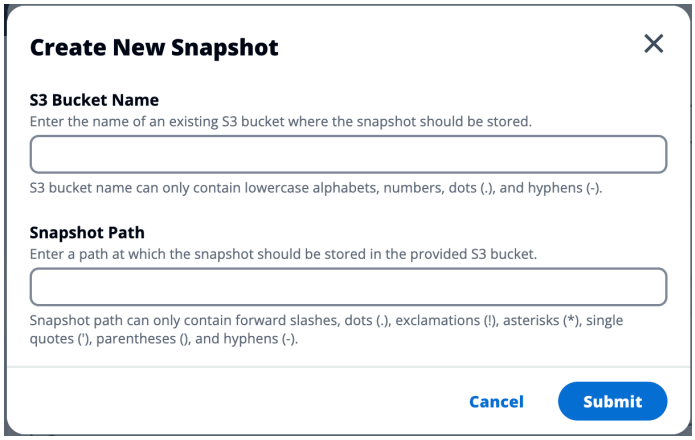
JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-role"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "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. Seleccione 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. Deberá 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 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. Selecciona el depósito que has creado en la lista de depósitos.
2. Seleccione 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:

   - *111122223333*-> tu ID AWS de cuenta
   - *{RES_ENVIRONMENT_NAME}*-> el nombre de su entorno RES
   - *amzn-s3-demo-bucket*-> el nombre de su bucket de S3

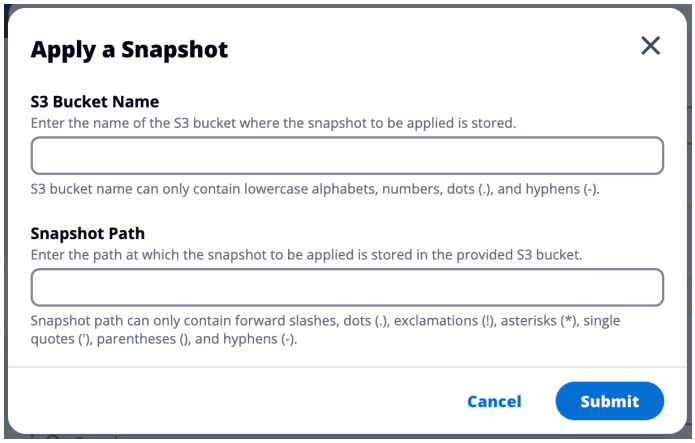
   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-role"
            },
```

```
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

Para aplicar la 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. Seleccione Enviar.



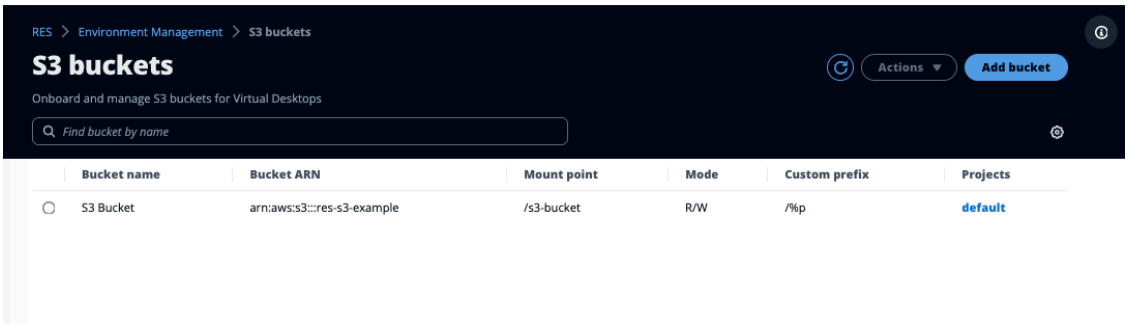
5. Transcurridos entre cinco y diez minutos, seleccione Actualizar en la página de administración de instantáneas para comprobar el estado.

Buckets 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.



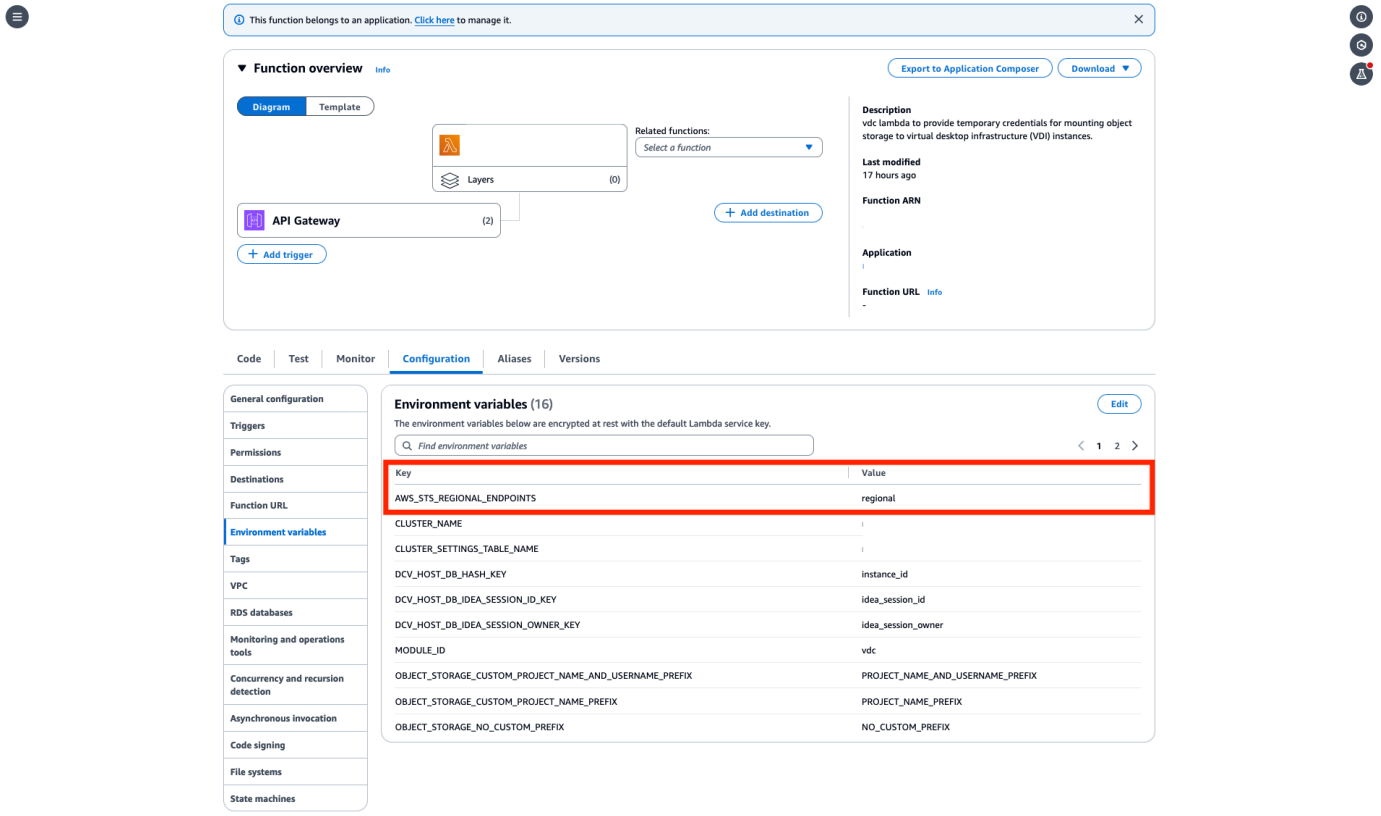
En las siguientes secciones se describe cómo administrar los buckets de Amazon S3 en sus proyectos de RES.

Temas

Requisitos previos del bucket de Amazon S3 para implementaciones de VPC aisladas

Si va a implementar Research and Engineering Studio en una VPC aislada, siga estos pasos para actualizar los parámetros de configuración de lambda después de implementar RES en su cuenta. AWS

1. Inicie sesión en la consola Lambda de la AWS cuenta en la que está desplegado Research and Engineering Studio.
2. Busque y navegue hasta la función Lambda denominada. *<RES-EnvironmentName>*`-vdc-custom-credential-broker-lambda`
3. Seleccione la pestaña Configuración de la función.



4. En el panel de navegación, elija Variables de entorno para ver esa sección.
5. Elija Editar y añada la siguiente variable de entorno nueva a la función:
   - Clave: `AWS_STS_REGIONAL_ENDPOINTS`
   - Valor: `regional`
6. Seleccione Save.

Añadir un bucket de Amazon S3

Para añadir un bucket de S3 a su entorno de 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.

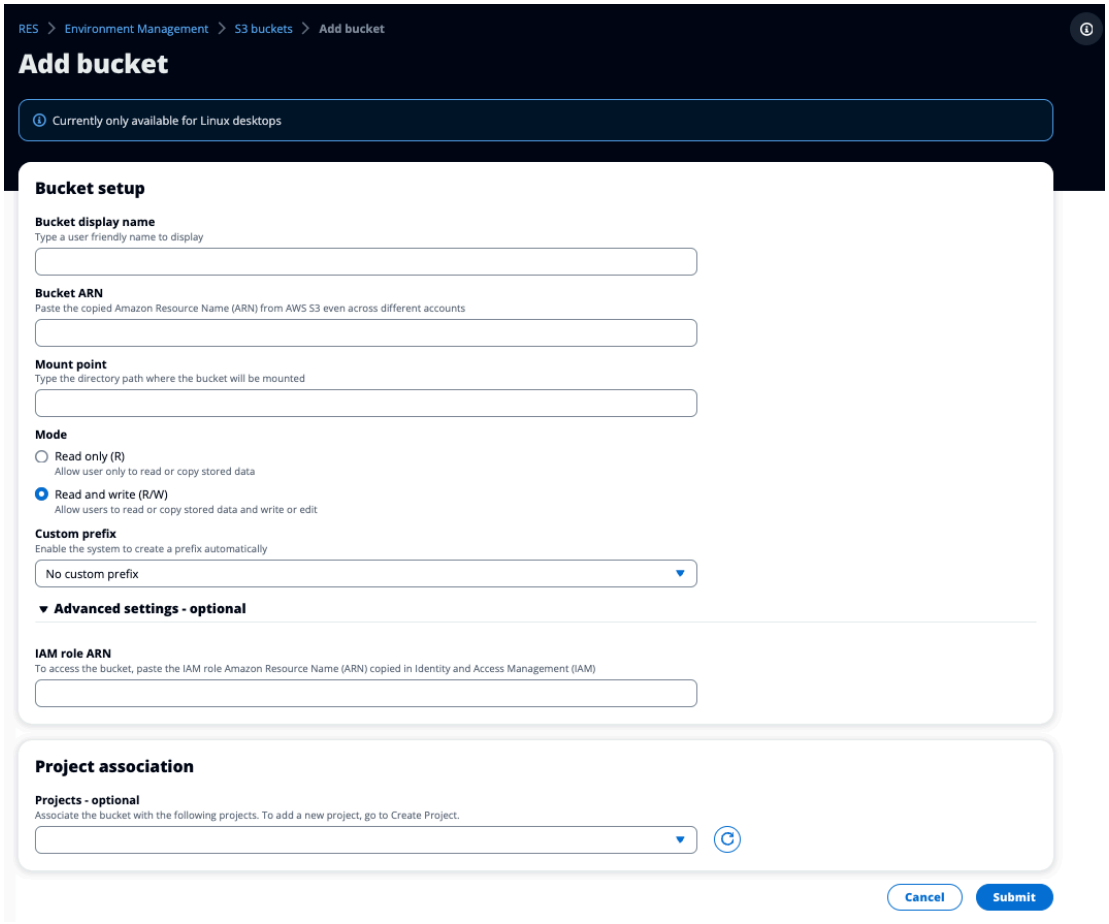
> **Important**
>
> - El ARN del bucket, el punto de montaje y el modo proporcionados no se pueden cambiar después de la creación.

- 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 a varios buckets de 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. Seleccione Enviar.

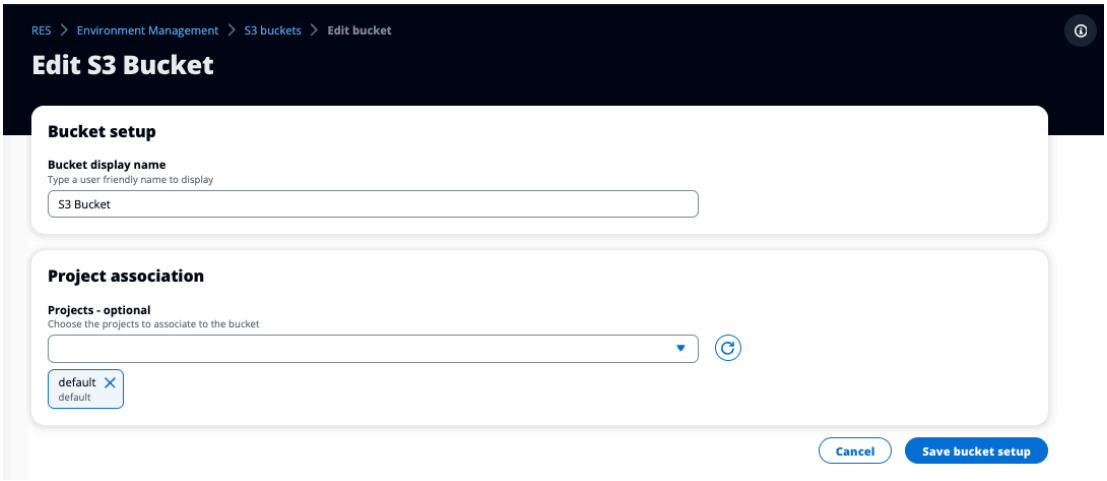


Editar un bucket de Amazon S3

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 debes 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, puede seleccionar un modo de Solo lectura (R) o Lectura y escritura (R/W).

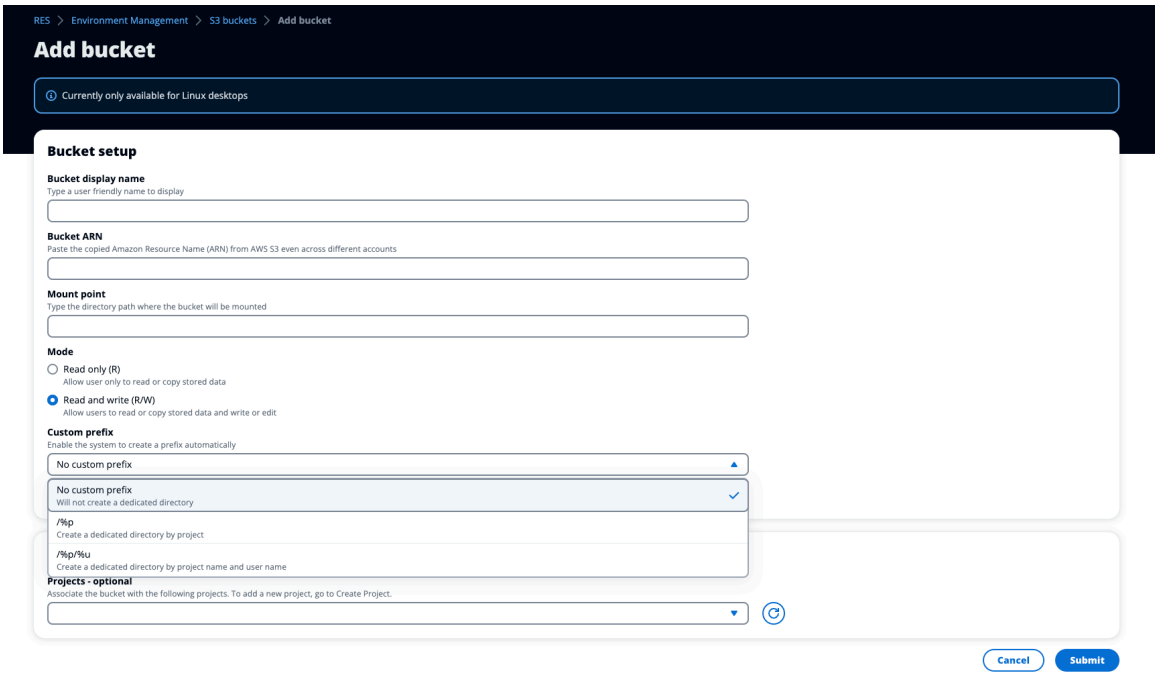
Solo lectura

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 lancen VDI 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



No hay 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 `arn:aws:s3:::bucket-name` con el ARN `No custom prefix` seleccionado y asocia este depósito a los proyectos A y B, los usuarios que lancen VDI desde los proyectos A y B tendrán acceso ilimitado de lectura y escritura al depósito.

Aislamiento de datos a nivel de 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 depósito de S3, bajo el prefijo, `/ProjectA` mientras que el usuario B solo puede acceder `/ProjectB` cuando utiliza sus VDI 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 utiliza sus VDI en el proyecto A.

Acceso a varios buckets de cuentas

RES tiene la capacidad de montar depósitos desde otras AWS cuentas, siempre que estos depósitos 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 Políticas.
3. Cree una política:
   a. Elija Crear política.
   b. Seleccione la pestaña JSON.
   c. Pegue la siguiente política de JSON (*amzn-s3-demo-bucket*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:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
```

```
    ]
}
```

d. Elija Siguiente.

4. Revisa y crea la política:

   a. Proporcione un nombre para la política (por ejemplo, "S3AccessPolicy«).

   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. Seleccione Roles en el panel de navegación.

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 (*111122223333*sustitúyala por el ID de cuenta real de la cuenta A y *{RES_ENVIRONMENT_NAME}* por el nombre de entorno de la implementación de RES):

      JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/<ENVIRONMENT_NAME>-vdc-custom-
credential-broker-lambda-role"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

   d. Elija Siguiente.

7. Adjunte las políticas de permisos:
    a. Busque y seleccione la política que creó anteriormente.
    b. Elija Siguiente.
8. Etiquete, revise y cree el rol:
    a. Introduzca el nombre de un rol (por ejemplo, "S3AccessRole«).
    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, selecciona S3 Bucket.
    d. Elige Añadir depósito y rellena 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. Seleccione la pestaña Permisos y elija la política de buckets.

b. Añada la siguiente política para conceder a la función de IAM de la cuenta A acceso al bucket (*111122223333*sustitúyala por el ID de cuenta real de la cuenta A y *amzn-s3-demo-bucket* 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:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

c. Seleccione Save.

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/vpcconsole/

2. Cree un punto final de VPC para S3:

a. En el panel de navegación izquierdo, seleccione Puntos de conexión.

b. Elija 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. Par VPC, seleccione la VPC en la que desee crear el punto de conexión.

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, elija 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 (*amzn-s3-demo-bucket*sustitúyelo por el nombre de su bucket de S3 *111122223333* y *444455556666* por los ID de AWS cuenta correspondientes a los que desee acceder):

> **Note**
>
> Este ejemplo de política utiliza `s3:*` y no restringe las operaciones del plano de control de S3, como la configuración de las notificaciones de eventos, la replicación o el inventario. Estas operaciones podrían permitir que los metadatos de los objetos (como los nombres de los depósitos y las claves de los objetos) se envíen a destinos de varias cuentas. Si esto le preocupa, añada sentencias Deny explícitas

para las acciones pertinentes del plano de control de S3 en la política de puntos finales de la VPC.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",
                        "444455556666"
                    ]
                }
            }
        }
    ]
}
```

5. Cree el punto final:
   a. Revise la configuración.
   b. Seleccione Crear punto de conexión.
6. Verifique el punto final:
   a. Una vez creado el punto final, vaya 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.

Resolución 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 consola EC2 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 los 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 los 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, elija Tables (Tablas).
   b. Busque y seleccione`<stack-name>.cluster-settings`.
3. Escanea la tabla:
   a. Elija Explorar elementos de la tabla.
   b. Asegúrese de que esté seleccionada la opción Escanear.
4. Añadir un filtro:
   a. Elija Filtros para abrir la sección de entrada de filtros.
   b. Configure el filtro para que coincida con su clave
      - Atributo: introduce la clave.
      - Condición: seleccionar 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. Seleccione Crear elemento.

b. Introduzca 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 que los VDI afectados por el ARN de rol de IAM incorrecto se vuelvan a montar.

Habilitando CloudTrail

Para activarla CloudTrail en su cuenta mediante la CloudTrail consola, siga 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.

Usa el producto

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

Temas

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.

Escritorios virtuales

El módulo de infraestructura de escritorios virtuales (VDI) permite a los usuarios crear y administrar escritorios virtuales Windows o Linux en ellos. AWS Los usuarios pueden lanzar instancias de Amazon EC2 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)
- Amazon Linux 2023 (x86 y ARM64)
- RHEL 8 (x86) y 9 (x86)
- Rocky Linux 9 (x86)
- Ubuntu 22.04.03 (x86)
- Windows Server 2019, 2022 (x86)

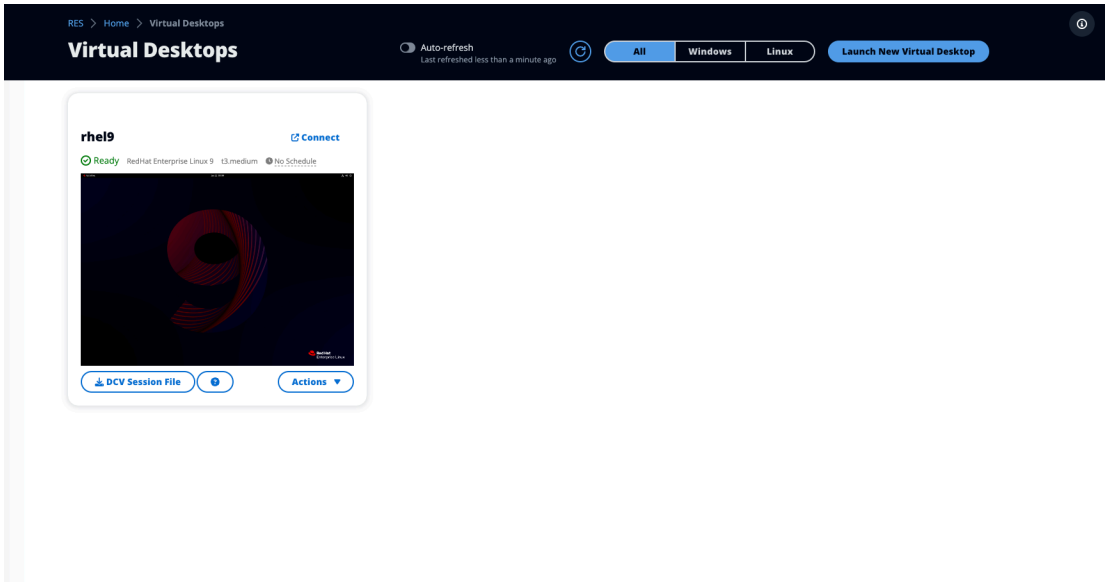
- Windows 10, 11 (x86)

> **Note**
>
> A partir de la versión 2026.03, Amazon Linux 2 y RHEL 8 ya no se incluyen como paquetes de software predeterminados. Si es necesario, se pueden seguir registrando paquetes de software personalizados con estos sistemas operativos.

Temas

Lance 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. Seleccione 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.

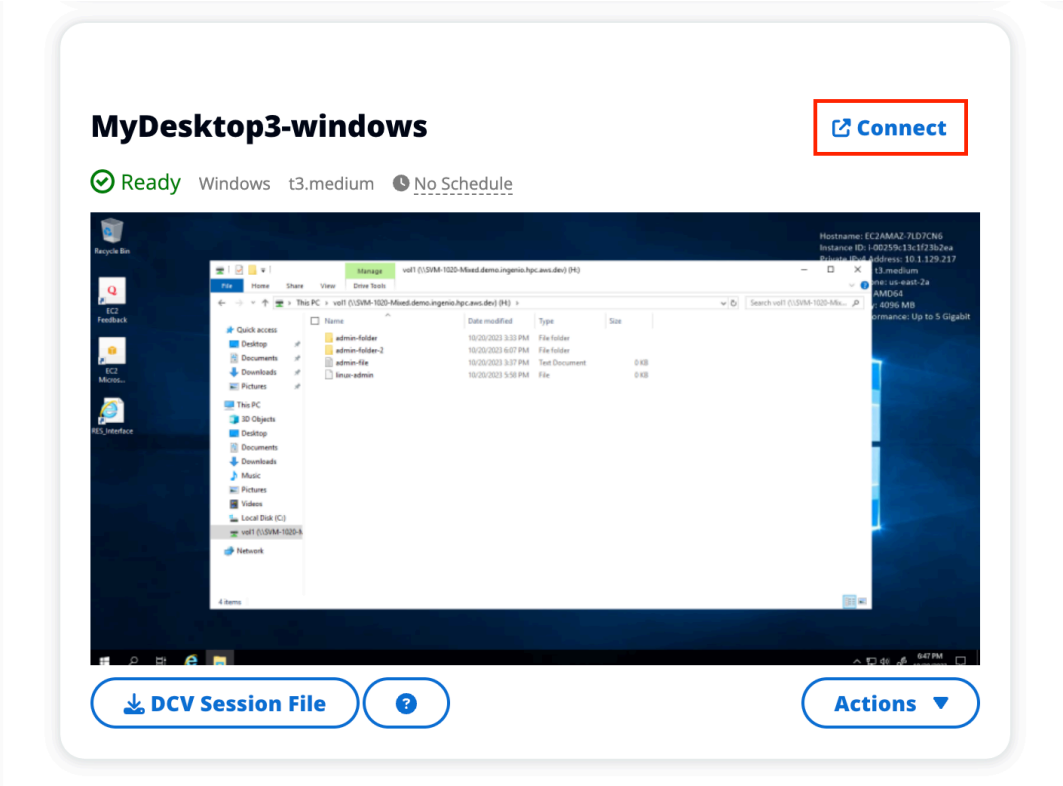
Acceda a su escritorio

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

Web connection

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

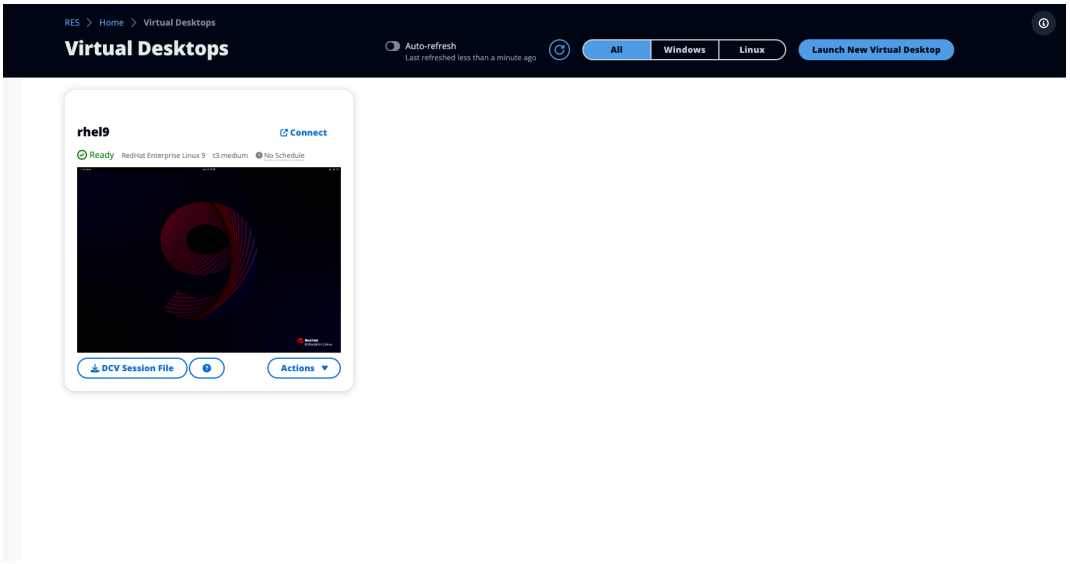
- Selecciona Connect o elige la miniatura para acceder al escritorio directamente a través del navegador.



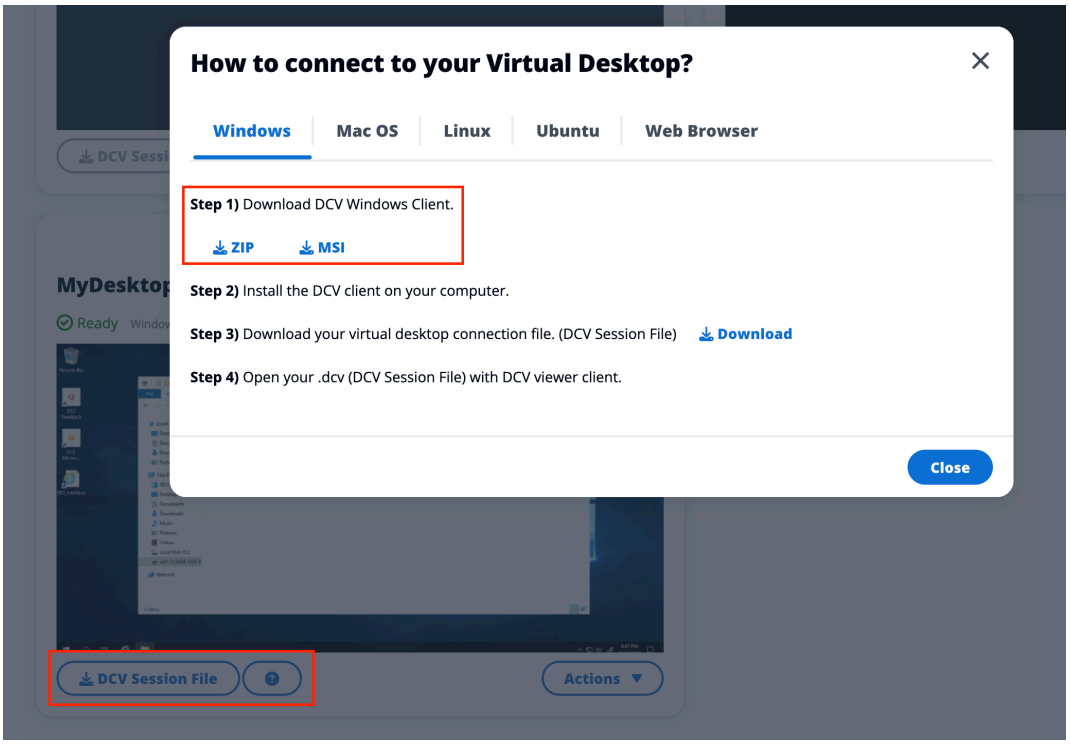
DCV connection

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.



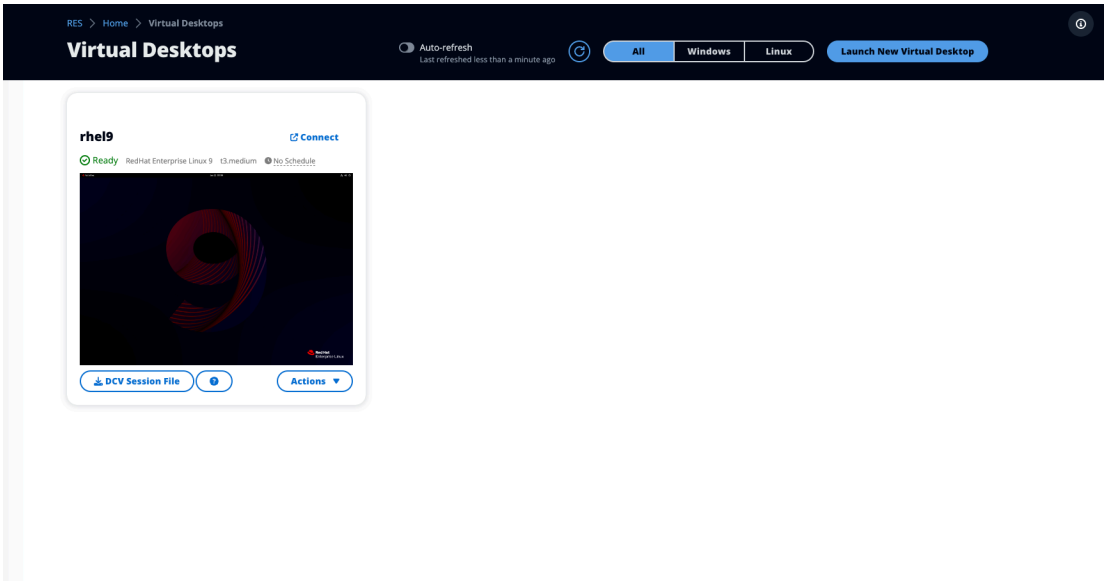
2. Para ver las instrucciones de instalación, elija la opción? icono.



Controle el estado de su escritorio

Para controlar el estado del escritorio:

1. Elija Acciones.



2. Elija el estado del escritorio virtual. Tiene cuatro estados entre los que puede seleccionar:

   - Detener

     La detención de una sesión no provoca la pérdida de datos y puede 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. Haga una copia de seguridad de sus datos en el sistema de archivos RES antes de finalizar.

   - Hibernar

     El estado del escritorio se guarda en el disco. Al reiniciar el escritorio, las aplicaciones se reanudan, 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

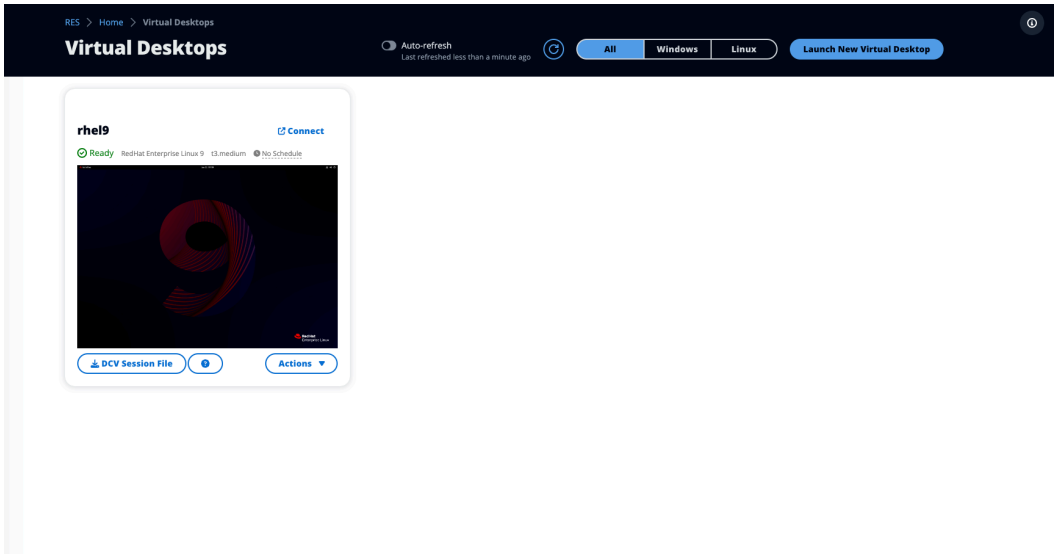
instancia. Para comprobar si la instancia admite este estado, consulta los requisitos previos de hibernación.

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. Tras confirmar que el escritorio se ha detenido, seleccione Acciones y, a continuación, seleccione Actualizar sesión.
3. Cambie el nombre de la sesión o elija un nuevo tamaño de escritorio.
4. Seleccione Enviar.
5. Tras la actualización de las instancias, reinicia el escritorio:

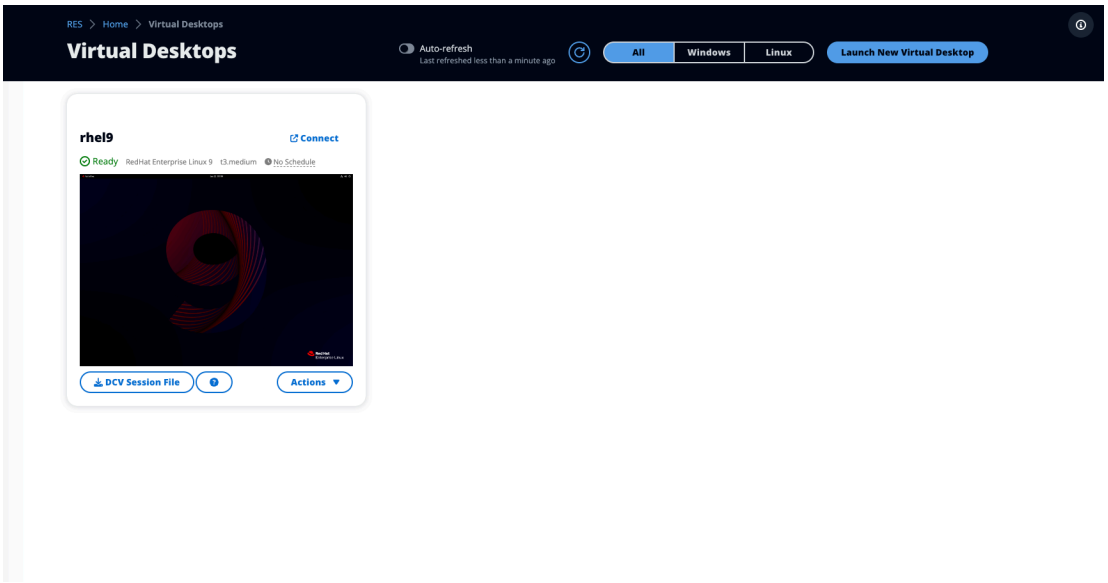
   a. Elija Acciones.

b. Elige el estado del escritorio virtual.

c. Elija Iniciar.

Recupere la información de la sesión

1. Elija Acciones.



2. Elija Mostrar información.

Programe escritorios virtuales

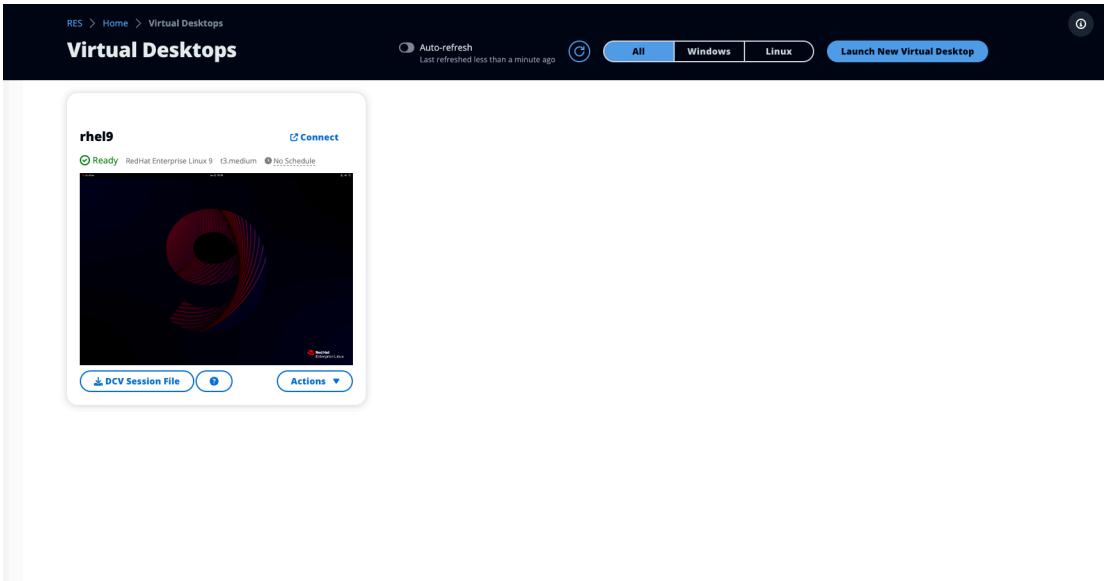
De forma predeterminada, los escritorios virtuales están programados para detenerse automáticamente los sábados y domingos. Los horarios de los escritorios individuales se pueden ajustar mediante las ventanas de programación a las que se accede desde el menú Acciones en los escritorios individuales, como se muestra en la siguiente sección. Para obtener más información, Establezca horarios predeterminados en todo el entorno consulte esa sección. Las computadoras de escritorio también se pueden detener si están inactivas para ayudar a reducir los costos. Consulte Infraestructura de escritorios virtuales: parada automática para obtener más información sobre VDI Autostop.

Temas

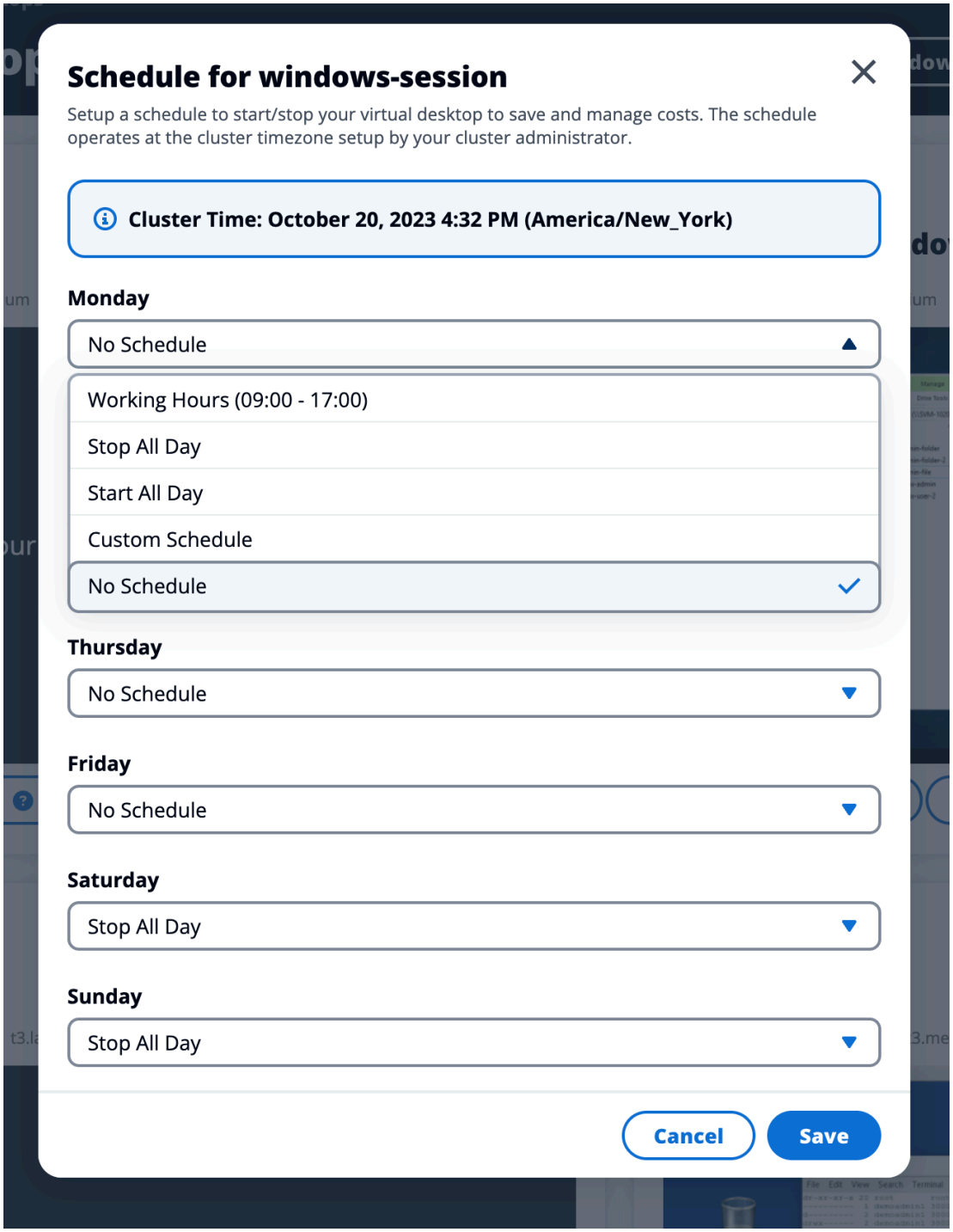
- Establezca horarios de escritorio individuales
- Establezca horarios predeterminados en todo el entorno
- Restablezca la programación a la predeterminada

Establezca horarios de escritorio individuales

1. Elija Acciones.



2. Elija Schedule.
3. Establezca su horario para cada día.
4. Seleccione Save.



Establezca horarios predeterminados en todo el entorno

La programación predeterminada se puede actualizar en DynamoDB:

1. Busque la tabla de configuración del clúster de su entorno:. `<env-name>.cluster-settings`

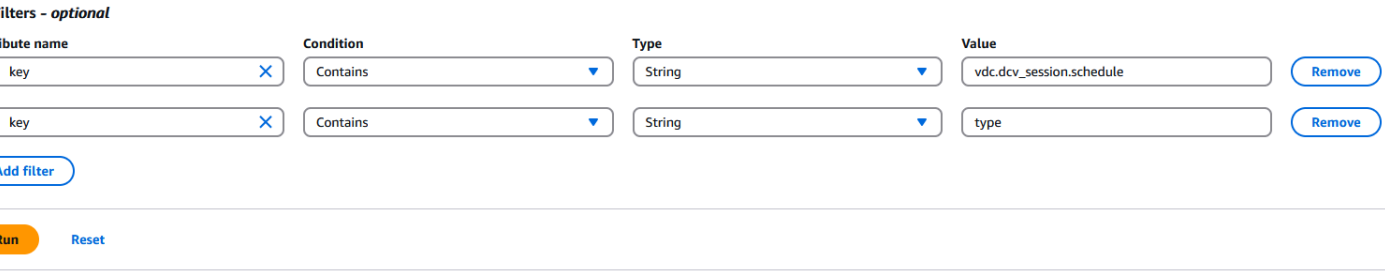
2. Seleccione Explorar elementos.
3. En Filtros, introduzca los dos filtros siguientes:

   Filtro 1

   - Nombre del atributo = **`key`**
   - Condición = **`Contains`**
   - Tipo = **`String`**
   - Valor = **`vdc.dcv_session.schedule`**

   Filtro 2

   - Nombre del atributo = **`key`**
   - Condición = **`Contains`**
   - Tipo = **`String`**
   - Valor = **`type`**



   Se mostrarán siete entradas que representan los tipos de programación predeterminados para cada día del formulario`vdc.dcv_session.schedule.<day>.type`. Los valores válidos son:

   - `NO_SCHEDULE`
   - `STOP_ALL_DAY`
   - `START_ALL_DAY`
   - `WORKING_HOURS`
   - `CUSTOM_SCHEDULE`

4. Si `CUSTOM_SCHEDULE` está establecido, debe proporcionar las horas de inicio y finalización personalizadas. Para ello, utilice el siguiente filtro en la tabla de configuración del clúster:

- Nombre del atributo = **`key`**
- Condición = **`Contains`**
- Tipo = **`String`**
- Valor = **`vdc.dcv_session.schedule`**

5. Busque el artículo formateado como `vdc.dcv_session.schedule.<day>.start_up_time` y `vdc.dcv_session.schedule.<day>.shut_down_time` para los días respectivos en los que desee establecer su horario personalizado. Dentro del elemento, elimina la entrada nula y sustitúyela por una entrada de cadena de la siguiente manera:

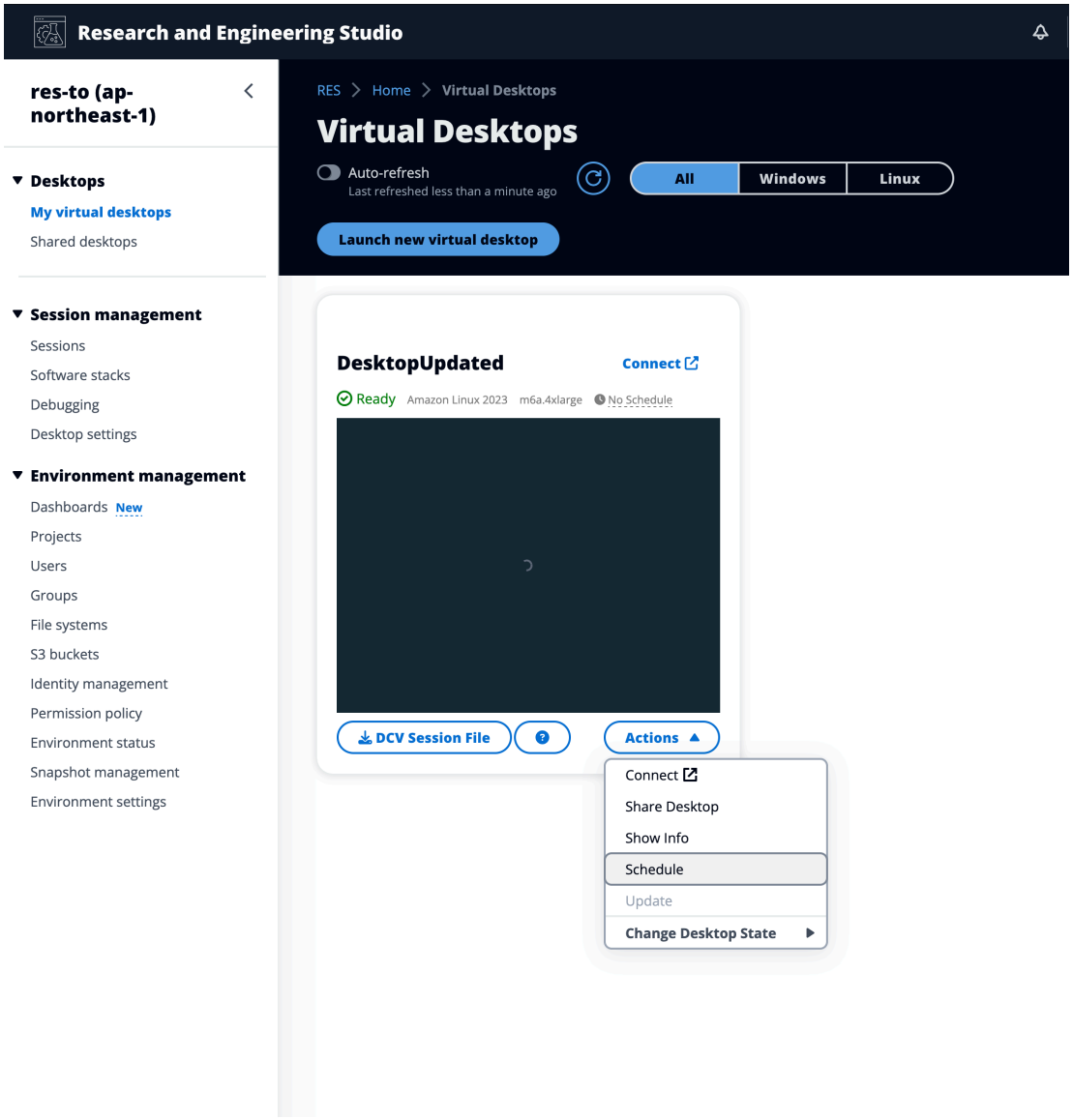
   - Nombre del atributo = **`value`**
   - Valor = ***`<The time>`***
   - Tipo = **`String`**

   El valor de la hora debe tener el formato de XX:XX un reloj de 24 horas. Por ejemplo, las 9 de la mañana serían las 09:00 y las 5 de la tarde serían las 17:00. La hora ingresada siempre corresponde a la hora local de la AWS región en la que se implementa el entorno RES.

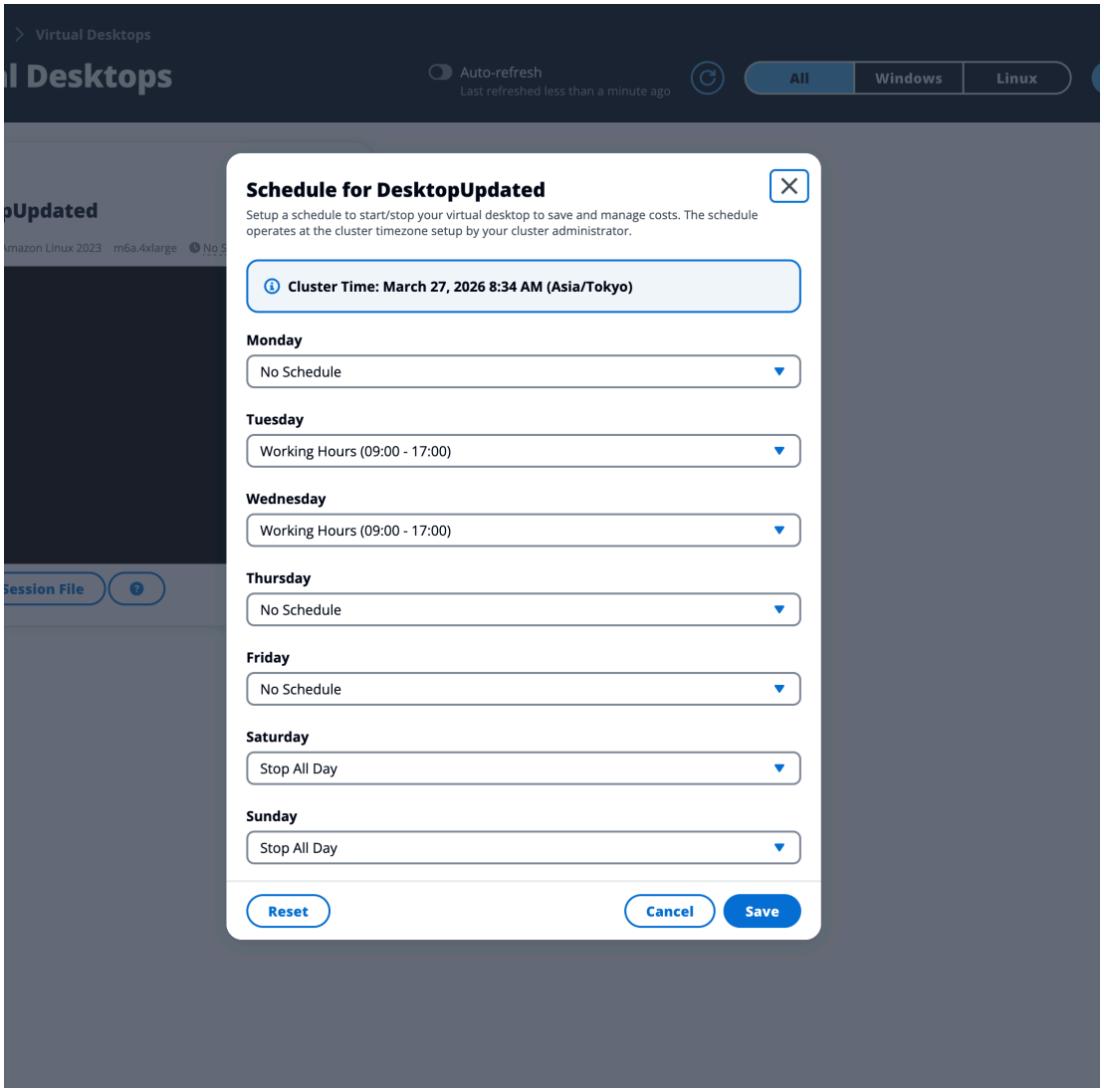
Restablezca la programación a la predeterminada

Si ha personalizado la programación de un escritorio virtual, puede restablecerla a la programación predeterminada del sistema establecida por el administrador.

1. Seleccione la sesión de escritorio virtual que desee restablecer.
2. Seleccione Acciones > Programar.



3. Haga clic en Restablecer.



4. Seleccione Save.

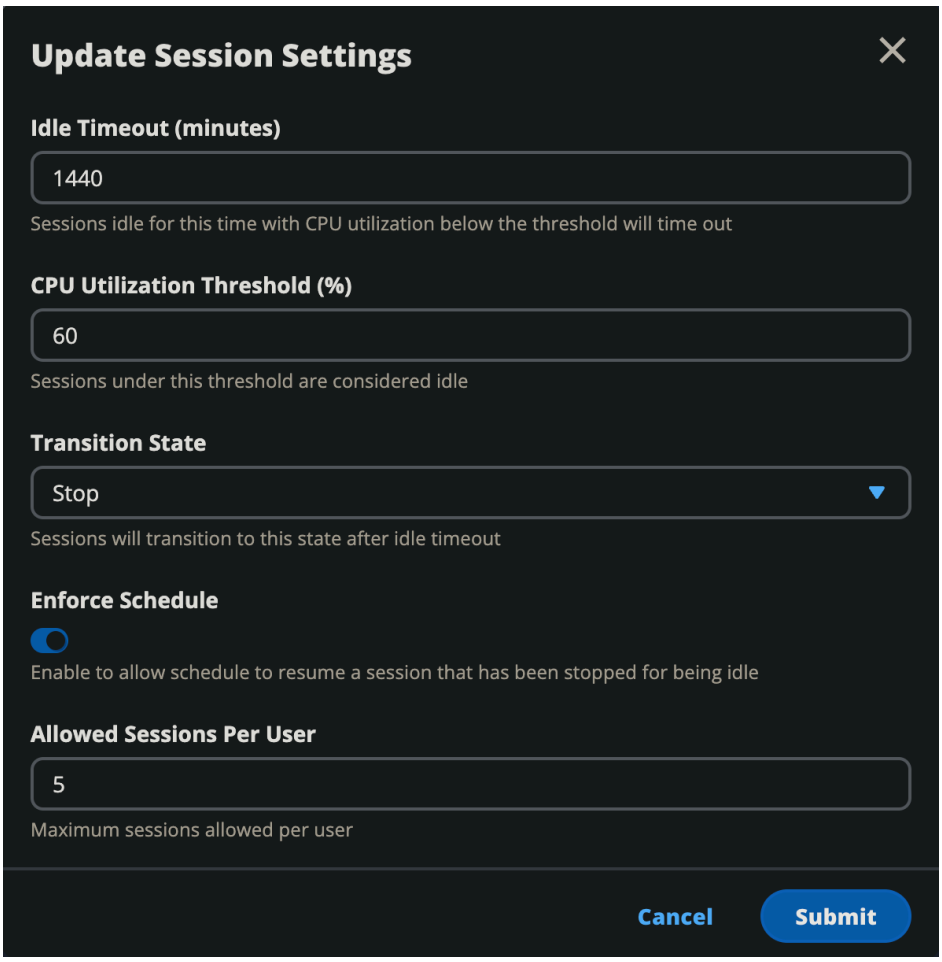
Infraestructura de escritorios virtuales: parada automática

Los administradores pueden configurar los ajustes para permitir detener o terminar los VDI inactivos. Hay 4 ajustes configurables:

1. Tiempo de espera de inactividad: se agotará el tiempo de espera de las sesiones inactivas durante este tiempo con un uso de la CPU inferior al umbral.
2. Umbral de uso de la CPU: las sesiones sin interacción y por debajo de este umbral (uso de vCPU) se consideran inactivas. Si se establece en 0, las sesiones nunca se considerarán inactivas.

> **Important**
>
> RES ejecuta un script de detección de inactividad al principio de cada minuto que comprueba el uso de la CPU. Este script en sí mismo provoca picos temporales de CPU, lo que puede impedir la detección de la inactividad si el umbral está demasiado bajo.

3. Estado de transición: cuando se agote el tiempo de inactividad, las sesiones pasarán a este estado (detenidas o finalizadas).
4. Hacer cumplir la programación: si se selecciona, una sesión que se haya detenido por estar inactiva se puede reanudar según su programación diaria.

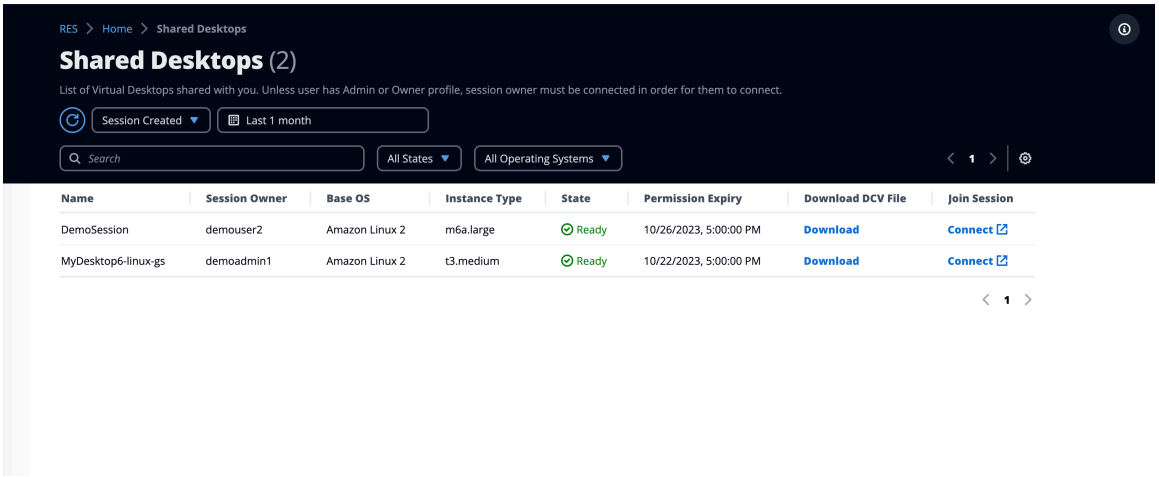


Estos ajustes están presentes en la página de configuración del escritorio, en la pestaña Servidor. Tras actualizar la configuración según sus requisitos, pulse Enviar para guardar la configuración. Las sesiones nuevas utilizarán la configuración actualizada, pero tenga en cuenta que las sesiones existentes seguirán utilizando la configuración que tenían cuando se lanzaron.

Cuando se agote el tiempo de espera, las sesiones finalizarán o pasarán a ese `STOPPED_IDLE` estado en función de su configuración. Los usuarios podrán iniciar `STOPPED_IDLE` sesiones desde la interfaz de usuario.

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.



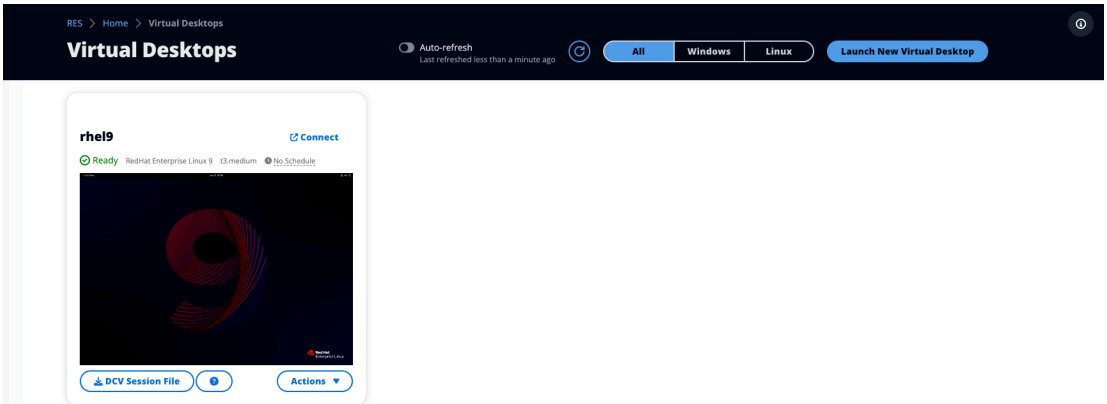
Al compartir una sesión, puede configurar los permisos para sus colaboradores. Por ejemplo, puedes conceder acceso de solo lectura a un compañero de equipo con el que estés colaborando.

Temas

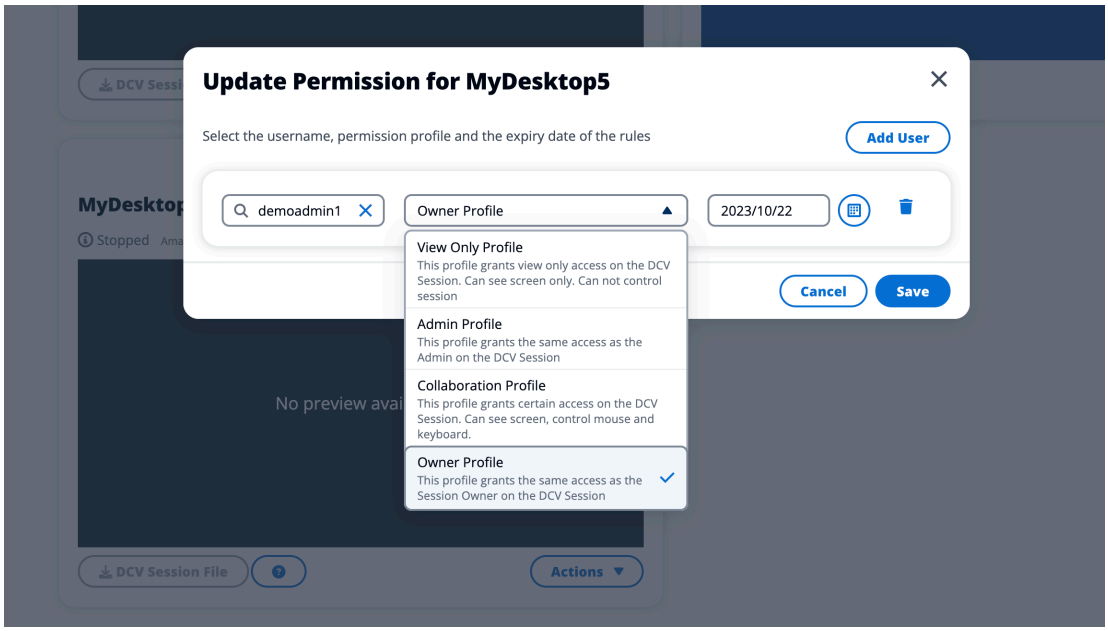
- Comparte un escritorio
- Acceder a un escritorio compartido

Comparte un escritorio

1. En la sesión de escritorio, selecciona Acciones.



2. Selecciona Permisos de sesión.
3. Seleccione el usuario y el nivel de permiso. También puede establecer una fecha de caducidad.
4. Seleccione Save.



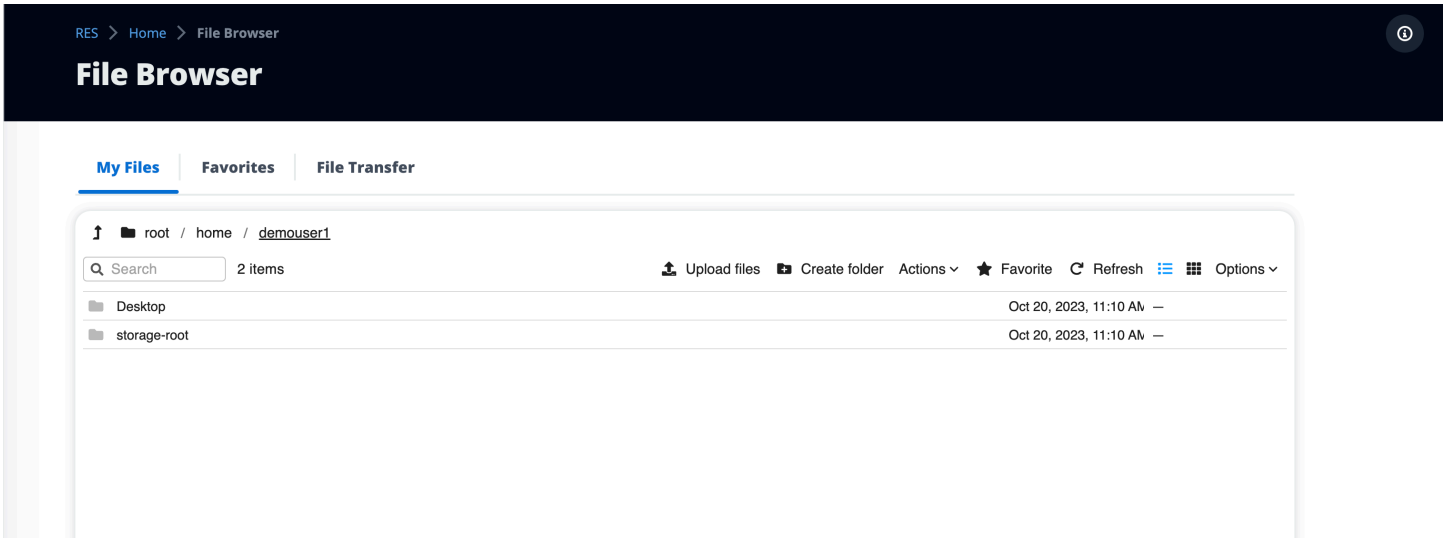
Para obtener más información sobre los permisos de IAM, consulte the section called “Política de permisos”.

Acceder 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 enAcceda a su escritorio.

Explorador de archivos

El explorador de archivos le permite acceder al sistema de archivos EFS compartido a nivel mundial a través del portal web. Puede administrar todos los archivos disponibles a los que tiene permiso de acceso en el sistema de archivos subyacente. Se trata del mismo sistema de archivos que comparten sus escritorios virtuales Linux. 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.

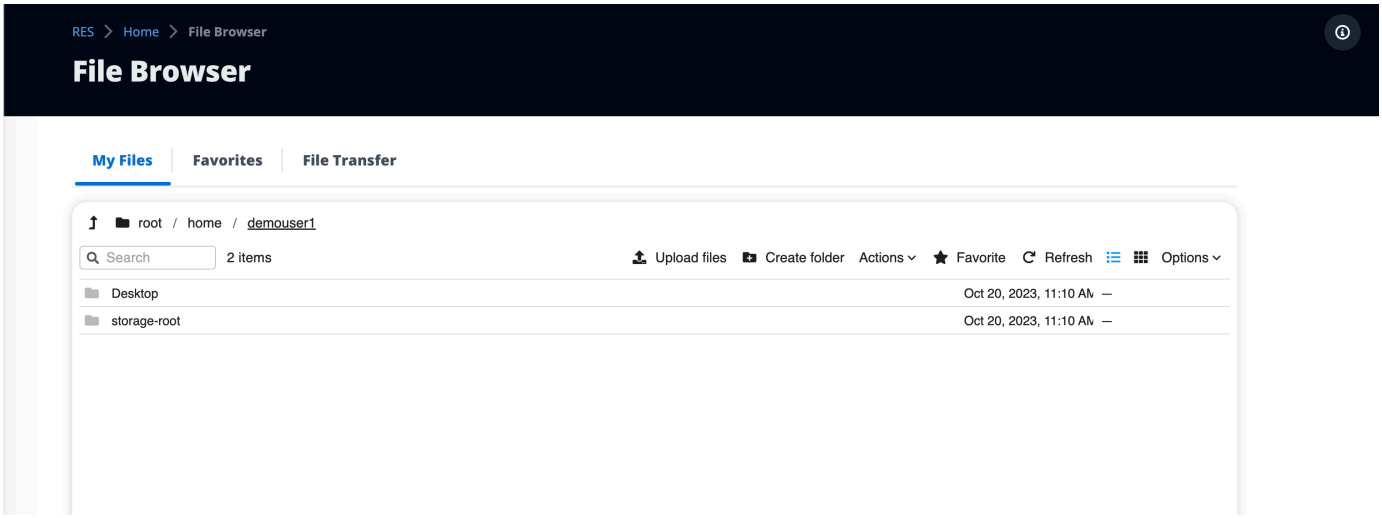


Temas

- Carga de archivos
- Eliminar archivos
- Administra los favoritos
- Edición de archivos
- Transferencia de archivos

Carga de archivos

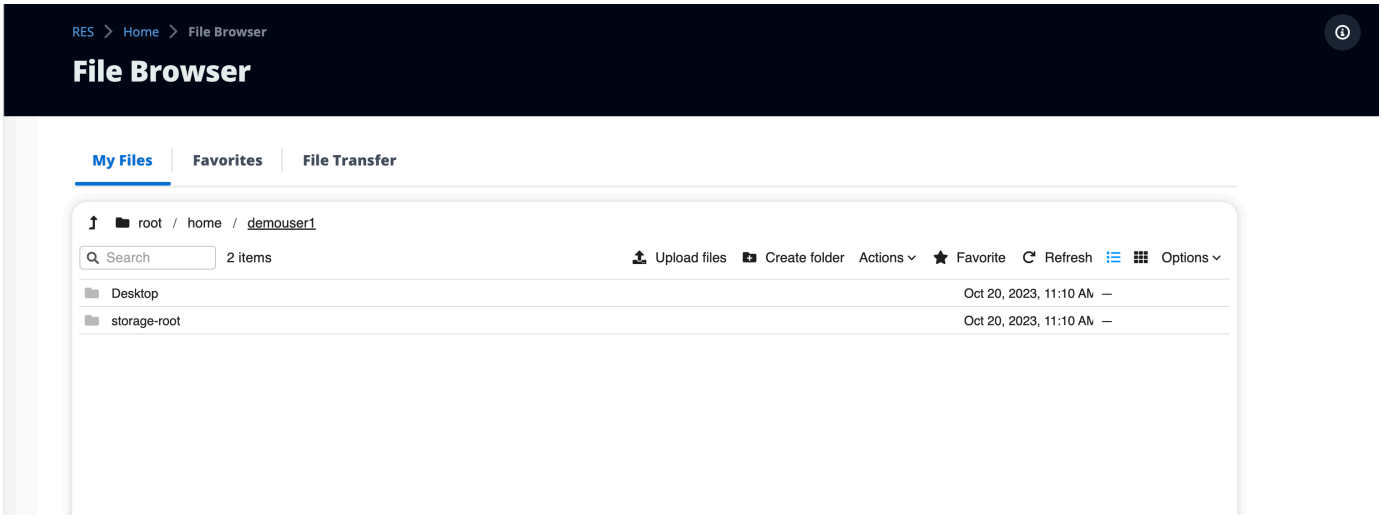
1. Selecciona Cargar archivos.



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

Eliminar archivos

1. Seleccione los archivos que desee eliminar.



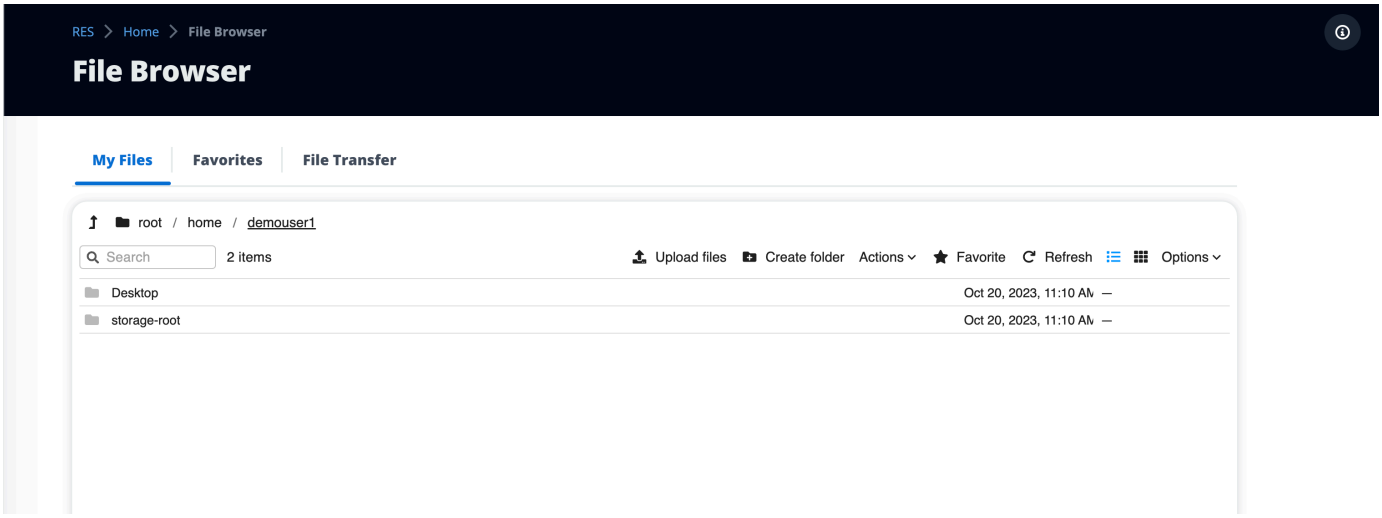
2. Elija Acciones.
3. Elija Eliminar archivos.

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, puede añadirlos a Favoritos.

1. Selecciona un archivo o una carpeta.



2. Selecciona Favorito.

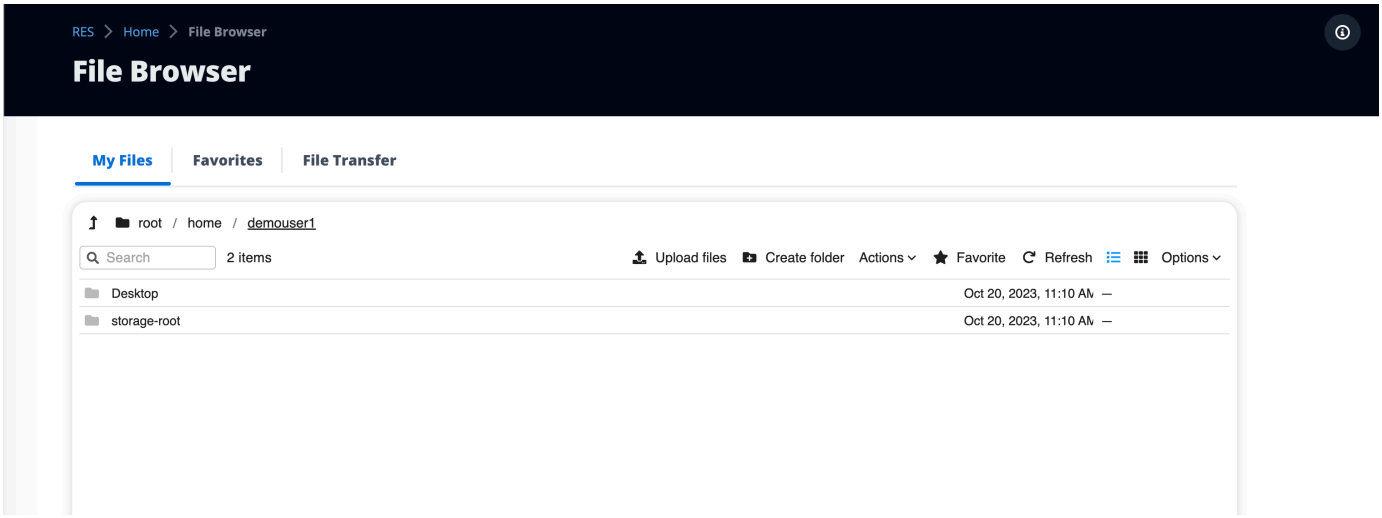
También puede hacer clic con el botón derecho en cualquier archivo o carpeta y seleccionar Favorito.

> **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. Seleccione el archivo que desee actualizar. Se abrirá un modal con el contenido del archivo.

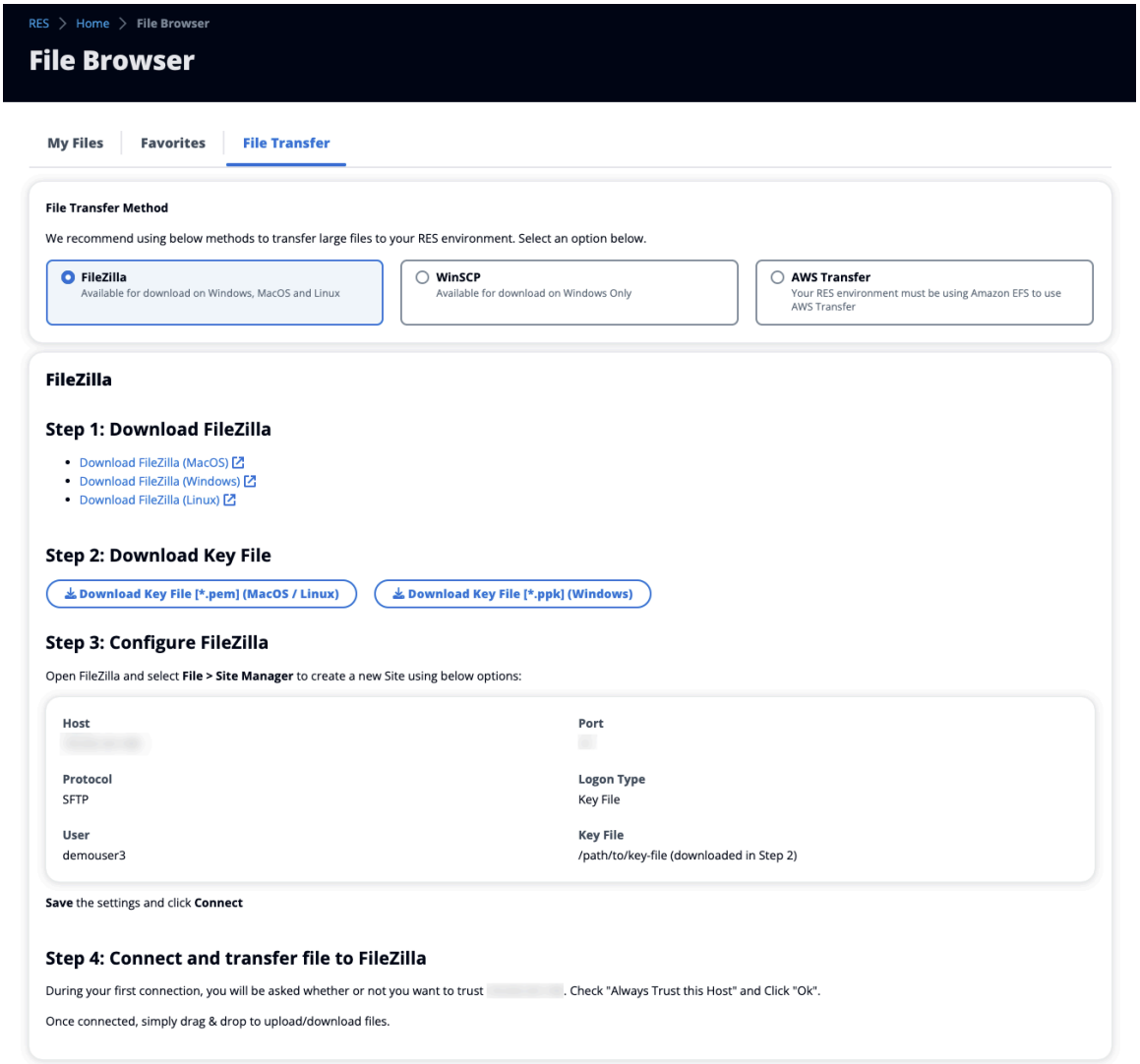


2. Realice las actualizaciones y seleccione Guardar.

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)


RES > Home > File Browser
File Browser
My Files
Favorites
File Transfer
File Transfer Method
We recommend using below methods to transfer large files to your RES environment. Select an option below.
FileZilla
Available for download on Windows, MacOS and Linux
WinSCP
Available for download on Windows Only
AWS Transfer
Your RES environment must be using Amazon EFS to use AWS Transfer
FileZilla
Step 1: Download FileZilla
Download FileZilla (MacOS)
Download FileZilla (Windows)
Download FileZilla (Linux)
Step 2: Download Key File
Download Key File [*.pem] (MacOS / Linux)
Download Key File [*.ppk] (Windows)
Step 3: Configure FileZilla
Open FileZilla and select File > Site Manager to create a new Site using below options:
Host
Port
Protocol
SFTP
Logon Type
Key File
User
demouser3
Key File
/path/to/key-file (downloaded in Step 2)
Save the settings and click Connect
Step 4: Connect and transfer file to FileZilla
During your first connection, you will be asked whether or not you want to trust . Check "Always Trust this Host" and Click "Ok".
Once connected, simply drag & drop to upload/download files.

Resolución de problemas

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

Temas

Contenido detallado:

- (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
- (02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo SAMAccountName atributo 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

Depuración y supervisión generales

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

- Fuentes útiles de información sobre registros y eventos
  - ¿Dónde encontrar las variables de entorno
  - Archivos de registro en el entorno (instancias de Amazon EC2)
  - CloudFormation Pilas
  - Fallos del sistema debidos a un problema y reflejados en la actividad del grupo Amazon EC2 Auto Scaling
- Apariencia típica de la consola Amazon EC2
  - 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 de Amazon 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.

¿Dónde encontrar las variables de entorno

De forma predeterminada, puede encontrar variables de entorno, como el nombre de usuario del propietario de la sesión, en las siguientes ubicaciones:

- Linux: `/etc/environment`
- Windows: `C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\environment_variables.json`

Archivos de registro en el entorno (instancias de Amazon EC2)

Los archivos de registro existen en las instancias de Amazon EC2 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.

- ///application.log opt/idea app/logs
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssd/
- var/log//mensajes
- //user-data.log var/log
- /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/
- //.log root/bootstrap logs/userdata
- //mensajes var/log
- /opt/idea/app/logs/
- /opt/res/.log logs/vdi_idle_check

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 DCVSessionManagerAgent
- PS C:\IDEA\Logs\\ RESIdleCheckVDI
- C:\Program Archivos\ RES\ app\

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 de AWS Lambda cómputo 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`
  - `virtual-desktop-app/ - virtual desktop bootstrap and DCV related`
  - `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"
```

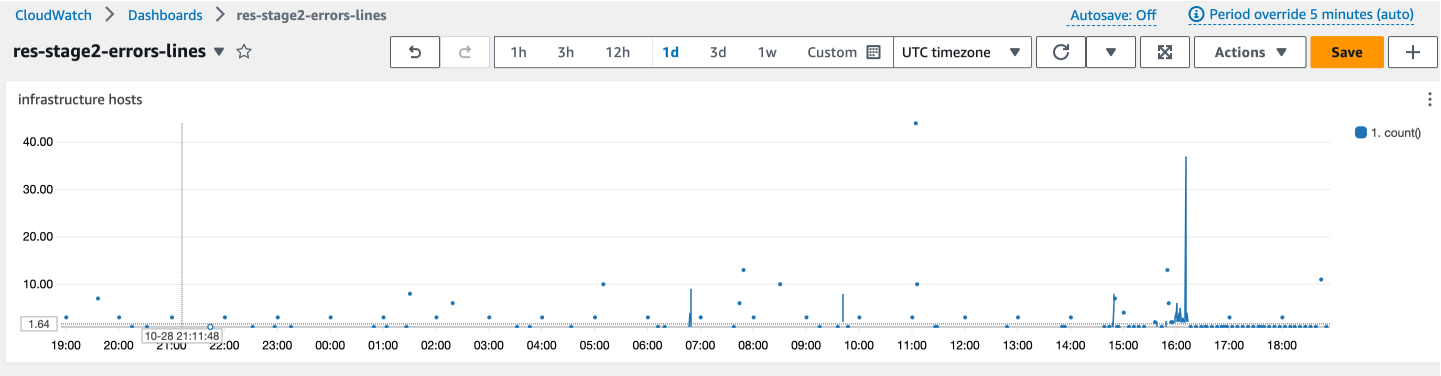
Otro método de supervisión de los problemas consiste en crear Amazon CloudWatch Dashboards que contengan widgets que muestren los datos de interés.

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

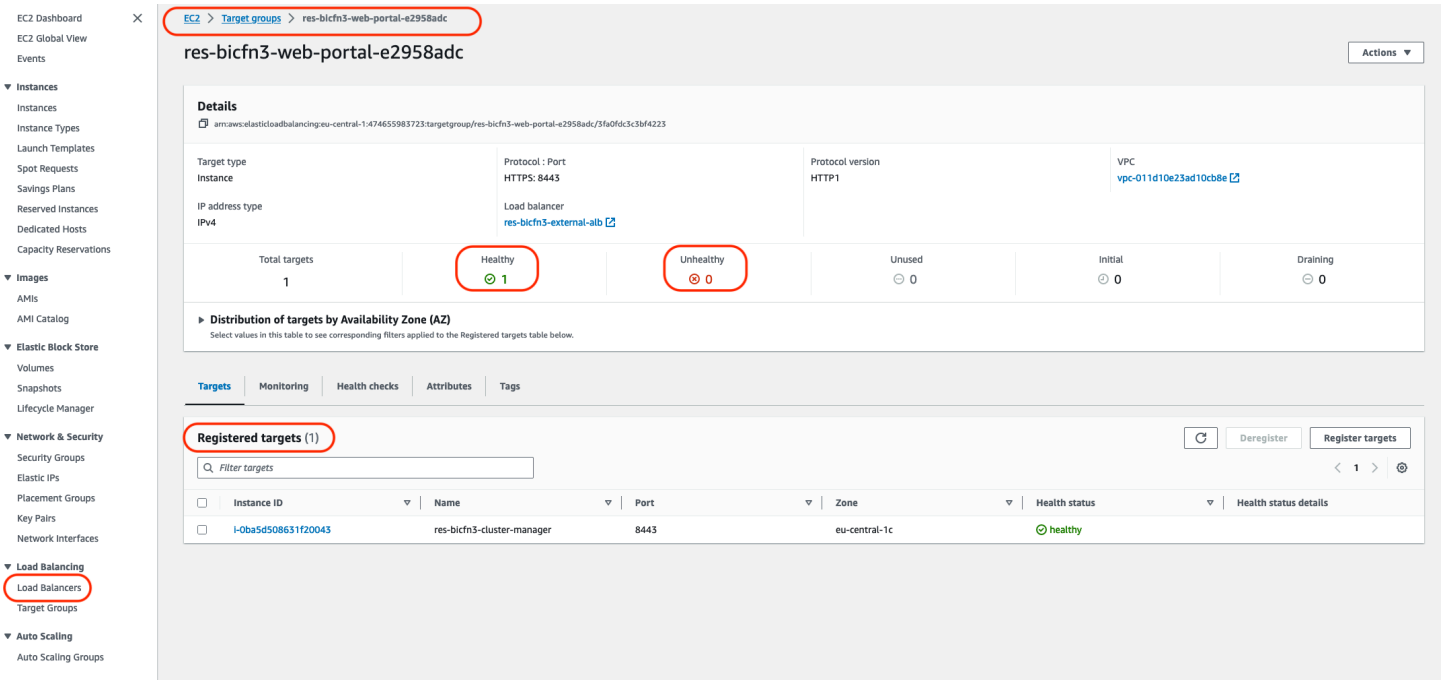
Fallos del sistema debidos a un problema y reflejados en la actividad del grupo Amazon EC2 Auto Scaling

Si las interfaces de usuario de RES indican errores en el servidor, la causa puede ser un problema con el software de la aplicación u otro problema.

Cada uno de los grupos de escalado automático (ASG) de instancias de Amazon EC2 de infraestructura 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 consola de Amazon EC2 para ver si hay varias instancias terminadas y consulte la pestaña Actividad del grupo de Auto Scaling para ver el ASG relacionado para determinar si las instancias de Amazon EC2 están en ciclo.

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.

La consola ASG puede mostrar una actividad similar a la siguiente si se produce este problema.

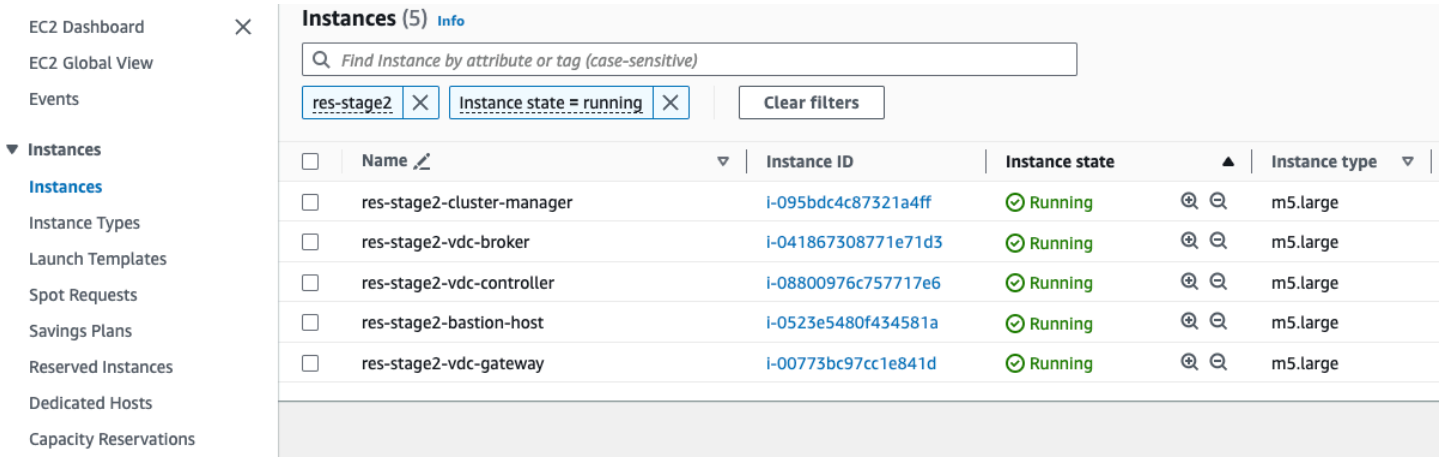


Apariencia típica de la consola Amazon EC2

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

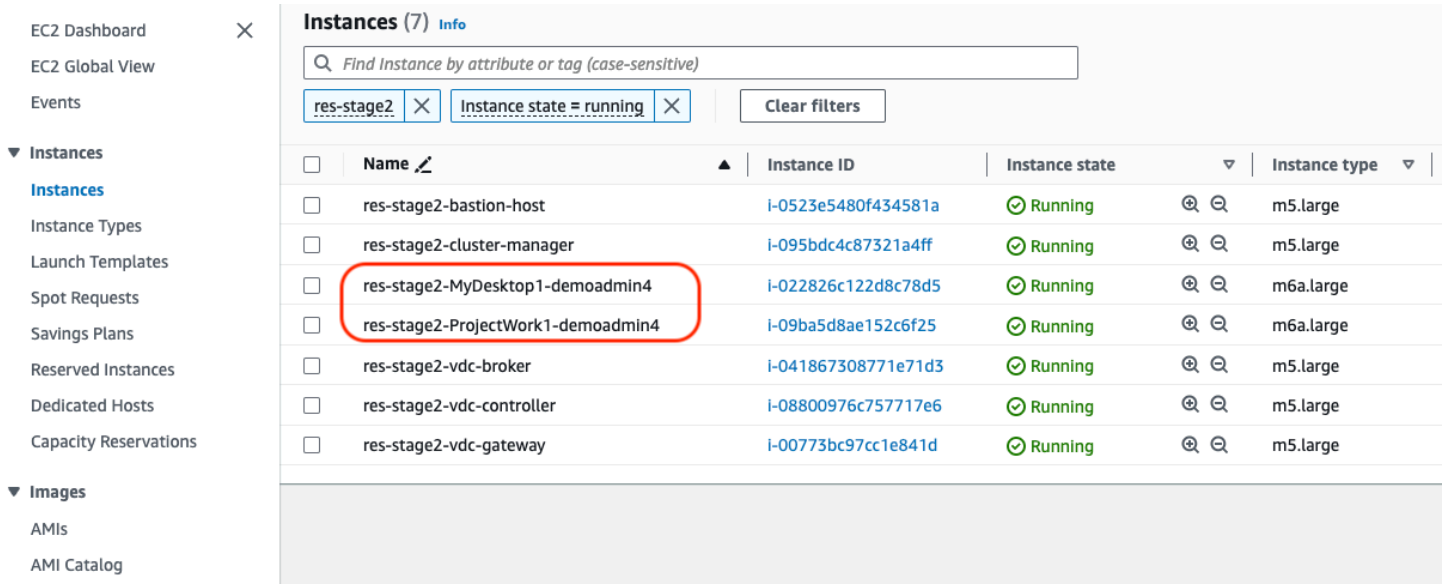
Hosts de infraestructura

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



Hosts de infraestructura y escritorios virtuales

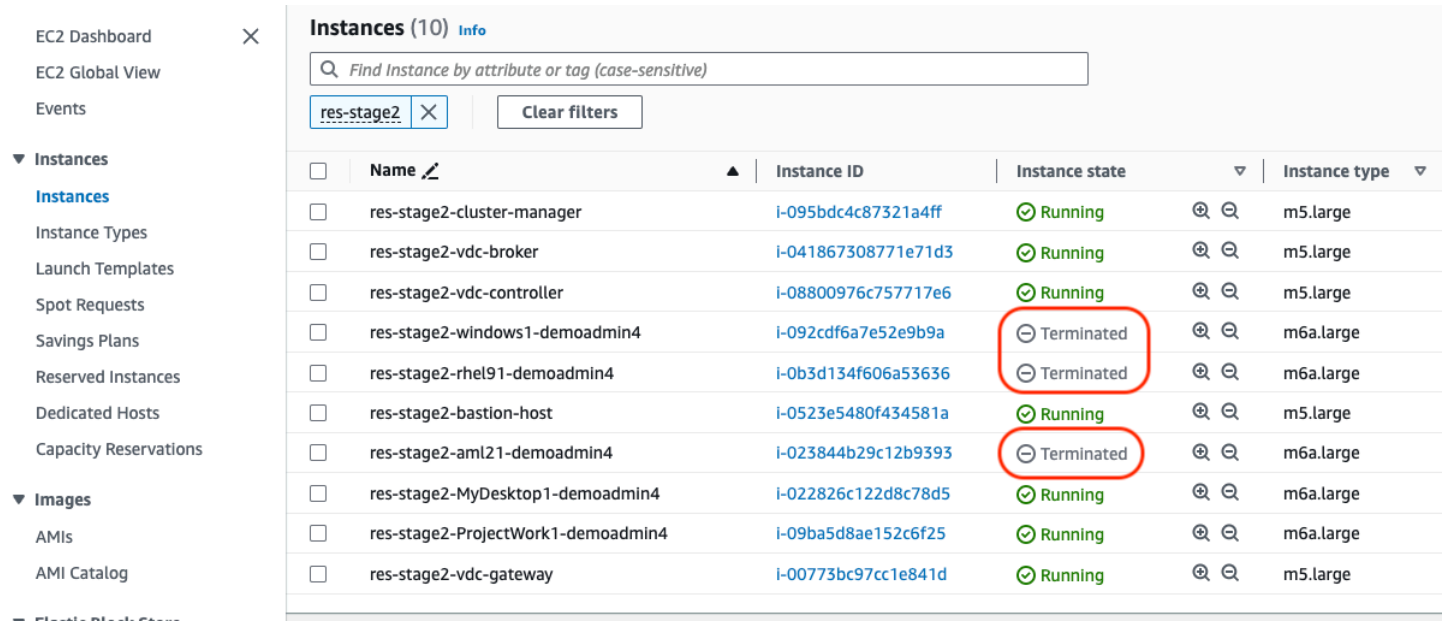
En la consola Amazon EC2, cuando los escritorios virtuales están en ejecución, tienen un aspecto similar al siguiente. En este caso, los escritorios virtuales aparecen en rojo. El sufijo del nombre de la instancia es el usuario que creó el escritorio. El nombre que aparece en el centro es el nombre de 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 consola Amazon EC2 muestra instancias terminadas, generalmente se trata de 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

Los siguientes son 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 de Amazon DCV

Amazon DCV se utiliza para sesiones de escritorios virtuales. AWS Amazon DCV. Los siguientes ejemplos muestran cómo determinar la versión del software DCV instalada.

Linux

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

Amazon 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

Amazon 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
  - CloudFormation la pila no se puede crear con el mensaje «se WaitCondition recibió el mensaje fallido». Error:States.TaskFailed»
  - No se recibió la notificación por correo electrónico después de que las 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
- Problemas de administración de identidades
  - No estoy autorizado a realizar iam: PassRole
  - Quiero permitir que personas ajenas a mi AWS cuenta accedan a los AWS recursos de mi Estudio de Investigación e Ingeniería
  - Al iniciar sesión en el entorno, vuelvo inmediatamente a la página de inicio de sesión
  - Se produjo el error «Usuario no encontrado» al intentar iniciar sesión
  - El usuario se agregó en Active Directory, pero no aparece en RES

Problemas de instalación

Temas

.....

CloudFormation la pila no se puede crear con el mensaje «se WaitCondition recibió el mensaje fallido». Error:States.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 que esté 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 CloudFormation pilas se crearan correctamente

Si no se recibió una invitación por correo electrónico después de haber creado correctamente las 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. Consulte la consola Amazon EC2 para ver si hay pruebas de casos de ciclismo.

   Si hay instancias de Amazon EC2 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 siguientes pasos the section called “Instancias cíclicas o controladora de vdc en estado fallido” para resolver el problema.

.....

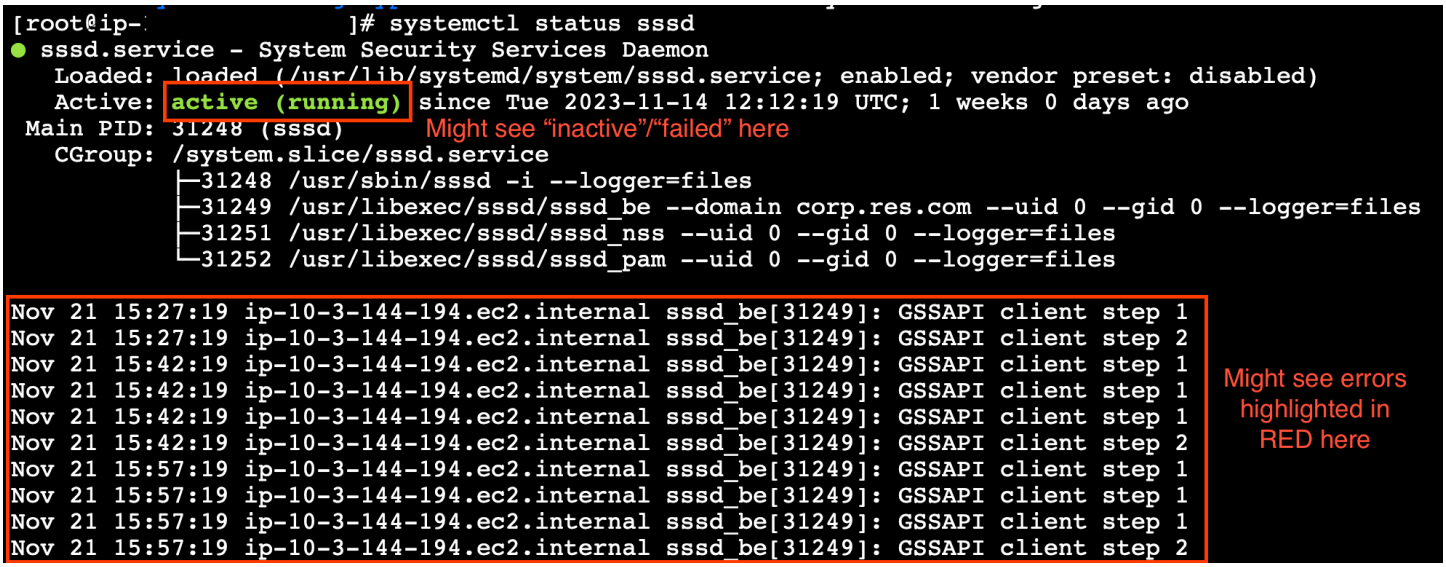
Instancias cíclicas o controladora de vdc en estado fallido

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 Directory Service.
        ii. Seleccione el ID de directorio para su directorio RES y elija Acciones.
        iii. Seleccione Restablecer contraseña de usuario.
        iv. Ingresa 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, a continuación, selecciona Texto sin formato.
        iv. Elija Edit (Edición de).
        v. Establece una nueva contraseña para el ServiceAccount usuario y selecciona 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 instancia de Amazon EC2 se lanzó a una RES-created subred o grupo de seguridad mediante la consola. AWS

Para resolver el problema, busque y cancele todas las instancias de Amazon EC2 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 los parches de Amazon EC2 se hayan producido inesperadamente 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 Amazon EC2 del entorno, revise el registro de la instancia local 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 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 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 la función 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 la función 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 PassRole acción iam:. Si necesitas ayuda, ponte en contacto con tu AWS administrador. El administrador 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

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre cómo proporcionar acceso a tus recursos en todas AWS las cuentas de tu propiedad, consulta Cómo proporcionar acceso a un usuario de IAM desde otra AWS cuenta de tu 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.

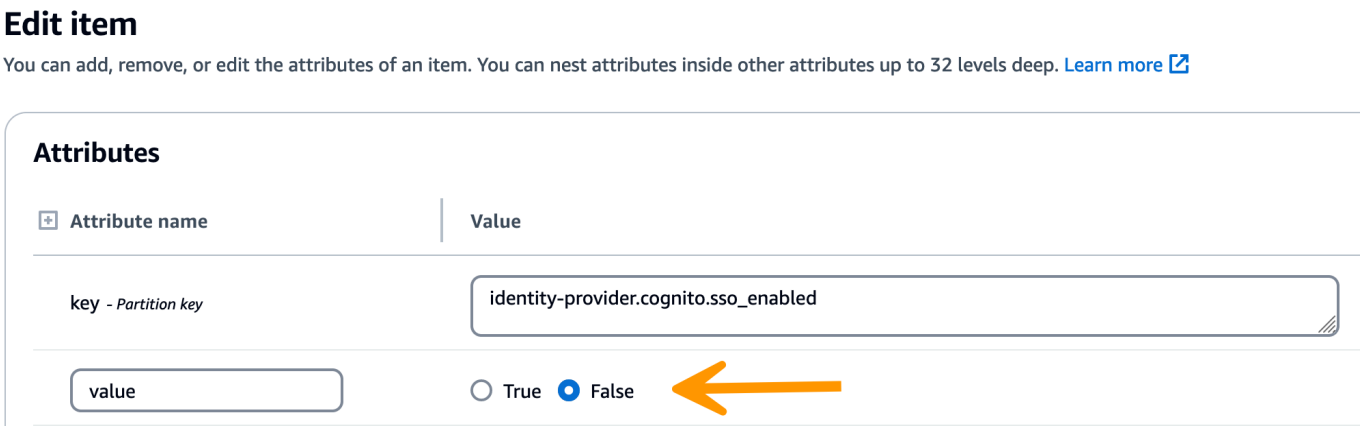
Para comprobar los registros:

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 Ejecutar.
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

> **Note**
>
> Esta sección se aplica a RES 2024.10 y versiones anteriores. Para ver la RES 2024.12 y versiones posteriores, consulte. Cómo ejecutar la sincronización manualmente (versiones 2024.12 y 2024.12.01) Para RES 2025.03 y versiones posteriores, consulte. Cómo iniciar o detener la sincronización manualmente (versión 2025.03 y versiones posteriores)

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. Seleccione Enviar y recibir mensajes.

4. En Cuerpo del mensaje, introduzca:

   `{ "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 se encuentra 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
- Creé Amazon FSx para NetApp ONTAP desde RES, pero no se unió 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.

Amazon FSx ONTAP

1. Ve a la consola de Amazon FSx.
2. Compruebe 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

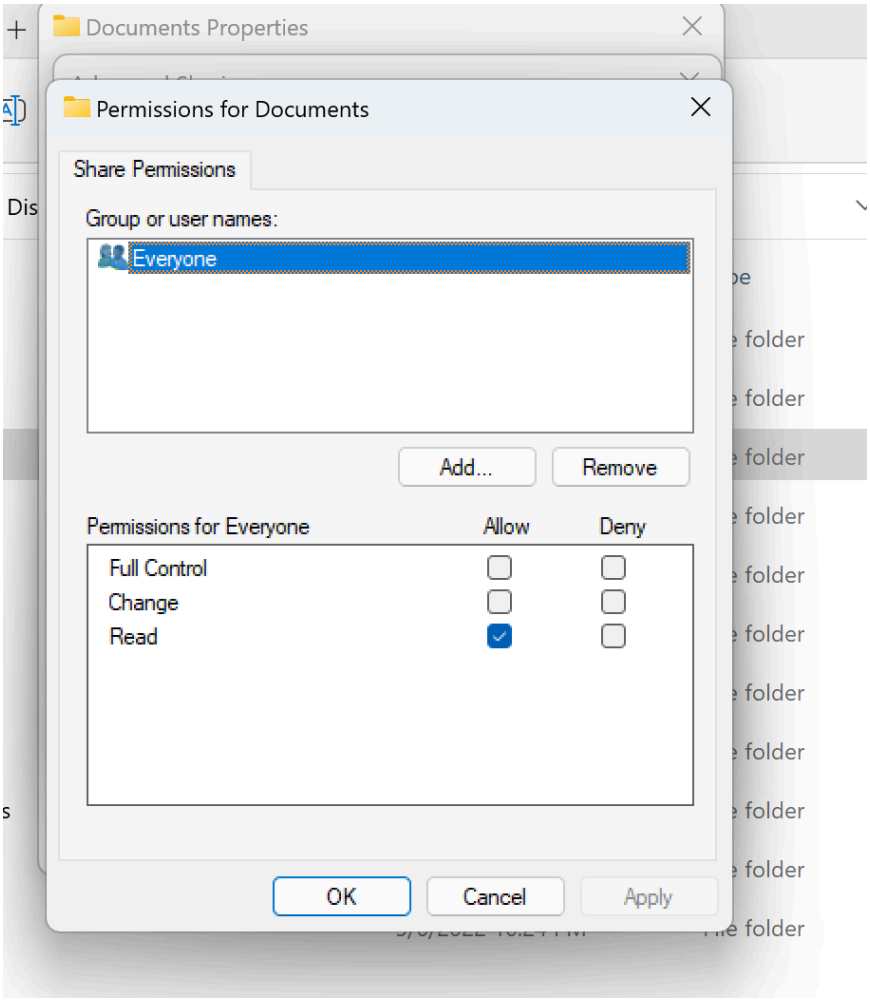
Uso de un volumen de estilo UNIX con cargas de trabajo de Linux

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 configurar los permisos de `Full ControlChange`,, `Allow` o `Read` para`Deny`:



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 Habilitación de cargas de trabajo multiprotocolo con Amazon FSx para ONTAP. NetApp

.....

Creé Amazon FSx para NetApp ONTAP desde RES, pero no se unió 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 su dominio, consulte Cómo unir SVM a un Active Directory de Microsoft y siga los pasos de la consola de Amazon FSx. Asegúrese de que los permisos necesarios estén delegados a la cuenta de servicio de Amazon FSx en AD. Una vez que el SVM se una al dominio correctamente,

vaya a Resumen del SVM > Puntos de enlace > Nombre DNS SMB y copie el nombre DNS, ya que 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. Elija Save and close.

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 Administración del entorno, seleccione File Systems, Onboard File System.

.....

Snapshots

Temas

- Una instantánea tiene el estado Fallido
- No se puede aplicar una instantánea y los registros indican que las tablas no se pudieron importar.

.....

Una instantánea tiene el estado Fallido

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

.....

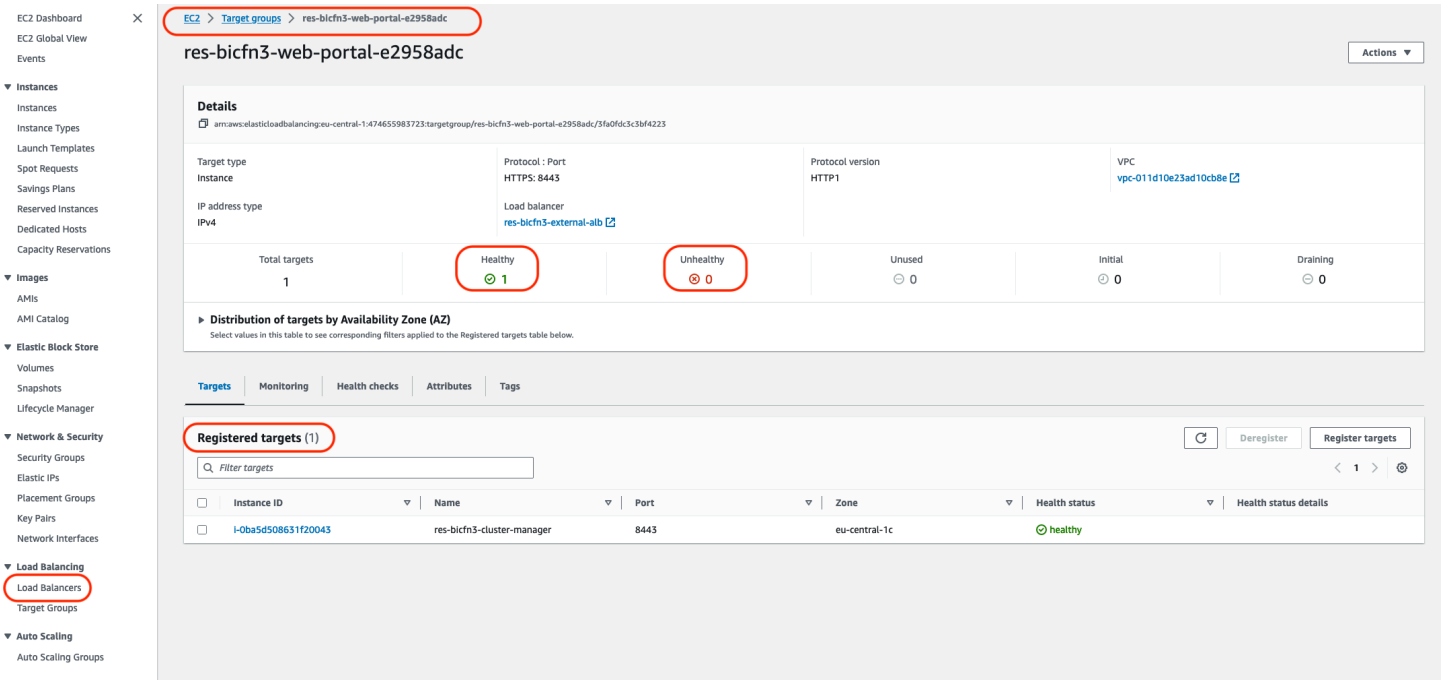
Grupos objetivo del balanceador de carga sin instancias en buen estado

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 instancias de Amazon EC2.

Los métodos para determinar el origen del problema consisten en comprobar primero en la consola de Amazon EC2 cualquier instancia de Amazon EC2 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 consola Amazon EC2, no muestra ninguna instancia registrada en buen estado.

A continuación se muestra un ejemplo de aspecto normal:



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

Si la entrada Unhealthy no es 0, eso indica que es posible que una instancia de Amazon EC2 esté circulando. Esto puede deberse a que el software de las aplicaciones instaladas no pasa las comprobaciones 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 públicas y privadas no tengan las AZ correspondientes. 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

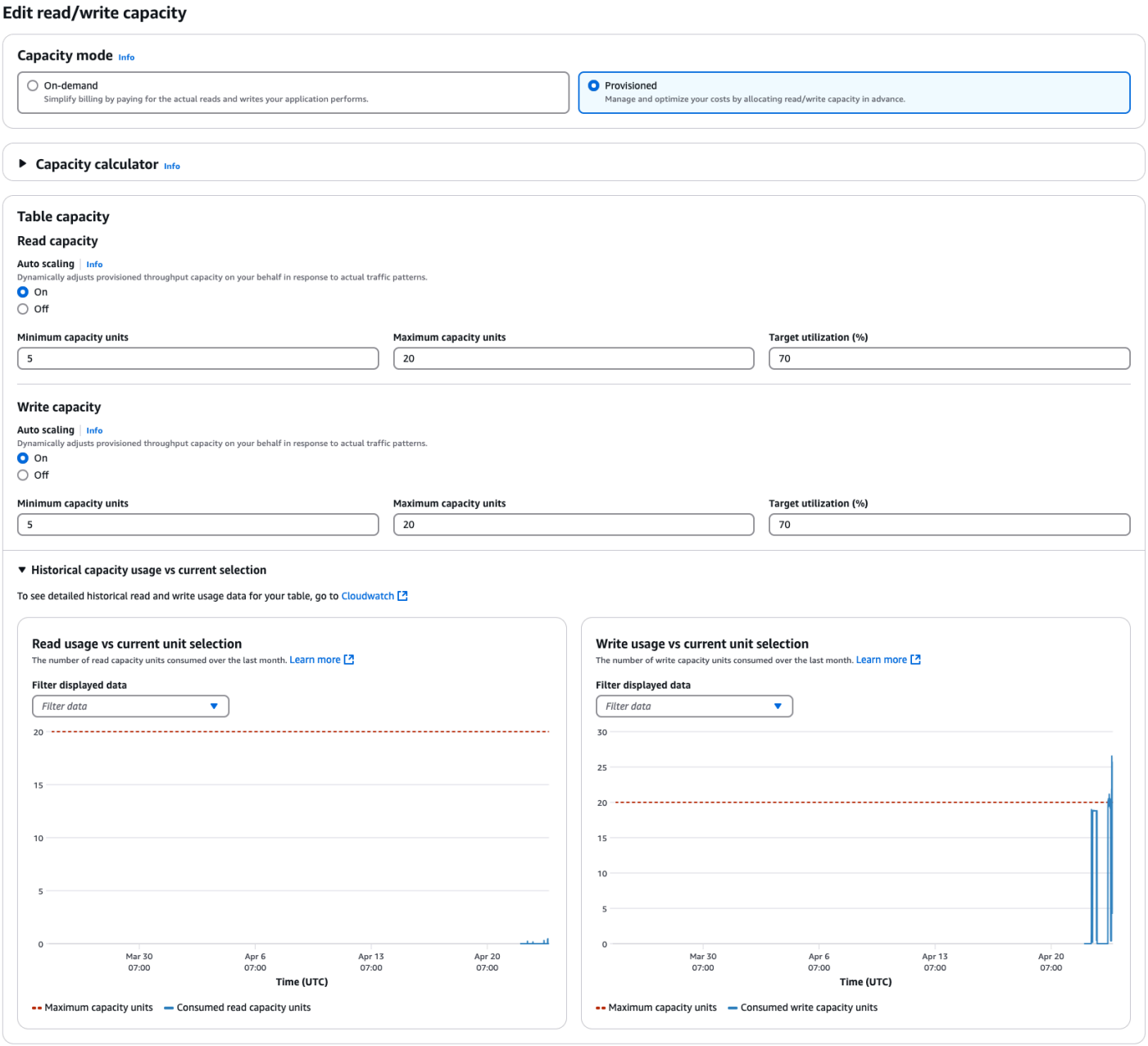
.....

Necesito iniciar o reanudar una gran cantidad de VDI en el portal web de RES

Al lanzar o reanudar una gran cantidad de VDI en lote, es posible que acaben en estado de error debido al rendimiento aprovisionado configurado (5 a 20) para las tablas de DynamoDB*environment-name*`.vdc.dcv-broker.dcvServer`.

Para solucionar este problema, puede cambiar las unidades de capacidad máxima de lectura y escritura de la *environment-name*`.vdc.dcv-broker.dcvServer` tabla en la consola de

AWS DynamoDB en función de los datos históricos de uso de la capacidad, como se muestra a continuación:



Tenga en cuenta que el lanzamiento de 5 VDI requiere aproximadamente 1 WCU de operaciones de escritura y el cambio de las unidades de capacidad de lectura/escritura puede afectar al coste de RES. Consulte los precios de la capacidad aprovisionada en la página de precios de Amazon DynamoDB para obtener más información.

.....

La cuenta de inicio de sesión de Windows Virtual Desktop está configurada como Administrador

Si puede iniciar un escritorio virtual de Windows en el portal web de RES, pero su cuenta de inicio de sesión está configurada como Administrador cuando se conecta, es posible que su VDI de Windows no se haya unido correctamente a Active Directory.

Para verificarlo, conéctese a la instancia de Windows desde la consola Amazon EC2 y compruebe los registros de arranque que aparecen en la sección. `C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\` Un mensaje de error que comienza con `[Join AD] authorization failed:` indica que la instancia no se ha podido unir al AD. Comprueba que el administrador de clústeres inicie sesión CloudWatch con el nombre del grupo de registros `/<res-environment-name>/cluster-manager` para obtener más información sobre el error:

- `Insufficient permissions to modify computer account`
  - Este error indica que su cuenta de servicio no tiene los permisos adecuados para añadir ordenadores al AD. Consulta la Configurar una cuenta de servicio para Microsoft Active Directory sección para ver los permisos que requiere la cuenta de servicio.
- `Invalid Credentials`
  - Las credenciales de tu cuenta de servicio en AD han caducado o has proporcionado credenciales incorrectas. Para comprobar o actualizar las credenciales de su cuenta de servicio, acceda al secreto que almacena la contraseña en la consola de Secrets Manager. Asegúrese de que el ARN de este secreto sea correcto en el campo ARN secreto de las credenciales de la cuenta de servicio, en el dominio de Active Directory, en la página de administración de identidades de su entorno RES.

.....

El certificado caduca cuando se utiliza un recurso externo CertificateRenewalNode

Si implementó la receta de recursos externos y aparece un error al conectarse a los `"The connection has been closed. Transport error"` VDI de Linux, la causa más probable es que el certificado haya caducado y no se actualice automáticamente debido a una ruta de instalación de pip incorrecta en Linux. Los certificados caducan a los 3 meses.

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:

```
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702  WARN HTTP:Splicer Connection{id=341
 client_address="x.x.x.x:50682"}: Error in connection task: TLS handshake error:
 received fatal alert: CertificateUnknown | redacted:/res-demo/vdc/dcv-connection-
gateway | dcv-connection-gateway_10.3.146.195 |
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702  WARN HTTP:Splicer Connection{id=341
 client_address="x.x.x.x:50682"}: Certificate error: AlertReceived(CertificateUnknown)
 | redacted:/res-demo/vdc/dcv-connection-gateway | dcv-connection-gateway_10.3.146.195
 |
```

Para resolver el problema:

1. En su AWS cuenta, vaya a EC2. Si hay una instancia con nombre`*-CertificateRenewalNode-*`, finalice la instancia.
2. Ve a Lambda. Debería ver una función Lambda llamada`*-CertificateRenewalLambda-*`. Compruebe en el código Lambda algo parecido a lo siguiente:

   ```
   export HOME=/tmp/home
   mkdir -p $HOME

   cd /tmp
   wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
   python3 ./get-pip.py
   pip3 install boto3
   eval $(python3 -c "from botocore.credentials import
    InstanceMetadataProvider, InstanceMetadataFetcher; provider =
    InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
    num_attempts=2)); c = provider.load().get_frozen_credentials();
    print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
    AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
    AWS_SESSION_TOKEN={c.token}')")

   mkdir certificates
   cd certificates
   git clone https://github.com/Neilpang/acme.sh.git
   cd acme.sh
   ```
3. Encuentra la plantilla de pila de certificados de recursos externos más reciente aquí. Busque el código Lambda en la plantilla: Recursos → → Propiedades CertificateRenewalLambda→ Código. Puede encontrar algo parecido a lo siguiente:

   ```
   sudo yum install -y wget
   ```

```
export HOME=/tmp/home
mkdir -p $HOME
cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
mkdir -p pip
python3 ./get-pip.py --target $PWD/pip
$PWD/pip/bin/pip3 install boto3
eval $(python3 -c "from botocore.credentials import
 InstanceMetadataProvider, InstanceMetadataFetcher; provider =
 InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
 num_attempts=2)); c = provider.load().get_frozen_credentials();
 print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
 AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
 AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
cd certificates
VERSION=3.1.0
wget https://github.com/acmesh-official/acme.sh/archive/refs/tags/$VERSION.tar.gz -
O acme-$VERSION.tar.gz
tar -xvf acme-$VERSION.tar.gz
cd acme.sh-$VERSION
```

4. Sustituya la sección del paso 2 de la función `*-CertificateRenewalLambda-*` Lambda por el código del paso 3. Seleccione Implementar y espere a que el cambio de código surta efecto.
5. Para activar manualmente la función Lambda, vaya a la pestaña Prueba y, a continuación, seleccione Probar. No se requiere ninguna entrada adicional. Esto debería crear una instancia EC2 de certificado que actualice el certificado y PrivateKey los secretos en Secret Manager.
6. Finalice la instancia dcv-gateway existente *<env-name>*`-vdc-gateway` y espere a que el grupo de autoescalado implemente automáticamente una nueva.

.....

Un escritorio virtual que funcionaba anteriormente ya no puede conectarse correctamente

Si se cierra una conexión de escritorio o ya no puede conectarse a ella, el problema puede deberse a un error en la instancia Amazon EC2 subyacente o a que la instancia Amazon EC2 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 la consola Amazon EC2 para determinar si la instancia se ha cerrado o detenido. Si está detenida, intente 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 General.
- Seleccione el icono de edición situado a la derecha de las sesiones permitidas por defecto por usuario y proyecto y cambie el valor por el 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 siguientes relacionados con el certificado:

```
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.

.....

Los VDI están atascados en estado de aprovisionamiento

Si el lanzamiento 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 Amazon Machine Image (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. Es posible que los identificadores de AMI AWS extraídos del 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 instancia de Amazon EC2. 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.

.....

Los VDI entran en 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, elimine los del usuario 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.

.....

La sesión de VDI pasa a una pantalla en blanco después de iniciar sesión

Cuando una sesión de VDI con el tipo de sesión de consola está en blanco y no responde después de iniciar sesión, significa que el servidor X no funciona. Es probable que esto se deba a un problema del sistema operativo en el que DCV intenta transmitir al escritorio, pero no hay ninguno

para transmitir. La causa más probable de esto es un problema con la configuración de Xorg. Se puede ejecutar el siguiente comando para depender menos de la configuración predeterminada de Xorg.

Linux basado en Debian:

```
dpkg-divert --package nice-xdcv --divert /usr/bin/Xorg.orig --rename /usr/bin/Xorg ln -
sf /usr/bin/Xdcv-console /usr/bin/Xorg
```

Linux basado en Red Hat:

```
rpm -q --whatprovides /usr/bin/Xorg && \
cp /usr/bin/Xorg /usr/bin/Xorg.orig && \
ln -sf /usr/bin/Xdcv-console /usr/bin/Xorg
```

.....

Componente de escritorio virtual

Temas

- La instancia de Amazon EC2 muestra repetidamente «Terminado» en la consola
- 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
- El proyecto no aparece en el menú desplegable al editar la pila de software para añadirla
- El registro de CloudWatch Amazon del administrador de clústeres muestra <user-home-init>«la cuenta aún no está disponible, esperando que se sincronice el usuario» (donde la cuenta es un nombre de usuario)
- Al intentar iniciar sesión en el escritorio de Windows, aparece el mensaje «Tu cuenta ha sido deshabilitada». Consulte a su administrador»
- Problemas de opciones de DHCP con external/customer la configuración de AD
- Error de Firefox MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

.....

La instancia de Amazon EC2 muestra repetidamente «Terminado» en la consola

Si una instancia de infraestructura aparece repetidamente como terminada en la consola Amazon EC2, 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 vdc-controller muestra estados de terminación repetidos en la consola Amazon EC2, 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 instancias Amazon EC2. Si el controlador vdc está circulando y aparece el siguiente error en el grupo de CloudWatch registros, puede deberse a que un secreto no se ha 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:

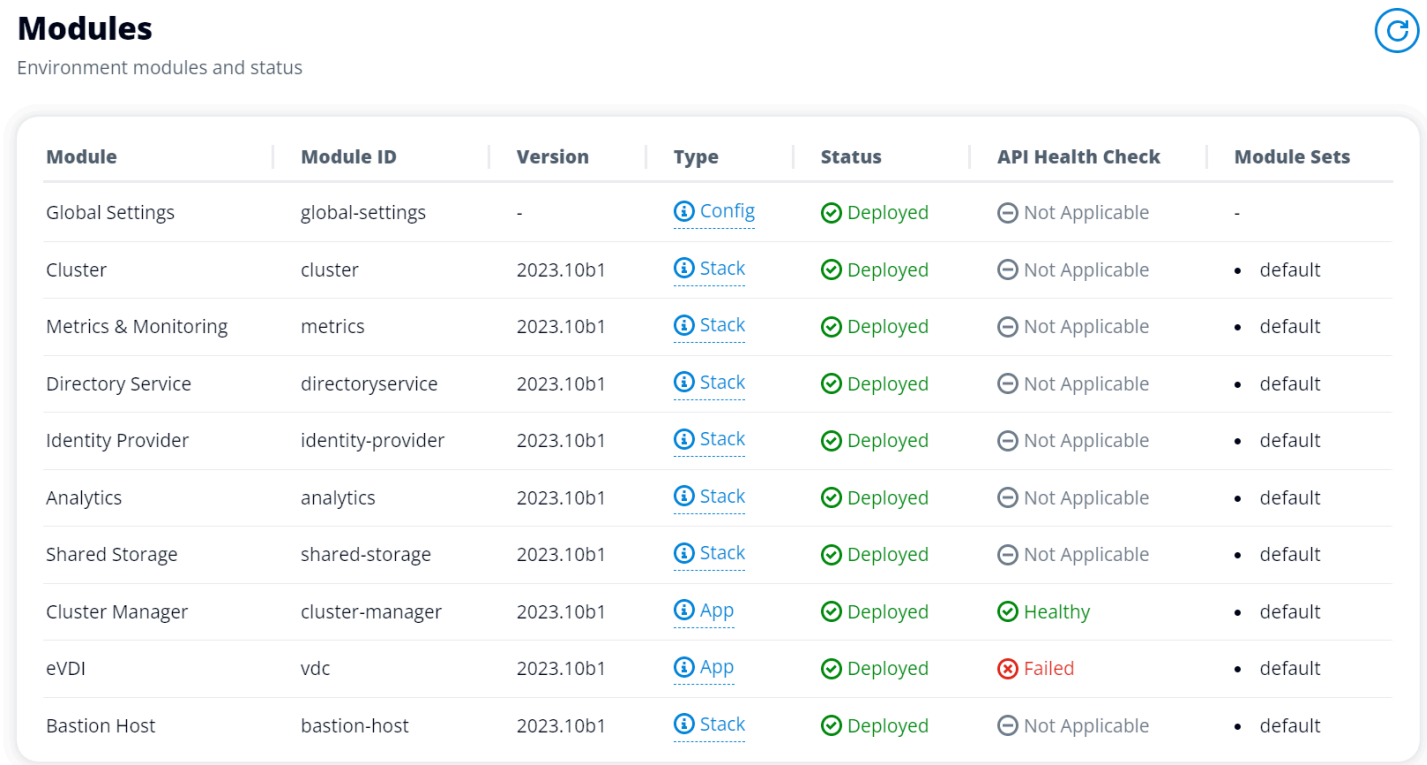
```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

Compruebe las etiquetas de la instancia Amazon EC2 y confirme 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. Busca el secreto correspondiente en el administrador de secretos y selecciona 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 elija 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 utilizarán 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, restablezca 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.

.....

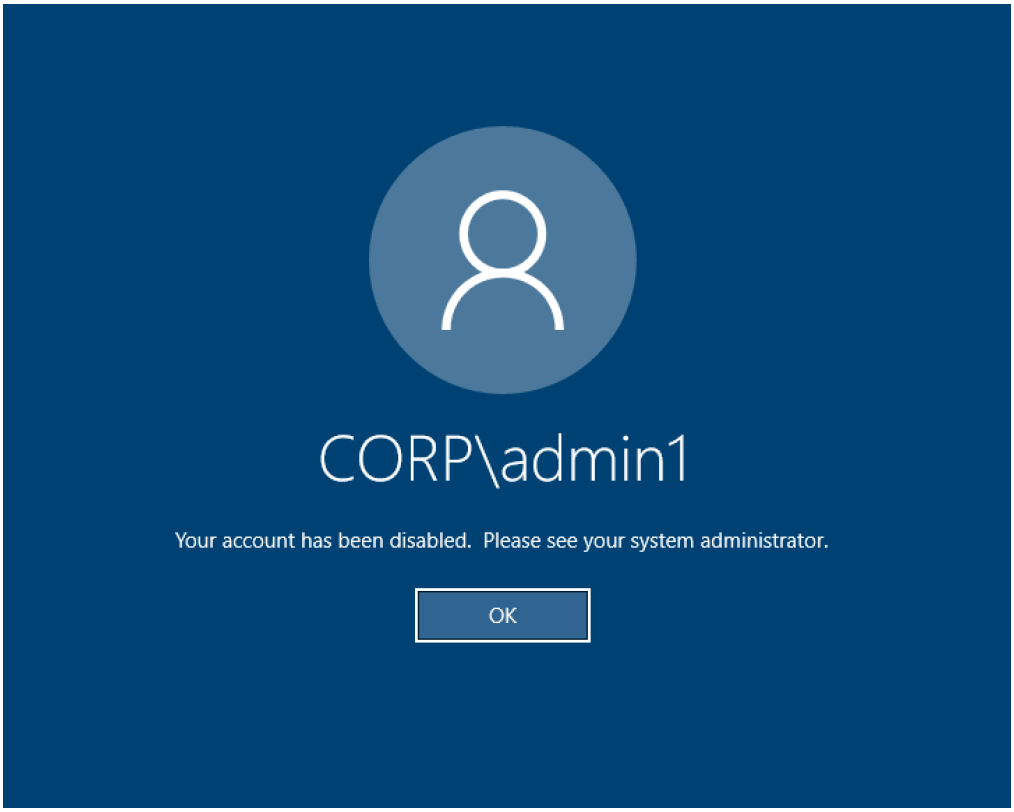
El registro de CloudWatch Amazon del administrador de clústeres muestra <user-home-init>«la cuenta aún no está disponible, esperando que se sincronice el usuario» (donde la cuenta es un nombre de usuario)

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 `ServiceAccountCredentialsSecretArn` parámetro utilizado en la creación del BI/RES entorno no fuera el valor correcto.

.....

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 registro de CloudWatch Amazon dcv-connection-gateway 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 las dos IP del controlador de dominio.
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

Puede solucionar este problema siguiendo las instrucciones que se encuentran en:. https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing

.....

Eliminación de Env

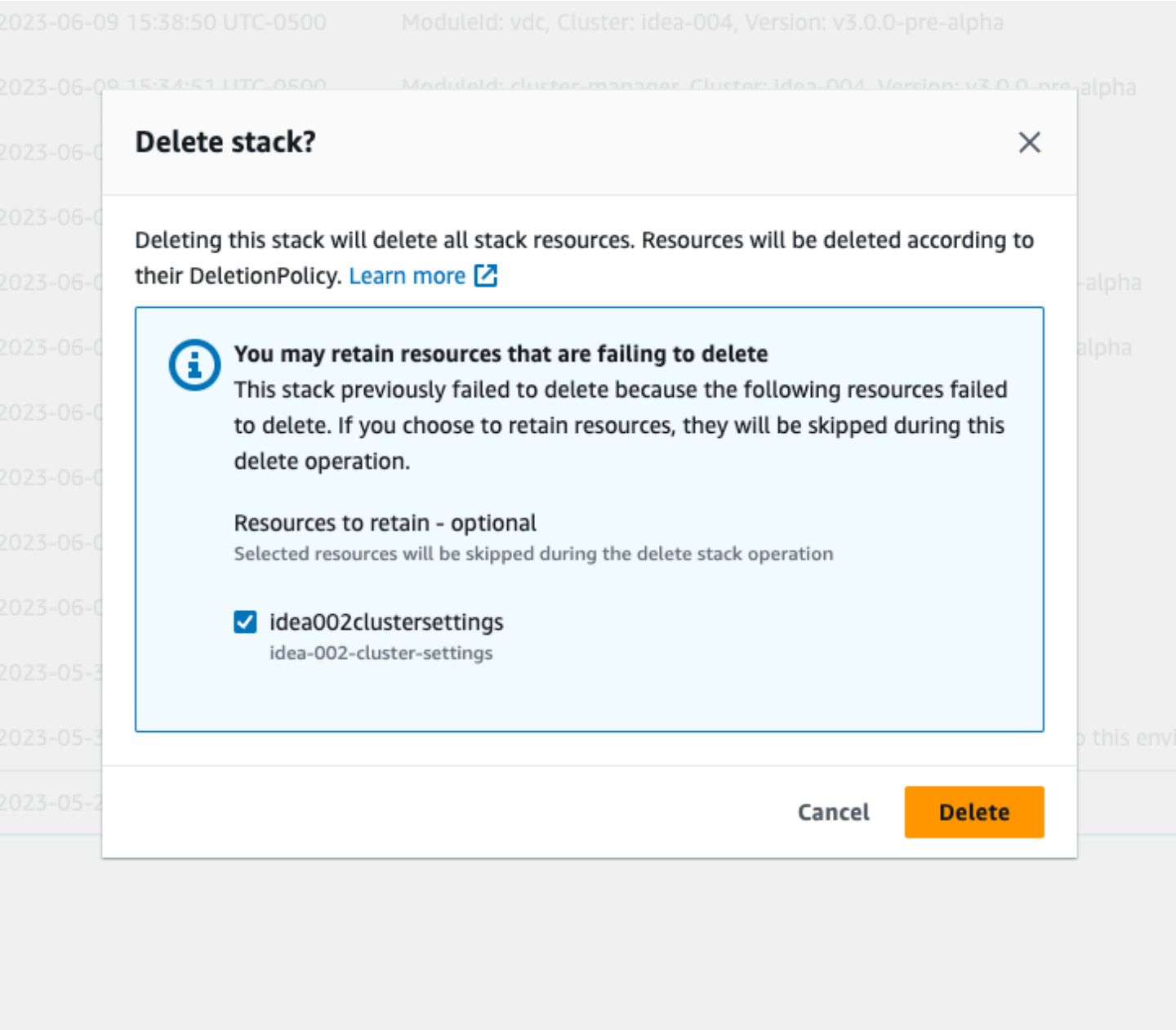
Temas

.....

La pila res-xxx-cluster tiene el estado «DELETE_FAILED» y no se puede eliminar manualmente debido al error «El rol no es válido o no se puede asumir»

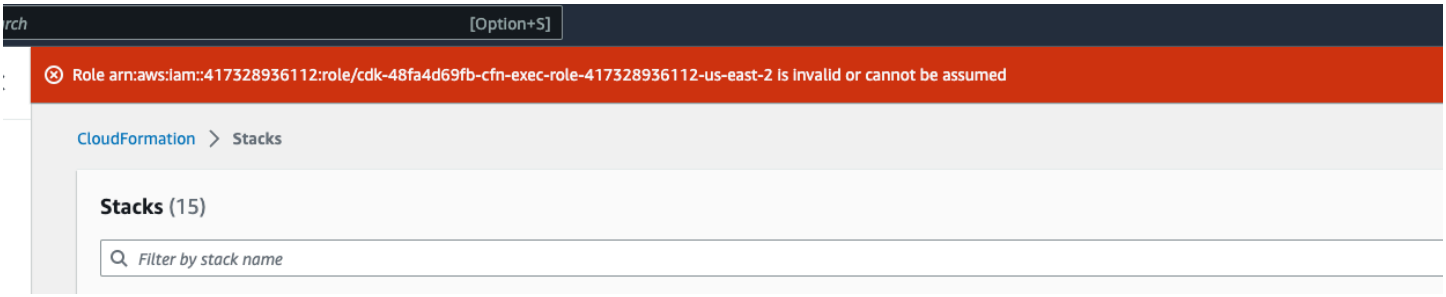
Si observa que la pila «res-xxx-cluster» tiene el estado «DELETE_FAILED» y no se puede eliminar manualmente, puede realizar los siguientes pasos para eliminarla.

Si ves la pila en el estado «DELETE_FAILED», primero intenta eliminarla manualmente. Es posible que aparezca un cuadro de diálogo confirmando la eliminación de la pila. Elija Eliminar.



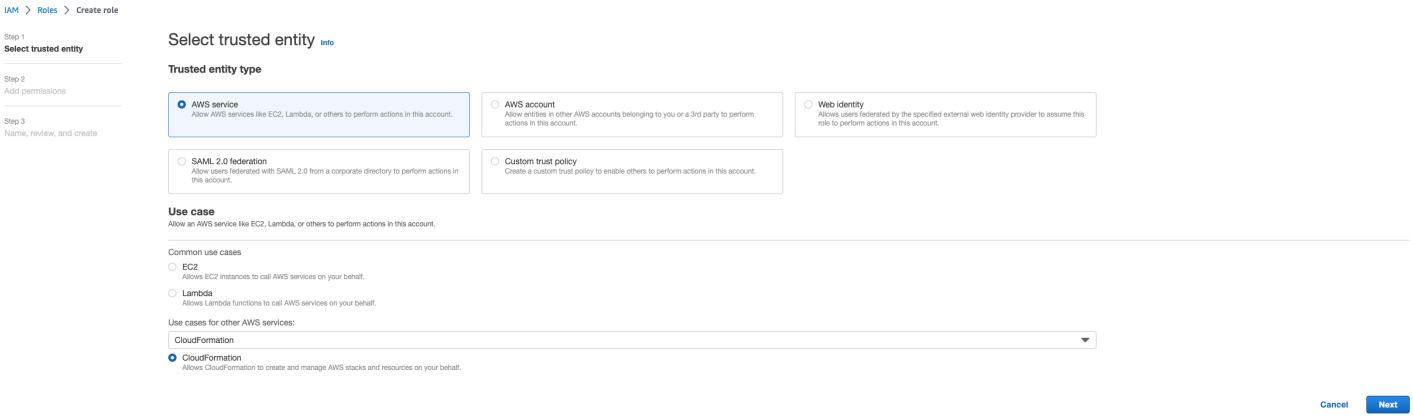
A veces, incluso si eliminas todos los recursos de la pila necesarios, es posible que sigas viendo el mensaje para seleccionar los recursos que deseas conservar. En ese caso, selecciona todos los recursos como «recursos a conservar» y selecciona Eliminar.

Es posible que veas un error parecido a `Role: arn:aws:iam::... is Invalid or cannot be assumed`

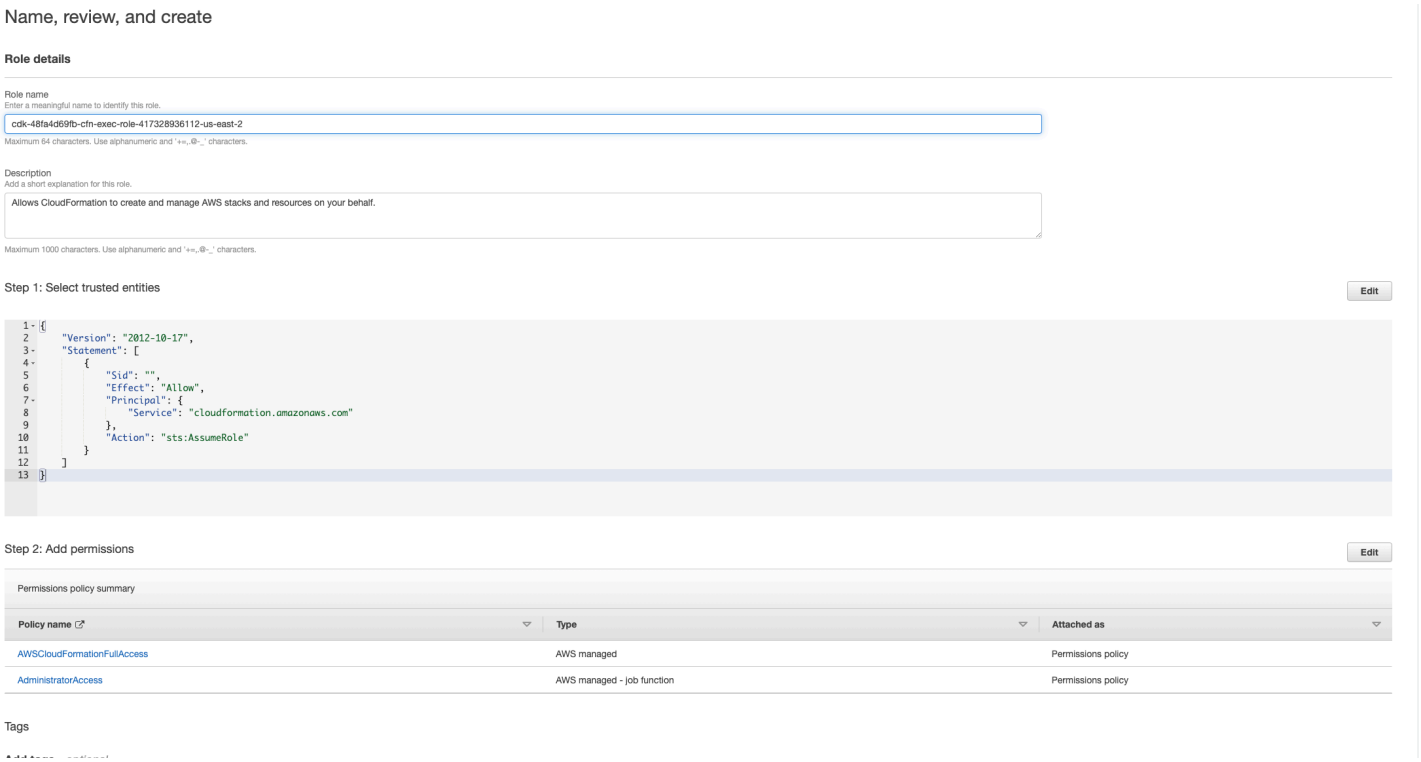


Esto significa que la función necesaria para eliminar la pila se eliminó primero antes que la pila. Para evitar esto, copia el nombre del rol. Vaya a la consola de IAM y cree un rol con ese nombre utilizando los parámetros que se muestran aquí, que son:

- En el tipo de entidad de confianza, elija AWS servicio.
- En Caso de uso, `Use cases for other AWS services` seleccione`CloudFormation`.



Elija 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 instancia EC2 desde la consola EC2

- Siga estas instrucciones para iniciar sesión en su instancia EC2 de Linux.
- Siga estas instrucciones para iniciar sesión en su instancia EC2 de Windows. A continuación, abra Windows PowerShell para ejecutar cualquier comando.

Recopilación de registros del host de Infrastructure

1. Cluster-manager: Obtenga los registros para el administrador de clústeres de los siguientes lugares y adjúntelos al ticket.
   a. Todos los registros del grupo de CloudWatch registros`<env-name>/cluster-manager`.
   b. Todos los registros del `/root/bootstrap/logs` directorio de la instancia `<env-name>-cluster-manager` EC2. Siga las instrucciones que aparecen al principio de esta sección en

la sección «Iniciar sesión en una instancia EC2 desde la consola EC2» para iniciar sesión en la instancia.

2. Vdc-controller: Obtenga los registros del controlador 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 instancia `<env-name>-vdc-controller` EC2. Siga las instrucciones que aparecen al principio de esta sección en la sección «Iniciar sesión en una instancia EC2 desde la consola EC2» para iniciar sesión en la instancia.

Una de las maneras de obtener los registros fácilmente es seguir las instrucciones de la sección. Descarga de registros de instancias EC2 de Linux El nombre del módulo sería el nombre de la instancia.

Recopilación de registros de VDI

Identifique la instancia de Amazon EC2 correspondiente

Si un usuario lanzó una VDI con un nombre de sesión`VDI1`, sería el nombre correspondiente de la instancia en la consola Amazon EC2. `<env-name>-VDI1-<user name>`

Recopile los registros de VDI de Linux

Inicie sesión en la instancia de Amazon EC2 correspondiente desde la consola de Amazon EC2 siguiendo las instrucciones que aparecen en «Iniciar sesión en una instancia EC2 desde la consola EC2» al principio de esta sección. Obtenga todos los registros de los `/var/log/dcv/` directorios `/root/bootstrap/logs` y de la instancia Amazon EC2 de VDI.

Una de las formas de obtener los registros sería subirlos a s3 y, a continuación, 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

Inicie sesión en la instancia de Amazon EC2 correspondiente desde la consola de Amazon EC2 siguiendo las instrucciones que aparecen en «Iniciar sesión en una instancia EC2 desde la consola EC2» al principio de esta sección. Obtenga todos los registros del `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\` directorio de la instancia EC2 de VDI.

Una de las formas de obtener los registros sería cargarlos en 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 instancia EC2 de VDI para permitir el acceso a S3.
2. Vaya a la consola EC2 y seleccione su instancia de VDI.
3. Seleccione el rol de IAM que está utilizando.
4. En la sección Políticas de permisos del menú desplegable Añadir permisos, elija Adjuntar políticas y, a continuación, seleccione la AmazonS3FullAccesspolítica.
5. Selecciona 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 EC2 de Linuxpara Linux.
   b. Descarga de registros de instancias EC2 de Windowspara Windows.
7. Por último, edite el rol para eliminar la `AmazonS3FullAccess` política.

> **Note**
>
> Todos los VDI utilizan la misma función de IAM, que es `<env-name>-vdc-host-role-<region>`

.....

Descarga de registros de instancias EC2 de Linux

Inicie sesión en la instancia EC2 desde la que desee descargar los registros y ejecute 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.

.....

Descarga de registros de instancias EC2 de Windows

Inicie sesión en la instancia EC2 desde la que desea 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.

.....

Fallo al eliminar la interfaz de red

Si observa un error de `detachvpcfromlambdacustomresource` eliminación en la sección Eventos de la eliminación de la pila de finalizadores de RES, lo más probable es que el servicio Lambda no haya eliminado o no haya eliminado a tiempo las interfaces de red conectadas a RES Lambdas.

Puede eliminar manualmente estas interfaces de red obsoletas accediendo a la página Interfaces de red de la consola Amazon EC2 y filtrándolas según las descripciones que contengan. `AWS Lambda VPC ENI-`*`{RES-Environment-Name}`* Debería haber hasta 14 interfaces de red, aunque podrían ser menos en función del número que Lambda haya podido eliminar correctamente. Elimine manualmente estas interfaces de red y, a continuación, reinicie la eliminación de la pila RES.

Entorno de demostración

Temas

- Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad
- El keycloak de la pila de demostración no funciona

.....

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 del usuario y de la 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 consola EC2 y finalice la instancia del administrador de clústeres. Las reglas de Auto Scaling activarán automáticamente el despliegue de una nueva instancia.

.....

El keycloak de la pila de demostración no funciona

Problema

Si tu servidor de keycloak se bloqueó y, al reiniciarlo, la IP de la instancia cambió, es posible que Keycloak se rompa: la página de inicio de sesión de tu portal de RES no se carga o queda atascada en un estado de carga que nunca se resuelve.

Mitigación

Tendrá que eliminar la infraestructura existente y volver a implementar la pila de Keycloak para restaurar Keycloak a un estado correcto. Siga estos pasos:

1. Ve a Cloudformation. Ahí deberías ver dos pilas relacionadas con Keycloak:

- *<env-name>*-RESSsoKeycloak-*<random characters>*(Pila 1)

  <env-name>-RESSsoKeycloak-*<random characters>*-RESSsoKeycloak-*(Pila 2)

2. Eliminar Stack1. Si se le solicita que elimine la pila anidada, seleccione Sí para eliminar la pila anidada.

   Asegúrese de que la pila se haya eliminado por completo.

3. Descarga la plantilla de pila Keycloak de RES SSO aquí.
4. Implemente esta pila manualmente con exactamente los mismos valores de parámetros que la pila eliminada. Para desplegarla desde la CloudFormation consola, vaya a Crear pila → Con nuevos recursos (estándar) → Elija una plantilla existente → Cargue un archivo de plantilla. Rellene los parámetros necesarios utilizando las mismas entradas que en la pila eliminada. Puedes encontrar estas entradas en la pila eliminada cambiando el filtro de la CloudFormation consola y accediendo a la pestaña Parámetros. Asegúrese de que el nombre del entorno, el key pair y otros parámetros coincidan con los parámetros de la pila original.
5. Una vez implementada la pila, el entorno estará listo para volver a usarse. Puede encontrarlos ApplicationUrl en la pestaña Resultados de la pila implementada.

.....

Problemas con Active Directory

Temas

- Mi VDI está atascada en el estado de aprovisionamiento durante mucho tiempo o no puedo iniciar sesión en mi VDI como usuario de AD una vez que la VDI está lista
- No puedo iniciar sesión en el portal web de RES después de configurar el SSO
- El usuario de AD no puede acceder al directorio principal mediante el explorador de archivos incluso después de iniciar correctamente los VDI de Linux
- El usuario administrador de AD no puede acceder al host Bastion después de habilitar el acceso SSH
- Vea y administre mi Active Directory implementado por la pila de recursos externos de RES

Mi VDI está atascada en el estado de aprovisionamiento durante mucho tiempo o no puedo iniciar sesión en mi VDI como usuario de AD una vez que la VDI está lista

Compruebe primero los registros de instalación y configuración de la VDI (`/root/bootstrap/logs/`y los `/opt/idea/app/logs/` directorios de Linux o `C:\Users\Administrator\RES\Bootstrap\Log\` los `C:\Program Files\RES\app\logs\` directorios de Windows) para ver si hay algún error de instalación o configuración.

Si encuentra un mensaje de error que indica que la instancia no se ha podido unir a Active Directory, normalmente se debe a que el administrador de clústeres no puede preestablecer la cuenta de equipo de la instancia en su AD. Comprueba los registros del administrador de clústeres en el grupo de *`/environment-name`*`/cluster-manager` CloudWatch registros y filtra los mensajes de error que contengan`[preset-computer]`. Entre los problemas más frecuentes se incluyen:

- Las credenciales de la cuenta de servicio de AD no son válidas.
  - Compruebe el secreto de la cuenta de servicio que proporcionó a RES. Asegúrese de que el nombre de usuario y la contraseña se proporcionan como un par clave-valor {*`username`*`:`*`password`*} y de que las credenciales son válidas. Tendrá que cerrar la instancia de Cluster Manager cerrando la instancia existente y permitiendo que el grupo de escalado automático lance una nueva automáticamente después de cambiar el secreto de la cuenta de servicio. A continuación, lance nuevos VDI para aplicar el cambio.
- La cuenta de servicio no tiene permiso para crear cuentas de ordenador en AD.
  - Asegúrese de que su cuenta de servicio tenga todos los permisos necesarios que se indican enConfigurar una cuenta de servicio para Microsoft Active Directory. Deberá lanzar nuevos VDI después de corregir los permisos de la cuenta de servicio en AD.
- No se puede conectar al servidor LDAP.
  - Asegúrese de que la configuración de AD permita la LDAP/LDAPS conexión dentro de la VPC y de que la opción DHCP de la VPC esté configurada correctamente después de Crear o cambiar un conjunto de opciones de DHCP para AWS Microsoft AD administrado si utiliza AD administrado. AWS
  - Para la conexión LDAPS, el `DomainTLSCertificateSecretArn` parámetro es obligatorio y debes proporcionar un certificado de CA válido para proteger la conexión. Tendrá que cerrar la instancia de Cluster Manager cerrando la instancia existente y permitiendo que el grupo de autoescalado lance una nueva automáticamente después de cambiar el secreto del certificado TLS. A continuación, lance nuevos VDI para aplicar el cambio.

- Para probar la conexión entre RES y su AD, ejecute el siguiente comando ldapsearch en la instancia de Cluster Manager (sustituya la unidad organizativa del usuario, el URI de la conexión LDAP y el nombre de usuario y la contraseña de la cuenta de servicio). Este comando debería mostrar todos los usuarios de la unidad organizativa proporcionada si el AD está configurado correctamente para permitir la conexión.

```
ldapsearch -x -b "OU=Users,OU=RES,OU=CORP,DC=corp,DC=res,DC=com" -D
 "ServiceAccount@corp.res.com" -H ldap://corp.res.com -w service-account-password
 "(objectClass=group)"
```

Si configuró DisableAdJoin en `true` al instalar RES, sus VDI de Linux solo se conectarán a Active Directory en lugar de unirse a él a través del servicio SSSD. Conéctese a su instancia de VDI desde la consola EC2 y ejecute el comando `id` *`username`* en ella. Si el comando no puede devolver el UID o el GID del usuario de AD correspondiente, compruebe el estado del servicio SSSD mediante el comando `sudo systemctl status sssd` de la instancia de VDI y los registros del servicio SSSD del directorio. `/var/log/sssd/`

Si necesita personalizar las configuraciones de SSSD para conectarse a su AD, puede editar el archivo de configuración de SSSD (`/etc/sssd/sssd.conf`) manualmente y reiniciar el servicio SSSD mediante el comando `sudo systemctl restart sssd` en el host infra/VDI (versión 2024.12.01 y versiones anteriores), o proporcionar configuraciones de SSSD adicionales desde el portal web de RES, Sincronización de Active Directory que se aplicarán automáticamente a sus VDI existentes o nuevos (versión 2025.03 y posteriores).

.....

No puedo iniciar sesión en el portal web de RES después de configurar el SSO

Compruebe las tablas *`environment-name`*`.accounts.users` y *`environment-name`*`.accounts.groups` DynamoDB para comprobar si los usuarios y los grupos están sincronizados desde Active Directory. Si las tablas están vacías o faltan los usuarios con los que está iniciando sesión, compruebe los registros de sincronización de AD en el grupo de registros (anteriores a la `/`*`environment-name`*`/cluster-manager` CloudWatch versión 2024.12) o en el grupo de `/`*`environment-name`*`/ad-sync` CloudWatch registros (versión 2024.12 y posteriores).

Además de los problemas comunes de configuración de AD que se mencionan en la sección Mi VDI está atascada en el estado de aprovisionamiento durante mucho tiempo o no puedo iniciar sesión en mi VDI como usuario de AD una vez que la VDI está lista, otros errores pueden incluir los siguientes:

- La cuenta de servicio no tiene permiso para consultar usuarios y grupos en AD.
  - Asegúrese de que su cuenta de servicio tenga todos los permisos necesarios que se indican enConfigurar una cuenta de servicio para Microsoft Active Directory.
- A los usuarios o grupos de Active Directory les faltan los atributos necesarios, como la dirección de correo electrónico.
  - Actualice los atributos de usuario o grupo en consecuencia para solucionar el problema.

Tras solucionar el problema de sincronización de AD, puedes esperar a la siguiente sincronización programada de AD, que se realiza cada hora, o activarla manualmente siguiendo las instrucciones de las versiones 2024.12 y 2024.12.01 o Cómo iniciar o detener la sincronización manualmente (versión 2025.03 y versiones posteriores) 2025.03 y posteriores. Cómo ejecutar la sincronización manualmente (versiones 2024.12 y 2024.12.01)

.....

El usuario de AD no puede acceder al directorio principal mediante el explorador de archivos incluso después de iniciar correctamente los VDI de Linux

Compruebe si el administrador de clústeres puede ver al usuario de AD ejecutando el comando `id` *`username`* en la instancia del administrador de clústeres. Si el comando no puede devolver el UID o el GID del usuario de AD correspondiente, compruebe los registros del administrador de clústeres incluidos en el `/`*`environment-name`*`/cluster-manager` CloudWatch grupo de registros y busque cualquier error relacionado con el inicio del servicio SSSD. Si no hay ningún error en los registros del administrador de clústeres, comprueba el estado del servicio SSSD mediante el comando `sudo systemctl status sssd` de la instancia del administrador de clústeres, así como los registros del servicio SSSD del directorio. `/var/log/sssd/`

Si el administrador de clústeres puede ver al usuario de AD, ejecute el comando para comprobar el UID/GID en el directorio principal del usuario (`/home/`*`username`*). `ls -n /home` Compara el UID/GID del directorio principal del usuario con el UID/ GID devuelto por el comando. `id` *`username`* Si el UID/GID no coincide, significa que el directorio principal del usuario puede crearse fuera de RES o a partir de una implementación anterior de RES. Haga una copia de seguridad de todos los datos importantes del usuario, elimine el directorio principal e inicie una nueva VDI de Linux con el usuario. El directorio principal se volverá a crear con el UID/GID adecuado una vez que la nueva VDI se haya aprovisionado correctamente.

.....

El usuario administrador de AD no puede acceder al host Bastion después de habilitar el acceso SSH

Compruebe si el usuario de AD está visible para el host de Bastion ejecutando el comando `id` *`username`* en la instancia de host de Bastion. Si el comando no puede devolver el UID o el GID del usuario de AD correspondiente, compruebe los registros de Bastion Host en el grupo de registros y busque cualquier error relacionado con el `/`*`environment-name`*`/bastion-host` CloudWatch inicio del servicio SSSD. Si no hay ningún error en los registros de Bastion Host, comprueba el estado del servicio SSSD con el comando `sudo systemctl status sssd` de la instancia de Bastion Host y de los registros del servicio SSSD del directorio. `/var/log/sssd/`

.....

Vea y administre mi Active Directory implementado por la pila de recursos externos de RES

Si su Active Directory AWS administrado se implementa mediante una pila de recursos externos de RES, debería haber una instancia con un nombre que comience por «`AdDomainWindowsNode-`*`external-resource-stack-name`*`-WindowsManagementHost`desplegada» en su AWS cuenta que pueda usarse para acceder a Active Directory y administrarlo. Puede iniciar sesión en la instancia mediante Fleet Manager en la consola de EC2 con las siguientes credenciales:

- nombre de usuario: Admin
- contraseña: AdminPassword parámetro proporcionado al implementar la pila de recursos externos

Para gestionar el Active Directory AWS gestionado, consulte Gestionar usuarios y grupos con una instancia de Amazon EC2 en la AWS Guía de administración de Directory Service.

.....

Problemas conocidos

- Problemas conocidos de la versión 2024.x
  - (2024.12 y 2024.12.01) Error de expresión regular al registrar un nuevo usuario de Cognito
  - (2024.12.01 y versiones anteriores) Error de certificado incorrecto no válido al conectarse a VDI mediante un dominio personalizado

- (2024.12 y 2024.12.01) Los usuarios de Active Directory no pueden usar SSH a Bastion Host
- (2024.10) Se interrumpe el autostop de VDI para entornos RES implementados en VPC aisladas
- (2024.10 y versiones anteriores) No se pudo iniciar VDI para los tipos de instancias mejoradas con gráficos
- (2024.08) Preparación del fallo de la AMI de la infraestructura
- (2024.08) Los escritorios virtuales no pueden montar el bucket de read/write Amazon S3 con el ARN del bucket raíz y un prefijo personalizado
- (2024.06) Se produce un error al aplicar la instantánea cuando el nombre del grupo de AD contiene espacios
- (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, regresión y vulnerabilidad de seguridad en los VDI de Ubuntu y RHEL9
- (2024.04-2024.04.02) Proporcionó un límite de permiso de IAM no 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
- (02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo SAMAccountName atributo 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

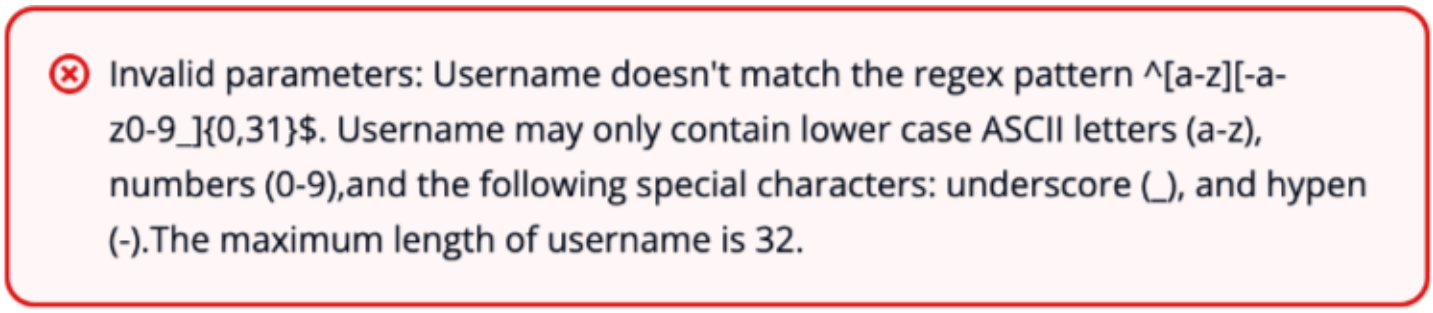
Problemas conocidos de la versión 2024.x

.....

(2024.12 y 2024.12.01) Error de expresión regular al registrar un nuevo usuario de Cognito

Descripción del error

Si intenta registrar usuarios de AWS Cognito a través del portal web que tengan prefijos de correo electrónico que contengan» . «, por ejemplo`<firstname>.<lastname>@<company>.com`, esto provocará un error que indique que el nombre de usuario de Cognito no coincide con el patrón de expresiones regulares definido.



Este error se debe a que RES genera automáticamente nombres de usuario a partir del prefijo de correo electrónico del usuario. Sin embargo, los nombres de usuario con «.» no son usuarios válidos para los VDI en determinadas distribuciones de Linux compatibles con RES. Esta corrección elimina cualquier «.» del prefijo del correo electrónico al generar un nombre de usuario, de modo que el nombre de usuario sea válido en los VDI de RES Linux.

Versiones afectadas

Versiones RES 2024.12 y 2024.12.01

Mitigación

1. Ejecute los siguientes comandos para descargar `patch.py` y `cognito_sign_up_email_fix.patch` para las versiones 2024.12 o 2024.12.01 y `<output-directory>` sustitúyalos `cognito_sign_up_email_fix.patch` por el directorio en el que desee descargar el script y el archivo del parche, así como por el nombre de su entorno RES: `<environment-name>`

   a. El parche se aplica a los RES 2024.12 y 2024.12.01.

   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>
RES_VERSION=<res-version> # either 2024.12 or 2024.12.01
```

```
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/cognito_sign_up_email_fix.patch --output
 ${OUTPUT_DIRECTORY}/cognito_sign_up_email_fix.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando de parche:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --
res-version ${RES_VERSION} --module cluster-manager --patch ${OUTPUT_DIRECTORY}/
cognito_sign_up_email_fix.patch
```

3. Reinicie la instancia de Cluster Manager para su entorno. También puede cancelar la instancia desde la consola de administración de Amazon EC2.

```
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}
```

4. Verifique el estado de la instancia de Cluster Manager comprobando la actividad del grupo de autoescalado empezando por el nombre`<RES-EnvironmentName>-cluster-manager-asg`. Espere hasta que la nueva instancia se lance correctamente.

.....

(2024.12.01 y versiones anteriores) Error de certificado incorrecto no válido al conectarse a VDI mediante un dominio personalizado

Descripción del error

Al implementar la receta de recursos externos y RES con un nombre de dominio de portal personalizado, CertificateRenewalNode no se actualiza el certificado TLS para la conexión VDI y aparece el siguiente error: `/var/log/user-data.log`

```
{
  "type": "urn:ietf:params:acme:error:unauthorized",
  "detail": "Error finalizing order :: OCSP must-staple extension is no longer
 available: see https://letsencrypt.org/2024/12/05/ending-ocsp",
  "status": 403
}
```

Como resultado, aparecerá un error que indica `net::ERR_CERT_DATE_INVALID` (Chrome) o `Error code: SSL_ERROR_BAD_CERT_DOMAIN` (FireFox) cuando se conecte a sus VDI en el portal web de RES.

Versiones afectadas

2024.12.01 y versiones anteriores

Mitigación

1. Navegue hasta la consola EC2. Si hay una instancia con nombre`CertificateRenewalNode-`, finalice la instancia.
2. Vaya a la consola Lambda. Abra el código fuente de la función Lambda denominada. `-CertificateRenewalLambda-` Identifique la línea que comienza con el argumento `./acme.sh --issue --dns dns_aws --ocsp-must-staple --keylength 4096` y elimínelo. `--ocsp-must-staple`
3. Seleccione Implementar y espere a que el cambio de código surta efecto.
4. Para activar manualmente la función Lambda: vaya a la pestaña Prueba y, a continuación, seleccione Probar. No se requiere ninguna entrada adicional. Esto debería crear una instancia EC2 de certificado que actualice el certificado y PrivateKey los secretos en Secret Manager. La instancia finalizará automáticamente una vez que se actualicen los secretos.
5. Finalice la instancia dcv-gateway existente `<env-name>-vdc-gateway` y espere a que el grupo de autoescalado implemente automáticamente una nueva.

Detalles del error

Let's Encrypt finalizará el soporte de OCSP en 2025. A partir del 30 de enero de 2025, Must-Staple las solicitudes de OCSP fallarán a menos que la cuenta solicitante haya emitido previamente un certificado que contenga la extensión OCSP Must Staple. Consulte https://letsencrypt.org/2024/12/05/ending-ocsp/para obtener más información.

.....

(2024.12 y 2024.12.01) Los usuarios de Active Directory no pueden usar SSH a Bastion Host

Descripción del error

Los usuarios de Active Directory reciben un error de permiso denegado cuando se conectan al Bastion Host siguiendo las instrucciones del portal web de RES.

La aplicación Python que se ejecuta en el host Bastion no puede iniciar el servicio SSSD debido a la falta de una variable de entorno. Como resultado, el sistema operativo desconoce a los usuarios de AD y no pueden iniciar sesión.

Versiones afectadas

2024.12 y 2024.12.01

Mitigación

1. Conéctese a la instancia de Bastion Host desde la consola EC2.
2. Edite `/etc/environment` y añada `environment_name=<res-environment-name>` como una nueva línea en IDEA_CLUSTER_NAME.
3. Ejecuta los siguientes comandos en la instancia:

```
source /etc/environment
sudo service supervisord restart
sudo systemctl restart supervisord
```

4. Intente volver a conectarse al Bastion Host siguiendo las instrucciones del portal web de RES.

.....

(2024.10) Se interrumpe el autostop de VDI para entornos RES implementados en VPC aisladas

Descripción del error

Con la versión 2024.10 RES, se agregó la parada automática de VDI para los VDI que están inactivos durante un período de tiempo determinado. Este ajuste se puede configurar en Configuración del escritorio → Servidor → Sesión.

Actualmente, la parada automática de VDI no es compatible con los entornos RES implementados en VPC aisladas.

Versiones afectadas

2024.10

Mitigación

Actualmente estamos trabajando en una solución que se incluirá en una futura versión. Sin embargo, aún es posible detener manualmente los VDI en entornos RES implementados en VPC aisladas.

.....

(2024.10 y versiones anteriores) No se pudo iniciar VDI para los tipos de instancias mejoradas con gráficos

Descripción del error

Cuando se lanza una VDI de Amazon Linux 2 - x86_64, RHEL 8 - x86_64 o RHEL 9 x86_64 en un tipo de instancia con gráficos mejorados (g4, g5), la instancia se atascará en el estado de aprovisionamiento. Esto significa que la instancia nunca pasará al estado «Preparada» y estará disponible para la conexión.

Esto se debe a que el servidor X no crea instancias correctamente en las instancias. Después de aplicar este parche, también le sugerimos que aumente el tamaño del volumen raíz de las pilas de software para las instancias gráficas a 50 GB a fin de garantizar que haya espacio suficiente para instalar todas las dependencias.

Versiones afectadas

Todas las versiones 2024.10 o anteriores de RES.

Mitigación

1. Descargue patch.py y graphic_enhanced_instance_types_fix.patch `<output-directory>` sustituyéndolas por el directorio en el que desee descargar el script y el archivo del parche y por el nombre de su entorno RES en el siguiente comando: `<environment-name>`

   a. El parche solo se aplica a la RES 2024.10.

   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/2024.10/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.10/patch_scripts/patches/graphic_enhanced_instance_types_fix.patch --
output ${OUTPUT_DIRECTORY}/graphic_enhanced_instance_types_fix.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando de parche:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.10 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
graphic_enhanced_instance_types_fix.patch
```

3. Para finalizar la instancia de Virtual Desktop Controller (vdc-controller) de su entorno, ejecute los siguientes comandos y sustituya el nombre del entorno RES donde se muestra.

```
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}
```

4. Lanza una nueva instancia cuando el grupo objetivo que comienza con el nombre `<RES-EnvironmentName>-vdc-ext` pase a estar en buen estado. Recomendamos que cualquier pila de software nueva que registre para las instancias de gráficos tenga al menos 50 GB de almacenamiento.

.....

(2024.08) Preparación del fallo de la AMI de la infraestructura

Descripción del error

Al preparar las AMI con EC2 Image Builder de acuerdo con las instrucciones que se indican en la documentación de requisitos previos, el proceso de creación falla y muestra el siguiente mensaje de error:

```
CmdExecution: [ERROR] Command execution has resulted in an error
```

Esto se debe a errores en el archivo de dependencias que se proporciona en la documentación.

Versiones afectadas

2024.08

Mitigación

Cree nuevos recursos de EC2 Image Builder:

(Siga estos pasos si nunca ha preparado AMI para instancias RES)

1. Descargue el archivo res-installation-scripts.tar.gz actualizado.
2. Siga los pasos que se indican en Preparar imágenes de máquinas de Amazon (AMI) en la página de requisitos previos.

Reutilización de recursos anteriores de EC2 Image Builder:

(Siga estos pasos si ha preparado AMI para instancias RES)

1. Descargue el archivo res-installation-scripts.tar.gz actualizado.
2. Vaya a EC2 Image Builder → Componentes → Haga clic en el componente creado para preparar las AMI RES.
3. Anote la ubicación del S3 que aparece en Contenido → DownloadRESInstallScripts paso → entradas → fuente.
4. La ubicación S3 que se encuentra arriba contiene el archivo de dependencias que se utilizó anteriormente. Sustituya este archivo por el archivo descargado en el primer paso.

.....

(2024.08) Los escritorios virtuales no pueden montar el bucket de read/write Amazon S3 con el ARN del bucket raíz y un prefijo personalizado

Descripción del error

Research and Engineering Studio 2024.08 no puede montar los buckets read/write S3 en una instancia de infraestructura de escritorio virtual (VDI) cuando utiliza un ARN de bucket raíz (es decir,`arn:aws:s3:::example-bucket`) y un prefijo personalizado (nombre del proyecto o nombre del proyecto y nombre de usuario).

Entre las configuraciones de bucket que no se ven afectadas por este problema se incluyen las siguientes:

- cubos de solo lectura
- read/write buckets con un prefijo como parte del ARN del bucket (es decir,`arn:aws:s3:::example-bucket/example-folder-prefix`) y un prefijo personalizado (nombre del proyecto o nombre del proyecto y nombre de usuario)
- read/write buckets con un ARN de bucket raíz, pero sin prefijos personalizados

Tras aprovisionar una instancia de VDI, el directorio de montaje especificado para ese bucket de S3 no tendrá el bucket montado. Aunque el directorio de montaje de la VDI estará presente, estará vacío y no contendrá el contenido actual del bucket. Al escribir un archivo en el directorio mediante la terminal, se `Permission denied, unable to write a file` generará el error y el contenido del archivo no se cargará en el depósito de S3 correspondiente.

Versiones afectadas

2024.08

Mitigación

1. Para descargar el script de parche y el archivo de parche (`patch.pyys3_mount_custom_prefix_fix.patch`), ejecute el siguiente comando y `<output-directory>` sustitúyalo por el directorio en el que desea descargar el script y el archivo de parche y `<environment-name>` por el nombre de su entorno RES:

   a. El parche solo se aplica a la RES 2024.08.

   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 en las que se implementa RES y asegúrese de tener permisos de Amazon 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/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
 ${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando de parche:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. Para finalizar la instancia de Virtual Desktop Controller (vdc-controller) de su entorno, ejecute los siguientes comandos. (Ya configuró la `ENVIRONMENT_NAME` variable con el nombre de su entorno RES en el primer paso).

```
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}
```

> **Note**
>
> Para las configuraciones de VPC privadas, si aún no lo ha hecho, para la <RES-EnvironmentName>-vdc-custom-credential-broker-lambda función asegúrese de añadir el nombre `AWS_STS_REGIONAL_ENDPOINTS` y el `Environment`

`variable` valor de. `regional` Para obtener más información, consulte Requisitos previos del bucket de Amazon S3 para implementaciones de VPC aisladas.

4. Una vez que el grupo objetivo que comienza con el nombre *<RES-EnvironmentName>*`-vdc-ext` pase a estar en buen estado, será necesario lanzar nuevos VDI que tengan los buckets read/write S3 con el ARN del bucket raíz y el prefijo personalizado montados correctamente.

.....

(2024.06) Se produce un error al aplicar la instantánea 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 en el que 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 la consola de administración de Amazon EC2.

```
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 en minúsculas y mayúsculas, dígitos, guiones (-), puntos (.), guiones bajos (_) y espacios con una longitud total entre 1 y 30, ambos inclusive.

.....

(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

Todas las versiones de RES 2024.06 o anteriores

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, regresión y vulnerabilidad de seguridad en los VDI de Ubuntu y RHEL9

Descripción del error

CVE-2024-6387, denominada RegresHion, se ha 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 para las VDI (infraestructura de escritorio virtual) de RHEL9 y Ubuntu 2024 en TODAS las versiones de RES utiliza una versión OpenSSH que es vulnerable a la amenaza de seguridad.

Esto significa que los VDI RHEL9 y Ubuntu2024 existentes podrían explotarse, pero el atacante necesitaría acceder al host bastión.

Puede encontrar más información sobre el problema aquí.

Versiones afectadas

Todas las versiones 2024.06 o anteriores de RES.

Mitigación

Tanto RHEL9 como Ubuntu han publicado parches para OpenSSH que corrigen la vulnerabilidad de seguridad. Estos se pueden extraer utilizando el administrador de paquetes respectivo de la plataforma.

Si ya tiene VDI de RHEL9 o Ubuntu, le recomendamos que siga las instrucciones de PATCH EXISTING VDI que aparecen a continuación. Para aplicar parches a los VDI futuros, le

recomendamos seguir las instrucciones de los VDI de PATCH FUTURE. Estas instrucciones describen cómo ejecutar un script para aplicar la actualización de la plataforma a sus VDI.

PARCHE LOS VDI EXISTENTES

1. Ejecute el siguiente comando para aplicar parches a todos los VDI de Ubuntu y RHEL9 existentes:

   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 todos los ID de instancia tengan un mensaje de ÉXITO.

PARCHE LOS VDI FUTUROS

1. Para descargar el script y el archivo del parche (patch.py y update_openssh.patch), ejecute los siguientes comandos y `<output-directory>` sustitúyalos por el directorio en el que desee descargar los archivos y `<environment-name>` por el nombre del entorno 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 a futuros VDI solo se admite en las versiones 2024.06 y posteriores de RES. Para parchear futuros VDI 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

.....

(2024.04-2024.04.02) Proporcionó un límite de permiso de IAM no 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 IAMPermissionBoundary parámetro no se asignó correctamente a un proyecto durante su creación.

Versiones afectadas

2024.04 - 2024.04.02

Mitigación

Siga estos pasos para permitir que los VDI hereden correctamente 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 sustitúyalo 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 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:

```
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 la consola de administración de Amazon EC2.

```
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

Las Amazon Machine Images (AMI) se utilizan para activar escritorios virtuales (VDI) 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.

AMI-ID `ami-0e190f8939a996caf`para este tipo de instancia, la configuración 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 Windows-NVIDIA predeterminada (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 Windows-NVIDIA instancias

.....

(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. Ejecute 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:

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 en el que 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}
```

.....

(02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo SAMAccountName atributo 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 nombre de usuario de SAMAccount 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 anteriores

Mitigación

1. Para descargar el script y el archivo del parche (patch.py y samaccountname_regex.patch), ejecute el siguiente comando y sustitúyalo 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 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:

```
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 la consola de administración de Amazon EC2.

```
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 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-----`

.....

Política de soporte del Estudio de Investigación e Ingeniería

Research and Engineering Studio (RES) admite varias versiones al mismo tiempo. RES usa un esquema de `YYYY.mm.patch` versiones, donde `YYYY.mm` representa una versión principal. `YYYY`representa el año, `mm` representa el mes de publicación e `patch` indica una versión incremental. Cada versión de RES tiene una fecha de fin de vida útil (EOSL) programada, que es el último día del `mm` mes del año YYYY +1. Por ejemplo, la fecha de la EOSL de 2025.09 es el 30 de septiembre de 2026. A partir de la fecha de EOSL no se proporcionará más soporte ni mantenimiento para ese lanzamiento.

Las nuevas versiones principales incluyen nuevas funciones, mejoras de rendimiento, actualizaciones de seguridad y correcciones de errores (). `YYYY.mm` Para los problemas críticos, AWS proporciona correcciones mediante versiones de parches, pero solo para las versiones que no han llegado a EOSL.

In-place las actualizaciones solo se admiten entre las versiones de parches de la misma versión principal (por ejemplo, del 04.01 al 2024.04.02). Para usar las actualizaciones de una nueva versión principal de RES, debe realizar una nueva instalación de esa versión. Para asegurarse de tener acceso a las funciones y actualizaciones de seguridad más recientes, le recomendamos que mantenga la instalación de RES actualizada con la versión más reciente.

Si está ejecutando una versión que se acerca a su fecha de fin de vida útil (EOSL), planifique actualizarla a una versión más reciente para mantener el soporte y el acceso a las mejoras más recientes. Para obtener instrucciones detalladas sobre cómo actualizar RES, consulta nuestra documentación. Si tiene alguna pregunta o necesita ayuda con la actualización, póngase en contacto con AWS Support.

Versión de Research and Engineering Studio	Fecha de fin del soporte (EOSL)
2023.11.x	11/30/2024
2024.01.x	1/31/2025
2024.04.x	4/30/2025
2024.06.x	6/30/2025
2024.08.x	8/31/2025

Versión de Research and Engineering Studio	Fecha de fin del soporte (EOSL)
2024.10.x	10/31/2025
2024.12.x	12/31/2025
2025.03.x	3/30/2026
2025.06.x	6/30/2026
2025.09.x	9/30/2026

Important

Usted es responsable de aplicar los parches a los hosts de infraestructura o VDI después de la implementación.

Avisos

Cada instancia de Amazon EC2 incluye dos licencias de Servicios de Escritorio Remoto (Terminal Services) para fines de administración. Esta información está disponible para ayudarle a aprovisionar estas licencias para sus administradores. También puede usarlo AWS Systems Manager Session Manager, que permite iniciar sesión de forma remota en instancias de Amazon EC2 sin RDP y sin necesidad de licencias de RDP. Si se necesitan licencias adicionales de Remote Desktop Services, las CAL de usuario de Remote Desktop deben adquirirse en Microsoft o en un distribuidor de licencias de Microsoft. Las CAL para usuarios de escritorios remotos con Software Assurance activo tienen las ventajas de la movilidad de licencias y se pueden instalar en entornos de inquilinos (compartidos) AWS predeterminados. 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 CHANGELOG.mdarchivo del GitHub repositorio.

Date	Cambio
Marzo de 2026	• Publica la versión 2026.03 Correcciones de seguridad: • Se ha corregido una vulnerabilidad de escalamiento de privilegios en el componente FileBrowser . • Se ha corregido una vulnerabilidad de ejecución remota de código entre usuarios mediante la inyección del nombre de sesión. • Se solucionó un problema por el que se podía usar un ARN de perfil de instancia externo al crear una sesión. Mejoras • Support para varios volúmenes desde un único sistema de archivos ONTAP. • Permite a los usuarios restablecer la programación de sus sesiones a la configuración predeterminada del sistema. • Permita a los administradores reiniciar los VDI con errores desde la página de sesiones. • Permita a los administradores establecer la instancia type/family al registrar una pila de software. • Permita a los administradores configurar la hora de caducidad del token DCV a través del portal RES.

Date	Cambio
	• Permita a los administradores añadir enlaces personalizados a la página de inicio de sesión del portal web. • Se agregaron umbrales de validación de sesiones de DCV configurables para admitir entornos con tiempos de arranque más prolongados. Cambios • Migración continua de VDC-related las API del host EC2 del VDC al servidor Lambda. • Se actualizó Python a la versión 3.12 o superior en los hosts de infraestructura y VDI. • Se eliminaron AL2 y RHEL8 de las pilas de software predeterminadas. Los paquetes de software AL2 y RHEL8 existentes en los entornos implementados no se ven afectados, pero ya no se incluirán como predeterminados en los nuevos entornos. • Se ha eliminado el acceso directo RES_Interface innecesario de los escritori os VDI. Correcciones de errores • Campo de filtro de sesiones fijo. • Se corrigió el error de arranque de Ubuntu 24.04 causado por el reinicio del servicio systemd. • Se corrigió el proyecto deletion/creation cuando se implementaba con el prefijo de recurso de IAM.

Date	Cambio
	• Se ha corregido un error al montar el sistema de archivos Lustre en los VDI. RHEL9/Rocky9 • Filtro de intervalo de fechas fijo para list_sessions y list_shared_permissions.

Date	Cambio
Diciembre de 2025	• Publica la versión 2025.12 Mejoras • Propagación de CloudFormation etiquetas personalizadas a todos los componentes de RES durante la implementación. • Permita a los administradores deshabilitar la unión a Active Directory para los hosts de Windows. • Permita a los administradores establece r horarios predeterminados para las instancias de escritorio de VDI. • El registro de acceso a los buckets de S3 está habilitado para cumplir con los requisitos de conformidad y auditoría. • SSL/TLS se requiere el cifrado en todas las comunicaciones del bucket de S3. • Se habilitó la recuperación puntual para las tablas de DynamoDB gestionadas por RES. • Se actualizaron los permisos del opt/cogni to_auth directorio/para el acceso exclusivo de root. Cambios • Se migraron VDC-related las API del host EC2 del VDC a la Lambda de backend. Correcciones de errores • Actualización de los tipos de instancias permitidos al lanzar una nueva VDI. • Se corrigieron las dependencias que faltaban en efs_utils.

Date	Cambio
	• Número total de sesiones del panel de costes fijos en el portal RES. • Se solucionó el problema por el que los usuarios podían omitir manualmente los tipos de instancias permitidos. • Se solucionó una condición de carrera que podía bloquear la conexión DCV para los VDI de Linux. • Se agregaron los sistemas operativos que faltaban en el menú desplegable del sistema operativo de la página Software Stack. • Se ha corregido un problema de cierre de sesión frecuente al utilizar un dominio personalizado con Chrome. • Se solucionó el problema por el que las configuraciones de SSSD en tiempo de ejecución no se aplicaban después de deshabilitar la unión a AD. • Se corrigió un error al eliminar el entorno RES causado por el resto de la función de VDI.

Date	Cambio
Septiembre de 2025	• Publica la versión 2025.09 Mejoras • La región apoya la expansión de ap-northeast-3, ap-southeast-3, me-central-1 y sa-east-1. • Eliminación de una cuenta de ordenador del dominio AD al finalizar la VDI. • Compatibilidad con alias de parámetros de Systems Manager para los ID de AMI para simplificar la administración de imágenes específicas del proyecto. • Integración con el grupo preexistente de Amazon Cognito para una configuración de autenticación simplificada durante la implementación. • Personalización de los rangos de CIDR en la plantilla de recursos CloudFormation externos durante la implementación para mejorar la planificación de la red y la integración con los recursos existentes. • Se agregó la funcionalidad de sincronización del correo electrónico de AD después de la inicialización. • Support para instancias g6f de Amazon EC2. Cambios • Eliminar el despliegue de la infraestructura de la tarea del instalador de ECS para simplificar el proceso de instalación. Correcciones de errores

Date	Cambio
	• Se resolvieron los errores persistentes de reanudación de la instancia. • Se resolvió que los usuarios pudieran ver las sesiones de escritorio de otros usuarios. • Se resolvió el problema de exclusividad del nombre de los roles de usuario de IAM en las implementaciones de cuentas únicas en varias regiones.
Julio de 2025	• Publica la versión 2025.06.01 Mejoras • Se mejoró el tiempo de lanzamiento de los hosts de infraestructura y los VDI predeterminados mediante el uso de Python predeterminado del sistema. • Se agregó compatibilidad con Ubuntu 24.04 VDI. Cambios • Los hosts Infra y los VDI ahora usan Python predeterminado del sistema si está disponible y cumple con los requisitos de RES (versión superior a la 3.9.16). Correcciones de errores • Se resolvieron los problemas de inicio de sesión en VDI de Windows y Linux cuando disable_ad_join era true. • Se resolvió un problema por el que las políticas de IAM personalizadas no se adjuntaban a las funciones específicas del proyecto.

Date	Cambio
Junio de 2025	• Publica la versión 2025.06 Mejoras • Se agregó soporte para la región AWS GovCloud (US-East). • Se agregó compatibilidad con el tipo de instancia g6e. • Se agregó soporte para lanzar sesiones de escritorio virtual con Amazon Linux 2023. • Se agregó soporte para iniciar sesiones de escritorio virtual con Rocky Linux 9. • Se agregó soporte para la personalización de rutas y prefijos de los recursos de IAM. • Se agregó la posibilidad de eliminar un sistema de archivos montado de la interfaz de usuario de RES. • Se ha añadido la posibilidad de recuperar los registros de arranque de VDI de Amazon. CloudWatch • Se ha habilitado la hibernación para RedHat 8 y 9 VDI. RedHat Cambios • Se han reducido los permisos de IAM para los hosts de infraestructura y los hosts de VDI. • Proceso de arranque mejorado para los hosts de infraestructura y los hosts de VDI. • Se aumentó la WCU de las tablas DynamoDB del broker DCV de 20 a 100. Correcciones de errores

Date	Cambio
	• Se resolvió un problema por el que RES no podía incluir Elastic Filesystem en la lista para su incorporación. • Se resolvió un problema por el que RES no podía aplicar la instantánea debido a que Elastic Filesystem aparecía en la lista. • Se resolvió un problema por el que no se podía ajustar la resolución de la sesión de la consola DCV. • Se ha resuelto un problema por el que se podía eliminar una programación de VDI personalizada al volver a guardarla sin modificarla. • Se ha resuelto un problema que provocaba que el explorador de archivos dejara de responder cuando había un gran número de usuarios y grupos en AD. • Se resolvió un problema por el que podían faltar sesiones de VDI en la administración de sesiones. • Se ha resuelto un problema por el que podía faltar una sesión de VDI en la página Mi escritorio virtual. • Se resolvió un problema por el que el tiempo de espera de inactividad no funcionaba en los VDI con la hibernación habilitada. • Se ha resuelto un problema que provocaba que las AMI de la pila de software fueran anteriores a las versiones anteriores de RES.

Date	Cambio
Marzo de 2025	• Publica la versión 2025.03 Secciones añadidas: • Desactivar un proyecto. • Eliminación de un proyecto. • Panel de análisis de costos. Secciones modificadas — • Escritorios virtuales. • Pilas de software (AMI). • Configurar las RES-ready AMI. • Configuración de escritorio. • Configurar el acceso SSH. • Sincronización de Active Directory.
Diciembre de 2024	• Publicar la versión 2024.12 Secciones añadidas: • Sincronización de Active Directory. • Configuración de los permisos de escritorio. • Configuración del acceso al explorador de archivos. • Configurar el acceso SSH. • Configuración de los usuarios de Amazon Cognito. Secciones modificadas — • Límites del entorno. • Configurar una VPC privada (opcional).

Date	Cambio

Octubre de 2024	• Versión de lanzamiento 2024.10: Se agregó soporte para:
	  • Límites del entorno.
	  • Perfiles para compartir escritorios.
	  • Infraestructura de escritorios virtuales: parada automática.

Agosto de 2024	• Versión de lanzamiento 2024.08: Se agregó soporte para —
	  • montar buckets de Amazon S3 en instancias de infraestructura de escritorio virtual (VDI) de Linux. Consulte Buckets de Amazon S3.
	  • permisos de proyectos personalizados, un modelo de permisos mejorado que permite personalizar las funciones existentes y añadir funciones personalizadas. Consulte Política de permisos.
	• Guía del usuario: se ha ampliado la Resolución 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: RES-ready AMI y plantillas de lanzamiento de proyectos
Marzo de 2024	Temas adicionales de solución de problemas, retención de CloudWatch registros y desinstal ación de versiones secundarias

Date	Cambio
Febrero de 2024	Versión de lanzamiento 2024.01.01: plantilla de despliegue actualizada
Enero de 2024	Versión de lanzamiento 2024.01
Diciembre de 2023	GovCloud instrucciones y plantillas añadidas
Noviembre de 2023	Versión inicial

Archivo de versiones anteriores

Están disponibles las siguientes versiones archivadas de esta guía del usuario:

- Versión 2025.12 de la guía del usuario de Research and Engineering Studio
- Versión 2025.09 de la guía del usuario de Research and Engineering Studio
- Versión 2025.06 de la guía del usuario de Research and Engineering Studio
- Versión 2025.03 de la guía del usuario de Research and Engineering Studio

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.