



Guía del usuario

Estudio de investigación e ingeniería



Estudio de investigación e ingeniería: Guía del usuario

Copyright © 2024 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

Información general	1
Características y ventajas	1
Conceptos y definiciones	3
Información general de la arquitectura	5
Diagrama de arquitectura	5
AWSservicios de este producto	7
Entorno de demostración	10
Cree una pila de demostración con un solo clic	10
Requisitos previos	10
Cree recursos e introduzca parámetros	11
Pasos posteriores a la implementación	13
Planificación de la implementación	14
Costo	14
Seguridad	14
Roles de IAM	14
Grupos de seguridad	15
Cifrado de datos	15
Soportado Regiones de AWS	15
Cuotas	16
Cuotas para AWS los servicios de este producto	16
AWS CloudFormation cuotas	17
Planificar la resiliencia	17
Implemente el producto	18
Requisitos previos	18
Crear una Cuenta de AWS con un usuario administrativo	19
Cree un par de claves SSH de Amazon EC2	19
Aumentar las cuotas de servicio	19
Crea un dominio público (opcional)	20
Crear dominio (GovCloud solo)	20
Proporcione recursos externos	21
Configure LDAPS en su entorno (opcional)	22
Configurar una VPC privada (opcional)	22
Crea recursos externos	34
Paso 1: lanza el producto	39

Paso 2: Inicia sesión por primera vez	48
Actualice el producto	50
Actualizaciones de versiones principales	50
Actualizaciones de versiones menores	50
Desinstale el producto	52
Usando el AWS Management Console	52
Usando AWS Command Line Interface	52
Eliminar el shared-storage-security-group	52
Eliminar los buckets de Amazon S3	53
Guía de configuración	54
Administrar usuarios y grupos	54
Configuración del SSO con IAM Identity Center	54
Configurar tu proveedor de identidad para el inicio de sesión único (SSO)	58
Establecer contraseñas para los usuarios	68
Crear subdominios	68
Cree un certificado ACM	69
Amazon CloudWatch Logs	70
Establecer límites de permisos personalizados	71
Configure las AMI preparadas para RES	76
Prepare la función de IAM para acceder al entorno RES	76
Crear el componente Image Builder de EC2	78
Prepare su receta de EC2 Image Builder	82
Configuración de la infraestructura de EC2 Image Builder	84
Configurar la canalización de imágenes de Image Builder	85
Ejecute la canalización de imágenes de Image Builder	86
Registre una nueva pila de software en RES	86
Guía del administrador	87
Administración de sesiones	87
Panel de control	88
Sesiones	89
Pilas de software (AMI)	92
Perfiles de permisos	96
Debugging	99
Configuración de escritorio	99
Gestión del entorno	100
Proyectos	101

Usuarios	107
Grupos	108
Sistemas de archivos	109
Estado del entorno	114
Administración de instantáneas	115
Configuración del entorno	121
Administración de secretos	122
Supervisión y control de costes	125
Permisos	130
Usa el producto	133
Escritorios virtuales	133
Sistemas operativos compatibles	134
Lanza un escritorio nuevo	134
Acceda a su escritorio	134
Controle el estado de su escritorio	136
Modificar un escritorio virtual	137
Recupera la información de la sesión	138
Programa escritorios virtuales	138
Escritorios compartidos	140
Comparte un escritorio	140
Accede a un escritorio compartido	141
Explorador de archivos	141
Cargar archivo (s)	142
Eliminar archivo (s)	142
Administra los favoritos	142
Editar archivos	143
Transferencia de archivos	143
Acceso mediante SSH	144
Resolución de problemas	145
Problemas de instalación	145
AWS CloudFormation la pila no se puede crear con el mensaje «se WaitCondition recibió el mensaje fallido». Error: estados. TaskFailed»	145
No se recibe la notificación por correo electrónico después de que las AWS CloudFormation pilas se hayan creado correctamente	146
Instancias cíclicas o controladora de vdc en estado fallido	147

La CloudFormation pila de entornos no se puede eliminar debido a un error en el objeto dependiente	150
Se encontró un error en el parámetro de bloque CIDR durante la creación del entorno	150
CloudFormation error al crear la pila durante la creación del entorno	151
La creación de una pila de recursos externos (demostración) falla con AdDomainAdminNode CREATE_FAILED	151
Problemas de gestión de identidad	151
Al iniciar sesión en el entorno, vuelvo inmediatamente a la página de inicio de sesión	152
Se produjo el error «Usuario no encontrado» al intentar iniciar sesión	153
El usuario se agregó en Active Directory, pero no aparece en RES	154
El usuario no estaba disponible al crear una sesión	154
Error al superar el límite de tamaño en el registro del administrador de clústeres CloudWatch	154
Avisos	155
Revisiones	156
.....	clvii

Información general

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

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

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

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

Características y ventajas

Research and Engineering Studio on AWS ofrece las siguientes funciones:

Interfaz de usuario basada en web

RES proporciona un portal basado en la web que los administradores, investigadores e ingenieros pueden utilizar para acceder a sus espacios de trabajo de investigación e ingeniería

y gestionarlos. Los científicos e ingenieros no necesitan tener experiencia Cuenta de AWS o experiencia en la nube para usar RES.

Configuración basada en proyectos

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

Herramientas de colaboración

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

Integración con la infraestructura de administración de identidades existente

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

Almacenamiento y acceso persistentes a los datos compartidos

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

Explorador de archivos

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

Sistema de archivos

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

Administrador global

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

Proyecto

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

Permisos basados en proyectos

Los permisos basados en proyectos describen una partición lógica de los hosts de datos y de VDI en un sistema en el que pueden existir varios proyectos. El acceso de un usuario a los datos y a los hosts de VDI de un proyecto viene determinado por sus funciones asociadas. Se debe asignar a un usuario el acceso (o la pertenencia a un proyecto) para cada proyecto al que necesite acceder. De lo contrario, un usuario no podrá acceder a los datos del proyecto 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

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

Pila de software

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

Hosts VDI

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

Para obtener una referencia general de los AWS términos, consulte el [AWS glosario](#) de la Referencia general.AWS

Información general de la arquitectura

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

Diagrama de arquitectura

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

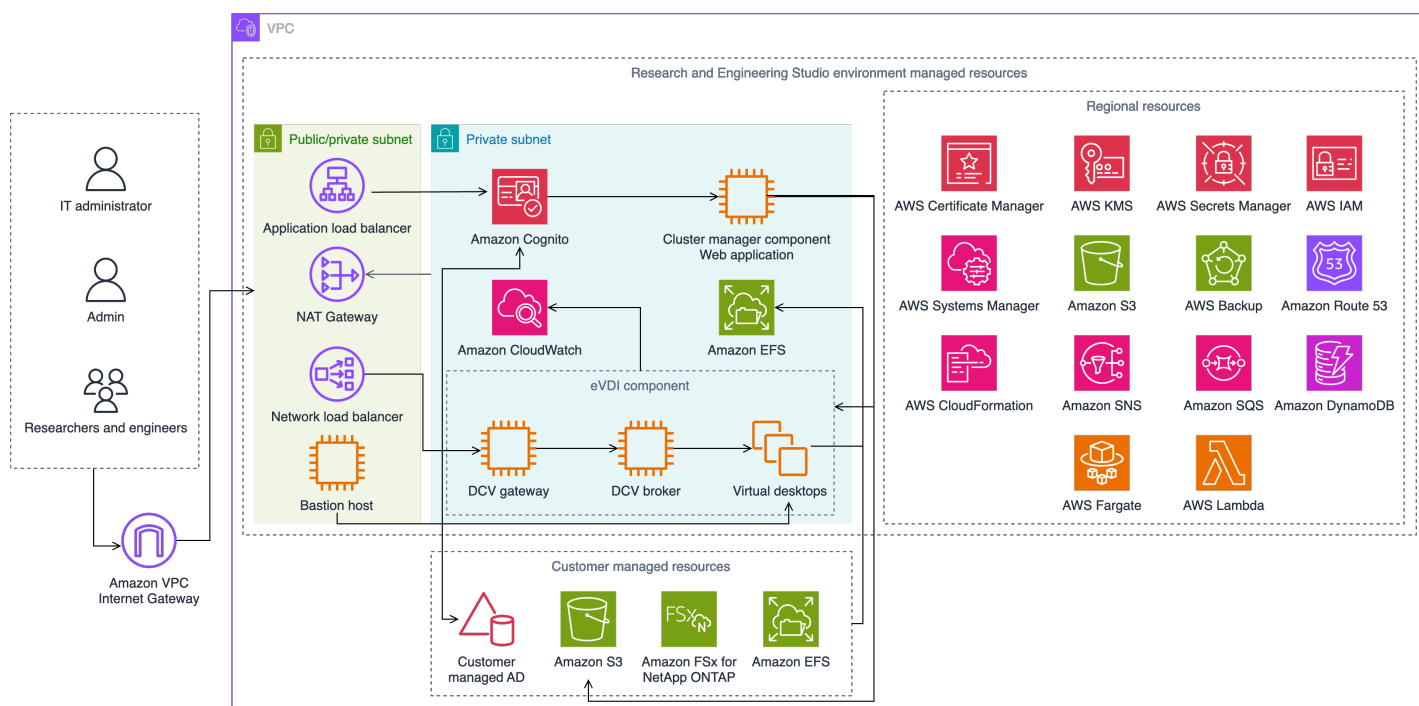


Figura 1: Estudio de investigación e ingeniería sobre AWS arquitectura

Note

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

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

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


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

Amazon CloudWatch recibe las métricas de los componentes de eVDI.

- c. Componente Bastion Host

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

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

 Note

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

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

AWSservicios de este producto

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

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

Servicio de AWS	Descripción
AWS Fargate	Admite. 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.

Cree un entorno de demostración

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

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

Cree una pila de demostración con un solo clic

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

Tiempo de implementación: aproximadamente 90 minutos

Requisitos previos

Temas

- [Cree una Cuenta de AWS con un usuario administrativo](#)
- [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 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 AWS se 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 [Creación de un par de claves con 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 elásticas de EC2-VPC de cinco a diez

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

Cree recursos e introduzca parámetros

1. Inicie sesión en la AWS CloudFormation consola AWS Management Console y ábrala 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	Descripción
EnvironmentName	< <i>res-demo</i> >	Nombre exclusivo asignado a su entorno RES que comienza con res- y no debe superar los 11 caracteres.
AdministratorEmail		La dirección de correo electrónico del usuario que completa la configuración del producto. Este usuario también funciona como un usuario rompeolas si se produce un error en la integración del inicio de sesión único de Active Directory.
KeyPair		El key pair que se utiliza para conectarse a los hosts de la infraestructura.
IPCIDR del cliente	<0.0.0.0/0>	Filtro de direcciones IP que limita la conexión al sistema. Puede actualizarlo ClientIpCidr después de la implementación.
InboundPrefixList		(Opcional) Proporcione una lista de prefijos gestionada para las IP que pueden acceder directamente a la interfaz de usuario web y a SSH desde el host bastión.

Pasos posteriores a la implementación

1. Restablezca las contraseñas de los usuariosAWS Directory Service: la pila de demostración crea cuatro usuarios con nombres de usuario que puede usar:admin1, user1admin2, y. user2
 - a. Vaya a la consola de Directory Service.
 - b. Seleccione el identificador de directorio de su entorno. Puede obtener el identificador del directorio a partir de la salida de la <StackName>*DirectoryService* pila.
 - c. En el menú desplegable Acciones de la parte superior derecha, selecciona Restablecer la contraseña del usuario.
 - d. Para todos los usuarios que quieras usar, coloca el nombre de usuario, escribe la contraseña que quieres tener y selecciona Restablecer contraseña.
2. Una vez que haya restablecido las contraseñas de los usuarios, tendrá que esperar a que Research and Engineering Studio sincronice los usuarios del entorno. Research and Engineering Studio sincroniza a los usuarios cada hora a las 24 horas. Puede esperar a que eso suceda o seguir los pasos que se indican [El usuario se agregó en Active Directory, pero no aparece en RES](#) para sincronizar los usuarios inmediatamente.

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

Planificación de la implementación

Costo

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

Note

Usted es responsable del coste de los AWS servicios utilizados durante la ejecución de este producto.

Recomendamos crear un [presupuesto AWS Cost Explorer](#) para ayudar a gestionar los costes. Los precios están sujetos a cambios. Para obtener más información, consulta la página web de precios de cada AWS servicio utilizado en este producto.

Seguridad

Cuando crea sistemas en una AWS infraestructura, las responsabilidades de seguridad se comparten entre usted y AWS. Este [modelo de responsabilidad compartida](#) reduce la carga operativa, ya que AWS opera, administra y controla los componentes, incluidos el sistema operativo anfitrión, la capa de virtualización y la seguridad física de las instalaciones en las que operan los servicios. Para obtener más información acerca de 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 Lambda, las instancias EC2, las instancias CSR de los sistemas de archivos y los puntos finales VPN remotos. Le recomendamos que revise los grupos de seguridad y restrinja aún más el acceso según sea necesario una vez que se implemente el producto.

Cifrado de datos

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

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

Compatible Regiones de AWS

Este producto utiliza servicios que actualmente no están disponibles en todas las Regiones de AWS. Debe lanzar este producto en una 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 las siguientes Regiones de AWS:

Nombres de las regiones	
Este de EE. UU. (Ohio)	Canadá (centro)

Nombres de las regiones	
Este de EE. UU. (Norte de Virginia)	Europa (Fráncfort)
Oeste de EE. UU. (Norte de California)	Europa (Irlanda)
Oeste de EE. UU. (Oregón)	Europa (Londres)
Asia-Pacífico (Bombay)	Europa (Milán)
Asia-Pacífico (Seúl)	Europa (París)
Asia-Pacífico (Singapur)	Israel (Tel Aviv)
Asia-Pacífico (Sídney)	AWS GovCloud (US-Oeste)
Asia-Pacífico (Tokio)	

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 AWS servicios incluidos en este producto

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

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

- Amazon Virtual Private Cloud
- Amazon EC2

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

AWS CloudFormation cuotas

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

Planificar la resiliencia

El producto implementa una infraestructura predeterminada con 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, recomendamos aumentar 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 de datos inesperada.

[La configuración de ASG se puede personalizar en la consola Amazon EC2 en https://console.aws.amazon.com/ec2/](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. Elija el grupo que desee modificar y, a continuación, elija Acciones y 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.

Implemente el producto

Note

Este producto utiliza [AWS CloudFormation plantillas y pilas](#) para automatizar su implementación. Las CloudFormation plantillas describen los AWS recursos incluidos en este producto y sus propiedades. La CloudFormation pila proporciona los recursos que se describen en las plantillas.

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

Temas

- [Requisitos previos](#)
- [Crear recursos externos](#)
- [Paso 1: lanzar el producto](#)
- [Paso 2: Inicie sesión por primera vez](#)

Requisitos previos

Temas

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

Crear una Cuenta de AWS con un usuario administrativo

Debe tener una Cuenta de AWS con un usuario administrativo:

1. 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 e indicar un código de verificación en el teclado del teléfono.

Al suscribirse a un Cuenta de AWS, Usuario raíz de la cuenta de AWS se 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 [Creación de un par de claves con 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 elásticas de EC2-VPC de cinco a diez

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

Crea un dominio público (opcional)

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

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

Crear dominio (GovCloud solo)

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

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

- a. res: = ModuleName virtual-desktop-controller
 - b. res: EnvironmentName = [nombre del entorno] (podría ser res-demo)
4. En la cuenta de GovCloud partición, cree un secreto con el valor de la PrivateKeySecretArn salida. Anote el nuevo ARN secreto y añada dos etiquetas al secreto para vdc-gateway poder acceder al valor secreto:
- a. res: = ModuleName virtual-desktop-controller
 - b. res: EnvironmentName = [nombre del entorno] (podría ser res-demo)

Proporcione recursos externos

Al implementar Research and Engineering Studio AWS, el producto utilizará recursos externos que necesitará. RES espera que esos recursos existan cuando se desplieguen.

- Redes (subredes de VPC, públicas y privadas)

Aquí es donde ejecutará las instancias de EC2 que se utilizan para alojar el entorno, 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 las páginas del entorno.

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

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

Tip

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

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

Configure LDAPS en su entorno (opcional)

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

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

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

Configurar una VPC privada (opcional)

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

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

Temas

- [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](#). Para implementarse en una VPC aislada, la infraestructura RES requiere la disponibilidad de dependencias sin tener acceso público a Internet.
2. Cree un rol de IAM con acceso de solo lectura a Amazon S3 y una identidad de confianza como Amazon EC2.
 - a. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
 - b. En Roles, elija Crear rol.
 - c. En la página Seleccionar entidad de confianza:
 - En Tipo de entidad de confianza, elija Servicio de AWS.
 - En Caso de uso en Servicio o Caso de uso, seleccione EC2 y elija Siguiente.
 - d. En Agregar permisos, seleccione las siguientes políticas de permisos y, a continuación, elija Siguiente:
 - Amazon S3 ReadOnlyAccess
 - Amazon SSM ManagedInstanceCore
 - EC2 InstanceProfileForImageBuilder
 - 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
Nombre del componente	Elija un nombre como: <i>< research-and-engineering-studio - infrastructure ></i>
Versión del componente	Recomendamos empezar con la versión 1.0.0.
Descripción	Entrada de usuario opcional.

- d. En la página Crear componente, elija Definir el contenido del documento.
 - i. Antes de introducir el contenido del documento de definición, necesitará un URI de archivo para el archivo tar.gz. Cargue el archivo tar.gz proporcionado por RES a un bucket de Amazon S3 y copie el URI del archivo de las propiedades del bucket.
 - ii. Introduzca lo siguiente:

 Note

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

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

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

parameters:
  - AWSAccountID:
    type: string
    description: RES Environment AWS Account ID
  - AWSRegion:
    type: string
    description: RES Environment AWS Region

phases:
  - name: build
    steps:
      - name: DownloadRESInstallScripts
        action: S3Download
        onFailure: Abort
        maxAttempts: 3
        inputs:
          - source: '<s3 tar.gz file uri>'
            destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
            expectedBucketOwner: '{{ AWSAccountID }}'
      - name: RunInstallScript
        action: ExecuteBash
        onFailure: Abort
        maxAttempts: 3
        inputs:
          commands:
            - 'cd /root/bootstrap/res_dependencies'
            - 'tar -xf res_dependencies.tar.gz'
            - 'cd all_dependencies'
```

```

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

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

```

e. Seleccione Crear componente.

4. Cree una receta de imágenes de Image Builder.

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

Sección	Parámetro	Entrada de usuario
Detalles de la receta	Nombre	Introduzca un nombre apropiado, como res-recipe-linux-x 86.
	Versión	Introduzca una versión, que normalmente empieza por la 1.0.0.
	Descripción	Añada una descripción opcional.
Imagen base	Seleccione una imagen	Seleccione imágenes gestionadas.
	SO	Amazon Linux
	Origen de la imagen	Inicio rápido (gestionado por Amazon)
	Nombre de la imagen	Amazon Linux 2 x86
	Opciones de control de versiones automático	Utilice la última versión del sistema operativo disponible.
Configuración de instancias	–	Mantén todo en la configuración predeterminada y asegúrate de que no esté seleccionada la opción Eliminar el agente SSM tras la ejecución de la canalización.

Sección	Parámetro	Entrada de usuario
Directorio de trabajo	Ruta del directorio de trabajo	/root/bootstrap/re s_dependencies
Componentes	Construya componentes	<p>Busque y seleccione lo siguiente:</p> <ul style="list-style-type: none"> • Administrado por Amazon: -2-linux aws-cli-version • Administrado por Amazon: amazon-cloudwatch-agent-linux • De su propiedad: componente de Amazon EC2 creado anteriormente. Introduzca su Cuenta de AWS ID y la información actual Región de AWS en los campos.
	Pruebe los componentes	<p>Busque y seleccione:</p> <ul style="list-style-type: none"> • Administrado por Amazon: simple-boot-test-linux

b. Elija Crear receta.

5. Cree la configuración de infraestructura de Image Builder.

a. En Recursos guardados, elija Configuraciones de infraestructura.

b. Elija Crear configuración de infraestructura.

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

Sección	Parámetro	Entrada de usuario
General	Nombre	Introduzca un nombre apropiado, como res-infra-linux-x 86.
	Descripción	Añada una descripción opcional.
	Rol de IAM	Seleccione el rol de IAM creado anteriormente.
AWS infraestructura	Tipo de instancia	Elija t3.medium.
	VPC, subred y grupos de seguridad	<p>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:</p> <ul style="list-style-type: none"> • VPC: seleccione la misma VPC que se utiliza para la configuración de la infraestructura. Esta VPC debe tener acceso a Internet. • Regla de entrada: <ul style="list-style-type: none"> • Tipo: SSH • Source (Fuente): Custom • 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. Selecciona Acciones y selecciona Ejecutar canalización.

La canalización puede tardar entre 45 minutos y una hora en crear una imagen AMI.
8. Anote el ID de AMI de la AMI generada y utilícelo como entrada para el parámetro InfrastructureHost AMI en [the section called "Paso 1: lanza el producto"](#).

Configurar puntos finales de VPC

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

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

Servicio de AWS	Nombre del servicio
Aplicación de escalado automático	com.amazonaws. <i>region</i> .application-autoscaling
AWS CloudFormation	com.amazonaws. <i>region</i> .cloudformation
Amazon CloudWatch	com.amazonaws. <i>region</i> .monitoring
Amazon CloudWatch Logs	com.amazonaws. <i>region</i> .logs
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb (requiere un punto final de puerta de enlace)
Amazon EC2	com.amazonaws. <i>region</i> .ec2
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
Amazon Elastic File System	com.amazonaws. <i>region</i> .elasticfilesystem
Elastic Load Balancing	com.amazonaws. <i>region</i> .elasticloadbalancing
Amazon EventBridge	com.amazonaws. <i>region</i> .events
Amazon FSx	com.amazonaws. <i>region</i> .fsx
AWS Key Management Service	com.amazonaws. <i>region</i> .kms
Amazon Kinesis Data Streams	com.amazonaws. <i>region</i> .kinesis-streams

Servicio de AWS	Nombre del servicio
Amazon S3	com.amazonaws. <i>region</i> .s3 (requiere un punto final de puerta de enlace que se crea de forma predeterminada en RES).
AWS Secrets Manager	com.amazonaws. <i>region</i> .secretsmanager
Amazon SES	com.amazonaws. <i>region</i> .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. <i>region</i> .sts
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> .sqs
AWS Systems Manager	com.amazonaws. <i>region</i> .ec2messages
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> .ssmmessages

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. Denegar todas las demás conexiones.
 - d. Active e inicie el servidor proxy.
 - e. Anote el PUERTO en el que escucha el servidor proxy.
 3. Configure su tabla de rutas para permitir el acceso al servidor proxy.
 - a. Vaya a la consola de VPC e identifique las tablas de enrutamiento de las subredes que utilizará para los hosts de infraestructura y los hosts de VDI.
 - b. Edite la tabla de rutas para permitir que todas las conexiones entrantes vayan a la instancia del servidor proxy creada en los pasos anteriores.
 - c. Haga esto para las tablas de enrutamiento de todas las subredes (sin acceso a Internet) que vaya a utilizar para la infraestructura o los VDI.
 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

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

Parámetro	Entrada
InfrastructureHostAMI	Utilice el ID de AMI de infraestructura creado en the 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.

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 la AWS CloudFormation consola AWS Management Console y ábrala 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 la región AWS GovCloud (EE. UU.-Oeste), [lance la plantilla](#) en la cuenta de GovCloud partición.

3. Introduzca los parámetros de la plantilla:

Parámetro	Predeterminado	Descripción
DomainName	corp.res.com	<p>Dominio utilizado para el directorio activo. El valor predeterminado se proporciona en el LDIF archivo que configura los usuarios de bootstrap. Si desea utilizar los usuarios predeterminados, 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.</p>
SubDomain (GovCloud solo)		<p>Este parámetro es opcional para las regiones comerciales, pero obligatorio para GovCloud las regiones.</p> <p>Si proporciona un SubDomain, el parámetro tendrá el prefijo del DomainName proporcionado. El nombre de dominio de Active Directory proporcionado pasará a ser un subdominio.</p>

Parámetro	Predeterminado	Descripción
AdminPassword		<p>La contraseña del administrador de Active Directory (nombre de usuarioAdmin). Este usuario se crea en Active Directory para la fase inicial de arranque y no se utiliza después.</p> <p>Nota: La contraseña de este usuario debe cumplir los requisitos de complejidad de contraseñas de Active Directory.</p>
ServiceAccountPassword		<p>Contraseña utilizada para crear una cuenta de servicio (ReadOnlyUser). Esta cuenta se utiliza para la sincronización.</p> <p>Importante: a partir de la versión 2024.06 de Research and Engineering Studio, debe proporcionar un ARN secreto que contenga la contraseña de texto sin formato del. ServiceAccount</p> <p>Nota: La contraseña de este usuario debe cumplir los requisitos de complejidad de contraseñas de Active Directory.</p>

Parámetro	Predeterminado	Descripción
Par de claves		<p>Conecta las instancias administrativas mediante un cliente SSH.</p> <p>Nota: El administrador de AWS Systems Manager sesiones también se puede usar para conectarse a instancias.</p>
Ruta LDIFS3	<pre>aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif</pre>	<p>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.</p> <p>Para ver el archivo, consulte el archivo res.ldif disponible en GitHub</p>
ClientIpCidr		<p>La dirección IP desde la que accederá al sitio. Por ejemplo, puede seleccionar su dirección IP y utilizarla a <code>[IPADDRESS]/32</code> para permitir el acceso únicamente desde su servidor. Puede actualizarla después de la implementación.</p>

Parámetro	Predeterminado	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- <i>[environment name]</i>	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	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 certificado público y un archivo de claves y se cargarán en ellos AWS Secrets Manager. Si tiene su propio dominio y certificados, EnvironmentName puede dejar este parámetro en blanco.

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

Paso 1: lanzar el producto

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

Tiempo de implementación: aproximadamente 60 minutos

Puede [descargar la CloudFormation plantilla de](#) este producto antes de implementarlo.

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

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

Note

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

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

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

2. Abre la [plantilla](#).

Para implementarla en AWS GovCloud (EE. UU. al oeste), lance esta [plantilla](#).

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

Note

Este producto utiliza el servicio Amazon Cognito, que actualmente no está disponible en todos. Regiones de AWS Debe lanzar este producto en un Región de AWS lugar en el que Amazon Cognito esté disponible. Para obtener la disponibilidad más reciente por región, consulte la [lista de Región de AWS todos los servicios](#).

4. En Parámetros, revisa los parámetros de esta plantilla de producto y modifícalos según sea necesario. Si ha implementado los recursos externos automatizados, puede encontrar estos parámetros en la pestaña Resultados de la pila de recursos externos.

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

Parámetro	Predeterminado	Descripción
		completa la configuración del producto. Este usuario también funciona como un usuario rompeolas si se produce un error en la integración del inicio de sesión único de Active Directory.
InfrastructureHostAMI	ami- <i>[solo números o letras]</i>	(Opcional) Puede proporcionar un identificador de AMI personalizado para usarlo en todos los hosts de la infraestructura. El sistema operativo base compatible actualmente es Amazon Linux 2. Para obtener más información, consulte Configure las AMI preparadas para RES-Ready .
SSH KeyPair		El key pair que se utiliza para conectarse a los hosts de la infraestructura.
ClientIP	<i>x.x.x .0/24 o x.x.x .0/32</i>	Filtro de direcciones IP que limita la conexión al sistema. Puede actualizarlo ClientIpCidr después de la implementación.

Parámetro	Predeterminado	Descripción
ClientPrefixList		(Opcional) Proporcione una lista de prefijos gestionada para las IP que pueden acceder directamente a la interfaz de usuario web y a SSH desde el host bastión.
YO SOY PermissionBoundary		(Opcional) Puede proporcionar un ARN de política administrada que se adjuntará como límite de permisos a todos los roles creados en RES. Para obtener más información, consulte Establecer límites de permisos personalizados .
VpcId		IP de la VPC en la que se lanzarán las instancias.
IsLoadBalancerInternetFacing		Seleccione true para implementar un balanceador de carga orientado a Internet (requiere subredes públicas para el balanceador de carga). Para las implementaciones que necesitan acceso restringido a Internet, selecciona false.

Parámetro	Predeterminado	Descripción
LoadBalancerSubnets		<p>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, elija subredes privadas. Para las implementaciones que necesitan acceso a Internet, elija subredes públicas. Si la pila de redes externas creó más de dos, seleccione todas las que se crearon.</p>
InfrastructureHostSubnets		<p>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.</p>
VdiSubnets		<p>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.</p>

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

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

Parámetro	Predeterminado	Descripción
EnableLdapIDMapping		Determina si el SSSD genera los números UID y GID o si se utilizan los números proporcionados por el AD. Establézcalo en True para usar el UID y el GID generados por SSSD, o en False para usar el UID y el GID proporcionados por el AD. En la mayoría de los casos, este parámetro debe estar establecido en True.
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.
SharedHomeFilesystemID		Un ID de EFS que se utilizará en el sistema de archivos doméstico compartido para los hosts VDI de Linux.
CustomDomainNameforWebApp		(Opcional) Subdominio utilizado por el portal web para proporcionar enlaces a la parte web del sistema.

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

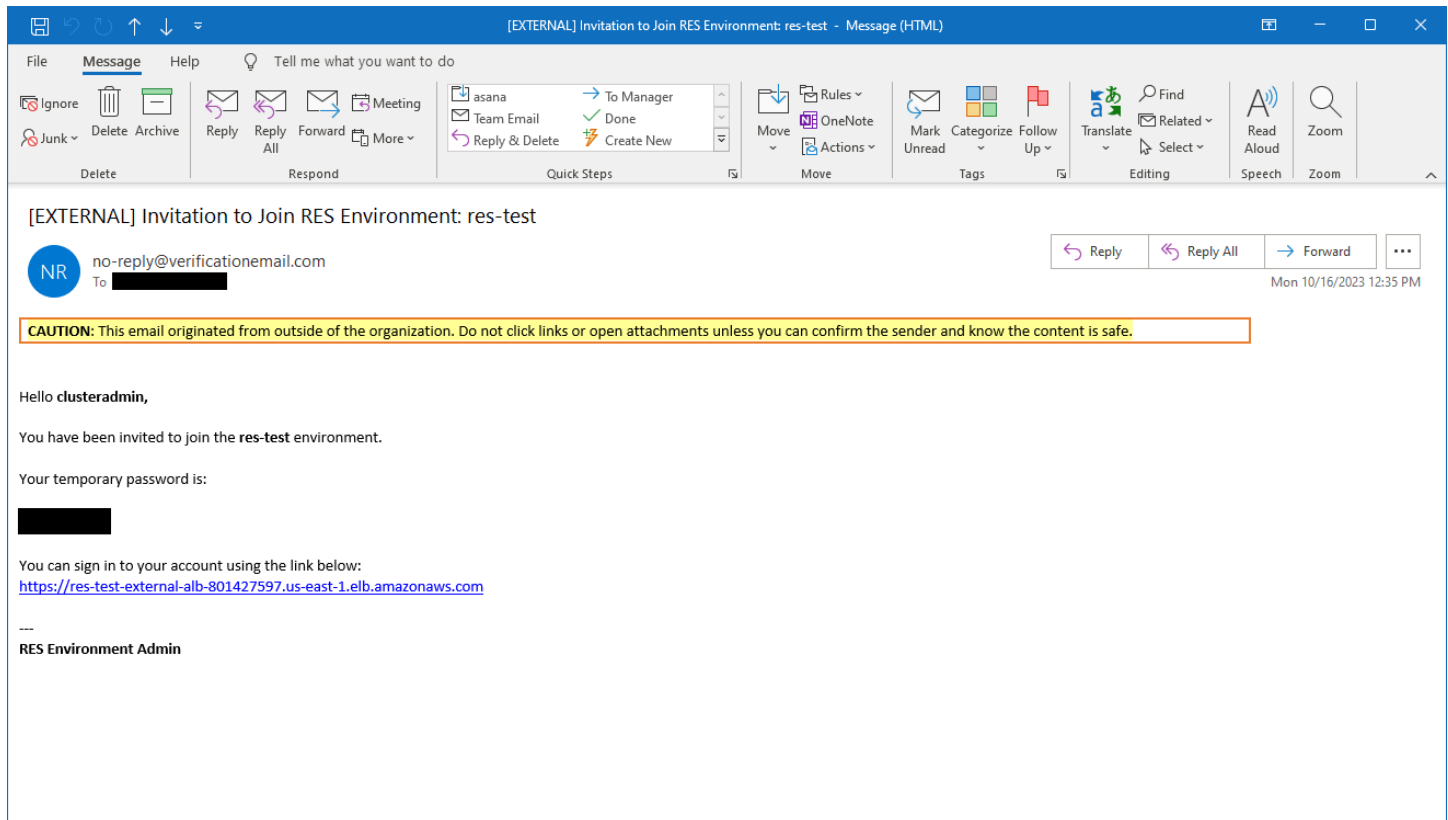
Parámetro	Predeterminado	Descripción
PrivateKeySecretARN para VDI		(Opcional) Este secreto ARN almacena la clave privada del certificado de su portal web. Si establece un nombre de dominio de portal para tus recursos externos automatizados, puedes encontrar este valor en la pestaña Resultados de la pila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

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

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

Paso 2: Inicie sesión por primera vez

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



Una vez que haya iniciado sesión por primera vez, podrá configurar los ajustes del portal web para conectarse al proveedor de SSO. Para obtener información sobre la configuración posterior a la implementación, consulte la [Guía de configuración](#)

Actualiza el producto

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

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

Temas

- [Actualizaciones de versiones principales](#)
- [Actualizaciones de versiones menores](#)

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

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

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

Para realizar una actualización menor de la versión:

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

Desinstalar el producto

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

Utilización del AWS Management Console

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

Usando AWS Command Line Interface

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

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

Eliminar el shared-storage-security-group

Warning

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

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

Eliminar los buckets de Amazon S3

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

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

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

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

Note

El `--force` comando vacía el contenido del depósito.

Guía de configuración

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

Temas

- [Administrar usuarios y grupos](#)
- [Crear subdominios](#)
- [Cree un certificado ACM](#)
- [Amazon CloudWatch Logs](#)
- [Establecer límites de permisos personalizados](#)
- [Configure las AMI preparadas para RES-Ready](#)

Administrar usuarios y grupos

Research and Engineering Studio puede utilizar cualquier proveedor de identidad compatible con SAML 2.0. Si implementó RES con recursos externos o planea usar el centro de identidad de IAM, consulte. [the section called “Configuración del SSO con IAM Identity Center”](#) Si tiene su propio proveedor de identidad compatible con SAML 2.0, consulte. [the section called “Configurar tu proveedor de identidad para el inicio de sesión único \(SSO\)”](#)

Temas

- [Configuración del inicio de sesión único con el Centro de identidades de IAM](#)
- [Configuración del proveedor de identidad para el inicio de sesión único \(SSO\)](#)
- [Establecer contraseñas para los usuarios](#)

Configuración del inicio de sesión único con el Centro de identidades de IAM

Si aún no tiene un centro de identidad conectado al directorio activo administrado, comience con. [the section called “Configure un centro de identidad”](#) Si ya tiene un centro de identidad conectado al directorio activo administrado, comience con [the section called “Conéctese a un centro de identidad”](#).


 Note

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

Paso 1: Configurar un centro de identidad

Habilitar un centro de identidad

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en <https://console.aws.amazon.com/iam/>.
2. Abra el Centro de identidades.
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.

Conectar el centro de identidades al directorio activo administrado

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

1. En la barra de navegación, selecciona Configuración.
2. En Fuente de identidad, selecciona Acciones y selecciona 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 [the section called “Conectar el centro de identidades al directorio activo administrado”](#) completado los cambios, aparecerá un banner 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 selecciona Guardar configuración.
7. El proceso de sincronización puede tardar unos minutos. Si recibes un mensaje de advertencia sobre los usuarios que no se están sincronizando, selecciona Reanudar la sincronización.

Habilitar usuarios

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

Paso 2: Conectarse a un centro de identidad

Configuración de la aplicación en Identity Center

1. Inicie sesión en el Centro de Identidad de IAM AWS Management Console y ábralo en <https://console.aws.amazon.com/singlesignon/>.
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 SSO 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 del portal RES. Para encontrar esto:
 - a. En Administración del entorno, selecciona Configuración general.
 - b. Elija la pestaña Identity provider.
 - c. En el inicio de sesión único, encontrarás la URL de redireccionamiento de SAML.
11. En Audiencia SAML de la aplicación, introduzca la URN de Amazon Cognito. Para crear la urna:
 - a. Desde el portal RES, abra la configuración general.
 - b. En la pestaña del 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. Seleccione Submit (Enviar).

Configuración de las asignaciones de atributos para la aplicación

1. En el Centro de identidad, abra los detalles de la aplicación que ha creado.
2. Elija Acciones y elija Editar asignaciones de atributos.
3. En Asunto, introduce \$ {user:email}.
4. En Formato, selecciona Dirección de correo electrónico.
5. Seleccione Agregar nueva asignación de atributos.
6. En Atributo de usuario de la aplicación, introduce el 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. Elija Guardar cambios.

Agregar usuarios a la aplicación en Identity Center

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 SSO en el entorno RES

1. Desde el entorno de Research and Engineering Studio, abra la configuración general en Administración del entorno.
2. Abra la pestaña del proveedor de identidades.
3. En Inicio de sesión único, selecciona el botón de edición situado 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 [the section called “Configuración de la aplicación en Identity Center”](#)
 - e. En el atributo de correo electrónico del proveedor, introduce el correo electrónico.
 - f. Seleccione Submit (Enviar).
5. Actualiza la página y comprueba que el estado se muestre como activado.

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

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

Note

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

Temas

- [Configure su proveedor de identidad](#)
- [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 autoaprovechado) 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 la aplicación
- URL del Assertion Consumer Service (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 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 los siguientes campos o afirmaciones configurados en la dirección de correo electrónico del usuario:
- Asunto o NameID de SAML
 - Correo electrónico SAML
4. Su IdP agrega campos o reclamos 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— Definido en `urn:amazon:cognito:sp:user-pool-id.user-pool-id` Sustitúyalo por el ID de tu grupo de usuarios de Amazon Cognito.

```
<saml:AudienceRestriction>
```

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

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

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

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

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

- AuthnStatement— Configúrelo de la siguiente manera:

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

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

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

Para obtener la URL del dominio

1. Inicie sesión en RES como administrador o administrador de clústeres.
 2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.
 3. Elija la URL del dominio.
6. Si su IdP acepta un certificado de firma para establecer la confianza en Amazon Cognito, descargue el certificado de firma de Amazon Cognito y cárguelo en su IdP.

Para obtener el certificado de firma

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

Cognito user pool sign-in [Info](#)

Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.

Cognito user pool sign-in options

User name
Email

User name requirements

User names are not case sensitive

Federated identity provider sign-in (1) [Info](#)
[Refresh](#) [Delete](#) [Add identity provider](#) [View signing certificate](#)

Your app users can sign-in through external social identity providers like Facebook, Google, Amazon, or Apple, and through your on-prem directories via SAML or Open ID Connect.

< 1 > ⚙️

Identity provider	Identity provider type	Created time	Last updated time
<input type="radio"/> idc	SAML	2 weeks ago	3 hours ago

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.

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

Configure RES para usar su proveedor de identidad

Para completar la configuración del inicio de sesión único para RES

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

The screenshot shows the 'Environment Settings' page for an environment named 'res-gaenv1'. The 'Identity Provider' tab is selected, displaying the following configuration:

Environment Settings		
Environment Name	AWS Region	S3 Bucket
res-gaenv1	us-east-1	res-gaenv1-cluster-us-east-1-088837573664
Identity Provider		
Provider Name	User Pool Id	Administrators Group Name
cognito-idp	us-east-1_reuFsm8SE	administrators-cluster-group
Managers Group Name	Domain URL	Provider URL
managers-cluster-group	https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazonaws.com	https://cognito-idp.us-east-1.amazonaws.com/us-east-1_reuFsm8SE
Single Sign-On		
Status	SAML Redirect URL	OIDC Redirect URL
Enabled	https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazonaws.com/saml2/idpresponse	https://res-gaenv1-9d4688cf-5c14-48d0-990f-ce96d346a24c.auth.us-east-1.amazonaws.com/oauth2/idpresponse

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

Single Sign On Configuration ✕

Identity Provider

Choose the third-party identity provider that you would like to configure.

SAML
Configure trust between Cognito and a SAML 2.0-compatible identity provider.

OIDC
Configure trust between Cognito and an OIDC identity provider,

Provider Name

Name used for the provider in cognito

Metadata Document Source

Provide a SAML metadata document. This document is issued by your SAML provider.

Upload metadata document

Enter metadata document endpoint URL

Metadata document


Provider Email Attribute

The Email attribute used to map email between your idp and the Amazon Cognito user pool

Refresh Token Expiration (hours)

Must be between 1 and 87600 (10 years)

- En Identity Provider, elija SAML.
- En Nombre del proveedor, introduce un nombre único para tu proveedor de identidad.

 Note

No se permiten los siguientes nombres:

- Cognito
- IdentityCenter

- 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.
 - En el campo Atributo de correo electrónico del proveedor, introduzca el valor del `textoemail`.
 - Seleccione Submit (Enviar).
- 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:

- Nombre del proveedor: no se puede modificar
- Documento de metadatos o URL: se puede modificar
- 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:

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

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

Attribute mapping (1) [Info](#) Edit

View, add, and edit attribute mappings between SAML and your user pool. < 1 > ⚙

User pool attribute	SAML attribute
email	email

Metadata document [Info](#) Replace metadata

View and update your SAML metadata. This document is issued by your SAML provider. It includes the issuer's name, expiration information, and keys that can be used to validate the response from the identity provider.

<p>Metadata document source Enter metadata document endpoint URL</p>	<p>Metadata document endpoint URL <code>https://portal.sso.us-west-2.amazonaws.com/saml/metadata/MDg4ODM3NTczNjY0X2lucy04M2EyYTcyMGUzZTFIMDI4</code></p>
---	---

6. Si ha editado la asignación de atributos, tendrá que actualizar la `<environment name>.cluster-settings` tabla en DynamoDB.
- a. Abra la consola de DynamoDB y seleccione Tablas en la barra de navegación.
 - b. Busque y seleccione la `<environment name>.cluster-settings` tabla y, en el menú Acciones, elija Explorar elementos.
 - c. En Escanear o consultar elementos, vaya a Filtros e introduzca los siguientes parámetros:
 - Nombre del atributo: `key`
 - Valor — `identity-provider.cognito.sso_idp_provider_email_attribute`
 - d. Elija 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.

▼ **Scan or query items**

Scan
 Query

Select a table or index: Table - res-jan19.cluster-settings
 Select attribute projection: All attributes

▼ **Filters** 6

Attribute name	Type	Condition	Value	
key	String	Equal to	identity-provider	Remove

Add filter

Run Reset

✔ Completed. Read capacity units consumed: 13
✕

Items returned (1)

- key (String)
- [identity-provider.cognito.ss](#)

Edit String ✕

email

Enter any string value.

Cancel Save

Actions Create item

8 < 1 > ⚙️ ✕

▼ | version ▼

1

Depuración de problemas de IdP de SAML

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

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

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

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

Establecer contraseñas para los usuarios

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

Crear subdominios

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

Note

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

1. [Inicie sesión en la consola de Route 53 AWS Management Console y ábrala en https://console.aws.amazon.com/route53/](https://console.aws.amazon.com/route53/).
2. Busca el dominio que creaste y selecciona Crear registro.
3. Introduce web como nombre del registro.
4. Elija CNAME como tipo de registro.
5. En Value, introduce el enlace que recibiste en el correo electrónico inicial.
6. Elija Crear registros.
7. Para crear un registro para el VDC, recupere la dirección NLB.

- a. [Inicie sesión en AWS Management Console y abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.](https://console.aws.amazon.com/cloudformation)
 - b. Elija <environment-name>-vdc.
 - c. Selecciona Recursos y abre<environmentname>-vdc-external-nlb.
 - d. Copia el nombre DNS del NLB.
8. Inicie sesión en la consola de Route 53 AWS Management Console y ábrala en <https://console.aws.amazon.com/route53/>.
 9. Busca tu dominio y selecciona Crear registro.
 10. En Nombre del registro, ingresavdc.
 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 certificado SSL/TLS público que hayas proporcionado o que hayas solicitado a (ACM). AWS Certificate Manager Si usa ACM, recibirá un nombre de AWS recurso que deberá proporcionar como parámetro para cifrar el canal SSL/TLS 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. [the section called “Crea recursos externos”](#)

Para crear un certificado para dominios personalizados:

1. Desde la consola, [AWS Certificate Manager](#)ábrala para solicitar un certificado público. Si va a realizar la implementación en EE. UU. AWS GovCloud (oeste de EE. UU.), cree el certificado en su cuenta de GovCloud partición.
2. Elija Solicitar un certificado público y, a continuación, Siguiente.

3. En Nombres de dominio, solicita un certificado para ambos `*.PortalDomainNamePortalDomainName`.
4. En Método de validación, selecciona Validación de DNS.
5. Seleccione Request (Solicitar).
6. En la lista de certificados, abra los certificados solicitados. Cada certificado tendrá el estado Pendiente de validación.

 Note

Si no ve sus certificados, actualice la lista.

7. Realice una de las siguientes acciones siguientes:
 - Implementación comercial: en los detalles del certificado de cada certificado solicitado, seleccione Crear registros en Route 53. El estado del certificado debe cambiar a Emitido.
 - GovCloud despliegue: si va a realizar el despliegue en AWS GovCloud (EE. UU. al oeste), copie la clave y el valor del CNAME. Desde la cuenta de partición comercial, utilice 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
<code>/aws/lambda/ < >-cluster-endpoints installation-stack-name</code>	¡Nunca caducan
<code>/aws/lambda/ < >-sync installation-stack-name cluster-manager-scheduled-ad</code>	¡Nunca caducan
<code>/aws/lambda/ < >-cluster-settings installation-stack-name</code>	¡Nunca caducan

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

Si desea cambiar la retención predeterminada de un grupo de registros, puede ir a la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/> y seguir las instrucciones para [cambiar la retención de datos de registro](#) en los registros. CloudWatch

Establecer límites de permisos personalizados

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

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

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

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

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



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

Configure las AMI preparadas para RES-Ready

Con las AMI preparadas para RES, puede preinstalar las dependencias de RES para instancias de escritorios virtuales (VDI) en sus AMI personalizadas. El uso de AMI preparadas para RES 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](#).

Temas

- [Prepare la función de IAM para acceder al entorno RES](#)
- [Crear el componente Image Builder de EC2](#)
- [Prepare su receta de EC2 Image Builder](#)
- [Configuración de la infraestructura de EC2 Image Builder](#)
- [Configurar la canalización de imágenes de Image Builder](#)
- [Ejecute la canalización de imágenes de Image Builder](#)
- [Registre una nueva pila de software en RES](#)

Prepare la función de IAM para acceder al entorno RES

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

Su función requiere:

- Las relaciones de confianza incluyen el servicio Amazon EC2
- Políticas de AmazonSSM y EC2 ManagedInstanceCore InstanceProfileForImageBuilder
- Política de RES personalizada con acceso limitado a DynamoDB y Amazon S3 al entorno RES implementado

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

Entidad de relación de confianza:

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

Política de RES:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RES DynamoDB Access",
      "Effect": "Allow",
      "Action": "dynamodb:GetItem",
      "Resource": "arn:aws:dynamodb:{AWS-Region}:{AWS-Account-ID}:table/{RES-EnvironmentName}.cluster-settings",
      "Condition": {
        "ForAllValues:StringLike": {
          "dynamodb:LeadingKeys": [
            "global-settings.gpu_settings.*",
            "global-settings.package_config.*"
          ]
        }
      }
    },
    {
      "Sid": "RES S3 Access",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-Account-ID}/idea/vdc/res-ready-install-script-packages/*"
    }
  ]
}
```

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.
5. Para el documento de definición, introduzca el siguiente archivo de definición. Si encuentra algún error, el archivo YAML es sensible al espacio y es la causa más probable.

Linux

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

```

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

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

```

```

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

```

Windows

```

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

```

```

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

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

```

```
delaySeconds: 0
```

6. Crea cualquier etiqueta opcional y selecciona Crear componente.

Prepare su receta de EC2 Image Builder

Note

Actualmente, está previsto que CentOS 7 llegue end-of-life el 30 de junio de 2024. La versión 2024.06 de Research and Engineering Studio será la última versión compatible con CentOS 7.


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)
- Centos 7 (x86 y ARM64)
- RHEL 7 (x86), 8 (x86) y 9 (x86)
- Ubuntu 22.04.3 (x86)
- Windows 2019, 2022 (x86)

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. Elija una imagen base compatible con RES.
6. En Configuración de instancias, instale un agente SSM si no viene preinstalado. Introduzca la información en Datos de usuario y cualquier otro dato de usuario necesario.

 Note

Para obtener información sobre cómo instalar un agente de SSM, consulte:

- [Instalación manual del agente SSM en instancias EC2 para Linux](#)
- [Instalación y desinstalación manual del agente SSM en instancias EC2 para Windows Server](#)

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

 Important

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

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

Modify a recipe

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

1. Para recetas basadas en Linux, añada el componente de `aws-cli-version-2-linux` compilación gestionado por Amazon a la receta. Los scripts de instalación de RES lo utilizan AWS CLI para proporcionar acceso de VDI a los valores de configuración de los ajustes del clúster de DynamoDB. Windows no requiere este componente.

2. Añada el componente EC2 Image Builder creado para su entorno Linux o Windows e introduzca los valores de parámetros necesarios. Los siguientes parámetros son entradas obligatorias: RES AWSAccountID EnvNameEnvRegion, RES y RES. EnvReleaseVersion

⚠ Important

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

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

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. [the section called “Prepare la función de IAM para acceder al entorno RES”](#)
2. Para el tipo de instancia, elija un tipo con al menos 4 GB de memoria y que sea compatible con la arquitectura AMI base que haya elegido. Consulte los [tipos de 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 AMI preparadas para RES, 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 en <https://console.aws.amazon.com/imagebuilder>.
2. En la barra 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 en [the section called "Prepare su receta de EC2 Image Builder"](#). Compruebe 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 en [the section called "Configuración 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 en [the section called "Prepare su receta de EC2 Image Builder"](#).

2. Elija 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 en [the section called “Configurar la canalización de imágenes de Image Builder”](#).
2. En Acciones, selecciona Ejecutar canalización.

Registre una nueva pila de software en RES

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

Guía del administrador

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

Temas

- [Administración de sesiones](#)
- [Gestión del entorno](#)
- [Administración de secretos](#)
- [Supervisión y control de costes](#)
- [Permisos](#)

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 \(AMI\)](#)
- [Perfiles de permisos](#)
- [Debugging](#)
- [Configuración de escritorio](#)

Panel de control

Research and Engineering Studio demoadmin1

res-stage (us-west-2) RES > Virtual Desktop > Dashboard

Virtual Desktop Dashboard

7 **8** [View Sessions](#)

Home

- Virtual Desktops
- Shared Desktops
- File Browser
- SSH Access

ADMIN ZONE

eVDI

- Dashboard**
- Sessions
- Software Stacks (AMIs)
- Permission Profiles
- Debug
- Settings

Environment Management

Instance Types **1**

Summary of all virtual desktop sessions by instance types.

Instance Type	Count
m6a.large	3

3 sessions

m6a.large

Session State **2**

Summary of all virtual desktop sessions by state.

Session State	Count
STOPPING	3

STOPPING

Base OS **3**

Summary of all virtual desktop sessions by Base OS.

Base OS	Count
Amazon Linux 2	2
Windows	1

Windows

Amazon Linu...

Project **4**

Summary of all virtual desktop sessions by Project Code.

Project Code	Count
project1	3

project1

Availability Zones **5**

Summary of all virtual desktop sessions by Availability Zone.

Availability Zone	Count
us-west-2a	3

us-west-2a

Software Stacks **6**

Summary of all virtual desktop sessions by Software Stack.

Software Stack	No. of Sessions
Amazon Linux 2 - x86_64	2
Windows - x86_64	1

No. of Sessions

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

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

Además, los administradores pueden:

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

Sesiones

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

RES > Virtual Desktops > Sessions

Sessions (2)

Virtual Desktop sessions for all users. End-users see these sessions as Virtual Desktops.

Created ▾ Last 1 month **1** **2** Actions ▾ Create Session **3**

Search **4** All States ▾ All Operating Systems ▾ < 1 > ⚙

<input type="checkbox"/>	Session Name ▾	Owner ▾	Base OS	Instance Ty...	State	Project	Created On
<input checked="" type="checkbox"/>	demoadmin1aml21 5	demoadmin1	Amazon Linux 2	m6a.large	ⓘ Stopped	project1	9/27/2023, 8:31:50 AM
<input type="checkbox"/>	demoadmin1windows1	demoadmin1	Windows	m6a.large	ⓘ Stopped	project1	9/27/2023, 8:38:23 AM

< 1 >

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

- c. Forzar la parada o hibernación de las sesiones
 - d. Finalizar sesión (s)
 - e. Forzar la finalización de la (s) sesión (s)
 - f. Salud de la (s) sesión (s)
 - g. Cree una pila de software
3. Elija Crear sesión para crear una sesión nueva.
 4. Busque una sesión por nombre y filtre por estado y sistema operativo.
 5. Elija el nombre de la sesión para ver más detalles.

Crear una sesión

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

Launch New Virtual Desktop



Session Name

Enter a name for the virtual desktop

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

User

Select the user to create the session for

Project

Select the project under which the session will get created

Operating System

Select the operating system for the virtual desktop

Software Stack

Select the software stack for your virtual desktop

Enable Instance Hibernation

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



Virtual Desktop Size

Select a virtual desktop instance type

Storage Size (GB)

Enter the storage size for your virtual desktop in GBs

Detalles de la sesión

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

RES > Virtual Desktop > Sessions > 8765705b-8919-48ba-901a-19e2c49cf043

Session: demoadmin1aml21

General Information

Session Name demoadmin1aml21	Owner demoadmin1	State ⓘ Stopped
---------------------------------	---------------------	--------------------

< **Details** | Server | Software Stack | Project | Permissions | Schedule | Monitoring | Session | >

Session Details

RES Session Id 8765705b-8919-48ba-901a-19e2c49cf043	DCV Session Id bd63e69a-e75a-427b-b4c8-39d7c43b95ad	Description -
Session Type VIRTUAL	Hibernation Enabled No	Created On 9/27/2023, 8:31:50 AM
Updated On 9/29/2023, 11:01:20 PM		

Pilas de software (AMI)

Note

Para ejecutar la pila de software CentOS7 proporcionada AWS GovCloud (US), tendrá que suscribirse a la AMI desde dentro AWS Marketplace mediante su cuenta [estándar vinculada](#).

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

The screenshot shows the 'Software Stacks' management interface. At the top, there is a breadcrumb trail: 'RES > Virtual Desktops > Software Stacks (AMIs)'. The main heading is 'Software Stacks' with a sub-heading 'Manage your Virtual Desktop Software Stacks'. A search bar is located on the left, and a dropdown menu for 'All Operating Systems' is on the right. A 'Register Software Stack' button is visible in the top right corner. The main content is a table with the following columns: Name, Description, AMI ID, Base OS, Root Volume Size, Min RAM, GPU Manufacturer, and Created On. The table lists various software stacks, including CentOS7, RHEL8, RHEL7, Ubuntu, Windows, and Amazon Linux 2, with their respective AMI IDs, base OS, root volume sizes, minimum RAM, GPU manufacturers, and creation dates.

Name	Description	AMI ID	Base OS	Root Volume Size	Min RAM	GPU Manufacturer	Created On
CentOS7 - ARM64	CentOS7 - ARM64	ami-07f692d95b2b9c8c5	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
CentOS7 - x86_64	CentOS7 - x86_64	ami-00f8e2c955f7ffa9b	CentOS 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
RHEL8 - x86_64	RHEL8 - x86_64	ami-0b530377951178d6b	RedHat Enterprise Linux 8	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
UBUNTU2204 - x86_64	UBUNTU2204 - x86_64	ami-073ffe13d826b7f8	Ubuntu 22.04	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
RHEL7 - x86_64	RHEL7 - x86_64	ami-0bb2449c2217cb9b0	RedHat Enterprise Linux 7	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
Windows - x86_64	Windows - x86_64	ami-0667133d0dc6089e1	Windows	30GB	4GB	N/A	6/7/2024, 11:25:19 AM
Windows - AMD	Windows - AMD	ami-05df91be1d294f195	Windows	30GB	4GB	AMD	6/7/2024, 11:25:20 AM
Windows - NVIDIA	Windows - NVIDIA	ami-00d7af9d003819a90	Windows	30GB	4GB	NVIDIA	6/7/2024, 11:25:20 AM
RHEL9 - x86_64	RHEL9 - x86_64	ami-099f85fc24d27c2a7	RedHat Enterprise Linux 9	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
Amazon Linux 2 - ARM64	Amazon Linux 2 - ARM64	ami-04ed2b27d86c17f09	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM
Amazon Linux 2 - x86_64	Amazon Linux 2 - x86_64	ami-0ee5c62243ab25259	Amazon Linux 2	10GB	4GB	N/A	6/7/2024, 11:25:19 AM

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

Register new Software Stack



Name

Enter a name for the software stack

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

Description

Enter a user friendly description for the software stack

AMI Id

Enter the AMI Id

AMI Id must start with ami-xxx

Operating System

Select the operating system for the software stack

GPU Manufacturer

Select the GPU Manufacturer for the software stack

Min. Storage Size (GB)

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

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

Projects

Select applicable projects for the software stack

Asigne una pila de software a un proyecto

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

Note

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

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

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

Software Stacks (9)

Manage your Virtual Desktop Software Stacks

Search

Update Software Stack: Amazon Linux 2 - ARM64

Stack Name
Enter a name for the Software Stack.
Amazon Linux 2 - ARM64
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
Amazon Linux 2 - ARM64

Projects
Select applicable projects for the software stack

Cancel Submit

Name	OS	AMI ID
Amazon Linux 2 - ARM64	Amazon Linux 2	
CentOS 7	OS 7	
CentOS 7	OS 7	
Windows	Windows	
RHEL8	Hat Enterprise Linu	
RHEL8	Hat Enterprise Linu	
Windows	Windows	
Amazon Linux 2	Amazon Linux 2	
Windows - AMD	Windows - AMD	ami-00f5db175bcde7485
Windows - AMD	Windows - AMD	ami-00f5db175bcde7485

Vea los detalles de la pila de software

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

Perfiles de permisos

Utilice los perfiles de permisos para crear y administrar perfiles reutilizables para los permisos.

Research and Engineering Studio

RES > Virtual Desktops > Permission Profiles

Permission Profiles

Manage your Virtual Desktop Permission Profiles

1

3 Actions Create Permission Profile

4

Profile ID	Title	Description	Created On
2 <input checked="" type="radio"/> observer_profile	View Only Profile	This profile grants view only access on the DCV Session. Can see screen only. Can not control session	10/3/2023, 2:27:32 PM
<input type="radio"/> admin_profile	Admin Profile	This profile grants the same access as the Admin on the DCV Session	10/3/2023, 2:27:32 PM
<input type="radio"/> collaborator_profile	Collaboration Profile	This profile grants certain access on the DCV Session. Can see screen, control mouse and keyboard.	10/3/2023, 2:27:32 PM
<input type="radio"/> owner_profile	Owner Profile	This profile grants the same access as the Session Owner on the DCV Session	10/3/2023, 2:27:32 PM

1. Busque un perfil de permisos.
2. Elija el ID del perfil para ver los detalles.
3. Cuando se selecciona un perfil, utilice el menú Acciones para editarlo.
4. Seleccione Crear perfil de permisos para crear un perfil nuevo.

Cree un perfil de permisos

1. Seleccione Crear perfil de permisos.
2. Introduzca los detalles del nuevo perfil y utilice los botones de permisos para seleccionar los permisos del perfil.
3. Seleccione Submit (Enviar).

Register new Permission Profile



Profile ID

Enter a Unique Profile ID for the Permission Profile

Title

Enter a user friendly Title for the Permission Profile

Description

Enter a user friendly description for the Permission Profile

Built In

All features

Display

Receive visual data from the NICE DCV server

Pointer

View NICE DCV server mouse position events and pointer shapes

Mouse

Input from the client mouse to the NICE DCV server

Keyboard

Input from the client keyboard to the NICE DCV server

Audio In

Send audio from the client to the NICE DCV server

Audio Out

Receive audio from the NICE DCV server to the client

Clipboard Copy

Copy data from the NICE DCV server to the client clipboard

Clipboard Paste

Copy data to the NICE DCV server from the client clipboard

File Upload

Upload files to the session storage

File Download

Download files from the session storage

USB

Use USB devices from the client

Printer

Create PDFs or XPS files from the NICE DCV server to the client

Smartcard

Read the smart card from the client

Stylus

Input from specialized USB devices, such as 3D pointing devices or graphic tablets

Keyboard SAS

Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well

Web Camera

Use the Web Camera connected to a client device in a session

Touch

Use native touch events from the client device

Screenshot

Save a screenshot of the remote desktop

Gamepad

Use gamepads connected to a client computer in a session

Unsupervised Access

Allow a user to connect to session without supervision

Cancel

Submit

Edite un perfil de permisos

1. Seleccione el perfil de permisos que necesita editar en la página de perfiles de permisos.
2. Elija Actions.
3. Seleccione Editar perfil de permisos.
4. Edite el perfil.
5. Seleccione Submit (Enviar).

Ver los detalles del perfil de permisos

En la lista de perfiles de permisos, elija el ID del perfil para ver los detalles. En la página de detalles, también puede seleccionar Editar para editar el perfil de permisos.

Debugging

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

The screenshot shows the NICE DCV Broker interface. On the left is a sidebar with navigation options: Home, Virtual Desktops, Shared Desktops, File Browser, SSH Access, ADMIN ZONE, eVDI (Dashboard, Sessions, Software Stacks (AMIs), Permission Profiles), Debug (Settings), and Settings. The main content area is titled "View hosts and sessions registered with NICE DCV Broker" and has two tabs: "VD Host" (selected) and "VD Sessions". The "VD Host" tab displays a JSON object representing a host configuration:

```

{
  "servers": [
    {
      "id": "aXAtMTAtMy0xNTctMTk0LmNvcnAucmVzLmNvbS0xMC4zLjE1Ny4xOTQ0tNmRmYjJmNWYyYTQ4NDYyN2E1MzgwZDU4YjIzM2I2Zjg="
      "ip": "10.3.157.194"
      "hostname": "ip-10-3-157-194.corp.res.com"
      "default_dns_name": "ip-10-3-157-194.corp.res.com"
      "port": null
      "endpoints": [
        {
          "port": 8443
        }
      ]
    }
  ]
}

```

Configuración de escritorio

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

- Tiempo de espera de inactividad de la sesión DCV
- Advertencia de tiempo de espera de inactividad

- Límite de utilización de la CPU
- Sesiones permitidas por usuario

The screenshot displays the configuration interface for the 'virtual-desktop-controller' module. The sidebar on the left provides navigation through sections like Home, ADMIN ZONE, eVDI, and Environment Management. The main panel shows the 'General' configuration tab, which includes settings for QUIC (Disabled), Subnet AutoRetry (Enabled), eVDI Subnets (listing two subnets: subnet-0706342f7d6fa0082 and subnet-023f50062d2b46030), and Randomize Subnets (Disabled). Below this, the 'OpenAPI Specification' section provides links to the eVDI API Spec and the Swagger Editor.

Gestión del entorno

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

Temas

- [Proyectos](#)
- [Usuarios](#)
- [Grupos](#)
- [Sistemas de archivos](#)
- [Estado del entorno](#)
- [Administración de instantáneas](#)
- [Configuración del entorno](#)

Proyectos

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

Temas

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

Vea los proyectos

Title	Project Code	Status	Budgets	Groups	Updated On
project-1	project-1	Enabled	--	• IDEAUsers	10/3/2023, 7:04:18 PM

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

1. Puedes usar el campo de búsqueda para buscar proyectos.
2. Cuando se selecciona un proyecto, puede utilizar el menú Acciones para:
 - a. Editar un proyecto
 - b. Habilitar o deshabilitar un proyecto
 - c. Actualizar las etiquetas del proyecto

3. Puede elegir Crear proyecto para crear un proyecto nuevo.

Crear un proyecto

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

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

Important

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

Para obtener información sobre las opciones avanzadas, consulte [Añadir una plantilla de lanzamiento](#).

3. (Opcional) Active los presupuestos del proyecto. Para obtener más información sobre los presupuestos, consulte [Supervisión y control de costes](#).
4. Asigne a los usuarios o grupos el rol apropiado («miembro del proyecto» o «propietario del proyecto»). Consulta [Permisos](#) las acciones que puede realizar cada rol.
5. Seleccione Submit (Enviar).

Create new Project

Project Definition

Title

Enter a user friendly project title

Project ID

Enter a project-id

Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (_), or periods (.). Must be between 3 and 40 characters long.

Description

Enter the project description

Do you want to enable budgets for this project?

Resource Configurations

Add file systems

Select applicable file systems for the Project

home [efs] X

Advanced Options

Team Configurations

Groups

Select applicable ldap groups for the Project

Add group**Role**

Choose a role for the group

Remove group**Users**

Select applicable users for the Project

Add user**Role**

Choose a role for the user

Remove user**Cancel****Submit**

Edit a project

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

Edit Project

Project Definition

Title
Enter a user friendly project title

Project ID
Enter a project-id

Project ID can only use lowercase alphabets, numbers, hyphens (-), underscores (_), or periods (.). Must be between 3 and 40 characters long.

Description
Enter the project description

Do you want to enable budgets for this project?

Resource Configurations

▼ **Advanced Options**

Add Policies
Select applicable policies for the Project

Add Security Groups
Select applicable security groups for the Project

► **Linux**

► **Windows**

Team Configurations

Groups Select applicable ldap groups for the Project	Role Choose a role for the group	<input type="button" value="Remove group"/>
<input type="text" value="group_1"/> <input type="button" value="Add group"/>	<input type="text" value="Project Member"/> <input type="button" value="Remove user"/>	
Users Select applicable users for the Project	Role Choose a role for the user	<input type="button" value="Remove user"/>
<input type="text" value="user1"/> <input type="button" value="Add user"/>	<input type="text" value="Project Member"/> <input type="button" value="Remove user"/>	

Añadir o eliminar etiquetas de un proyecto

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

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

Vea los sistemas de archivos asociados a un proyecto

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

The screenshot shows the 'Projects' management interface. At the top, there is a header with the title 'Projects' and the subtitle 'Environment Project Management'. On the right side of the header, there are buttons for 'Actions' and 'Create Project'. Below the header is a search bar with the placeholder text 'Search'. The main content area displays a table of projects with the following columns: Title, Project Code, Status, Budgets, Groups, and Updated On. A single project is listed with the title 'project-1', project code 'project-1', status 'Enabled', and updated on '10/3/2023, 9:06:30 PM'. Below the table, there is a panel titled 'File Systems in project-1' which is expanded to show a table with columns: Title, Name, File System ID, Mount Target, Projects, Scope, Provider, and Created through RES?. The table in this panel is currently empty, displaying 'No records'.

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: ///user/scripts/example.sh

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

▼ Linux

Run Script When VDI Starts
Scripts that execute at the start of a VDI

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="https://sample.samplecontent.com/sample"/>	<input type="text"/>		<input type="button" value="Remove Scripts"/>
<input type="text" value="file:///root/bootstrap/latest/launch/script"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

Run Script when VDI is Configured
Scripts that execute after RES configurations are completed

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

▼ Windows

Run Script When VDI Starts
Scripts that execute at the start of a VDI

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

Run Script when VDI is Configured
Scripts that execute after RES configurations are completed

Script	Arguments - optional	Info	
<input type="text" value="s3://sample-res-scripts/sample.sh"/>	<input type="text" value="1,2"/>		<input type="button" value="Remove Scripts"/>

Ejemplo de configuración de un proyecto

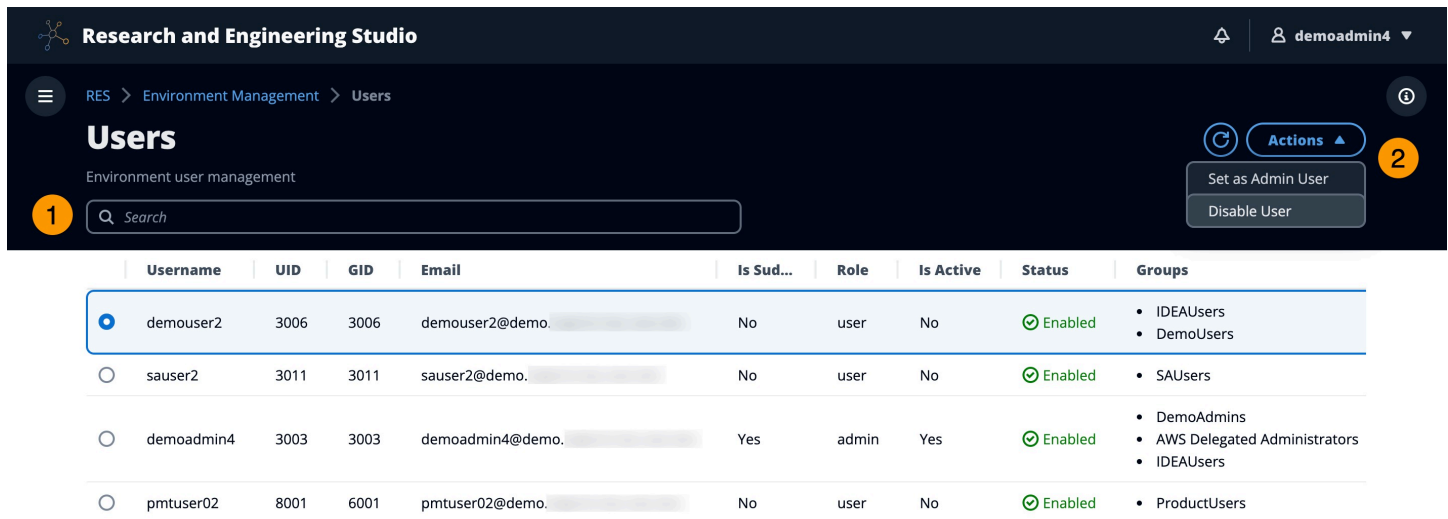
Usuarios

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

Note

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

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



Research and Engineering Studio demoadmin4

RES > Environment Management > Users

Users

Environment user management

1 Search

2 Actions

- Set as Admin User
- Disable User

	Username	UID	GID	Email	Is Sud...	Role	Is Active	Status	Groups
<input checked="" type="radio"/>	demouser2	3006	3006	demouser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> IDEAUsers DemoUsers
<input type="radio"/>	sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> SAUsers
<input type="radio"/>	demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> DemoAdmins AWS Delegated Administrators IDEAUsers
<input type="radio"/>	pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> ProductUsers

Desde la página de usuarios, puedes:

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

Grupos

Todos los grupos sincronizados desde el directorio activo aparecen en la página Grupos. Para obtener más información sobre la configuración y la administración de grupos, consulte la [Guía de configuración](#).

Research and Engineering Studio

RES > Environment Management > Groups

Groups

Environment user group management

1 Search

Title	Group Name	Type	Role	Status	GID
IDEAUsers	IDEAUsers	external	user	Enabled	4000
SAAAdmins	SAAAdmins	external	user	Enabled	3035
AWS Delegated Administrators	AWS Delegated Administrators	external	admin	Enabled	3999

2 Actions

Disable Group

3 Users in IDEAUsers

Username	UID	GID	Email	Is Sudo?	Role	Is Active	Status	Groups	Syn
demoadmin1	3000	3000	demoadmin1@demo...	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> DemoAdmins AWS Delegated Administrators IDEAUsers 	10/3
demoadmin4	3003	3003	demoadmin4@demo...	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> DemoAdmins AWS Delegated Administrators IDEAUsers SAAAdmins 	10/3

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.

Sistemas de archivos

Research and Engineering Studio

RES > Environment Management > File System

File Systems

Create and manage file systems for Virtual Desktops

1 Search

2 Actions

3 Onboard File System

4 Create File System

Add File System to Project

Remove File System from Project

Title	Name	File System ID	Scope	Provider
FSx ONTAP for Linux	fsx_01_linux	fs-0d2a998473da4bf80	project	fsx_netapp_ontap

Desde la página Sistemas de archivos, puede:

1. Buscar sistemas de archivos.
2. Cuando se selecciona un sistema de archivos, utilice el menú Acciones para:
 - a. Añadir el sistema de archivos a un proyecto
 - b. Elimine el sistema de archivos de un proyecto
3. Incorpore un nuevo sistema de archivos.
4. Cree un sistema de archivos.
5. Cuando se selecciona un sistema de archivos, puede expandir el panel de la parte inferior de la pantalla para ver los detalles del sistema de archivos.

Cree un sistema de archivos

1. Seleccione Crear sistema de archivos.
2. Introduzca los detalles del nuevo sistema de archivos.
3. Proporcione los ID de subred de la VPC. Puede encontrar los ID en la pestaña Administración del entorno > Configuración > Red.
4. Seleccione Submit (Enviar).

Create new File System



Title

Enter a user friendly file system title

Eg. EFS 01

Name

Enter a file system name

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

File System Provider

Select applicable file system type

Projects

Select applicable project



Subnet ID 1

Enter subnet id to create mount target

Subnet ID 2

Enter second subnet to create mount target

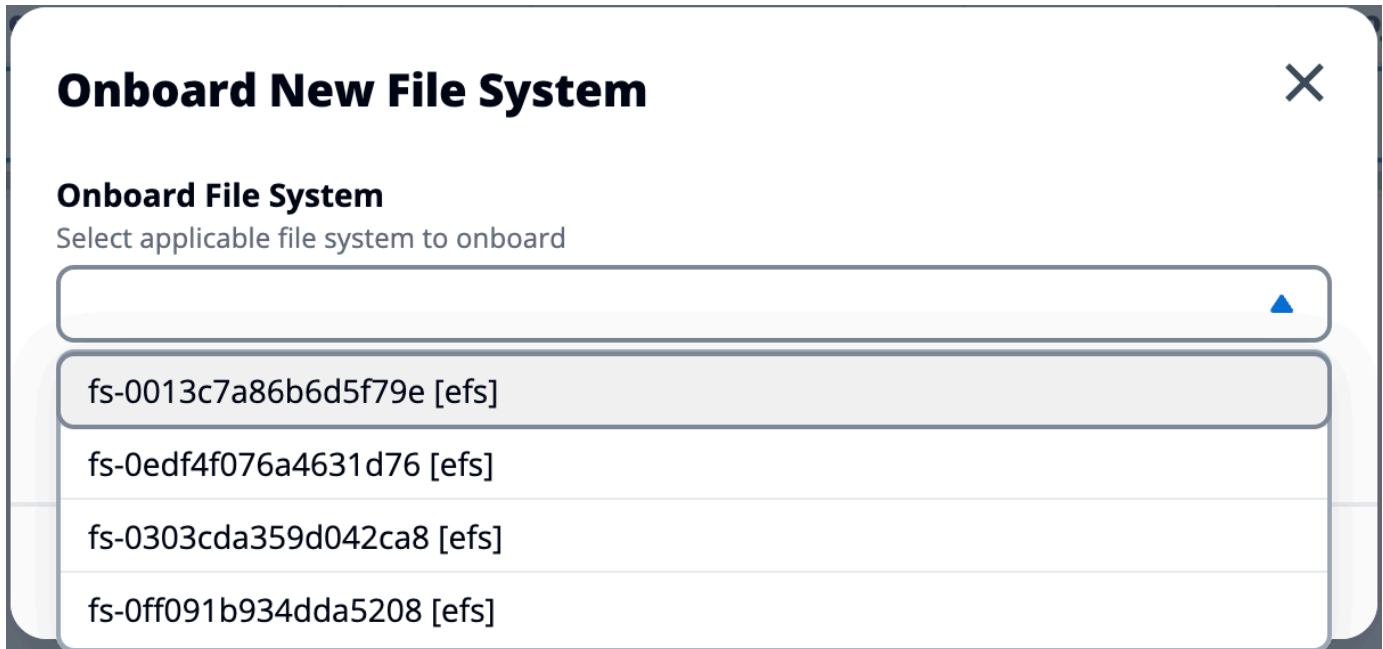
Subnet ID 1 and Subnet ID 2 should be in two different AZs

Mount Directory

Enter directory to mount the file system

Incorpore un sistema de archivos

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



3. Introduzca los detalles del sistema de archivos.
4. Seleccione Submit (Enviar).

Onboard New File System ✕

Onboard File System

Select applicable file system to onboard

fs-0edf4f076a4631d76 [efs] ▼



Title

Enter a user friendly file system title

File System Name

Enter a file system name

File System name cannot contain white spaces or special characters. Only use lowercase alphabets, numbers and underscore (_). Must be between 3 and 18 characters long.

Mount Directory

Enter directory to mount the file system

Mount directory cannot contain white spaces or special characters. Only use lowercase alphabets, numbers, and hyphens (-). Must be between 3 and 18 characters long. Eg. /efs-01

Cancel

Submit

Estado del entorno

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

Research and Engineering Studio
demoadmin4

RES > Environment Management > Status
i

Environment Status

View Environment Settings

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	2023.10	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10	App	Deployed	Healthy	• default
eVDI	vdc	2023.10	App	Deployed	Healthy	• default
Bastion Host	bastion-host	2023.10	Stack	Deployed	Not Applicable	• default

Infrastructure Hosts

Cluster hosts and status

Instance Name	Module ID	Node Type	Version	Instance Type	Availability Zone	Instance State	Private IP	Public IP
res-demo2-bastion-host	bastion-host	Infra	2023.10	m5.large	us-east-2a	Running	10.1.3.148	3.145.15
res-demo2-vdc-controller	vdc	App	2023.10	m5.large	us-east-2a	Running	10.1.129.105	-
res-demo2-vdc-broker	vdc	Infra	2023.10	m5.large	us-east-2b	Running	10.1.149.12	-
res-demo2-cluster-manager	cluster-manager	App	2023.10	m5.large	us-east-2b	Running	10.1.155.249	-
res-demo2-vdc-gateway	vdc	Infra	2023.10	m5.large	us-east-2b	Running	10.1.153.135	-

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.

The screenshot displays the 'Snapshot Management' interface. At the top, there is a breadcrumb trail: 'RES > Environment Management > Snapshot Management'. The main title is 'Snapshot Management'. Below this, there are two main sections: 'Created Snapshots' and 'Applied Snapshots'. Each section has a search bar, a table with columns 'S3 Bucket Name', 'Snapshot Path', 'Status', and 'Created On', and a 'No records' message. The 'Created Snapshots' section has a 'Create Snapshot' button, and the 'Applied Snapshots' section has an 'Apply Snapshot' button. Numbered callouts (1-4) highlight the search bar, the 'Create Snapshot' button, the 'Applied Snapshots' title, and the 'Apply Snapshot' button respectively.

RES > Environment Management > Snapshot Management

Created Snapshots

Snapshots created from the environment

Search

S3 Bucket Name	Snapshot Path	Status	Created On
No records			

Create Snapshot

Applied Snapshots

Snapshots applied to the environment

Search

S3 Bucket Name	Snapshot Path	Status	Created On
No records			

Apply Snapshot

Desde la página de administración de instantáneas, puede:

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

Crear una instantánea

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

Note

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

Para añadir permisos al depósito:

1. Elige el depósito que has creado en la lista de depósitos.
2. Elija la pestaña Permisos.
3. En Política de bucket, elija Editar.
4. Agrega la siguiente declaración a la política de cubos. Reemplace estos valores por sus propios valores:
 - AWS_ACCOUNT_ID
 - RES_ENVIRONMENT_NAME
 - AWS_REGION
 - S3_BUCKET_NAME

Important

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

```
{  
  "Version": "2012-10-17",
```

```

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

```

Para crear la instantánea:

1. Elija Create Snapshot (Crear instantánea).
2. Introduzca el nombre del bucket de Amazon S3 que creó.

- Introduzca la ruta en la que desea almacenar la instantánea en el depósito. Por ejemplo, **october2023/23**.
- Seleccione Submit (Enviar).

Create New Snapshot ✕

S3 Bucket Name
Enter the name of an existing S3 bucket where the snapshot should be stored.

S3 bucket name can only contain lowercase alphabets, numbers, dots (.), and hyphens (-).

Snapshot Path
Enter a path at which the snapshot should be stored in the provided S3 bucket.

Snapshot path can only contain forward slashes, dots (.), exclamations (!), asterisks (*), single quotes ('), parentheses (), and hyphens (-).

Cancel **Submit**

- 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. Elige el depósito que has creado en la lista de depósitos.
2. Elija la pestaña Permisos.
3. En Política de bucket, elija Editar.
4. Agrega la siguiente declaración a la política de cubos. Reemplace estos valores por sus propios valores:
 - `AWS_ACCOUNT_ID`
 - `RES_ENVIRONMENT_NAME`
 - `AWS_REGION`
 - `S3_BUCKET_NAME`

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

```
    },
    "Action": [
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::{S3_BUCKET_NAME}",
      "arn:aws:s3:::{S3_BUCKET_NAME}/*"
    ]
  },
  {
    "Sid": "AllowSSLRequestsOnly",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::{S3_BUCKET_NAME}",
      "arn:aws:s3:::{S3_BUCKET_NAME}/*"
    ],
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    },
    "Principal": "*"
  }
]
}
```

Para aplicar una instantánea:

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

Apply a Snapshot ✕

S3 Bucket Name
Enter the name of the S3 bucket where the snapshot to be applied is stored.

S3 bucket name can only contain lowercase alphabets, numbers, dots (.), and hyphens (-).

Snapshot Path
Enter the path at which the snapshot to be applied is stored in the provided S3 bucket.

Snapshot path can only contain forward slashes, dots (.), exclamations (!), asterisks (*), single quotes ('), parentheses (), and hyphens (-).

Cancel **Submit**

5. Después de cinco a diez minutos, seleccione Actualizar en la página de administración de instantáneas para comprobar el estado.

Configuración del entorno

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

- General

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

- Proveedor de identidad

Muestra información como el estado del inicio de sesión 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.

The screenshot displays the 'Environment Settings' page in the Research and Engineering Studio. The page is titled 'Environment Settings' and includes a 'View Environment Status' button. The settings are organized into several sections:

- Environment Overview:**
 - Environment Name: res-demo2
 - AWS Region: us-east-2
 - S3 Bucket: res-demo2-cluster-us-east-2-930513735672
- Navigation Tabs:** General (selected), Network, Identity Provider, Directory Service, Analytics, Metrics, CloudWatch Logs, SES, EC2, Bi.
- General Settings:**
 - Administrator Username: clusteradmin
 - Administrator Email: [redacted]
 - Home Directory: /internal/res-demo2
 - Locale: en_US
 - Timezone: America/New_York
 - Default Encoding: utf-8
- Web Portal:**
 - Title: Research and Engineering Studio
 - Subtitle: -
 - Copyright Text: Copyright {year} Amazon Inc. or its affiliates. All Rights Reserved.
- OpenAPI Specification:**
 - Environment Manager API Spec: <https://res.demo.ingenio.hpc.aws.dev/cluster-manager/api/v1/openapi.yml>
 - Swagger Editor: <https://editor.swagger.io/?url=https://res.demo.ingenio.hpc.aws.dev/cluster-manager/api/v1/openapi.yml>

Administración de secretos

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

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

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

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

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

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

Supervisión y control de costes

Note

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

Recomendamos crear un [presupuesto](#) a través de [AWS Cost Explorer](#) para ayudar a administrar los costos. Los precios están sujetos a cambios. Para obtener más información, consulte la página web de precios de cada uno de los [the section called “AWSservicios 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 AWS Management Console y abra la AWS Billing consola en <https://console.aws.amazon.com/billing/>.
2. Elija las etiquetas de asignación de costes.
3. Busque y seleccione las `res:EnvironmentName` etiquetas `res:Project` y.
4. Seleccione Activar.

Billing ×

Home

▼ Billing

Bills

Payments

Credits

Purchase orders

Cost & usage reports

Cost categories

Cost allocation tags 2

Free tier

Billing Conductor

▼ Cost Management

Cost explorer

Budgets

Budgets reports

Savings Plans

▼ Preferences

Billing preferences

Payment preferences

Consolidated billing

Tax settings

▼ Permissions

Affected entities

Cost allocation tags info

Cost allocation tags activated: 3

Download CSV

User-defined cost allocation tags | AWS generated cost allocation tags

User-defined cost allocation tags (2/47) info

Undo Deactivate Activate

Find cost allocation tags 11 matches

res Clear filters

Tag key	Status	Last updated date	Last used month
<input type="checkbox"/> res:BackupPlan	Inactive	-	November 2023
<input type="checkbox"/> res:ClusterName	Inactive	-	November 2023
<input type="checkbox"/> res:DCVSessionUUID	Inactive	-	November 2023
<input type="checkbox"/> res:EndpointName	Inactive	-	November 2023
<input checked="" type="checkbox"/> res:EnvironmentName 3	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleId	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleName	Inactive	-	November 2023
<input type="checkbox"/> res:ModuleVersion	Inactive	-	November 2023
<input type="checkbox"/> res:NodeType	Inactive	-	November 2023
<input checked="" type="checkbox"/> res:Project	Inactive	-	November 2023

Note

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

Para crear un presupuesto para los recursos de RES:

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

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

Note

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

12. En Valores, seleccione el nombre del proyecto.

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

Budget scope [Info](#)

Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget

Scope options

All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope

Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.

Filters [Info](#)

Remove all

Dimension

Tag

Tag

res:Project

Values

Filter tags by values

project1 X

Cancel

Apply filter

Add filter

▼ Advanced options

Aggregate costs by

Unblended costs

Supported charge types

Upfront reservation fees X

Recurring reservation charges X

Other subscription costs X

Taxes X

Support charges X

Discounts X

Cancel

Previous

Next

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

Ahora que se ha creado el presupuesto, puede activar el presupuesto para los proyectos. Para activar los presupuestos de un proyecto, consulte [the 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.

The screenshot shows the 'Projects' page in the RES Environment Management console. The page has a dark header with 'Projects' and 'Create Project' button. Below the header is a search bar and a table with the following columns: Title, Project Code, Status, Budgets, Groups, and Updated On. A single row is visible for 'project1' with status 'Enabled'. A 'Budget Exceeded' warning is shown in the Budgets column, indicating 'Actual Spend for budget: RES1-Project1-Budget1' and 'Limit: 500.00 USD, Forecasted: 3945.34 USD'. The Groups column lists 'DemoUsers', 'DemoAdmins', and 'ProductUsers'. The Updated On date is '10/31/2023, 12:44:12 PM'.

Title	Project Code	Status	Budgets	Groups	Updated On
project1	project1	Enabled	Actual Spend for budget: RES1-Project1-Budget1 Limit: 500.00 USD, Forecasted: 3945.34 USD Budget Exceeded	<ul style="list-style-type: none"> DemoUsers DemoAdmins ProductUsers 	10/31/2023, 12:44:12 PM

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.

Permisos

	Miembro del proyecto	Propietario del proyecto	Administrador global	Ámbito
Agregue usuarios como miembros o		X	X	Propietario del proyecto: proyectos de su propiedad

	Miembro del proyecto	Propietario del proyecto	Administrador global	Ámbito
propietarios del proyecto				Administrador global: cualquier proyecto
Agregue grupos como miembro o propietario del proyecto		X	X	Propietario del proyecto: proyectos de su propiedad Administrador global: cualquier proyecto
Eliminar usuarios		X	X	Propietario del proyecto: proyectos de su propiedad Administrador global: cualquier proyecto
Eliminación de grupos		X	X	Propietario del proyecto: proyectos de su propiedad Administrador global: cualquier proyecto

	Miembro del proyecto	Propietario del proyecto	Administrador global	Ámbito
Iniciar o detener instancias de VDI	X	X	X	Miembro del proyecto/ propietario del proyecto: instancias de VDI que poseen cuando forman parte de un proyecto. Administrador global: cualquier instancia de VDI.

Usa el producto

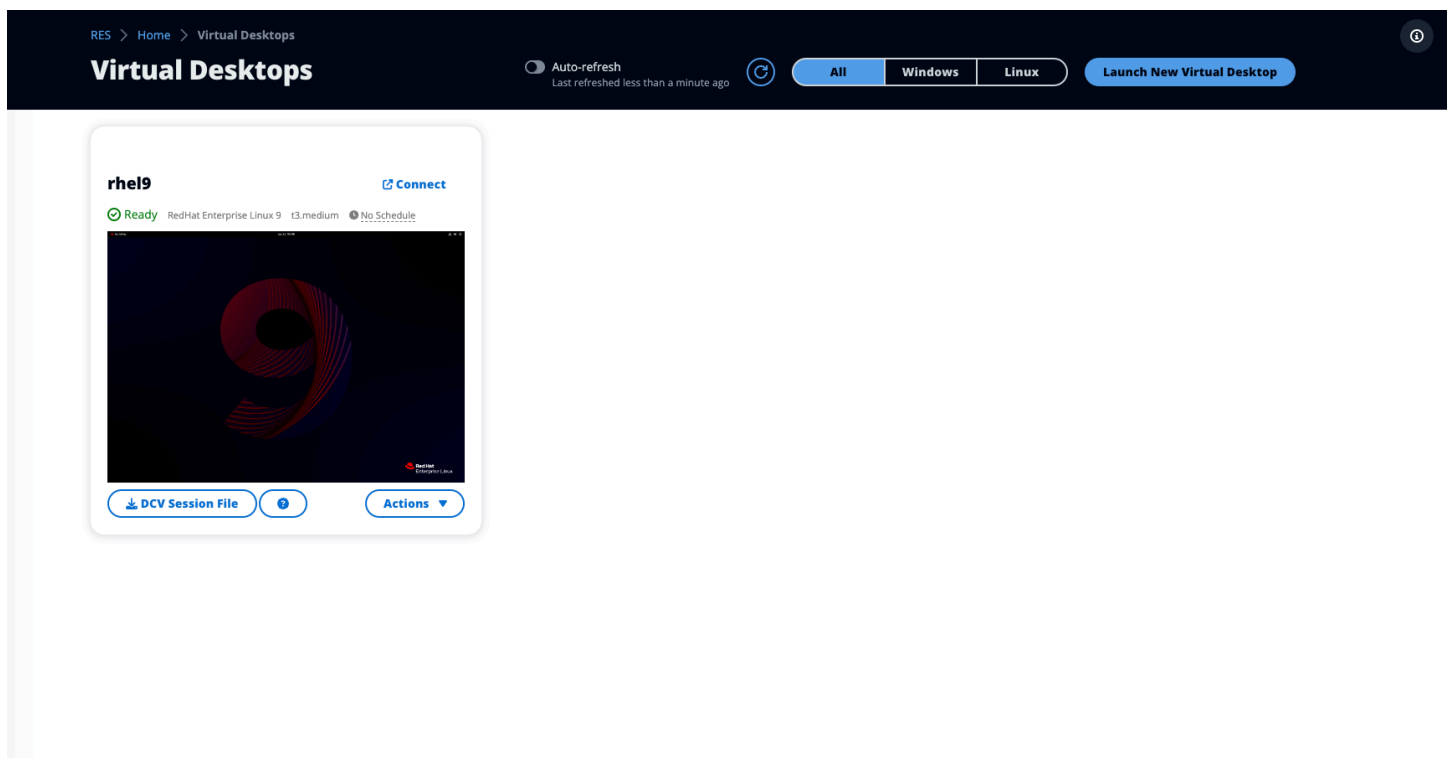
En esta sección se ofrece orientación a los usuarios sobre el uso de escritorios virtuales para colaborar con otros usuarios.

Temas

- [Escritorios virtuales](#)
- [Escritorios compartidos](#)
- [Explorador de archivos](#)
- [Acceso mediante SSH](#)

Escritorios virtuales

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



Sistemas operativos compatibles

Note

Actualmente, está previsto que CentOS 7 llegue end-of-life el 30 de junio de 2024. La versión 2024.06 de Research and Engineering Studio será la última versión compatible con CentOS 7.

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

- Amazon Linux 2 (x86 y ARM64)
- Centos 7 (x86 y ARM64)
- RHEL 7 (x86), 8 (x86) y 9 (x86)
- Ubuntu 22.04.03 (x86)
- Windows 2019, 2022 (x86)

Lanza un escritorio nuevo

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

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

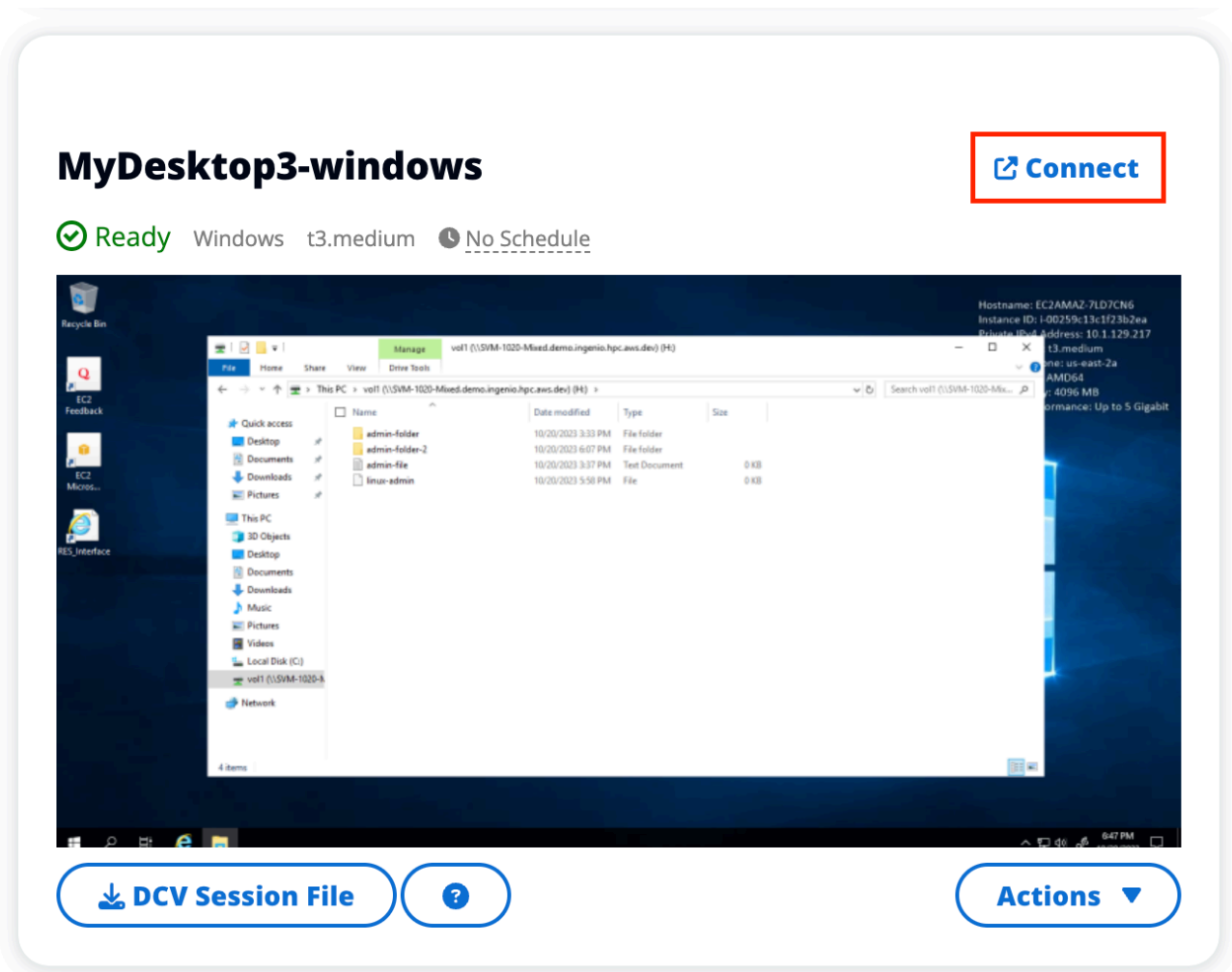
Acceda a su escritorio

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

Web connection

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

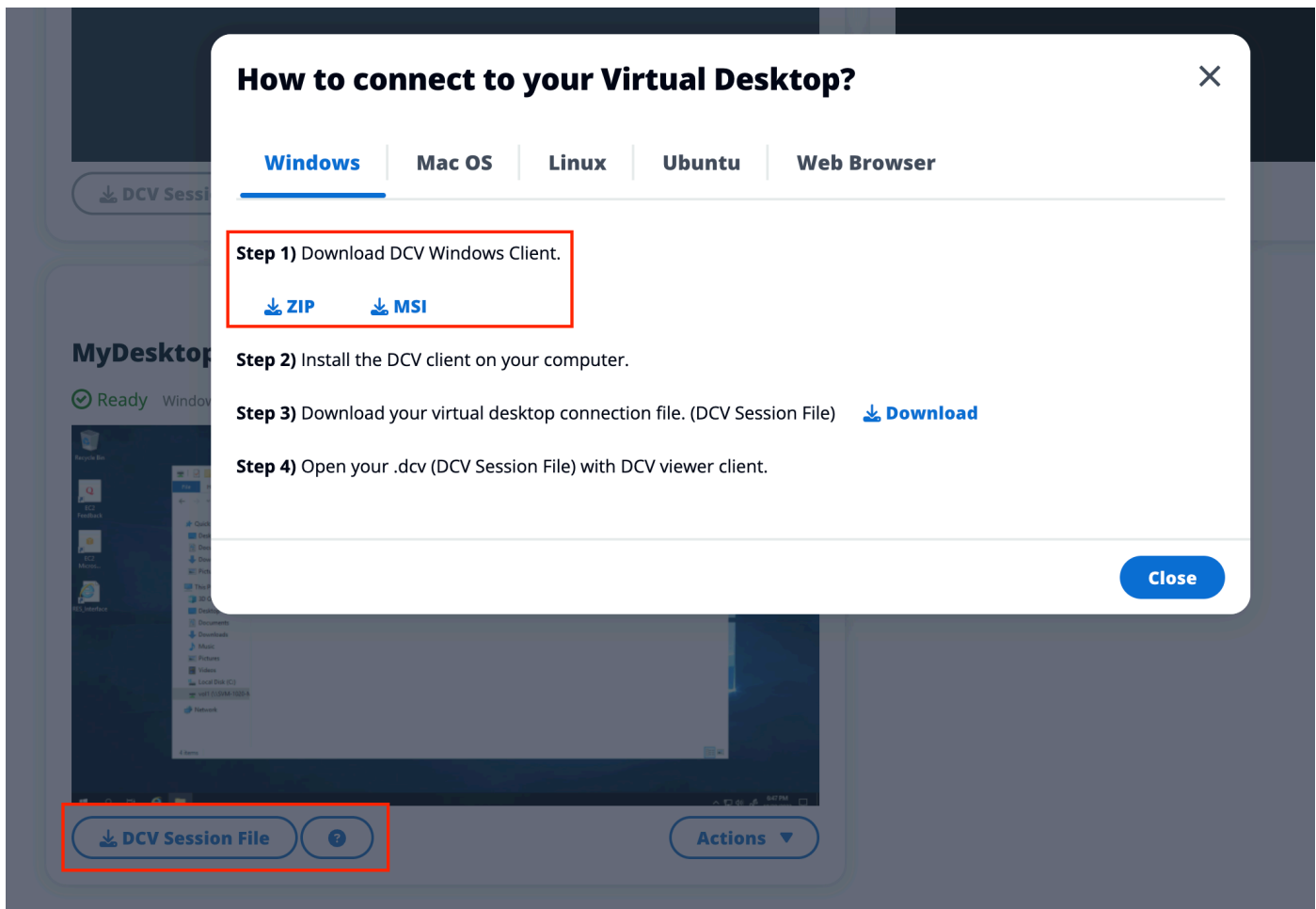
- Selecciona Connect o elige la miniatura para acceder al escritorio directamente a través del navegador.



DCV connection

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

1. Elija el archivo de sesión DCV para descargar el. dcvarchivo. 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 Actions.
2. Elija el estado del escritorio virtual. Puede elegir entre cuatro estados:

- Detener

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

- Reiniciar

Reinicia la sesión actual.

- Finalizar

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


- Hibernar

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

Modifica un escritorio virtual

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

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

 Note

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

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

Recupere la información de la sesión

1. Elija Actions.
2. Selecciona Mostrar información.


Programe escritorios virtuales

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

1. Elija Actions.
2. Elija Schedule.
3. Establece tu horario para cada día.
4. Seleccione Guardar.

Schedule for windows-session ✕

Setup a schedule to start/stop your virtual desktop to save and manage costs. The schedule operates at the cluster timezone setup by your cluster administrator.

 **Cluster Time: October 20, 2023 4:32 PM (America/New_York)**

Monday

No Schedule 

Working Hours (09:00 - 17:00)

Stop All Day

Start All Day

Custom Schedule

No Schedule 

Thursday

No Schedule 

Friday

No Schedule 

Saturday

Stop All Day 

Sunday

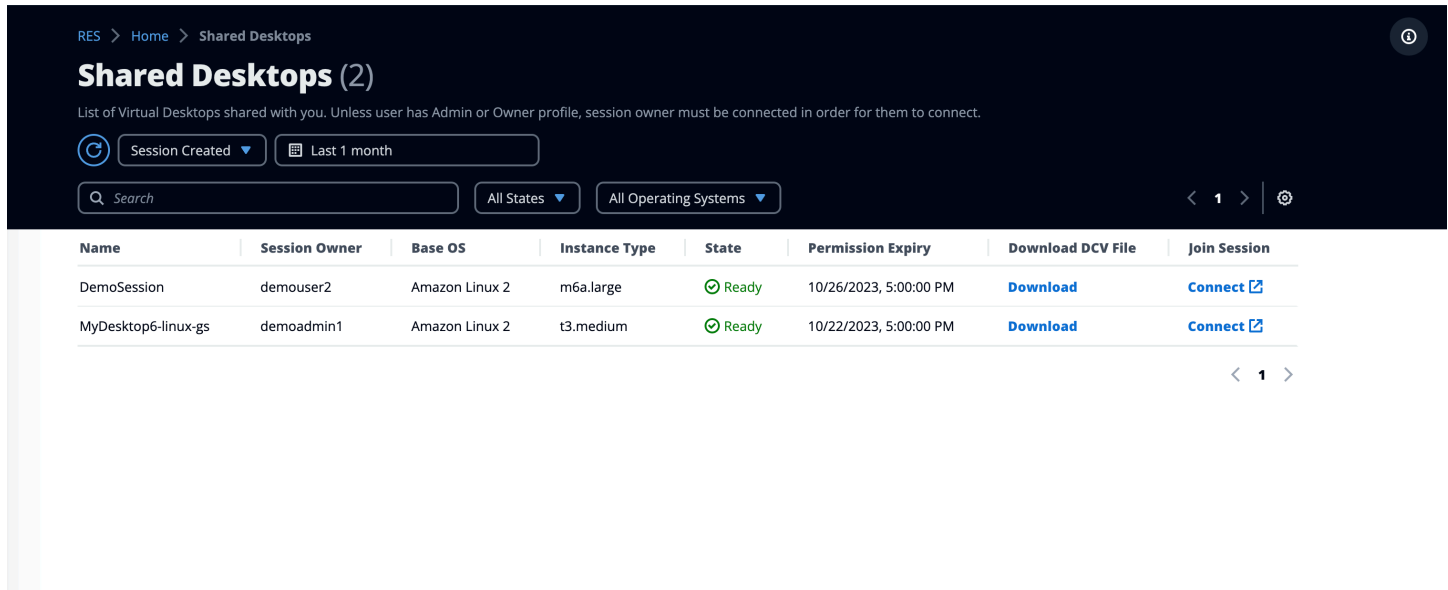
Stop All Day 

Cancel

Save

Escritorios compartidos

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



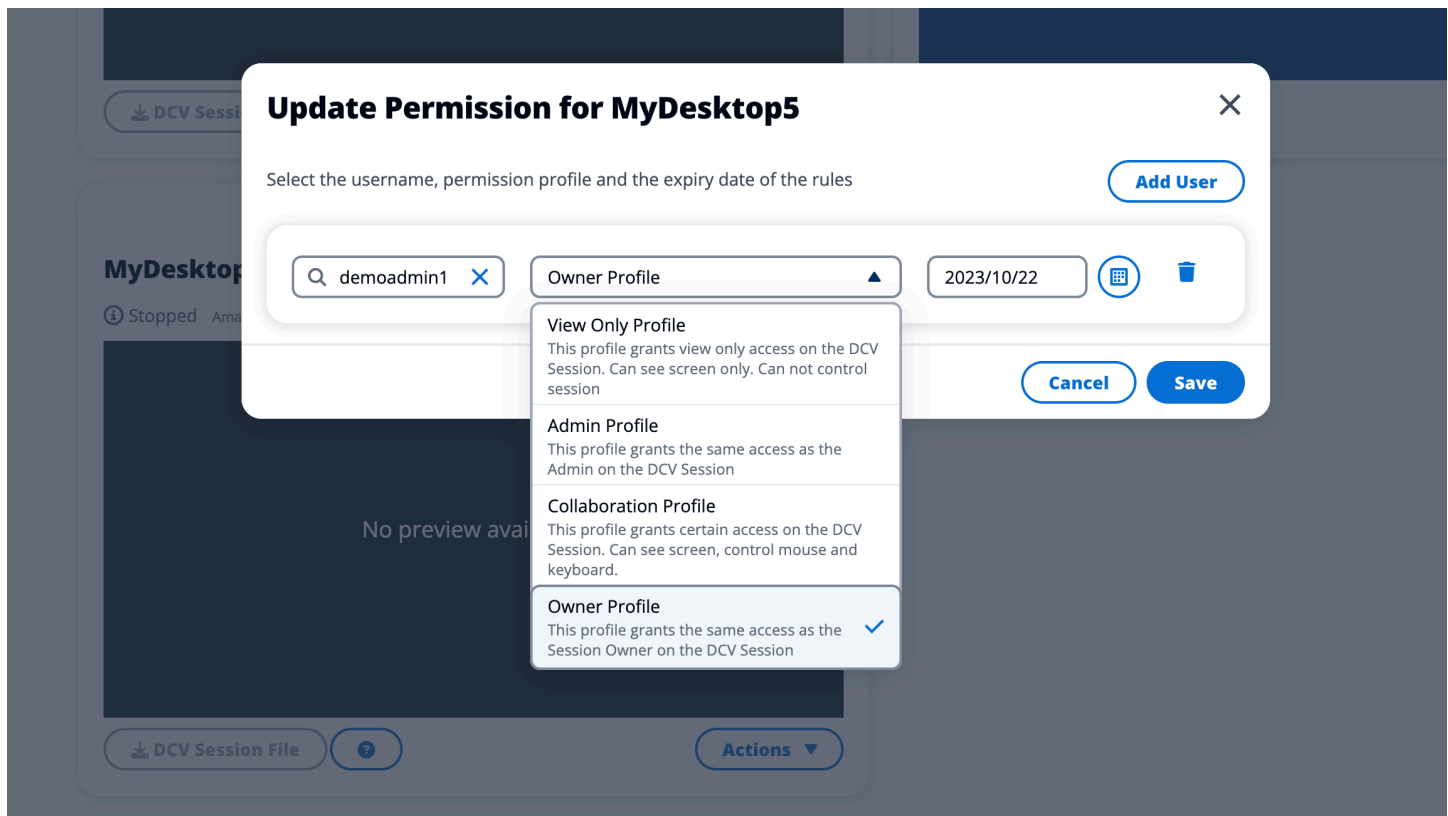
The screenshot shows the 'Shared Desktops' interface. At the top, there is a breadcrumb trail: 'RES > Home > Shared Desktops'. The main heading is 'Shared Desktops (2)'. Below the heading, a note states: 'List of Virtual Desktops shared with you. Unless user has Admin or Owner profile, session owner must be connected in order for them to connect.' There are filters for 'Session Created' (set to 'Last 1 month') and a search bar. Below the filters, there are dropdowns for 'All States' and 'All Operating Systems'. The main content is a table with the following data:

Name	Session Owner	Base OS	Instance Type	State	Permission Expiry	Download DCV File	Join Session
DemoSession	demouser2	Amazon Linux 2	m6a.large	Ready	10/26/2023, 5:00:00 PM	Download	Connect
MyDesktop6-linux-gs	demoadmin1	Amazon Linux 2	t3.medium	Ready	10/22/2023, 5:00:00 PM	Download	Connect

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

Comparte un escritorio

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



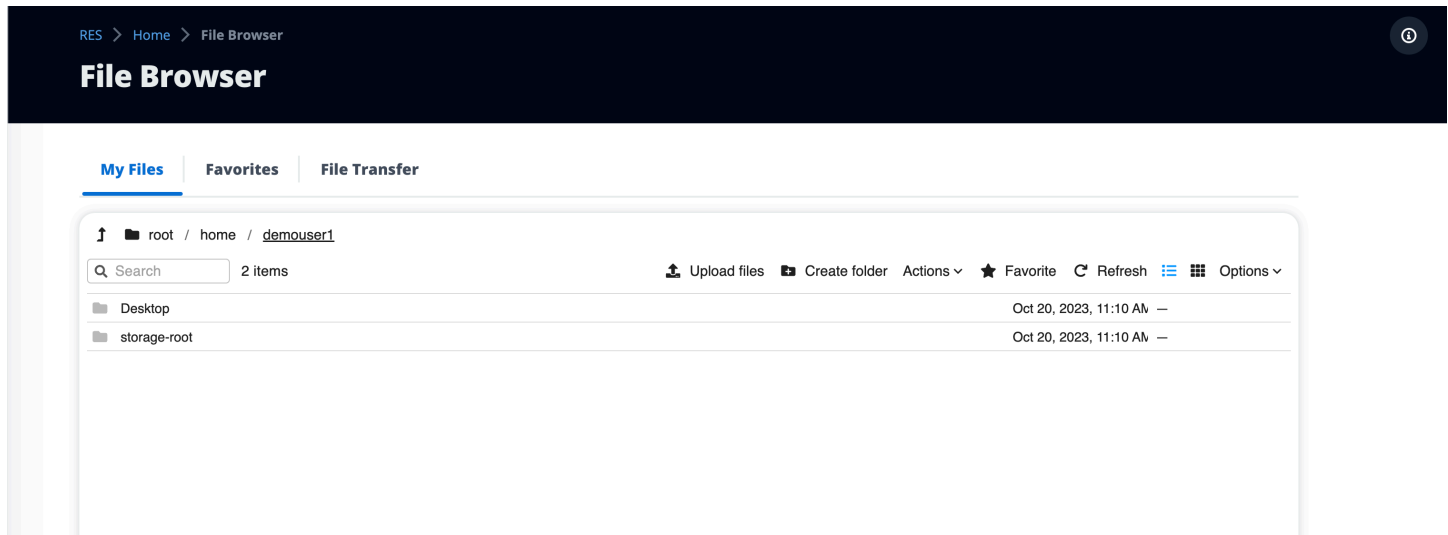
Para obtener más información sobre los permisos, consulte [the section called “Perfiles de permisos”](#).

Acceda a un escritorio compartido

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

Explorador de archivos

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



Cargar archivo (s)

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

Eliminar archivo (s)

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

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

Administra los favoritos

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

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

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

Note

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

Edita archivos

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

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

Transferencia de archivos

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

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

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 [Redacted]	Port [Redacted]
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 [Redacted]. Check "Always Trust this Host" and Click "Ok".

Once connected, simply drag & drop to upload/download files.

Acceso mediante SSH

Para usar SSH para acceder al host del bastión:

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

Solución de problemas

Este documento contiene información sobre cómo monitorear el sistema y cómo solucionar problemas específicos que puedan ocurrir. Si no puede encontrar la solución a un problema, puede encontrar otros [temas de solución de problemas en GitHub](#).

Temas

- [Problemas de instalación](#)
- [Problemas de administración de identidad](#)

Problemas de instalación

Temas

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

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

Para identificar el problema, examine el grupo de CloudWatch registros de Amazon denominado <stack-name> -

InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce> - <nonce>. Si hay varios grupos de registros con el mismo nombre, examine el primero 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 recibe la notificación por correo electrónico después de que las AWS CloudFormation pilas se hayan creado correctamente

Si no se recibió una invitación por correo electrónico después de AWS CloudFormation crearla correctamente, 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 cuyo <envname> prefijo aparece como terminado y, a continuación, se sustituyen por una nueva instancia, es posible que haya un problema con la configuración de la red o de Active Directory.

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

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

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

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

Instancias cíclicas o controladora de vdc en estado fallido

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

Para comprobar el problema:

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

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

```
[root@ip-... ]# systemctl status sssd
● sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-14 12:12:19 UTC; 1 weeks 0 days ago
 Main PID: 31248 (sss)           Might see "inactive"/"failed" here
   CGroup: /system.slice/sss.service
           └─31248 /usr/sbin/sss -i --logger=files
             └─31249 /usr/libexec/sss/sss_be --domain corp.res.com --uid 0 --gid 0 --logger=files
               └─31251 /usr/libexec/sss/sss_nss --uid 0 --gid 0 --logger=files
                 └─31252 /usr/libexec/sss/sss_pam --uid 0 --gid 0 --logger=files

Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
```

Might see errors highlighted in RED here

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 podría ser 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, significa que 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 se muestran los registros `Invalid credentials`, es posible que la ServiceAccount contraseña introducida durante la creación de la pila sea incorrecta.

1. Desde la AWS consola, abre Secrets Manager.
2. Busque la opción `directoryserviceServiceAccountPassword`. El secreto debería ser `[stack name]-directoryservice-ServiceAccountPassword`.
3. Abre el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y selecciona Texto sin formato.
4. Si ha olvidado la contraseña o no está seguro de si es correcta, puede restablecerla en Active Directory y Secrets Manager.
 - a. Para restablecer la contraseña en AWS Managed Microsoft AD:
 - i. Abra la AWS consola y vaya a AWS Directory Service.
 - ii. Seleccione el ID de directorio para su directorio RES y elija Acciones.
 - iii. Elija Restablecer la contraseña de usuario.
 - iv. Introduzca el ServiceAccount nombre de usuario.
 - v. Introduce una contraseña nueva y selecciona Restablecer contraseña.
 - b. Para restablecer la contraseña en Secrets Manager:

- i. Abre la AWS consola y ve a Secrets Manager.
 - ii. Busque la opción `directoryserviceServiceAccountPassword`. El secreto debería ser `[stack name]-directoryservice-ServiceAccountPassword`.
 - iii. Abre el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y selecciona Texto sin formato.
 - iv. Elija Editar.
 - v. Establece una nueva contraseña para el ServiceAccount usuario y selecciona Guardar.
5. Si el valor se actualizó, 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 subred o grupo de seguridad creado por RES 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 en la creación de 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 ejecución de SSM RunCommand /Automation, compruebe si la 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 identidad

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

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

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

Temas

- [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](#)
- [El usuario no estaba disponible al crear una sesión](#)
- [Se ha superado el límite de tamaño: error en el registro del administrador del CloudWatch clúster](#)

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 CloudWatch consola en <https://console.aws.amazon.com/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 en <https://console.aws.amazon.com/dynamodb/>.
2. En Tablas, busque la tabla denominada *<environment-name>*.cluster-settings.
3. Abra 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. Elija 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.

Edit item

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#)

Attributes

Attribute name	Value
key - Partition key	identity-provider.cognito.sso_enabled
value	<input type="radio"/> True <input checked="" type="radio"/> 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 recibe el error «Usuario no encontrado» al iniciar sesión en la interfaz RES, el usuario está presente en Active Directory, pero no en RES. Si ha agregado recientemente el usuario a AD, es posible que 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. [the section called “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 [the section called “Configurar tu proveedor de identidad para el inicio de sesión único \(SSO\)”](#).
2. Asegúrese de que tanto el asunto SAML como el correo electrónico SAML coincidan con la dirección de correo electrónico del usuario.

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

Si ha agregado un usuario a Active Directory pero no aparece en RES, debe activarse la sincronización de AD. La sincronización de AD se realiza cada hora mediante una función Lambda para importar las entradas de AD al entorno RES. En ocasiones, se produce un retraso hasta que se ejecute el siguiente proceso de sincronización tras 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 en <https://console.aws.amazon.com/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 a la de todas las llamadas en un plazo de cinco minutos o se ignorará la solicitud.

El usuario no estaba disponible al crear una sesión

Si es un administrador que está creando una sesión, pero descubre que un usuario que está en Active Directory no está disponible al crear una sesión, es posible que el usuario tenga que iniciar sesión por primera vez. Las sesiones solo se pueden crear para usuarios activos. Los usuarios activos deben iniciar sesión en el entorno al menos una vez.

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

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

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

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](#), lo que permite el acceso remoto a 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 archivo ChangeLog.md del repositorio. GitHub](#)

Date	Cambio
Noviembre de 2023	Versión inicial
Diciembre de 2023	GovCloud instrucciones y plantillas añadidas
Enero de 2024	Versión de lanzamiento 2024.01
Febrero de 2024	Versión de lanzamiento 2024.01.01: plantilla de despliegue actualizada
Marzo de 2024	Temas adicionales de solución de problemas : conservación de CloudWatch registros y desinstalación de versiones secundarias
Abril de 2024	Versión de lanzamiento 2024.04: plantillas de lanzamiento de proyectos y AMI preparadas para RES
Junio de 2024	<ul style="list-style-type: none">• Versión de lanzamiento 2024.06: compatibilidad con Ubuntu, permisos para el propietario del proyecto.• Guía del usuario: añadida Cree un entorno de demostración

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