



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
AWS servicios de este producto .....	7
Entorno de demostración .....	11
Cree una pila de demostración con un solo clic .....	11
Requisitos previos .....	11
Cree recursos e introduzca parámetros .....	12
Pasos posteriores a la implementación .....	14
Planificación de la implementación .....	15
Costo .....	15
Seguridad .....	15
IAMroles .....	16
Grupos de seguridad .....	16
Cifrado de datos .....	16
Consideraciones de seguridad del producto .....	17
Cuotas .....	20
Cuotas para AWS los servicios de este producto .....	20
AWS CloudFormation cuotas .....	21
Planificar la resiliencia .....	21
Soportado Regiones de AWS .....	21
Implemente el producto .....	24
Requisitos previos .....	24
Crear una Cuenta de AWS con un usuario administrativo .....	25
Crea un par de EC2 SSH claves de Amazon .....	25
Aumentar las cuotas de servicio .....	25
Crea un dominio público (opcional) .....	26
Crear dominio (GovCloud solo) .....	26
Proporcione recursos externos .....	27
Configure LDAPS en su entorno (opcional) .....	28
Configurar un privado VPC (opcional) .....	28
Crea recursos externos .....	40

Paso 1: lanza el producto .....	46
Paso 2: Inicia sesión por primera vez .....	55
Actualice el producto .....	57
Actualizaciones de versiones principales .....	57
Actualizaciones de versiones menores .....	57
Desinstale el producto .....	59
Usando el AWS Management Console .....	59
Usando AWS Command Line Interface .....	59
Eliminar el shared-storage-security-group .....	59
Eliminar los buckets de Amazon S3 .....	60
Guía de configuración .....	61
Administrar usuarios y grupos .....	61
Configuración SSO con Identity Center IAM .....	61
Configurar su proveedor de identidad para SSO .....	65
Establecer contraseñas para los usuarios .....	75
Crear subdominios .....	75
Crea un ACM certificado .....	76
Amazon CloudWatch Logs .....	77
Establecer límites de permisos personalizados .....	79
Preparado para la configuración RES AMIs .....	83
Prepare IAM el rol para acceder al RES entorno .....	83
Componente Create EC2 Image Builder .....	85
Prepara tu receta EC2 de Image Builder .....	89
Configurar EC2 la infraestructura de Image Builder .....	91
Configurar la canalización de imágenes de Image Builder .....	92
Ejecute la canalización de imágenes de Image Builder .....	93
Registre una nueva pila de software en RES .....	93
Guía del administrador .....	94
Administración de secretos .....	94
Supervisión y control de costes .....	97
Administración de sesiones .....	102
Panel de control .....	104
Sesiones .....	105
Pilas de software () AMIs .....	108
Debugging .....	112
Configuración de escritorio .....	113

Gestión del entorno .....	114
Estado del entorno .....	115
Configuración del entorno .....	116
Usuarios .....	117
Grupos .....	118
Proyectos .....	119
Política de permisos .....	126
Sistemas de archivos .....	141
Administración de instantáneas .....	146
Buckets de Amazon S3 .....	152
Usa el producto .....	169
SSHacceso .....	169
Escritorios virtuales .....	169
Lanza un escritorio nuevo .....	170
Acceda a su escritorio .....	171
Controle el estado de su escritorio .....	173
Modificar un escritorio virtual .....	175
Recupera la información de la sesión .....	176
Programe escritorios virtuales .....	176
VDIparada automática .....	179
Escritorios compartidos .....	181
Comparte un escritorio .....	181
Accede a un escritorio compartido .....	183
Explorador de archivos .....	183
Cargar archivo (s) .....	184
Eliminar archivo (s) .....	184
Administra los favoritos .....	185
Editar archivos .....	185
Transferencia de archivos .....	186
Resolución de problemas .....	188
Depuración y supervisión generales .....	191
Fuentes útiles de información sobre registros y eventos .....	192
Apariencia típica de Amazon EC2 Console .....	196
DCVDepuración de Windows .....	198
Encuentra información sobre DCV la versión de Amazon .....	199
Problema RunBooks .....	199

---

Problemas de instalación .....	201
Problemas de gestión de identidad .....	211
Almacenamiento .....	215
Instantáneas .....	220
Infraestructura .....	221
Lanzamiento de escritorios virtuales .....	222
Componente de escritorio virtual .....	227
Eliminación de Env .....	234
Entorno de demostración .....	241
Problemas conocidos .....	242
Problemas conocidos de la versión 2024.x .....	243
Avisos .....	261
Revisiones .....	262
.....	cclxiv

# 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 proporciona un panel de control único para que los usuarios puedan lanzar escritorios virtuales seguros para realizar investigaciones científicas, diseños de productos, simulaciones de ingeniería o cargas de trabajo de análisis de datos. Los usuarios pueden conectarse al RES portal con sus credenciales corporativas actuales y trabajar en proyectos individuales o colaborativos.

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

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

Esta guía proporciona información general sobre Research and Engineering Studio on AWS, su arquitectura y componentes de referencia, consideraciones para planificar la implementación y los pasos de configuración para la implementación 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 utilizarloRES.

### 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 para conectarse RES 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 RES portal 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 ellosRES. Los servicios de almacenamiento compatibles incluyen Amazon Elastic File System para escritorios Linux y Amazon FSx NetApp ONTAP para escritorios Windows y Linux.

### Supervisión e informes

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

### Gestión del presupuesto y los costes

AWS Budgets Conéctese a sus RES proyectos para monitorear los costos de cada proyecto. Si superas tu presupuesto, puedes limitar el inicio de VDI las sesiones.

# Conceptos y definiciones

En esta sección se describen los conceptos clave y se define la terminología específica de Research and Engineering Studio sobre AWS:

## Explorador de archivos

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

## Sistema de archivos

El sistema de archivos actúa como 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 RES los recursos que se comparten en un RES entorno. 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 RES administradora, 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; esto garantiza la gobernanza del flujo de datos y evita que se compartan datos y VDI hosts entre proyectos.

## Permisos basados en proyectos

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

## Miembro del proyecto

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

## Propietario del proyecto

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

## Pila de software

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

## VDIhospeda

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

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

## Información general de la arquitectura

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

## Diagrama de arquitectura

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

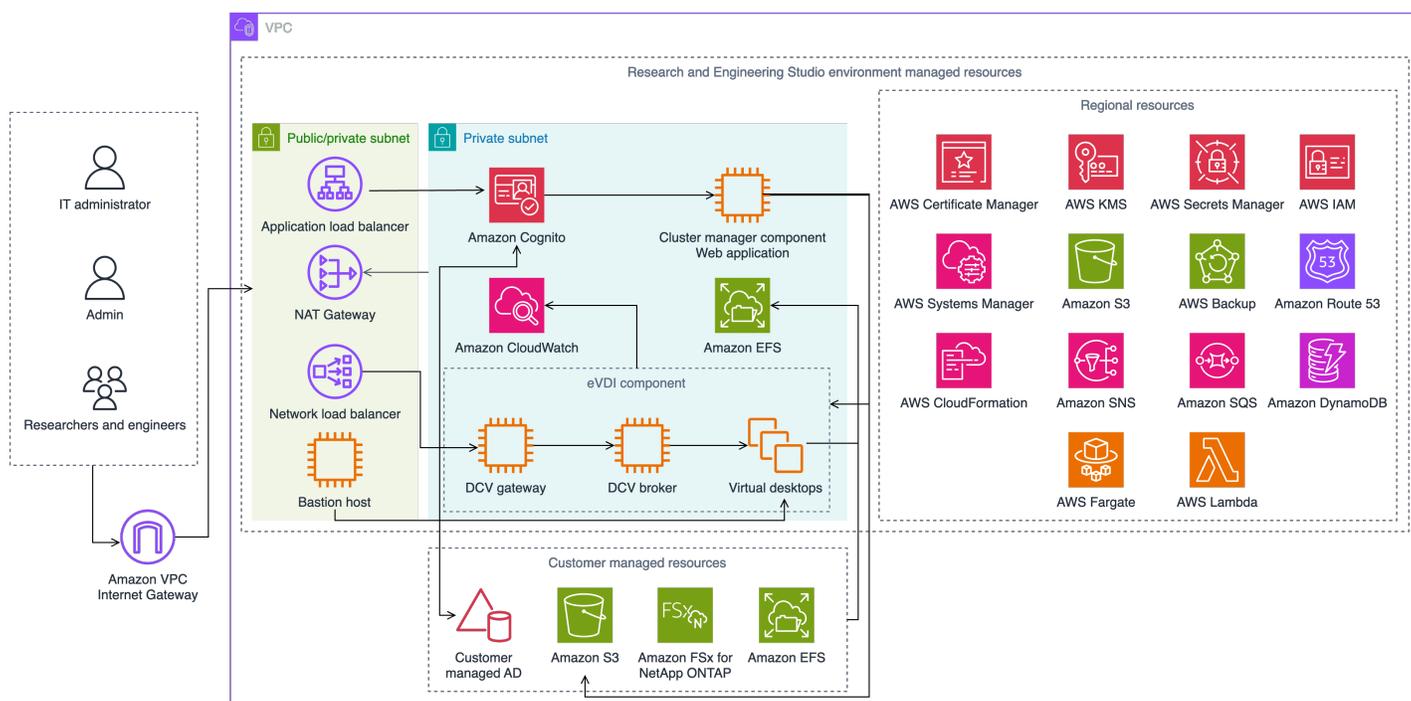


Figura 1: Estudio de investigación e ingeniería sobre AWS arquitectura

### Note

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

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

1. RESinstala componentes para el portal web, además de:

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

Amazon CloudWatch recibe métricas de los VDI componentes electrónicos.

- c. Componente Bastion Host

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

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

 Note

Te recomendamos que lo AWS Certificate Manager utilices para generar un certificado de confianza para tu dominio.

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

## AWS servicios de este producto

AWS servicio	Tipo	Descripción
<a href="#">Amazon Elastic Compute Cloud</a>	Core	Proporciona los servicios informáticos subyacentes para crear escritorios virtuales con el sistema operativo y la pila de software que elijan.
<a href="#">Elastic Load Balancing</a>	Core	Bastion, el administrador de clústeres y los VDI hosts se crean en grupos de Auto Scaling detrás del balanceador de cargas. ELB equilibra el tráfico del portal web entre los hosts. RES
<a href="#">Amazon Virtual Private Cloud</a>	Core	Todos los componentes principales del producto se crean dentro de suVPC.
<a href="#">Amazon Cognito</a>	Core	Administra las identidades y la autenticación de los usuarios. Los usuarios de Active Directory se asignan a usuarios y grupos de Amazon Cognito para autenticar los niveles de acceso.
<a href="#">Amazon Elastic File System</a>	Core	Proporciona el sistema de /home archivos para el explorador de archivos y los VDI hosts, así como los sistemas de archivos externos compartidos.

AWS servicio	Tipo	Descripción
<a href="#">Amazon DynamoDB</a>	Core	Almacena datos de configuración, como usuarios, grupos, proyectos, sistemas de archivos y ajustes de componentes.
<a href="#">AWS Systems Manager</a>	Core	Almacena documentos para ejecutar comandos para la administración de VDI sesiones.
<a href="#">AWS Lambda</a>	Core	Admite funcionalidades del producto, como la actualización de la configuración de la tabla de DynamoDB, el inicio de los flujos de trabajo de sincronización de Active Directory y la actualización de la lista de prefijos.
<a href="#">Amazon CloudWatch</a>	Compatible	Proporciona métricas y registros de actividad para todos los EC2 hosts de Amazon y las funciones de Lambda.
<a href="#">Amazon Simple Storage Service</a>	Apoyando	Almacena los archivos binarios de las aplicaciones para el arranque y la configuración del host.
<a href="#">AWS Key Management Service</a>	Apoyando	Se utiliza para el cifrado en reposo con SQS colas de Amazon, tablas de DynamoDB y temas de Amazon. SNS

AWS servicio	Tipo	Descripción
<a href="#">AWS Secrets Manager</a>	Apoyando	Almacena las credenciales de las cuentas de servicio en Active Directory y los certificados autofirmados para VDI.
<a href="#">AWS CloudFormation</a>	De apoyo	Proporciona un mecanismo de despliegue para el producto.
<a href="#">AWS Identity and Access Management</a>	Apoyando	Restringe el nivel de acceso de los hosts.
<a href="#">Amazon Route 53</a>	Apoyando	Crea una zona alojada privada para resolver el balanceador de cargas interno y el nombre de dominio del host del bastión.
<a href="#">Amazon Simple Queue Service</a>	Apoyando	Crea colas de tareas para respaldar las ejecuciones asíncronas.
<a href="#">Amazon Simple Notification Service</a>	Apoyando	Admite el modelo de publicación-suscriptor entre VDI componentes como el controlador y los hosts.
<a href="#">AWS Fargate</a>	Apoyando	Instala, actualiza y elimina entornos mediante las tareas de Fargate.
<a href="#">Amazon FSx File Gateway</a>	Opcional	Proporciona un sistema de archivos compartidos externo.
<a href="#">Amazon FSx para NetApp ONTAP</a>	Opcional	Proporciona un sistema de archivos compartidos externo.

AWS servicio	Tipo	Descripción
<a href="#">AWS Certificate Manager</a>	Opcional	Genera un certificado de confianza para su dominio personalizado.
<a href="#">AWS Backup</a>	Opcional	Ofrece funciones de copia de seguridad para los EC2 hosts de Amazon, los sistemas de archivos y DynamoDB.

## Cree un entorno de demostración

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

Tenga en cuenta que, después de implementar la pila, debe seguir lo [Pasos posteriores a la implementación](#) siguiente 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](#)
- [Crea un par de EC2 SSH claves de Amazon](#)
- [Aumentar las cuotas de servicio](#)

### Cree una Cuenta de AWS con un usuario administrativo

Debe tener una Cuenta de AWS con un usuario administrativo:

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

Parte del procedimiento de registro consiste en recibir una llamada telefónica 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](#).

## Crea un par de EC2 SSH claves de Amazon

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

## Aumentar las cuotas de servicio

Recomendamos [aumentar las cuotas de servicio](#) para:

- [Amazon VPC](#)
  - Aumente la cuota de direcciones IP elásticas por NAT puerta de enlace de cinco a ocho
  - Aumente las NAT puertas de enlace por zona de disponibilidad de cinco a diez
- [Amazon EC2](#)
  - Aumente el EC2 VPC elástico IPs de cinco a diez

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

## Cree recursos e introduzca parámetros

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

### Note

Asegúrese de estar en su cuenta de administrador.

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

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

#### 4. Seleccione Crear pila.

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

# Planificación de la implementación

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

## Costo

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

### Note

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

Te 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

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de cumplimiento que se aplican a Research and Engineering Studio on AWS, consulte [AWS Servicios dentro del alcance por programa de cumplimiento AWS](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Para saber cómo aplicar el modelo de responsabilidad compartida a los AWS servicios utilizados por Research and Engineering Studio, consulte [Consideraciones de seguridad para los servicios de este producto](#). Para obtener más información acerca de la seguridad de AWS, visite [Nube de AWS Seguridad](#).

## IAM roles

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

RES admite políticas internas basadas en la identidad. 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 cliente existente con el que Active Directory está integrado RES. Para obtener más información, consulte [Creación de IAM políticas](#) 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 RES de usuario, 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 EC2 instancias, las instancias de sistemas CSR de archivos y los puntos finales remotos VPN. 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 RES propia. Al realizar la implementación RES, puede especificar una AWS KMS key. RES utiliza sus credenciales para conceder el acceso clave. Si la proporciona a un cliente que es propiedad y está gestionado AWS KMS key, los datos inactivos del cliente se cifrarán con esa clave.

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

## Consideraciones de seguridad para los servicios de este producto

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

AWS información de seguridad del servicio	Tipo de servicio	Cómo se utiliza el servicio en RES
<a href="#">Amazon Elastic Compute Cloud</a>	Core	Proporciona los servicios informáticos subyacentes para crear escritorios virtuales con el sistema operativo y la pila de software que elijan.
<a href="#">Elastic Load Balancing</a>	Core	Bastion, el administrador de clústeres y los VDI hosts se crean en grupos de Auto Scaling detrás del balanceador de cargas. ELB equilibra el tráfico del portal web entre los hosts. RES
<a href="#">Amazon Virtual Private Cloud</a>	Core	Todos los componentes principales del producto se crean dentro de suVPC.
<a href="#">Amazon Cognito</a>	Core	Administra las identidades y la autenticación de los usuarios. Los usuarios de Active Directory se asignan a usuarios y grupos de Amazon Cognito para autenticar los niveles de acceso.
<a href="#">Amazon Elastic File System</a>	Core	Proporciona el sistema de /home archivos para el explorador de archivos y los VDI hosts, así como los

AWS información de seguridad del servicio	Tipo de servicio	Cómo se utiliza el servicio en RES
		sistemas de archivos externos compartidos.
<a href="#">Amazon DynamoDB</a>	Core	Almacena los datos de configuración, como los usuarios, los grupos, los proyectos, los sistemas de archivos y la configuración de los componentes.
<a href="#">AWS Systems Manager</a>	Core	Almacena documentos para ejecutar comandos para la administración de VDI sesiones.
<a href="#">AWS Lambda</a>	Core	Admite funcionalidades del producto, como la actualización de la configuración de la tabla de DynamoDB, el inicio de los flujos de trabajo de sincronización de Active Directory y la actualización de la lista de prefijos.
<a href="#">Amazon CloudWatch</a>	Compatible	Proporciona métricas y registros de actividad para todos los EC2 hosts de Amazon y las funciones de Lambda.
<a href="#">Amazon Simple Storage Service</a>	Apoyando	Almacena los archivos binarios de las aplicaciones para el arranque y la configuración del host.

AWS información de seguridad del servicio	Tipo de servicio	Cómo se utiliza el servicio en RES
<a href="#">AWS Key Management Service</a>	Apoyando	Se utiliza para el cifrado en reposo con SQS colas de Amazon, tablas de DynamoDB y temas de Amazon. SNS
<a href="#">AWS Secrets Manager</a>	Apoyando	Almacena las credenciales de las cuentas de servicio en Active Directory y los certifica dos autofirmados paraVDIs.
<a href="#">AWS CloudFormation</a>	De apoyo	Proporciona un mecanismo de despliegue para el producto.
<a href="#">AWS Identity and Access Management</a>	Apoyando	Restringe el nivel de acceso de los hosts.
<a href="#">Amazon Route 53</a>	Apoyando	Crea una zona alojada privada para resolver el balanceador de cargas interno y el nombre de dominio del host del bastión.
<a href="#">Amazon Simple Queue Service</a>	Apoyando	Crea colas de tareas para respaldar las ejecuciones asíncronas.
<a href="#">Amazon Simple Notification Service</a>	Apoyando	Admite el modelo de publicación-suscriptor entre VDI componentes como el controlador y los hosts.
<a href="#">AWS Fargate</a>	Apoyando	Instala, actualiza y elimina entornos mediante las tareas de Fargate.

AWS información de seguridad del servicio	Tipo de servicio	Cómo se utiliza el servicio en RES
<a href="#">Amazon FSx File Gateway</a>	Opcional	Proporciona un sistema de archivos compartidos externo.
<a href="#">Amazon FSx para NetApp ONTAP</a>	Opcional	Proporciona un sistema de archivos compartidos externo.
<a href="#">AWS Certificate Manager</a>	Opcional	Genera un certificado de confianza para su dominio personalizado.
<a href="#">AWS Backup</a>	Opcional	Ofrece funciones de copia de seguridad para los EC2 hosts de Amazon, los sistemas de archivos y DynamoDB.

## Cuotas

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

### Cuotas de los AWS servicios de este producto

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

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

- Amazon Virtual Private Cloud
- Amazon EC2

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

## AWS CloudFormation cuotas

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

## Planificar la resiliencia

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

ASGlos ajustes se pueden personalizar en la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>. El producto crea cuatro de forma ASGs predeterminada y cada nombre termina en -asg. Puede cambiar los valores mínimos y deseados por una cantidad adecuada para su entorno de producción. Seleccione el grupo que desee modificar y, a continuación, elija Acciones y, a continuación, seleccione Editar. Para obtener más informaciónASGs, consulte [Escalar el tamaño de su grupo de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

## Compatible Regiones de AWS

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

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

Nombres de las regiones	Región	Versiones anteriores	Última versión (2024.10)
Este de EE. UU. (Norte de Virginia)	us-east-1	yes	sí

Nombres de las regiones	Región	Versiones anteriores	Última versión (2024.10)
Este de EE. UU. (Ohio)	us-east-2	yes	sí
Oeste de EE. UU. (Norte de California)	us-west-1	yes	sí
Oeste de EE. UU. (Oregón)	us-west-2	yes	sí
Asia-Pacífico (Tokio)	ap-northeast-1	yes	sí
Asia Pacífico (Seúl)	ap-northeast-2	yes	sí
Asia Pacífico (Bombay)	ap-south-1	yes	sí
Asia-Pacífico (Singapur)	ap-southeast-1	yes	sí
Asia Pacífico (Sídney)	ap-southeast-2	yes	sí
Canadá (centro)	ca-central-1	yes	sí
Europe (Fráncfort)	eu-central-1	yes	sí
Europa (Milán)	eu-south-1	yes	sí
Europa (Irlanda)	eu-west-1	yes	sí
Europa (Londres)	eu-west-2	yes	sí
Europa (París)	eu-west-3	yes	sí
Europa (Estocolmo)	eu-north-1	no	yes
Israel (Tel Aviv)	il-central-1	yes	sí

Nombres de las regiones	Región	Versiones anteriores	Última versión (2024.10)
AWS GovCloud (US-Oeste)	us-gov-west-1	yes	sí

# Implemente el producto

## Note

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

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

## Temas

- [Requisitos previos](#)
- [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](#)
- [Crea un par de EC2 SSH claves de Amazon](#)
- [Aumentar las cuotas de servicio](#)
- [Crea un dominio público \(opcional\)](#)
- [Crear dominio \(GovCloud solo\)](#)
- [Proporcione recursos externos](#)
- [LDAPSConfigúrelo en su entorno \(opcional\)](#)
- [Configura una privada VPC \(opcional\)](#)

## Crear una Cuenta de AWS con un usuario administrativo

Debe tener una Cuenta de AWS con un usuario administrativo:

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

Parte del procedimiento de registro consiste en recibir una llamada telefónica 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](#).

## Crear un par de EC2 SSH claves de Amazon

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

## Aumentar las cuotas de servicio

Recomendamos [aumentar las cuotas de servicio](#) para:

- [Amazon VPC](#)
  - Aumente la cuota de direcciones IP elásticas por NAT puerta de enlace de cinco a ocho.
  - Aumente las NAT puertas de enlace por zona de disponibilidad de cinco a diez.
- [Amazon EC2](#)
  - Aumente el EC2 VPC elástico IPs de cinco a diez

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

## Crea un dominio público (opcional)

Recomendamos utilizar un dominio personalizado para el producto a fin de que sea fácil de usar URL. 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, cópielo ARN de la sección sobre el estado del certificado.

## Crear dominio (GovCloud solo)

Si va a realizar el despliegue en la región AWS GovCloud (EE. UU.-Oeste) y utiliza un dominio personalizado para Research and Engineering Studio, 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 secreto ARN 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 secreto ARN y añada dos etiquetas al secreto para vdc-gateway poder acceder al valor secreto:
- a. res: ModuleName = virtual-desktop-controller
  - b. res: EnvironmentName = [nombre del entorno] (podría ser res-demo)

## Proporcione recursos externos

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

- Redes (VPCsubredes públicas y subredes privadas)

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

- Almacenamiento (AmazonEFS)

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

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

El servicio de directorio autentica a los usuarios en el RES 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 \(GovCloud solo\)](#)

## LDAPSConfigúrelo en su entorno (opcional)

Si planea usar la LDAPS comunicación 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 yRES.

1. Siga los pasos que se indican en [Cómo habilitar el lado del servidor LDAPS para su AWS Managed Microsoft AD](#) Puedes saltarte este paso si ya lo has activado. 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. Seleccione X.509 codificado en base 64 (. CER) y elija Siguiente.
  - g. Seleccione un directorio y, a continuación, elija Siguiente.
3. Crea un secreto en AWS Secrets Manager:

Al crear tu Secret in the Secrets Manager, selecciona Otro tipo de secreto en Tipo de secreto y pega tu certificado PEM codificado en el campo Plaintext.
4. Anota lo ARN creado e introdúcelo como `DomainTLSCertificateSecretARN` parámetro.  
[Paso 1: lanzar el producto](#)

## Configura una privada VPC (opcional)

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

embargo, la RES implementación estándar se basa en el acceso a Internet para instalar las dependencias. Para realizar RES la instalación en un VPC entorno privado, deberá cumplir los siguientes requisitos previos:

## Temas

- [Prepare imágenes de máquinas de Amazon \(AMIs\)](#)
- [Configure los puntos VPC finales](#)
- [Conéctese a servicios sin puntos VPC finales](#)
- [Establezca los parámetros de VPC despliegue privados](#)

## Prepare imágenes de máquinas de Amazon (AMIs)

1. Descarga [las dependencias](#). Para desplegarse de forma aislada VPC, la RES infraestructura requiere la disponibilidad de dependencias sin tener acceso público a Internet.
2. Cree un IAM rol con acceso de solo lectura a Amazon S3 y una identidad de confianza como Amazon. EC2
  - a. Abra la IAM consola en. <https://console.aws.amazon.com/iam/>
  - b. En Funciones, elija Crear función.
  - c. En la página Seleccionar entidad de confianza:
    - En Tipo de entidad de confianza, elija Servicio de AWS.
    - En Caso de uso en Servicio o Caso de uso, elija EC2 Siguiente.
  - d. En Añadir permisos, selecciona las siguientes políticas de permisos y, a continuación, selecciona Siguiente:
    - Amazon S3 ReadOnlyAccess
    - AmazonSSMManaged InstanceCore
    - EC2InstanceProfileForImageBuilder
  - e. Agregue un nombre y una descripción del rol y, a continuación, elija Crear rol.
3. Cree el componente generador de EC2 imágenes:
  - a. Abra la consola EC2 de Image Builder en <https://console.aws.amazon.com/imagebuilder>.
  - b. En Recursos guardados, elija Componentes y elija Crear componente.
  - c. En la página Crear componente, introduzca los siguientes detalles:

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

Parámetro	Entrada de usuario
Sistema operativo (OS) de imagen	Linux
Versiones de sistema operativo compatibles	Amazon Linux 2
Nombre del componente	Introduzca un nombre como: <i>&lt;research-and-engineering-studio-infrastructure&gt;</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 archivo URI para el archivo tar.gz. Cargue el archivo tar.gz proporcionado por RES en un bucket de Amazon S3 y copie el archivo URI 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 va a configurar variables de https\_proxy entorno, no\_proxy los parámetros son necesarios para evitar que la instancia utilice el proxy para consultar el host local, los metadatos de la instancia, las direcciones IP y los servicios compatibles con los puntos VPC finales. 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 SSM agente tras la ejecución de la canalización.
Directorio de trabajo	Ruta del directorio de trabajo	/root/bootstrap/requirements_dependencies

Sección	Parámetro	Entrada de usuario
Componentes	Construya componentes	<p>Busque y seleccione lo siguiente:</p> <ul style="list-style-type: none"> <li>• Administrado por Amazon: -2-linux aws-cli-version</li> <li>• Administrado por Amazon: amazon-cl oudwatch-agent-linux</li> <li>• De tu propiedad: EC2 componente de Amazon creado anteriormente. Pon tu Cuenta de AWS ID y la actual Región de AWS en los campos.</li> </ul>
	Pruebe los componentes	<p>Busque y seleccione:</p> <ul style="list-style-type: none"> <li>• Administrado por Amazon: simple-boot-test-linux</li> </ul>

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.

Sección	Parámetro	Entrada de usuario
	Descripción	Añada una descripción opcional.
	IAMrol	Seleccione el IAM rol 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 necesitas crear un grupo de seguridad, puedes crear uno desde la EC2 consola de Amazon con las siguientes entradas:</p> <ul style="list-style-type: none"> <li>• VPC: Seleccione el mismo VPC que se utiliza para la configuración de la infraestructura. VPC debe tener acceso a Internet.</li> <li>• Regla de entrada: <ul style="list-style-type: none"> <li>• Tipo: SSH</li> <li>• Source (Fuente): Custom</li> <li>• CIDR bloque: 0.0.0.0/0</li> </ul> </li> </ul>

d. Elija Crear configuración de infraestructura.

6. Cree una nueva canalización EC2 de Image Builder:

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

- b. En la página Especificar los detalles de la canalización, introduce lo siguiente y selecciona Siguiente:
    - Nombre de la canalización y descripción opcional
    - En Crear un cronograma, defina un cronograma o elija Manual si desea iniciar el proceso de AMI horneado manualmente.
  - c. En la página Elegir receta, selecciona Usar receta existente e ingresa el nombre de la receta creada anteriormente. Elija Next (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 Next (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 RES entorno implementado, de modo que RES se puedan lanzar correctamente las instancias de infraestructura host desde ella. Si se utilizan los valores predeterminados del servicio, la imagen de salida se creará en la región en la que se utilice el servicio EC2 Image Builder.
    - Si desea implementarlo RES en varias regiones, puede elegir Crear una nueva configuración de distribución y agregar allí más regiones.
  - g. Revisa tus selecciones y selecciona Crear canalización.
7. Ejecute la canalización EC2 de Image Builder:
- a. En Image Pipelines, busca y selecciona la canalización que has creado.
  - b. Elige Acciones y selecciona Ejecutar canalización.
- El proceso de creación de una AMI imagen puede tardar entre 45 minutos y una hora aproximadamente.
8. Anote el AMI ID del generado AMI y utilícelo como entrada para el InfrastructureHost AMI parámetro en [the section called “Paso 1: lanza el producto”](#).

## Configure los puntos VPC finales

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

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

Servicio de AWS	Nombre del servicio
<a href="#">Application Auto Scaling</a>	com.amazonaws. <i>region</i> .escalado automático de aplicaciones
<a href="#">AWS CloudFormation</a>	com.amazonaws. <i>region</i> cloudformation.
<a href="#">Amazon CloudWatch</a>	com.amazonaws. <i>region</i> .monitoreo
<a href="#">Amazon CloudWatch Logs</a>	com.amazonaws. <i>region</i> .logs
<a href="#">Amazon DynamoDB</a>	com.amazonaws. <i>region</i> .dynamodb (requiere un punto final de puerta de enlace)
<a href="#">Amazon EC2</a>	com.amazonaws. <i>region</i> ec2.
<a href="#">Amazon ECR</a>	com.amazonaws. <i>region</i> .ecr.api com.amazonaws. <i>region</i> .ecr.dkr
<a href="#">Amazon Elastic File System</a>	com.amazonaws. <i>region</i> elasticfilesystem.
<a href="#">Elastic Load Balancing</a>	com.amazonaws. <i>region</i> .balanceo de carga elástico
<a href="#">Amazon EventBridge</a>	com.amazonaws. <i>region</i> .events
Amazon FSx	com.amazonaws. <i>region</i> .fsx
<a href="#">AWS Key Management Service</a>	com.amazonaws. <i>region</i> kms.

Servicio de AWS	Nombre del servicio
<a href="#">Amazon Kinesis Data Streams</a>	com.amazonaws. <i>region</i> .kinesis-streams
<a href="#">AWS Lambda</a>	com.amazonaws. <i>region</i> lambda.
<a href="#">Amazon S3</a>	com.amazonaws. <i>region</i> .s3 (requiere un punto final de puerta de enlace que se crea de forma predeterminada en.) RES  Se requieren puntos de enlace de interfaz Amazon S3 adicionales para el montaje cruzado de los buckets en un entorno aislado. Consulte <a href="#">Acceso a los puntos finales de la interfaz de Amazon Simple Storage Service</a> .
<a href="#">AWS Secrets Manager</a>	com.amazonaws. <i>region</i> secretsmanager.
<a href="#">Amazon SES</a>	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).
<a href="#">AWS Security Token Service</a>	com.amazonaws. <i>region</i> .sts
<a href="#">Amazon SNS</a>	com.amazonaws. <i>region</i> .sns
<a href="#">Amazon SQS</a>	com.amazonaws. <i>region</i> sqs.
<a href="#">AWS Systems Manager</a>	com.amazonaws. <i>region</i> Mensajes.ec2  com.amazonaws. <i>region</i> ssm.  com.amazonaws. <i>region</i> Mensajes.ssm

## Conéctese a servicios sin puntos VPC finales

Para integrarlo con servicios que no admiten VPC puntos finales, 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 implementar un estudio de investigación e ingeniería 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 RES implementación.
  - 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 el 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 lo que escucha el servidor proxy. PORT
3. Configure su tabla de rutas para permitir el acceso al servidor proxy.
  - a. Vaya a la VPC consola e identifique las tablas de enrutamiento de las subredes que utilizará para los hosts y VDI hosts de infraestructura.
  - 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 VDIs Infrastructure/.
4. Modifique el grupo de seguridad de la EC2 instancia del servidor proxy y asegúrese de que permite TCP las conexiones entrantes en las que escucha PORT el servidor proxy.

## Establezca los parámetros de VPC despliegue privados

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

Parámetro	Entrada
InfrastructureHostAMI	Utilice el AMI ID de infraestructura creado en <a href="#">the section called “Prepare imágenes de máquinas de Amazon (AMIs)”</a> .
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 si desea permitir VPC CIDR el acceso a todas las direcciones VPC IP.

## Crear recursos externos

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

Puede [descargar la plantilla de recetas](#) antes de la implementación.

Tiempo de despliegue: aproximadamente entre 40 y 90 minutos

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

### Note

Asegúrese de estar en su cuenta de administrador.

2. Inicie [la plantilla](#) en la consola.

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

3. Introduzca los parámetros de la plantilla:

Parámetro	Predeterminado	Descripción
DomainName	corp.res.com	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.
SubDomain (GovCloud solo)		Este parámetro es opcional para las regiones comerciales, pero obligatorio para GovCloud las regiones.  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.

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>Importante: el formato de este campo puede ser (1) una contraseña de texto sin formato o (2) el ARN de un AWS secreto formateado como un par clave/valor. <code>{"password": "somepassword"}</code></p> <p>Nota: La contraseña de este usuario debe cumplir los <a href="#">requisitos de complejidad de contraseñas</a> de Active Directory.</p>

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

Parámetro	Predeterminado	Descripción
LDIFS3Path	<code>aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif</code>	<p>La ruta de Amazon S3 a un LDIF archivo importado durante la fase de arranque de la configuración de Active Directory. Para obtener más información, consulte <a href="#">LDIFSupport</a>. 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 <a href="#">res.ldif</a> 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 <a href="#">Trabajar con listas de prefijos administradas por el cliente</a> .
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 RES pila. 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 despliega la pila RES principal y los recursos de autenticación, frontend y backend.

**Note**

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

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

1. Inicia sesión en AWS Management Console <https://console.aws.amazon.com/cloudformation> y abre la AWS CloudFormation consola.
2. [Abre la plantilla.](#)

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

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

**Note**

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

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

Parámetro	Predeterminado	Descripción
EnvironmentName	<i>&lt;res-demo&gt;</i>	Nombre exclusivo asignado a su RES entorno que comienza con res-, no más de 11 caracteres y sin letras mayúsculas.

Parámetro	Predeterminado	Descripción
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.
InfrastructureHostAMI	<i>ami-[numbers or letters only]</i>	(Opcional) Puede proporcionar un AMI identificador 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 <a href="#">Preparado para configurar RES AMIs</a> .
SSHKeyPair		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 IPs permitir el acceso directo a la interfaz de usuario web y SSH al host del bastión.
IAMPermissionBoundary		(Opcional) Puedes proporcionar una política gestionada a ARN que se adjuntará como límite de permisos a todos los roles creados en ellos. RES Para obtener más información, consulte <a href="#">Establecer límites de permisos personalizados</a> .
VpcId		ID del VPC lugar en el que se lanzarán las instancias.
IsLoadBalancerInternetFacing		Selecciona true para implementar un balanceador de cargas orientado a Internet (se requieren 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, selecciona subredes privadas. Para las implementaciones que necesitan acceso a Internet, seleccione subredes públicas. Si la pila de redes externas creó más de dos, seleccione todas las que se crearon.</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 diferentes zonas de disponibilidad donde se lanzarán las VDI instancias. 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.
ADShortName	<i>corp</i>	El nombre abreviado del directorio activo. También se denomina BIOS nombre de red.
LDAPBase	<b><i>DC=corp,DC=res,DC=com</i></b>	Un LDAP camino hacia la base dentro de la LDAP jerarquía.
LDAPConnectionURI		Una única ruta ldap://a la que puede acceder el servidor host de Active Directory. Si implementaste los recursos externos automatizados con el dominio AD predeterminado, puedes usar ldap://corp.res.com.
ServiceAccountCredentialsSecretArn		Proporcione un secreto ARN que contenga el nombre de usuario y la contraseña del usuario de Active Directory, con el formato de un par de nombre de ServiceAccount usuario, contraseña, clave y valor.
Sou del usuario		Unidad organizativa dentro de AD para los usuarios que se sincronizarán.

Parámetro	Predeterminado	Descripción
Grupo SOU		Unidad organizativa dentro de AD para los grupos que se sincronizarán.
SudoersGroupName	RESAdministrators	Nombre de grupo que contiene todos los usuarios con acceso directo a las instancias en el momento de la instalación y acceso de administrador activadoRES.
Computador/SOU		Unidad organizativa de AD a la que se unirán las instancias.
D: omainTLSCertificate Secreto ARN		(Opcional) Proporcione un secreto de TLS certificado de dominio ARN para permitir TLS la comunicación con AD.
EnableLdapIDMapping		Determina si UID los GID números son generados por el AD SSSD o si se utilizan los números proporcionados por el AD. Establézcalo en UID True para usar los SSSD generados yGID, o en False para usarlos UID y GID proporcionados por el AD. En la mayoría de los casos, este parámetro debe estar establecido en True.

Parámetro	Predeterminado	Descripción
DisableADJoin	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 EFS ID que se utilizará en el sistema de archivos doméstico compartido de los hosts Linux. VDI
CustomDomainNameforWebApp		(Opcional) Subdominio utilizado por el portal web para proporcionar enlaces a la parte web del sistema.
CustomDomainNameforVDI		(Opcional) Subdominio utilizado por el portal web para proporcionar enlaces a la VDI parte del sistema.

Parámetro	Predeterminado	Descripción
ACMCertificateARNforWebApp		<p>(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. <a href="#">Guía de configuración</a></p>
CertificateSecretARNforVDI		<p>(Opcional) Este ARN secreto 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.</p>

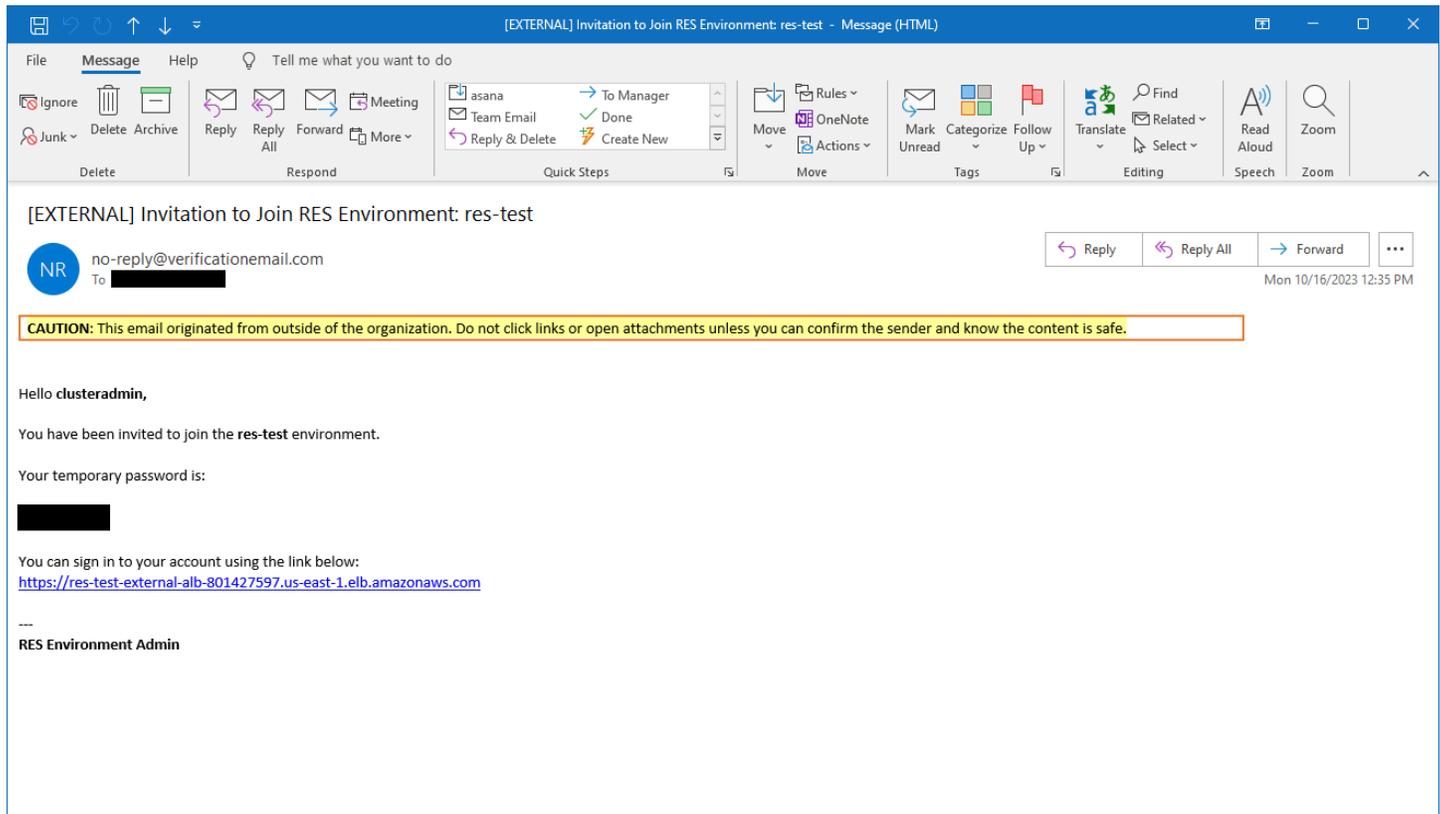
Parámetro	Predeterminado	Descripción
PrivateKeySecretARNforVDI		(Opcional) Este ARN secreto almacena la clave privada del certificado de su portal web. Si estableces un nombre de dominio de portal para tus recursos externos automatizados, puedes encontrar este valor en la pestaña Resultados de la pila 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 COMPLETE estado CREATE \_ 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. Úselo URL para iniciar sesión en su 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 SSO proveedor. Para obtener información sobre la configuración posterior a la implementación, consulte la [Guía de configuración](#). Tenga en cuenta que clusteradmin se trata de una cuenta única: puede utilizarla para crear proyectos y asignar miembros de usuarios o grupos a esos proyectos; no puede asignar paquetes de software ni implementar un escritorio por sí misma.

# 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 añade 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 RES entorno anterior al más reciente sin perder la configuración del entorno. También puede usar este proceso para probar y verificar las actualizaciones de su entorno antes de incorporar usuarios.

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

1. Cree una instantánea de su entorno actual. Consulte [the section called “Crear una instantánea”](#).
2. Vuelva a implementarlo 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 RES, no es necesaria una nueva instalación. Puedes actualizar la RES pila existente actualizando su AWS CloudFormation plantilla. Compruebe la versión de su RES entorno 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. Abre la AWS CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
3. En Stacks, busca y selecciona la pila principal. Debería aparecer como `<stack-name>`.
4. Elija Actualizar.
5. Selecciona Reemplazar la plantilla actual.
6. Para Origen de plantilla, elija Cargar un archivo de plantilla.
7. Selecciona Elegir archivo y carga la plantilla que has descargado.
8. En Especificar los detalles de la pila, selecciona Siguiente. No es necesario actualizar los parámetros.
9. En Configurar las opciones de pila, seleccione Siguiente.
10. En Revisar `<stack-name>`, selecciona Enviar.

# Desinstalar el producto

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

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

## Eliminar los buckets de Amazon S3

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

1. Inicie sesión en la consola de Amazon S3 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. Selecciona cada depósito de Amazon S3 y, a continuación, selecciona Vacío. Debe vaciar cada cubo.
5. Seleccione el depósito S3 y elija Eliminar.

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

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

### Note

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

# Guía de configuración

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

## Temas

- [Administrar usuarios y grupos](#)
- [Crear subdominios](#)
- [Cree un ACM certificado](#)
- [Amazon CloudWatch Logs](#)
- [Establecer límites de permisos personalizados](#)
- [Preparado para configurar RES AMIs](#)

## Administrar usuarios y grupos

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

## Temas

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

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

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

 Note

Si va a realizar la implementación en la región AWS GovCloud (EE. UU. Oeste), configúrela 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 el Centro IAM de Identidad

1. Inicie sesión en la [consola de AWS Identity and Access Management](#).
2. Abra el Centro de Identidad.
3. Seleccione Habilitar.
4. Elija Activar con AWS Organizations.
5. Elija Continuar.

 Note

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

### Conexión de IAM Identity Center a un Active Directory administrado

Después de activar IAM Identity Center, complete estos pasos de configuración recomendados:

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

## Sincronizar usuarios y grupos con el centro de identidad

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

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

## Habilitar usuarios

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

## Paso 2: Conectarse a un centro de identidad

### Configuración de la aplicación en IAM Identity Center

1. Abra la [consola IAM de Identity Center](#).
2. Elija Aplicaciones.
3. Elija Añadir aplicación.
4. En las preferencias de configuración, elija Tengo una aplicación que quiero configurar.
5. En Tipo de aplicación, selecciona SAML2.0.
6. Elija Next (Siguiente).
7. Introduzca el nombre para mostrar y la descripción que desee utilizar.
8. En Metadatos de IAM Identity Center, copie el enlace del archivo de SAMLmetadatos de IAM Identity Center. Lo necesitará al configurar IAM Identity Center con el RES portal.

9. En Propiedades de la aplicación, introduzca el inicio de la aplicación URL. Por ejemplo, <your-portal-domain>/sso.
10. En Aplicación ACS URL, introduzca la redirección URL desde el RES portal. Para encontrar esto:
  - a. En Administración del entorno, selecciona Configuración general.
  - b. Seleccione la pestaña Proveedor de identidades.
  - c. En el inicio de sesión único, encontrarás la SAML redirección. URL
11. En SAMLAudiencia de aplicaciones, introduzca Amazon CognitoURN.

Para crear la urna:

- a. Desde el RES portal, 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. Después de entrar en Amazon CognitoURN, selecciona Enviar.

#### Configuración de las asignaciones de atributos para la aplicación

1. En el Centro de identidades, abra los detalles de la aplicación que ha creado.
2. Elija Acciones y, a continuación, elija Editar asignaciones de atributos.
3. En Asunto, introduzca **`\${user:email}`**.
4. En Formato, elija. emailAddress
5. Seleccione Agregar nueva asignación de atributos.
6. En Atributo de usuario de la aplicación, introduce «correo electrónico».
7. En Asignar a este valor de cadena o atributo de usuario en IAM Identity Center, introduzca. **`\${user:email}`**
8. En Formato, escriba «sin especificar».
9. Elija Guardar cambios.

## Agregar usuarios a la aplicación en Identity Center IAM

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

## Configuración del centro de IAM identidad en el RES entorno

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

## Configurar tu proveedor de identidad para el inicio de sesión único ( ) SSO

Research and Engineering Studio se integra con cualquier proveedor de identidad SAML 2.0 para autenticar el acceso de los usuarios al RES portal. Estos pasos proporcionan instrucciones para la integración con el proveedor de identidad SAML 2.0 que elija. Si tiene intención de utilizar IAM Identity Center, consulte [Configuración del inicio de sesión único \(SSO\) con Identity Center IAM](#).

### Note

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

## Temas

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

## 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 RES Amazon Cognito.

1. RES presupone que tiene un AD (AD AWS gestionado o AD autoaprovisionado) con las identidades de usuario autorizadas para acceder al RES portal y a los proyectos. 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 su proveedor de identidad (IdP). Esta configuración requiere los siguientes parámetros:
  - SAMLRedireccionamiento URL: el URL que utiliza su IdP para enviar la respuesta SAML 2.0 al proveedor de servicios.

### Note

Según el IdP, la SAML redirección URL puede tener un nombre diferente:

- Aplicación URL
- Assertion Consumer Service () ACS URL
- ACSPOSTVinculante URL

Para obtener el URL

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

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

 Note

Según el IdP, la SAML audiencia URI puede tener un nombre diferente:

- ClientID
- Audiencia de la aplicación SAML
- ID de entidad SP

Proporcione la entrada en el siguiente formato.

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

Para encontrar tu SAML audiencia URI

1. Inicia sesión 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 SAML afirmación publicada RES debe tener los siguientes campos o afirmaciones configurados en la dirección de correo electrónico del usuario:
- SAMLAsunto o NameID
  - SAMLcorreo electrónico
4. Su IdP agrega campos/reclamos a la SAML afirmación 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`. Reemplazar *user-pool-id* con el ID de su grupo de usuarios de Amazon Cognito.

```
<saml:AudienceRestriction>
```

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

- Respuesta: configurada en `InResponseTo`. `https://user-pool-domain/saml2/idpresponse` Reemplazar *user-pool-domain* con el nombre de dominio de su 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 SAML solicitud 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 SAML aplicación tiene un URL campo de cierre de sesión, configúrelo en: `<domain-url>/saml2/logout`.

## Para obtener el dominio URL

1. Inicie sesión RES como administrador o administrador de clústeres.
  2. Vaya a Administración del entorno ⇒ Configuración general ⇒ Proveedor de identidad.
  3. Elija el dominio URL.
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. Seleccione la pestaña Experiencia de inicio de sesión.
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
<a href="#">idc</a>	SAML	2 weeks ago	3 hours ago

Puede usar este certificado para configurar Active DirectoryIDP, añadir uno y habilitar la SAML compatibilidad con esta parte de confianza. `relying party trust`

### Note

Esto no se aplica a Keycloak y. IDC

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

## RESConfigúrelo para usar su proveedor de identidad

Para completar la configuración del inicio de sesión único para RES

- Inicia sesión 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 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, introduzca un nombre único para su proveedor de identidad.

 Note

No se permiten los siguientes nombres:

- Cognito
- IdentityCenter

- c. En Fuente del documento de metadatos, elija la opción adecuada y cargue el XML documento de metadatos o proporcione el documento URL del proveedor de identidad.
  - d. En el campo Atributo de correo electrónico del proveedor, introduzca el valor del `textoemail`.
  - e. Elija Enviar.
4. Vuelva a cargar la página de configuración del entorno. El inicio de sesión único está habilitado si la configuración es correcta.

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

Si utilizó los [recursos externos](#) proporcionados para crear un RES entorno 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 RES SSO de activación solicita tres parámetros de configuración:

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

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

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

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

**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><b>Metadata document source</b> Enter metadata document endpoint URL</p>	<p><b>Metadata document endpoint URL</b> https://portal.sso.us-west-2.amazonaws.com/saml/metadata/MDg4ODM3NTczNjY0X2lucy04M2EyYTcyMGUzZTFIMDI4</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, seleccione Explorar elementos.
  - c. En Escanear o consultar elementos, vaya a Filtros e introduzca los siguientes parámetros:
    - Nombre del atributo: `key`
    - Valor — `identity-provider.cognito.sso_idp_provider_email_attribute`
  - d. 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

---

Completed. Read capacity units consumed: 13

---

**Items returned (1)**

Item	Actions
<input type="checkbox"/> key (String)	
<input type="checkbox"/> identity-provider.cognito.ss	

**Edit String**

email

Enter any string value.

**8**

| version |

| 1

## Depuración de problemas de SAML IdP

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

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

Amazon CloudWatch Logs: puedes comprobar tus RES CloudWatch registros en 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 SAML integración con Amazon Cognito, [consulte SAML Añadir proveedores de identidad 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 de usuario.
3. Seleccione el usuario e introduzca una contraseña nueva.
4. Seleccione Restablecer contraseña.

## Crear subdominios

Si utilizas un dominio personalizado, tendrás que configurar subdominios para que sean compatibles con la web y VDI algunas partes de tu portal.

### Note

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

1. Abra la [consola Route 53](#).
2. Busca el dominio que creaste y selecciona Crear registro.
3. Introduce «web» como nombre del registro.
4. Seleccione CNAME como tipo de registro.
5. En Value, introduce el enlace que recibiste en el correo electrónico inicial.
6. Elija Crear registros.
7. Para crear un registro para elVDC, recupera la NLB dirección.
  - a. Abra la [consola de AWS CloudFormation](#).

- b. Elija `<environment-name>-vdc`.
  - c. Elija Recursos y abra `<environmentname>-vdc-external-nlb`.
  - d. Copia el DNS nombre deNLB.
8. Abra la [consola Route 53](#).
  9. Busca tu dominio y selecciona Crear registro.
  10. En Nombre del registro, ingresavdc.
  11. En Tipo de registro, seleccione CNAME.
  12. Para elNLB, introduzca elDNS.
  13. Elija Crear registro.

## Cree un ACM certificado

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

### Tip

Si va a implementar el paquete de demostración de recursos externos, tendrá que introducir el dominio que haya elegido `PortalDomainName` al implementar la pila de recursos externos. [Crear recursos externos](#)

Para crear un certificado para dominios personalizados:

1. Desde la consola, [AWS Certificate Manager](#)ábrala para solicitar un certificado público. Si va a realizar la implementación en AWS GovCloud (EE. UU. al oeste), 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 DNSla validación.

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, elija 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 CNAME clave y el valor. 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 certificado ARN para introducirlo como parámetro `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/ &lt;installation-stack-name&gt;-cluster-endpoints</code>	Nunca caducan
<code>/aws/lambda/ &lt;installation-stack-name&gt;-cluster-manager-scheduled-ad-sync</code>	Nunca caducan
<code>/aws/lambda/ &lt;installation-stack-name&gt;-cluster-settings</code>	Nunca caducan

CloudWatch Grupos de registros	Retención
<code>/aws/lambda/ &lt;installation-stack-name&gt;-oauth-credentials</code>	Nunca caducan
<code>/aws/lambda/ &lt;installation-stack-name&gt;-self-signed-certificate</code>	Nunca caducan
<code>/aws/lambda/ &lt;installation-stack-name&gt;-update-cluster-prefix-list</code>	Nunca caducan
<code>/aws/lambda/ &lt;installation-stack-name&gt;-vdc-scheduled-event-transformer</code>	Nunca caducan
<code>/aws/lambda/ &lt;installation-stack-name&gt;-vdc-update-cluster-manager-client-scope</code>	Nunca caducan
<code>/&lt;installation-stack-name&gt; /cluster-manager</code>	6 meses
<code>/&lt;installation-stack-name&gt; /vdc/controller</code>	6 meses
<code>/&lt;installation-stack-name&gt; /vdc/dcv-broker</code>	6 meses
<code>/&lt;installation-stack-name&gt; /vdc/dcv-connection-gateway</code>	6 meses

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

## Establecer límites de permisos personalizados

A partir del 24 de abril de 2020, si lo desea, puede modificar las funciones creadas RES adjuntando límites de permisos personalizados. Se puede definir un límite de permisos personalizado como parte de la RES AWS CloudFormation instalación proporcionando los límites de permisos ARN como parte del parámetro. IAMPermissionBoundary Si este parámetro se deja vacío, no se establece ningún límite de permisos en ningún RES rol. A continuación se muestra la lista de acciones que RES los roles 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",
"textextract:*",
"timestream:*",
"transcribe:*",
"transfer:*",
"translate:*",
"vpc-lattice:*",
"waf-regional:*",
"waf:*",
"wafv2:*",
"wellarchitected:*",
"wisdom:*",
```

```
        "xray:*"  
    ]  
}  
]
```

## Preparado para configurar RES AMIs

Con Amazon Machine Images (AMIs) RES listo para usar, puede preinstalar RES dependencias para instancias de escritorios virtuales (VDIs) en su versión personalizada. AMIs El uso RES de -ready AMIs mejora los tiempos de arranque de las VDI instancias utilizando las imágenes preconfiguradas. Con EC2 Image Builder, puede crear y registrar sus AMIs nuevas pilas de software. Para obtener más información sobre Image Builder, consulte la [Guía del usuario de Image Builder](#).

Antes de empezar, debe [implementar la última versión de RES](#).

### Temas

- [Prepare IAM el rol para acceder al RES entorno](#)
- [Componente Create EC2 Image Builder](#)
- [Prepara tu receta EC2 de Image Builder](#)
- [Configurar EC2 la infraestructura de Image Builder](#)
- [Configurar la canalización de imágenes de Image Builder](#)
- [Ejecute la canalización de imágenes de Image Builder](#)
- [Registre una nueva pila de software en RES](#)

## Prepare IAM el rol para acceder al RES entorno

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

Su función requiere:

- Las relaciones de confianza incluyen el EC2 servicio de Amazon.
- A mazonSSMManaged InstanceCore y EC2InstanceProfileForImageBuilder políticas.

- RESPolítica personalizada con acceso limitado a DynamoDB y Amazon S3 al entorno implementado. RES

(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"
    }
  ]
}
```

RESpolítica:

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

```

```

        "Sid": "RESS3Access",
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": [
            "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-Region}-{AWS-Account-
ID}/idea/vdc/res-ready-install-script-packages/*",
            "arn:aws:s3:::research-engineering-studio-{AWS-Region}/host_modules/*"
        ]
    }
]
}

```

## Componente Create EC2 Image Builder

Siga las instrucciones para [crear un componente mediante la consola de Image Builder](#) de la Guía del usuario de Image Builder.

Introduzca los detalles del componente:

1. En Tipo, elija Construir.
2. En el caso del sistema operativo (SO) Image, elija Linux o Windows.
3. En Nombre del componente, introduzca un nombre descriptivo, como **research-and-engineering-studio-vdi-*<operating-system>***.
4. Introduzca el número de versión del componente y, si lo desea, añada una descripción.
5. Para el documento de definición, introduzca el siguiente archivo de definición. Si encuentra algún error, el YAML archivo 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_{{ RESEnvReleaseVersion }}'
            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. Cree las etiquetas opcionales y elija Crear componente.

## Prepara tu receta EC2 de Image Builder

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

RESes compatible con los siguientes sistemas operativos de imagen:

- Amazon Linux 2 (x86 yARM64)
- Ubuntu 22.04.3 (x86)
- RHEL8 (x86) y 9 (x86)
- Windows 2019, 2022 (x86)

Create a new recipe

1. Abra la consola EC2 de Image Builder en <https://console.aws.amazon.com/imagebuilder>.
2. En Recursos guardados, selecciona Recetas de imágenes.
3. Seleccione Crear receta de imagen.
4. Introduce un nombre único y un número de versión.
5. Seleccione una imagen base compatible conRES.

6. En Configuración de instancias, instale un SSM agente 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 SSM agente, consulte:

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

7. Para recetas basadas en Linux, añada el componente de `aws-cli-version-2-linux` compilación gestionado por Amazon a la receta. RESlos scripts de instalación lo utilizan AWS CLI para proporcionar VDI acceso 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: `AWSAccountIDRESEnvName`, `RESEnvRegion`, y `RESEnvReleaseVersion`.

 Important

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

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

## Modify a recipe

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

1. Para recetas basadas en Linux, añada el componente de `aws-cli-version-2-linux` compilación gestionado por Amazon a la receta. RESlos scripts de instalación lo utilizan AWS

CLI para proporcionar VDI acceso 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: `AWSAccountIDRESEnvName`, `RESEnvRegion`, y `RESEnvReleaseVersion`.

 Important

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

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

## Configurar EC2 la infraestructura de Image Builder

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

- Para crear una nueva configuración de infraestructura, consulte [Crear una configuración de infraestructura](#).
- Para usar una configuración de infraestructura existente, [actualice una configuración de infraestructura](#).

Para configurar la infraestructura de Image Builder:

1. Para IAM el rol, introduzca el rol que configuró anteriormente [Prepare IAM el rol para acceder al RES entorno](#).
2. Para el tipo de instancia, elija un tipo con al menos 4 GB de memoria y que sea compatible con la AMI arquitectura base que haya elegido. Consulte los [tipos de EC2 instancias de Amazon](#).
3. VPC En el caso de los grupos de subred y de seguridad, debe permitir el acceso a Internet para descargar los 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 RES de imágenes para que esté lista AMIs, puede optar por crear una canalización nueva o utilizar una existente. Para obtener más información, consulte [Creación y actualización de canalizaciones de AMI imágenes](#) 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 el panel de navegación, elija Image Pipelines.
3. Seleccione Crear canalización de imágenes.
4. Especifica los detalles de tu canalización introduciendo un nombre único, una descripción opcional, un cronograma y una frecuencia.
5. En Elegir receta, elija Usar receta existente y seleccione la receta creada en [Prepara tu receta EC2 de Image Builder](#). Comprueba que los detalles de la receta sean correctos.
6. En Definir el proceso de creación de imágenes, elija el flujo de trabajo predeterminado o personalizado según el caso de uso. En la mayoría de los casos, los flujos de trabajo predeterminados son suficientes. Para obtener más información, consulte [Configurar flujos de trabajo de imágenes para la canalización de EC2 Image Builder](#).
7. En Definir la configuración de infraestructura, elija Elegir la configuración de infraestructura existente y seleccione la configuración de infraestructura creada en [Configurar EC2 la infraestructura de Image Builder](#). Compruebe que los detalles de su infraestructura sean correctos.
8. En Definir la configuración de distribución, elija Crear la configuración de distribución mediante los valores predeterminados del servicio. La imagen de salida debe residir en el mismo lugar Región de AWS que su RES entorno. 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 [Prepara tu receta EC2 de 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 [Configurar la canalización de imágenes de Image Builder](#).
2. En Acciones, selecciona Ejecutar canalización.

## Registre una nueva pila de software en RES

1. Siga las instrucciones [the section called “Pilas de software \(\) AMIs”](#) para registrar una pila de software.
2. En AMIID, introduzca el AMI ID de la imagen de salida integrada [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 secretos](#)
- [Supervisión y control de costes](#)
- [Administración de sesiones](#)
- [Gestión del entorno](#)

## Administración de secretos

Research and Engineering Studio mantiene los siguientes secretos de uso AWS Secrets Manager. REScrea 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	RESgenerado	El administrador ingresó
<code>&lt;envname&gt; -sso-client-secret</code>	Secreto de OAuth2 cliente de inicio de sesión único para el entorno	✓	
<code>&lt;envname&gt; -vdc-client-secret</code>	vdc ClientSecret	✓	
<code>&lt;envname&gt; -vdc-client-id</code>	vdc ClientId	✓	
<code>&lt;envname&gt; -vdc-gateway-certificate-private-key</code>	Certificado autofirmado: clave privada para el dominio	✓	

Nombre del secreto	Descripción	RESgenerado	El administrador ingresó
<i>&lt;envname&gt;</i> - vdc-gateway- certificate- certificate	Certificado autofirma do para dominio	✓	
<i>&lt;envname&gt;</i> -cluster- manager-c lient-secret	administrador de clústeres ClientSecret	✓	
<i>&lt;envname&gt;</i> -cluster- manager-c lient-id	administrador de clústeres ClientId	✓	
<i>&lt;envname&gt;</i> - external- private-key	Certificado autofirma do: clave privada para el dominio	✓	
<i>&lt;envname&gt;</i> - external- certificate	Certificado autofirma do para dominio	✓	
<i>&lt;envname&gt;</i> - internal- private-key	Certificado autofirma do, clave privada para el dominio	✓	
<i>&lt;envname&gt;</i> - internal- certificate	Certificado autofirma do para dominio	✓	

Nombre del secreto	Descripción	RESgenerado	El administrador ingresó
<code>&lt;envname&gt;-director-service-ServiceAccountUserDN</code>	El atributo de nombre distintivo (DN) del ServiceAccount usuario.	✓	

La `<envname>-cluster-settings` tabla de DynamoDB contiene los siguientes ARN valores secretos:

Clave	Origen
<code>identity-provider.cognito.sso_client_secret</code>	
<code>vdc.dcv_connection_gateway.certificate.certificate_secret_arn</code>	pila
<code>vdc.dcv_connection_gateway.certificate.private_key_secret_arn</code>	pila
<code>cluster.load_balancers.internal_alb.certificates.private_key_secret_arn</code>	pila
<code>directoryservice.root_username_secret_arn</code>	
<code>vdc.client_secret</code>	pila
<code>cluster.load_balancers.external_alb.certificates.certificate_secret_arn</code>	pila
<code>cluster.load_balancers.internal_alb.certificates.certificate_secret_arn</code>	pila
<code>directoryservice.root_password_secret_arn</code>	
<code>cluster.secretsmanager.kms_key_id</code>	

Clave	Origen
<code>cluster.load_balancers.external_alb. certificates.private_key_secret_arn</code>	pila
<code>cluster-manager.client_secret</code>	

## 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 “AWS servicios de este producto”](#).

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

1. Inicie sesión en AWS Management Console y abra la 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

[User-defined cost allocation tags](#) | [AWS generated cost allocation tags](#)

[Download CSV](#)

**User-defined cost allocation tags (2/47) Info** Undo Deactivate Activate

Find cost allocation tags 11 matches

res × Clear filters

< 1 2 > ⌕

<input type="checkbox"/>	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

Una vez desplegadas, las RES etiquetas pueden tardar hasta un día en aparecer.

Para crear un presupuesto de RES recursos:

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 Next (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 Next (Siguiete).

### 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 Next (Siguiente).
17. (Opcional.) Si se configuró una alerta, utilice Adjuntar acciones para configurar las acciones deseadas con la alerta.
18. Elija Next (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 a web interface for 'Projects' under 'Environment Management'. It features a search bar, a 'Create Project' button, and a table of project budgets. The table has columns for Title, Project Code, Status, Budgets, Groups, and Updated On. A single row is visible for 'project1', which is 'Enabled' but has a 'Budget Exceeded' warning. The warning details show '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' column shows '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 <b>Budget Exceeded</b> Limit: 500.00 USD, Forecasted: 3945.34 USD	<ul style="list-style-type: none"> <li>DemoUsers</li> <li>DemoAdmins</li> <li>ProductUsers</li> </ul>	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 un plazo de quince minutos RES. Como alternativa, puede editar un proyecto para deshabilitar un presupuesto.

## 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 \(\) AMIs](#)
- [Debugging](#)
- [Configuración de escritorio](#)

# Panel de control

**Research and Engineering Studio** demoadmin1

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

## Virtual Desktop Dashboard

[View Sessions](#)

### Instance Types 1

Summary of all virtual desktop sessions by instance types.

Instance Type	Count
m6a.large	3

### Session State 2

Summary of all virtual desktop sessions by state.

Session State	Count
STOPPING	3

### Base OS 3

Summary of all virtual desktop sessions by Base OS.

Base OS	Count
Amazon Linux 2	2
Windows	1

### Project 4

Summary of all virtual desktop sessions by Project Code.

Project Code	Count
project1	3

### Availability Zones 5

Summary of all virtual desktop sessions by Availability Zone.

Availability Zone	Count
us-west-2a	3

### 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

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** Actions **2** 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 <b>5</b>	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 la (s) 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. Seleccione el nombre de la sesión para ver más detalles.

### Crear una sesión

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

# Launch New Virtual Desktop ✕

## Session Name

Enter a name for the virtual desktop

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

## User

Select the user to create the session for

## Project

Select the project under which the session will get created

## Operating System

Select the operating system for the virtual desktop

## 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, seleccione 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	Owner	State
demoadmin1aml21	demoadmin1	Stopped

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

#### Session Details

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

## Pilas de software () AMIs

### Note

Para ejecutar la pila de SO7 software Cent proporcionada AWS GovCloud (US), tendrás que suscribirte a The AMI Within AWS Marketplace con tu [cuenta estándar vinculada](#).

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

RES > Virtual Desktops > Software Stacks (AMIs)

## Software Stacks

Manage your Virtual Desktop Software Stacks

Search  All Operating Systems ▼

Actions ▼ Register Software Stack

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

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

## Register new Software Stack



### Name

Enter a name for the software stack

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

### Description

Enter a user friendly description for the software stack

### AMI Id

Enter the AMI Id

AMI Id must start with ami-xxx

### Operating System

Select the operating system for the software stack

### 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

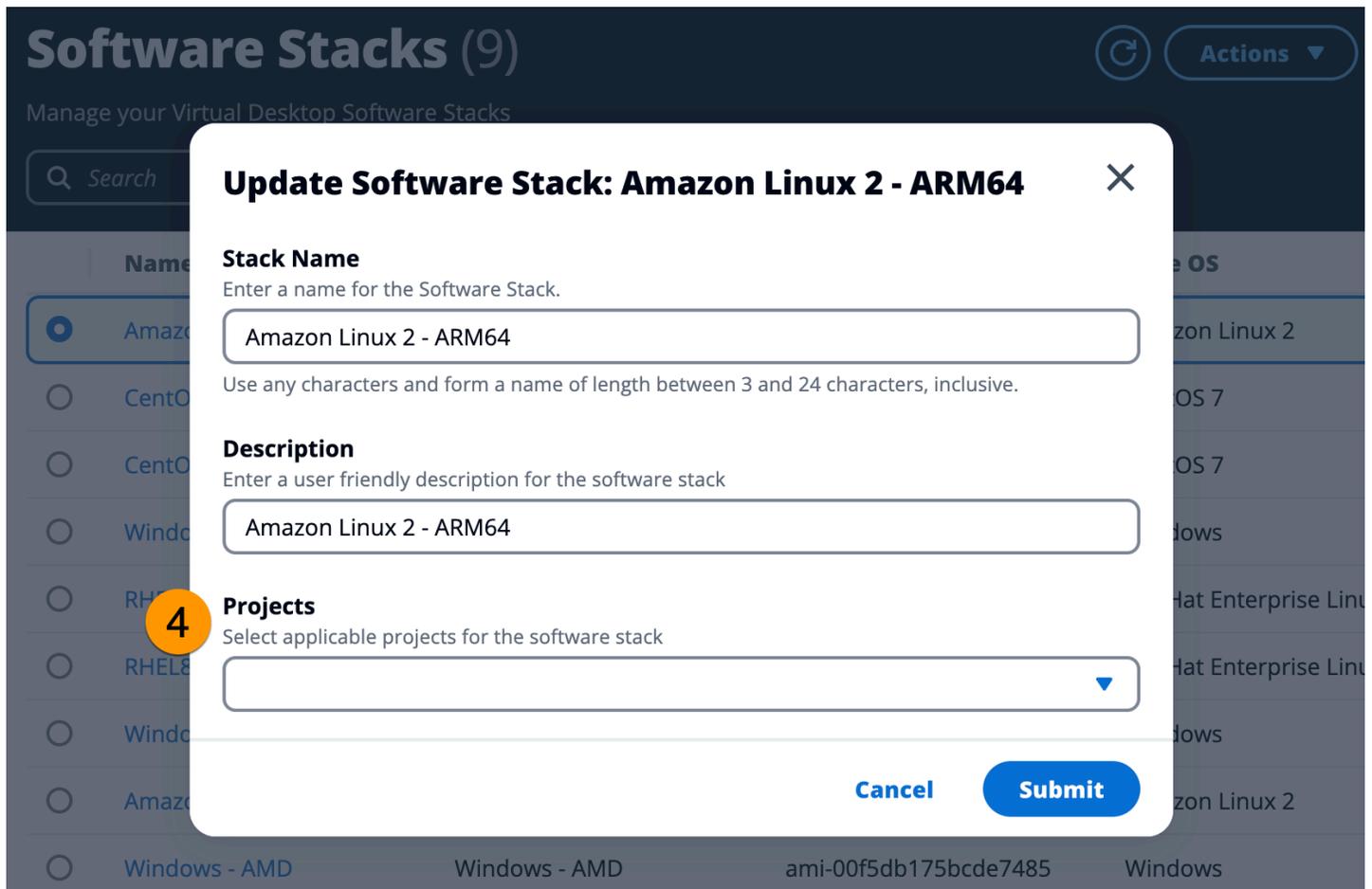
Al crear una nueva pila de software, puede asignar la pila a los proyectos. Si necesita añadir la pila a un proyecto después de la creación inicial, haga lo siguiente:

### 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. Elija Enviar.

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

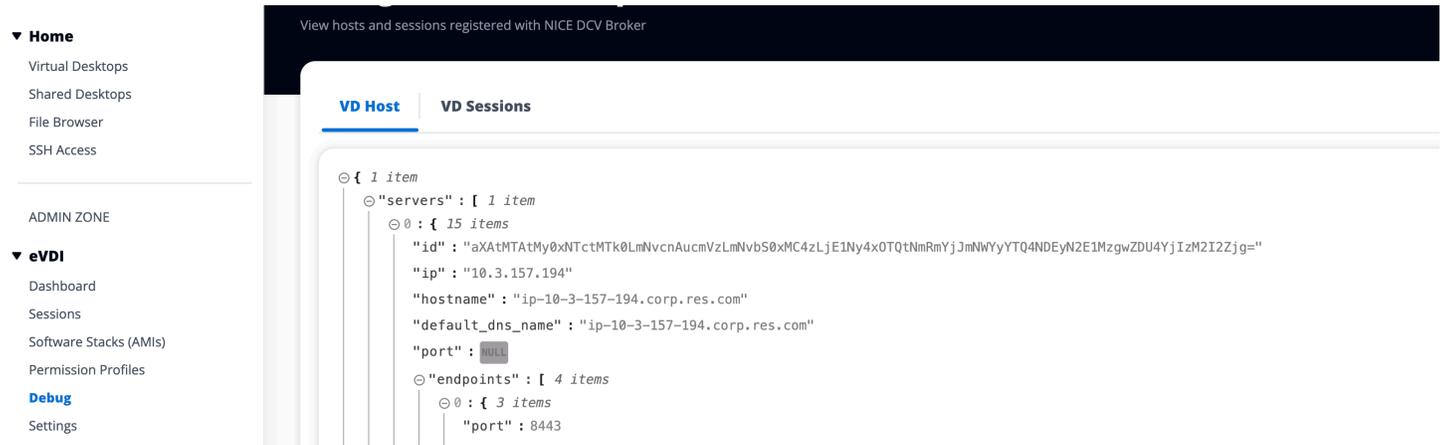


## Vea los detalles de la pila de software

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

## Debugging

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



## Configuración de escritorio

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

### DCV tiempo de espera de inactividad de la sesión

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

### Advertencia de tiempo de espera de inactividad

El tiempo transcurrido el cual se enviará al cliente una advertencia de inactividad.

### CPU umbral de utilización

La CPU utilización que debe considerarse inactiva.

### Sesiones permitidas por usuario

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

### Tamaño máximo del volumen raíz

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

## Tipos de instancias permitidos

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

The screenshot displays the 'Virtual Desktop Settings' interface for the 'res-beta08 (us-east-2)' environment. The page is divided into two main sections: 'DCV Session' and 'DCV Host'. The 'DCV Session' section includes settings for 'Idle Timeout' (1440 minutes), 'Idle Timeout Warning' (300 seconds), 'CPU Utilization Threshold' (30%), and 'Allowed Sessions Per User' (5). The 'DCV Host' section includes 'Allowed Security Groups', 'Max Root Volume Size' (100 GB), 'Denied Instance Types', and 'Allowed Instance Types' (a1.metal, c4.xlarge, g4ad, m6a, m6g, t3, g6.12xlarge). The interface also shows a navigation menu on the left and a top navigation bar with the environment name and settings options.

## 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

- [Estado del entorno](#)
- [Configuración del entorno](#)
- [Usuarios](#)
- [Grupos](#)
- [Proyectos](#)
- [Política de permisos](#)

- [Sistemas de archivos](#)
- [Administración de instantáneas](#)
- [Buckets de Amazon S3](#)

## Estado del entorno

La página del 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
View Environment Settings

## Environment Status

### Modules

Environment modules and status

Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	<a href="#">Config</a>	Deployed	Not Applicable	-
Cluster	cluster	2023.10	<a href="#">Stack</a>	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10	<a href="#">Stack</a>	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10	<a href="#">Stack</a>	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10	<a href="#">Stack</a>	Deployed	Not Applicable	• default
Analytics	analytics	2023.10	<a href="#">Stack</a>	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10	<a href="#">Stack</a>	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10	<a href="#">App</a>	Deployed	Healthy	• default
eVDI	vdc	2023.10	<a href="#">App</a>	Deployed	Healthy	• default
Bastion Host	bastion-host	2023.10	<a href="#">Stack</a>	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	<a href="#">Infra</a>	2023.10	m5.large	us-east-2a	Running	10.1.3.148	3.145.15
res-demo2-vdc-controller	vdc	<a href="#">App</a>	2023.10	m5.large	us-east-2a	Running	10.1.129.105	-
res-demo2-vdc-broker	vdc	<a href="#">Infra</a>	2023.10	m5.large	us-east-2b	Running	10.1.149.12	-
res-demo2-cluster-manager	cluster-manager	<a href="#">App</a>	2023.10	m5.large	us-east-2b	Running	10.1.155.249	-
res-demo2-vdc-gateway	vdc	<a href="#">Infra</a>	2023.10	m5.large	us-east-2b	Running	10.1.153.135	-

## Configuración del entorno

La página de 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 aprovisionó 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 VPC ID y la lista IDs de prefijos de acceso.

- Directory Service

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

## 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

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"> <li>IDEAUsers</li> <li>DemoUsers</li> </ul>
<input type="radio"/>	sauser2	3011	3011	sauser2@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> <li>SAUsers</li> </ul>
<input type="radio"/>	demoadmin4	3003	3003	demoadmin4@demo.	Yes	admin	Yes	Enabled	<ul style="list-style-type: none"> <li>DemoAdmins</li> <li>AWS Delegated Administrators</li> <li>IDEAUsers</li> </ul>
<input type="radio"/>	pmtuser02	8001	6001	pmtuser02@demo.	No	user	No	Enabled	<ul style="list-style-type: none"> <li>ProductUsers</li> </ul>

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

Search

Title	Group Name	Type	Role	Status	GID
<input checked="" type="radio"/> IDEAUsers	IDEAUsers	external	user	Enabled	4000
<input type="radio"/> SAAAdmins	SAAAdmins	external	user	Enabled	3035
<input type="radio"/> AWS Delegated Administrators	AWS Delegated Administrators	external	admin	Enabled	3999

**Users in IDEAUsers**

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

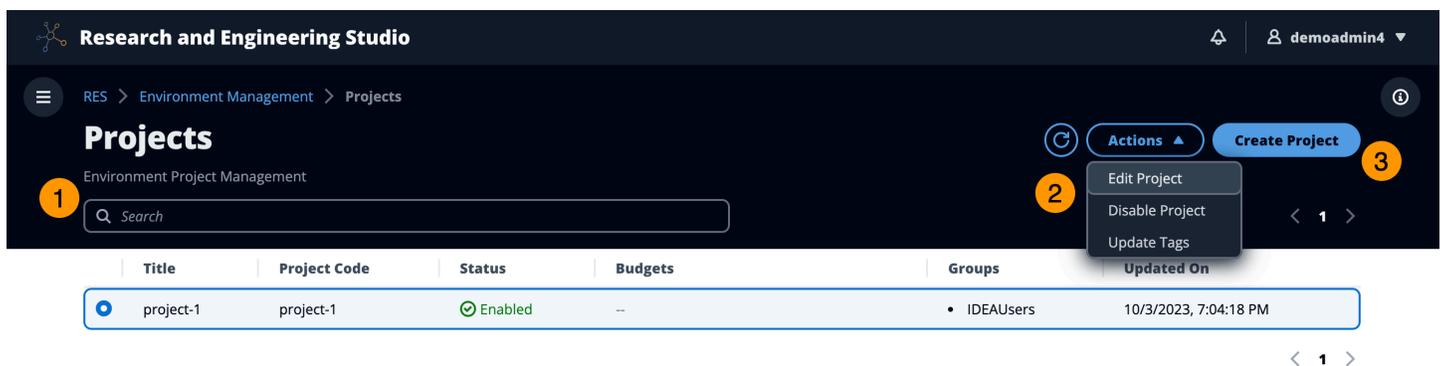
# Proyectos

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



The screenshot shows the 'Projects' section in the Research and Engineering Studio. The interface includes a search bar (1), a table of projects, and an actions menu (2) with options like 'Edit Project', 'Disable Project', and 'Update Tags'. A 'Create Project' button (3) is also visible.

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. El sistema de archivos del directorio principal puede utilizar el sistema de archivos principal compartido (predeterminado)EFS, FSx para Lustre o almacenamiento por volumen. FSx NetApp ONTAP EBS

Es importante tener en cuenta que el sistema de archivos principal compartido, en el caso de LustreEFS, FSx se puede compartir entre varios proyectos y FSx NetApp ONTAP. VDIs Sin embargo, la opción de almacenamiento por EBS volumen requerirá que todos VDI los miembros de ese proyecto tengan su propio directorio principal que no se comparta entre otros VDIs proyectos.

## 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

**Storage resources**

Add file systems and/or S3 buckets to the project.

**Home directory filesystem**

Select the filesystem that will be used to create the user home directories on Linux desktops.

**► Advanced Options**

5. Asigne a los usuarios o grupos el rol apropiado («miembro del proyecto» o «propietario del proyecto»). Consulta [Perfiles de permisos predeterminados](#) las acciones que puede realizar cada rol.
6. Elija 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

<b>Groups</b> Select applicable ldap groups for the Project	<b>Role</b> Choose a role for the group	<b>Remove group</b>
group_1	Project Member	
<b>Add group</b>		
<b>Users</b> Select applicable users for the Project	<b>Role</b> Choose a role for the user	<b>Remove user</b>
user1	Project Member	
<b>Add user</b>		

**Cancel** **Submit**

## Edita un proyecto

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

<b>Groups</b> Select applicable ldap groups for the Project	<b>Role</b> 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 group"/>	
<b>Users</b> Select applicable users for the Project	<b>Role</b> 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's a header with 'Projects' and 'Environment Project Management'. A search bar is present. Below is a table of projects:

Title	Project Code	Status	Budgets	Groups	Updated On
project-1	project-1	Enabled	--	• IDEAUsers	10/3/2023, 9:06:30 PM

Below the table, the 'File Systems in project-1' panel is expanded, showing a table with the following columns:

Title	Name	File System ID	Mount Target	Projects	Scope	Provider	Created through RES?
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, IAM políticas y scripts de lanzamiento, para todas las VDI instancias del proyecto.

### Agregue políticas

Puede añadir una IAM política para controlar el VDI acceso 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 IAM funciones, 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 VDI instancias de su proyecto. Para incorporar un grupo de seguridad, etiquételo con el siguiente par clave-valor:

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

Para obtener más información sobre los grupos de seguridad, consulte [Controle el tráfico a sus AWS recursos mediante grupos de seguridad](#) en la Guía del VPC usuario de Amazon.

## Agregue scripts de lanzamiento

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

### Ejecutar el script al VDI iniciar

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

### Ejecute el script cuando VDI esté configurado

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

Los scripts admiten las siguientes opciones:

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

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

**▼ 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

## Política de permisos

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

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

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

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

## Temas

- [Permisos de gestión de proyectos](#)
- [VDIpermisos de administración de sesiones](#)
- [Administrar los perfiles de permisos](#)
- [Perfiles de permisos predeterminados](#)
- [Límites del entorno](#)
- [Perfiles para compartir escritorios](#)

## Permisos de gestión de proyectos

### Actualizar la membresía del proyecto

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

### Team Configurations

**Groups** [Info](#)

group\_1 ▼

group\_2 ▼

[Add group](#)

No users attached. Click 'Add user' below to get started.

[Add user](#)

**Permission profile** [Info](#)

Project Owner ▼ [Remove](#)

⚠ Users/groups assigned to this permission profile can grant themselves or others higher privileges for this project by re-assigning personnel to a different permission profile

Project Member ▼ [Remove](#)

[Cancel](#) [Submit](#)

## Actualizar el estado del proyecto

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

Title	Project Code	Status	Budgets	Groups	Users	Updated On
project2	Project2	Enabled	--	• group_2	• user1	7/15/2024, 11:45:22 AM
project3	Project3	Enabled	--	• group_1 • group_2	-	7/15/2024, 8:05:20 AM

## VDI permisos de administración de sesiones

### Crear una sesión

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

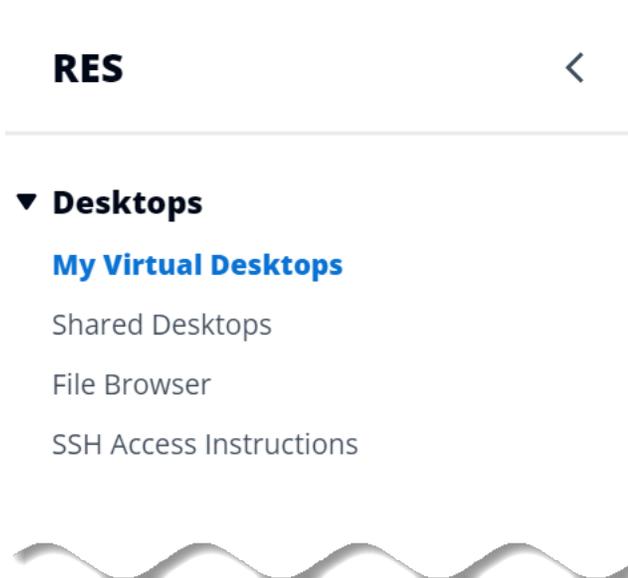
Si un usuario que no es administrador no tiene permisos para crear una sesión, se le deshabilitará el botón Iniciar un nuevo escritorio virtual, tal y como se muestra a continuación:

## Cree o finalice las sesiones de otros

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

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

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

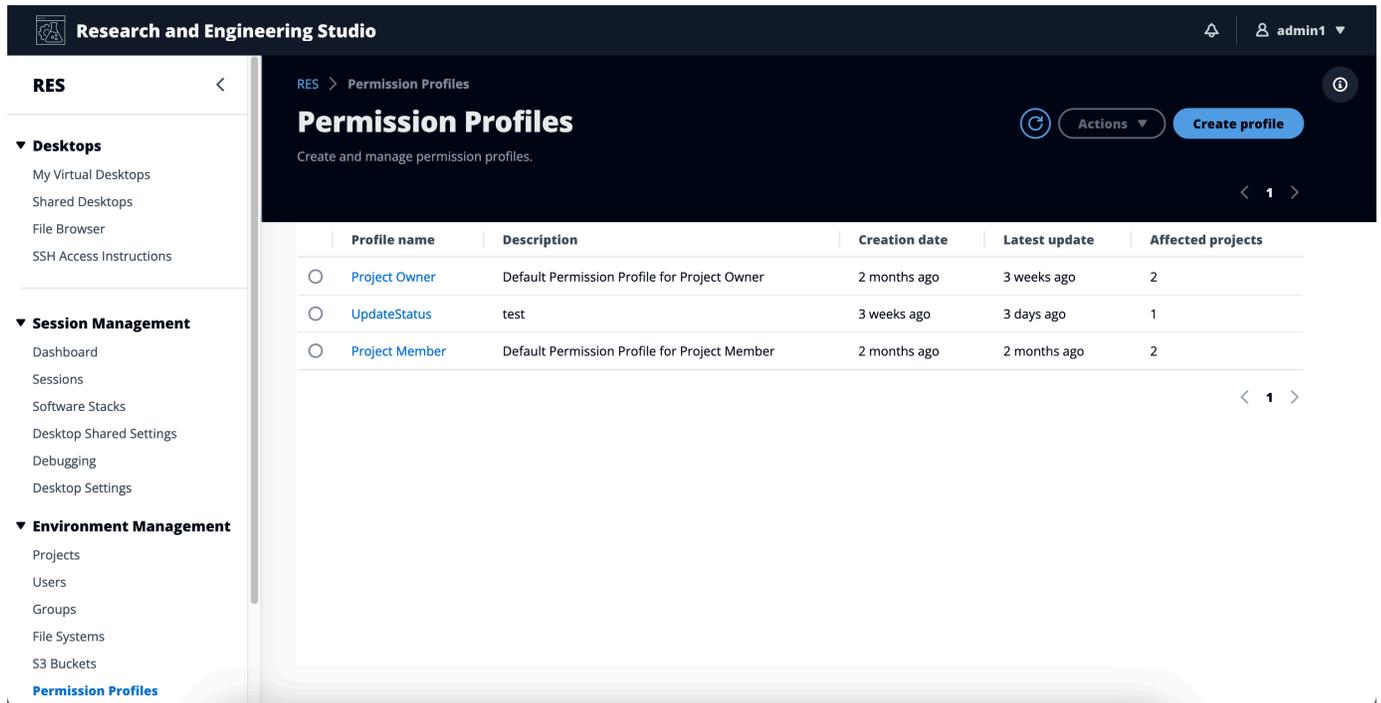


## Administrar los perfiles de permisos

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

Enumere los perfiles de permisos

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



The screenshot shows the 'Permission Profiles' page in the Research and Engineering Studio. The page has a dark header with the studio name and a user profile 'admin1'. A left sidebar contains navigation options under 'RES', including Desktops, Session Management, and Environment Management. The main content area features a title 'Permission Profiles' with a subtitle 'Create and manage permission profiles.' and a 'Create profile' button. Below this is a table with the following data:

	Profile name	Description	Creation date	Latest update	Affected projects
<input type="radio"/>	<a href="#">Project Owner</a>	Default Permission Profile for Project Owner	2 months ago	3 weeks ago	2
<input type="radio"/>	<a href="#">UpdateStatus</a>	test	3 weeks ago	3 days ago	1
<input type="radio"/>	<a href="#">Project Member</a>	Default Permission Profile for Project Member	2 months ago	2 months ago	2

## Ver los perfiles de permisos

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

RES > Permission Profiles > Project Owner

## Project Owner

Edit Delete

### General Settings

<b>Profile ID</b> project_owner	<b>Description</b> Default Permission Profile for Project Owner	<b>Creation date</b> 3 weeks ago
		<b>Latest update</b> 3 weeks ago

**Permissions** | Affected projects

### Permissions (4)

Permissions granted to this permission profile.

**Project management permissions (selected 2/2)**

<b>Update project membership</b> Update users and groups associated with a project. Enabled	<b>Update project status</b> Enable or disable a project. Enabled
---	---

**VDI session management permissions (selected 2/2)**

<b>Create session</b> Create your own session. Users can always terminate their own sessions with or without this permission. Enabled	<b>Create/Terminate other's session</b> Create/Terminate another user's session within a project. Enabled
---	---

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

RES > Permission Profiles > Project Owner

## Project Owner

Edit Delete

### General Settings

<b>Profile ID</b> project_owner	<b>Description</b> Default Permission Profile for Project Owner	<b>Creation date</b> 2 months ago
		<b>Latest update</b> 4 hours ago

**Permissions** | **Affected projects**

### Affected projects (2)

List of projects using this permission profile.

Project name	Groups	Users
<a href="#">Project1</a>	1	2
<a href="#">Project3</a>	2	0

## Cree perfiles de permisos

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

The screenshot shows the 'Create permission profile' form in the RES application. The breadcrumb navigation is 'RES > Permission Profiles > Create Profile'. The form is titled 'Create permission profile' and is divided into two main sections: 'Permission profile definition' and 'Permissions'.

**Permission profile definition**

**Profile name**  
Assign a name to the profile

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

**Profile description**  
Optionally add more details to describe the specific profile

**Permissions**  
Permissions granted to this permission profile.

**Project management permissions**

<b>Update project membership</b> Update users and groups associated with a project. <input type="checkbox"/>	<b>Update project status</b> Enable or disable a project. <input type="checkbox"/>
--	--

**VDI session management permissions**

<b>Create session</b> Create a session within a project <input type="checkbox"/>	<b>Create/Terminate other's session</b> Create/Terminate another user's session within a project <input type="checkbox"/>
--	---

At the bottom right of the form, there are two buttons: 'Cancel' and 'Create profile'.

## Editar perfiles de permisos

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

RES > Permission Profiles > Project Member > Edit

## Edit Project Member

### Permission profile definition

**Profile name**  
Assign a name to the profile

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

**Profile description**  
Optionally add more details to describe the specific profile

### Permissions

Permissions granted to this permission profile.

#### Project management permissions

<b>Update project membership</b> Update users and groups associated with a project. <input type="checkbox"/>	<b>Update project status</b> Enable or disable a project. <input type="checkbox"/>
--	--

#### VDI session management permissions

<b>Create session</b> Create your own session. Users can always terminate their own sessions with or without this permission. <input checked="" type="checkbox"/>	<b>Create/Terminate other's session</b> Create/Terminate another user's session within a project. <input type="checkbox"/>
---	--

[Cancel](#) [Save changes](#)

## Eliminar perfiles de permisos

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

The screenshot shows the 'Permission Profiles' page in the Research and Engineering Studio. A green notification bar at the top states: '1 permission profile deleted successfully. This deletion did not impact any ongoing projects.' The page title is 'Permission Profiles' with a subtitle 'Create and manage permission profiles.' Below the title is a table with the following data:

Profile name	Description	Creation date	Latest update	Affected projects
<a href="#">Project Owner</a>	Default Permission Profile for Project Owner	2 months ago	3 minutes ago	2
<a href="#">Project Member</a>	Default Permission Profile for Project Member	2 months ago	2 months ago	2

## Perfiles de permisos predeterminados

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

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

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

## Límites del entorno

Los límites del entorno permiten a los administradores configurar los permisos que se aplicarán a nivel mundial para todos los usuarios. Esto incluye permisos como el acceso al explorador de archivos y los permisos de escritorio.

## Environment boundaries

Define the environment boundaries to set the maximum permissions applicable to users. Then create and manage project roles and desktop sharing profiles. Enabled permissions in the environment boundaries can be modified in roles and profiles listed below, while disabling permissions overwrites their status and automatically turns them to 'Disabled globally'.

### ▼ File browser permissions (enabled 1/1)

- Access data**  
Display File browser in the navigation menu and access data via web portal.

### ▼ Desktop permissions (enabled 12/12)

- |   |   |   |
|---|---|---|
| <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Display</b><br/>Receive visual data from the NICE DCV server</li> <li><input checked="" type="checkbox"/> <b>Pointer</b><br/>View NICE DCV server mouse position events and pointer shapes</li> <li><input checked="" type="checkbox"/> <b>Mouse</b><br/>Input from the client mouse to the NICE DCV server</li> <li><input checked="" type="checkbox"/> <b>Audio Out</b><br/>Receive audio from the NICE DCV server to the client</li> </ul> | <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Keyboard</b><br/>Input from the client keyboard to the NICE DCV server</li> <li><input checked="" type="checkbox"/> <b>Keyboard SAS</b><br/>Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well</li> <li><input checked="" type="checkbox"/> <b>Screenshot</b><br/>Save a screenshot of the remote desktop</li> </ul> | <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Clipboard Copy</b><br/>Copy data from the NICE DCV server to the client clipboard</li> <li><input checked="" type="checkbox"/> <b>Clipboard Paste</b><br/>Copy data to the NICE DCV server from the client clipboard</li> <li><input checked="" type="checkbox"/> <b>File Upload</b><br/>Upload files to the session storage</li> <li><input checked="" type="checkbox"/> <b>File Download</b><br/>Download files from the session storage</li> </ul> |
|---|---|---|

### ▼ Desktop advanced settings (enabled 8/8)

- |   |  |  |
|---|--|--|
| <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Audio In</b><br/>Send audio from the client to the NICE DCV server</li> <li><input checked="" type="checkbox"/> <b>Printer</b><br/>Create PDFs or XPS files from the NICE DCV server to the client</li> </ul> | <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>USB</b><br/>Use USB devices from the client</li> <li><input checked="" type="checkbox"/> <b>Smartcard</b><br/>Read the smart card from the client</li> <li><input checked="" type="checkbox"/> <b>Stylus</b><br/>Input from specialized USB devices, such as 3D pointing devices or graphic tablets</li> </ul> | <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Web Camera</b><br/>Use the Web Camera connected to a client device in a session</li> <li><input checked="" type="checkbox"/> <b>Touch</b><br/>Use native touch events from the client device</li> <li><input checked="" type="checkbox"/> <b>Gamepad</b><br/>Use gamepads connected to a client computer in a session</li> </ul> |
|---|--|--|

## Configuración del acceso al explorador de archivos

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

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

## Configuración de permisos de escritorio

Los administradores pueden activar o desactivar los permisos de escritorio para administrar globalmente la VDI funcionalidad de todos los propietarios. Todos estos permisos, o un subconjunto, se pueden usar para crear perfiles de uso compartido de escritorios que determinen qué acciones

pueden realizar los usuarios con los que se comparte un escritorio. Si se deshabilita algún permiso de escritorio, se deshabilitarán automáticamente los permisos correspondientes en los perfiles de uso compartido del escritorio. Estos permisos se etiquetarán como «Deshabilitados globalmente». Incluso si el administrador vuelve a habilitar este permiso de escritorio, el permiso del perfil de uso compartido del escritorio permanecerá deshabilitado hasta que el administrador lo habilite manualmente.

## Perfiles para compartir escritorios

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

### Crear perfil

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

Project roles | **Desktop sharing profiles**

### Desktop sharing profiles

Manage your desktop sharing profiles.

Search

Actions Create profile

Desktop sharing profile ID	Title	Description	Created On
testprofile_1	testProfile_1		9/15/2024, 9:29:55
observer_profile	View Only Profile	This profile grants view only access on the DCV Session. Can see screen only. Can not control session	9/11/2024, 2:10:22

## Profile definition

### Profile name

Assign a name to the profile.

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

### Profile description - *optional*

Optionally add more details to describe the specific profile.

## Permissions

Permissions granted to this sharing profile. To enable the permissions that are 'Disabled globally', go back to the Environment boundaries and enable them there.

### ▼ Desktop permissions (enabled 12/12)

- |  |   |  |
|--|---|--|
| <p><input checked="" type="radio"/> <b>Display</b><br/>Receive visual data from the NICE DCV server</p> <p><input checked="" type="radio"/> <b>Pointer</b><br/>View NICE DCV server mouse position events and pointer shapes</p> <p><input checked="" type="radio"/> <b>Mouse</b><br/>Input from the client mouse to the NICE DCV server</p> <p><input checked="" type="radio"/> <b>Audio Out</b><br/>Receive audio from the NICE DCV server to the client</p> <p><input checked="" type="radio"/> <b>Unsupervised Access</b><br/>Allow a user to connect to session without supervision</p> | <p><input checked="" type="radio"/> <b>Keyboard</b><br/>Input from the client keyboard to the NICE DCV server</p> <p><input checked="" type="radio"/> <b>Keyboard SAS</b><br/>Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well</p> <p><input checked="" type="radio"/> <b>Screenshot</b><br/>Save a screenshot of the remote desktop</p> | <p><input checked="" type="radio"/> <b>Clipboard Copy</b><br/>Copy data from the NICE DCV server to the client clipboard</p> <p><input checked="" type="radio"/> <b>Clipboard Paste</b><br/>Copy data to the NICE DCV server from the client clipboard</p> <p><input checked="" type="radio"/> <b>File Upload</b><br/>Upload files to the session storage</p> <p><input checked="" type="radio"/> <b>File Download</b><br/>Download files from the session storage</p> |
|--|---|--|

### ► Desktop advanced settings (enabled 8/8)

Cancel

Save changes

## Editar perfil

Para editar un perfil:

1. Seleccione el perfil deseado.
2. Elija Acciones y, a continuación, seleccione Editar para modificar el perfil.
3. Ajuste los permisos según sea necesario.
4. Elija Guardar cambios.

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

## Desktop sharing profiles

Manage your desktop sharing profiles.

Desktop sharing profile ID	Title	Description	Created On
<input checked="" type="radio"/> testprofile_1	testProfile_1		9/15/2024, 9:29:55
<input 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	9/11/2024, 2:10:22

### Profile definition

**Profile name**

Assign a name to the profile.

Must start with a letter. Must contain 1 to 64 alphanumeric characters.

**Profile description - optional**

Optionally add more details to describe the specific profile.

### Permissions

Permissions granted to this sharing profile. To enable the permissions that are 'Disabled globally', go back to the Environment boundaries and enable them there.

▼ Desktop permissions (enabled 12/12)

- 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
- Audio Out**  
Receive audio from the NICE DCV server to the client
- Unsupervised Access**  
Allow a user to connect to session without supervision
- Keyboard**  
Input from the client keyboard to the NICE DCV server
- Keyboard SAS**  
Use the secure attention sequence (CTRL+Alt+Del). Note: Requires Keyboard permissions as well
- Screenshot**  
Save a screenshot of the remote desktop
- 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

► Desktop advanced settings (enabled 8/8)

# Sistemas de archivos

Title	Name	File System ID	Scope	Provider
Shared Storage - Home	home	fs-0b4ce6b191491f3e4	cluster	efs
FSx Lustre	fsx_lustre	fs-0a9042e216f9e3109	project	fsx_lustre
FSx ONTAP	fsx_ontap	fs-0105118574b6e9890	project	fsx_netapp_ontap
efs home	efs_home	fs-0df4c9ac93b975142	project	efs

Desde la página Sistemas de archivos, puede:

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

## Temas

- [Cree un sistema de archivos](#)
- [Incorpore un 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 la subred IDs desde. VPC Puede encontrarla IDs en la pestaña Administración del entorno > Configuración > Red.

#### 4. Elija Enviar.

# Create new File System



## Title

Enter a user friendly file system title

Eg. EFS 01

## Name

Enter a file system name

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

## File System Provider

Select applicable file system type

## Projects

Select applicable project



## Subnet ID 1

Enter subnet id to create mount target

## Subnet ID 2

Enter second subnet to create mount target

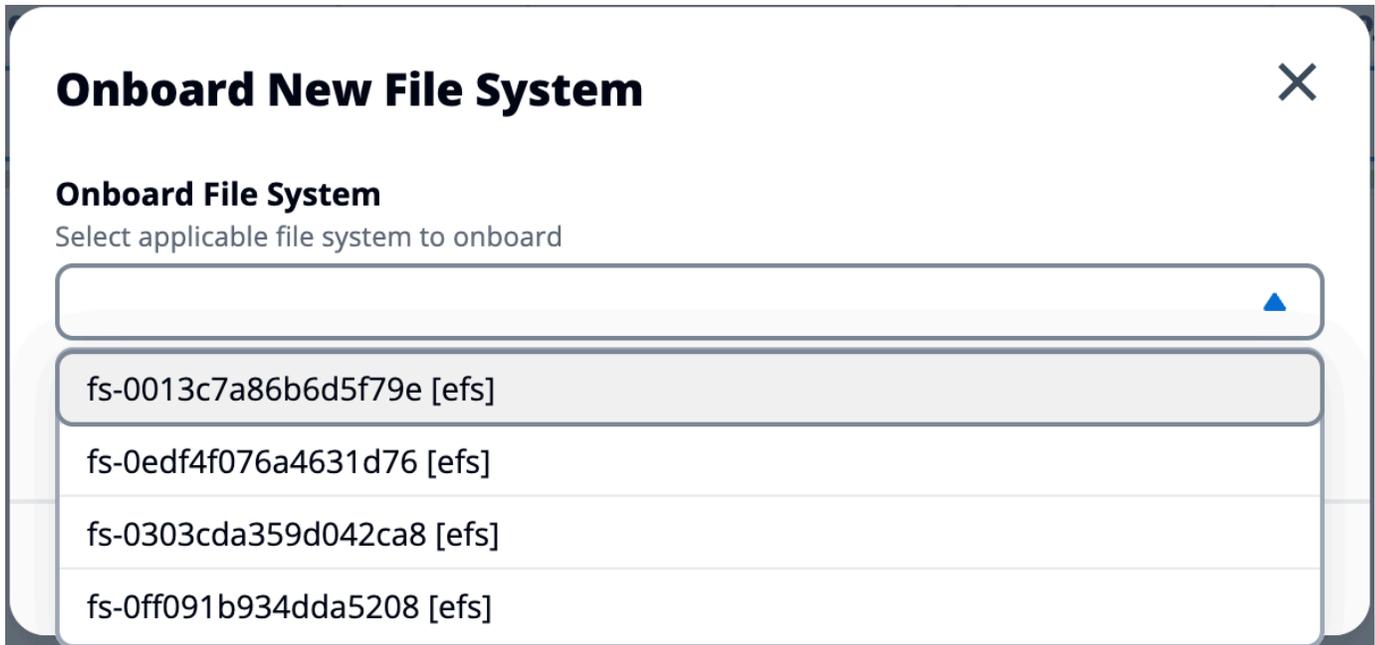
Subnet ID 1 and Subnet ID 2 should be in two different AZs

## 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.

### Note

De forma predeterminada, los administradores y propietarios de proyectos tienen la posibilidad de elegir un sistema de archivos principal al crear un nuevo proyecto, que no se puede editar posteriormente.

Los sistemas de archivos destinados a usarse como directorios principales en los proyectos deben incorporarse configurando su ruta de Mount Directory en. /home Esto rellenará el sistema de archivos incorporado en las opciones desplegadas del sistema de archivos del directorio principal. Esta función ayuda a mantener los datos aislados en todos los proyectos, ya que solo los usuarios asociados al proyecto tendrán acceso al sistema de archivos a través del suyo. VDIs VDIs montará el sistema de archivos en el punto de montaje seleccionado durante la incorporación de un sistema de archivos.

4. Elija Enviar.

# Onboard New File System



## Onboard File System

Select applicable file system to onboard

fs-0edf4f076a4631d76 [efs]



## Title

Enter a user friendly file system title

## File System Name

Enter a file system name

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

## Mount Directory

Enter directory to mount the file system

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

Cancel

Submit

## 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.

### Temas

- [Crear una instantánea](#)
- [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, sigue estos pasos:

1. Selecciona el depósito que has creado en la lista de depósitos.
2. Selecciona la pestaña Permisos.
3. En Política de bucket, elija Editar.
4. Añada la siguiente declaración a la política de bucket. Reemplace estos valores por sus propios valores:
  - AWS\_ACCOUNT\_ID
  - RES\_ENVIRONMENT\_NAME
  - AWS\_REGION
  - BUCKETS3\_ \_ 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](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.
3. Introduzca la ruta en la que desea almacenar la instantánea en el depósito. Por ejemplo, **october2023/23**.
4. Elija 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**

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

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

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

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

Para añadir permisos al depósito:

1. Selecciona el depósito que has creado en la lista de depósitos.
2. Selecciona la pestaña Permisos.
3. En Política de bucket, elija Editar.
4. Añada la siguiente declaración a la política de bucket. Reemplace estos valores por sus propios valores:
  - `AWS_ACCOUNT_ID`
  - `RES_ENVIRONMENT_NAME`
  - `AWS_REGION`
  - `BUCKETS3__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. Elija 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.

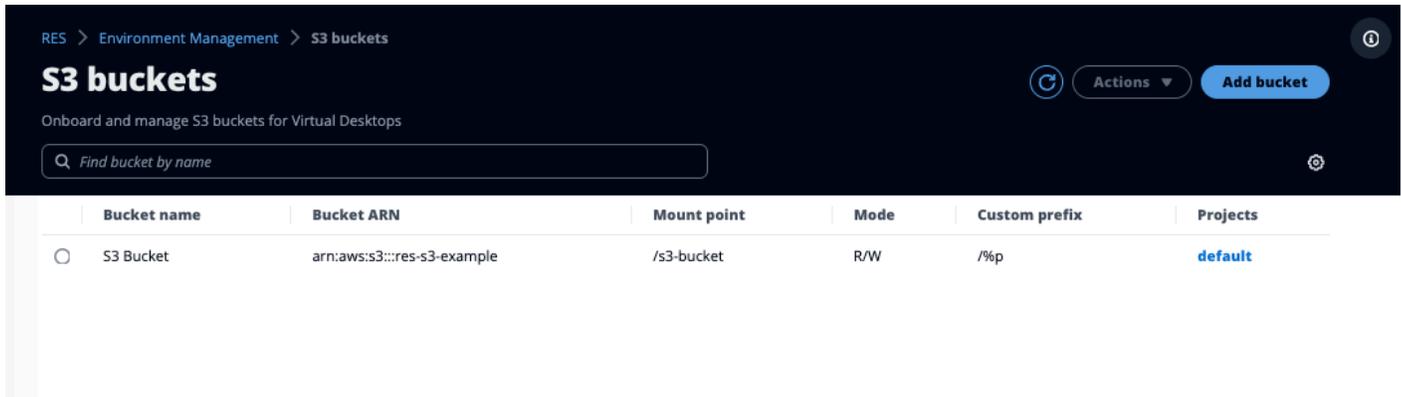
## Buckets de Amazon S3

Research and Engineering Studio (RES) admite el montaje de [buckets de Amazon S3](#) en instancias de Linux Virtual Desktop Infrastructure (VDI). RESLos administradores pueden incorporar buckets de S3RES, adjuntarlos a proyectos, editar su configuración y eliminar los buckets en la pestaña de buckets de S3 de la sección Administración del entorno.

El panel de mandos de S3 proporciona una lista de los depósitos de S3 integrados que tiene a su disposición. Desde el panel de mandos de S3, puedes:

1. Utilice Añadir depósito para incorporar un depósito de S3 aRES.
2. Seleccione un depósito de S3 y utilice el menú Acciones para:
  - Editar un bucket
  - Eliminar un balde

3. Usa el campo de búsqueda para buscar por nombre de bucket y encontrar los buckets S3 integrados.



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

## Temas

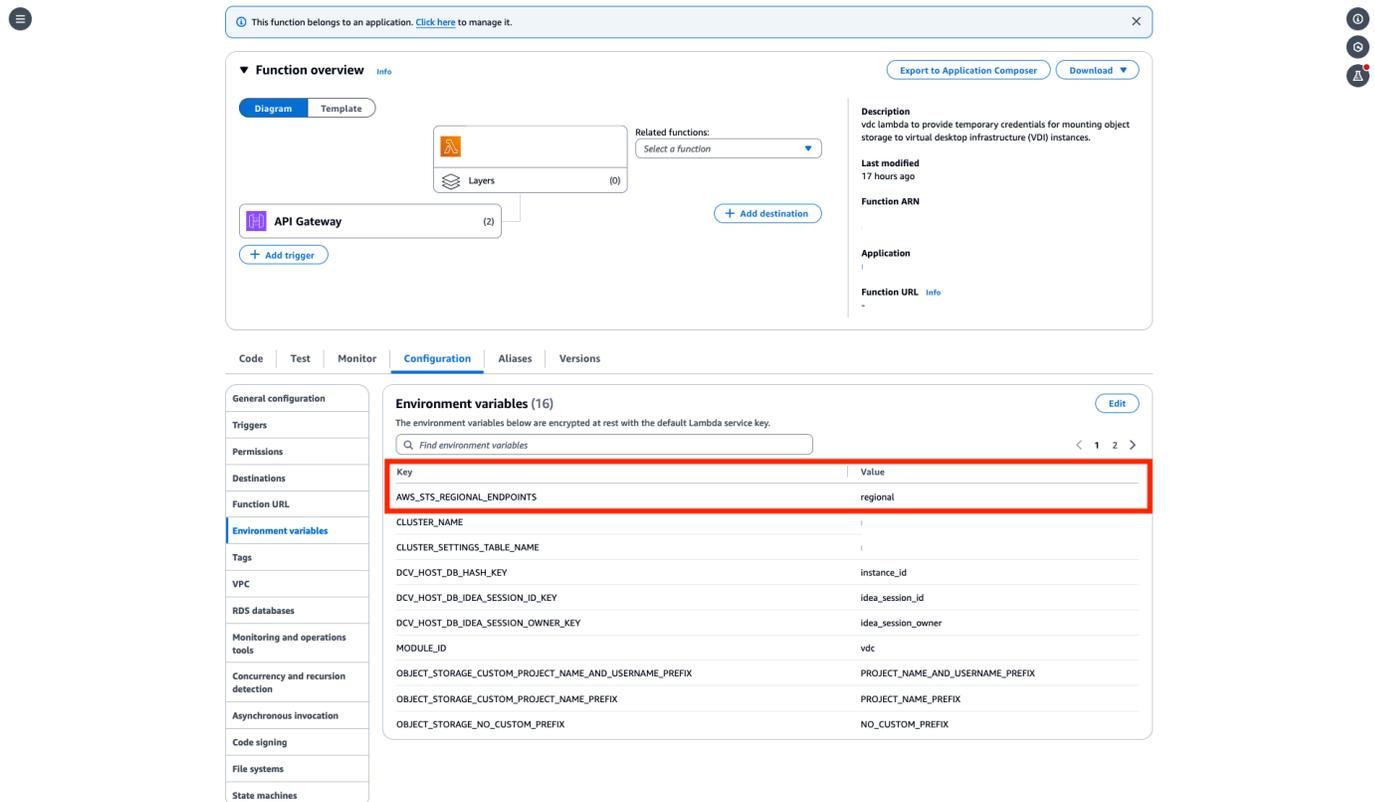
- [Requisitos previos del bucket de Amazon S3 para implementaciones aisladas VPC](#)
- [Añadir un bucket de Amazon S3](#)
- [Editar un bucket de Amazon S3](#)
- [Eliminar un bucket de Amazon S3](#)
- [Aislamiento de datos](#)
- [Acceso al bucket entre cuentas](#)
- [Evitar la exfiltración de datos en un entorno privado VPC](#)
- [Resolución de problemas](#)
- [Habilitando CloudTrail](#)

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

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

1. Inicie sesión en la consola Lambda de la AWS cuenta en la que está desplegado Research and Engineering Studio.

- Busque y navegue hasta la función Lambda denominada. `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`
- Seleccione la pestaña Configuración de la función.



The screenshot shows the AWS Lambda console interface. At the top, there's a notification bar and a 'Function overview' section with tabs for 'Diagram' and 'Template'. Below that, there's a diagram showing the function connected to an 'API Gateway'. The 'Configuration' tab is selected, and the 'Environment variables' section is highlighted with a red box. This section contains a table of 16 environment variables. The first row is highlighted in red and shows the variable 'AWS\_STS\_REGIONAL\_ENDPOINTS' with the value 'regional'.

Key	Value
AWS_STS_REGIONAL_ENDPOINTS	regional
CLUSTER_NAME	
CLUSTER_SETTINGS_TABLE_NAME	
DCV_HOST_DB_HASH_KEY	instance_id
DCV_HOST_DB_IDEA_SESSION_ID_KEY	idea_session_id
DCV_HOST_DB_IDEA_SESSION_OWNER_KEY	idea_session_owner
MODULE_ID	vdc
OBJECT_STORAGE_CUSTOM_PROJECT_NAME_AND_USERNAME_PREFIX	PROJECT_NAME_AND_USERNAME_PREFIX
OBJECT_STORAGE_CUSTOM_PROJECT_NAME_PREFIX	PROJECT_NAME_PREFIX
OBJECT_STORAGE_NO_CUSTOM_PREFIX	NO_CUSTOM_PREFIX

- En el lado izquierdo, elija Variables de entorno para ver esa sección.
- Elija Editar y añada la siguiente variable de entorno nueva a la función:
  - Clave: `AWS_STS_REGIONAL_ENDPOINTS`
  - Valor: `regional`
- Seleccione Guardar.

## Añadir un bucket de Amazon S3

Para añadir un bucket de S3 a su RES entorno:

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

**⚠ Important**

- El depósitoARN, el punto de montaje y el modo proporcionados no se pueden cambiar después de la creación.
- El depósito ARN puede contener un prefijo que aisle el depósito S3 incorporado de ese prefijo.

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

**⚠ Important**

- Consulte [Aislamiento de datos](#) para obtener más información relacionada con el aislamiento de datos con modos específicos.

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

RES > Environment Management > S3 buckets > Add bucket

## Add bucket

Currently only available for Linux desktops

### Bucket setup

**Bucket display name**  
Type a user friendly name to display

**Bucket ARN**  
Paste the copied Amazon Resource Name (ARN) from AWS S3 even across different accounts

**Mount point**  
Type the directory path where the bucket will be mounted

**Mode**

Read only (R)  
Allow user only to read or copy stored data

Read and write (R/W)  
Allow users to read or copy stored data and write or edit

**Custom prefix**  
Enable the system to create a prefix automatically

**Advanced settings - optional**

**IAM role ARN**  
To access the bucket, paste the IAM role Amazon Resource Name (ARN) copied in Identity and Access Management (IAM)

### Project association

**Projects - optional**  
Associate the bucket with the following projects. To add a new project, go to Create Project.

Cancel Submit

## Editar un bucket de Amazon S3

1. Seleccione un depósito de S3 de la lista de depósitos de S3.
2. En el menú Acciones, selecciona Editar.
3. Introduce tus actualizaciones.

### Important

- Al asociar un proyecto a un bucket de S3, no se montará el bucket en las instancias de infraestructura de escritorios virtuales existentes de ese proyecto. VDI El depósito solo

se montará en las VDI sesiones iniciadas en un proyecto una vez que el depósito se haya asociado a ese proyecto.

- La disociación de un proyecto de un bucket de S3 no afectará a los datos del bucket de S3, pero provocará que los usuarios de escritorio pierdan el acceso a esos datos.

#### 4. Selecciona Guardar configuración del bucket.

The screenshot shows the 'Edit S3 Bucket' configuration page. The breadcrumb navigation at the top reads 'RES > Environment Management > S3 buckets > Edit bucket'. The page title is 'Edit S3 Bucket'. There are two main sections: 'Bucket setup' and 'Project association'. In the 'Bucket setup' section, there is a 'Bucket display name' field with the text 'S3 Bucket' and a sub-label 'Type a user friendly name to display'. In the 'Project association' section, there is a 'Projects - optional' dropdown menu with the text 'Choose the projects to associate to the bucket'. Below the dropdown, there is a tag labeled 'default' with an 'x' icon to remove it. At the bottom right of the form, there are two buttons: 'Cancel' and 'Save bucket setup'.

## Eliminar un bucket de Amazon S3

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

### Important

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

## Aislamiento de datos

Al añadir un depósito de S3 a RES, tiene opciones para aislar los datos del depósito para destinarlos a proyectos y usuarios específicos. En la página Añadir cubo, puede seleccionar un modo de Solo lectura (R) o Lectura y escritura (R/W).

### Solo lectura

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

### Lee y escribe

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

- No hay prefijo personalizado
- `/%p`
- `/%p/%u`

RES > Environment Management > S3 buckets > Add bucket

## Add bucket

Currently only available for Linux desktops

### Bucket setup

**Bucket display name**  
Type a user friendly name to display

**Bucket ARN**  
Paste the copied Amazon Resource Name (ARN) from AWS S3 even across different accounts

**Mount point**  
Type the directory path where the bucket will be mounted

**Mode**

Read only (R)  
Allow user only to read or copy stored data

Read and write (R/W)  
Allow users to read or copy stored data and write or edit

**Custom prefix**  
Enable the system to create a prefix automatically

No custom prefix ▲

No custom prefix ✓  
Will not create a dedicated directory

/%p  
Create a dedicated directory by project

/%p/%u  
Create a dedicated directory by project name and user name

**Projects - optional**  
Associate the bucket with the following projects. To add a new project, go to Create Project.

Cancel Submit

## Sin aislamiento de datos personalizado

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

## Aislamiento de datos por proyecto

Cuando /%p se selecciona el prefijo personalizado, los datos del depósito se aíslan para cada proyecto específico asociado al mismo. La %p variable representa el código del proyecto. Por ejemplo, si un administrador añade un depósito y RES utiliza el ARN `arn:aws:s3:::bucket-name` punto de montaje /%p seleccionado y un punto de montaje de `/bucket`, y asocia este depósito al proyecto A y al proyecto B, el usuario A del proyecto A puede escribir un archivo en `/bucket`. El usuario B del proyecto A también puede ver el archivo en el que escribió el usuario A `/bucket`. Sin embargo, si el usuario B lanza a VDI en el Proyecto B y busca `/bucket`, no verán

el archivo que escribió el usuario A, ya que los datos están aislados por proyecto. El archivo que escribió el usuario A se encuentra en el depósito de S3 bajo el prefijo, /ProjectA mientras que el usuario B solo puede acceder /ProjectB cuando utiliza el suyo VDIs del Proyecto B.

### Aislamiento de datos por proyecto y por usuario

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

### Acceso al bucket entre cuentas

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

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

1. Inicie sesión en la consola AWS de administración de la RES cuenta que necesita acceder al bucket de S3 (cuenta A).
2. Abre la IAM consola:
  - a. Navegue hasta el IAM panel de control.
  - b. En el panel de navegación, seleccione Políticas.
3. Cree una política:
  - a. Elija Crear política.
  - b. Seleccione la pestaña JSON.
  - c. Pegue la siguiente JSON política (`<BUCKET-NAME>` sustitúyala por el nombre del depósito de S3 ubicado en la cuenta B):

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

- d. Elija Next (Siguiente).
4. Revisa y crea la política:
    - a. Proporcione un nombre para la política (por ejemplo, AccessPolicy «S3»).
    - b. Añada una descripción opcional para explicar el propósito de la política.
    - c. Revisa la política y selecciona Crear política.
  5. Abre la IAM consola:
    - a. Navegue hasta el IAM panel de control.
    - b. Seleccione Roles en el panel de navegación.
  6. Crea un rol:
    - a. Elija Crear rol.
    - b. Elija una política de confianza personalizada como tipo de entidad de confianza.
    - c. Pegue la siguiente JSON política (<ACCOUNT\_ID> sustitúyala por el ID de cuenta real de la cuenta A, <ENVIRONMENT\_NAME> por el nombre del entorno de la RES implementación y <REGION> por la AWS región en la que RES se implementa):

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

- d. Elija Next (Siguiente).
7. Adjunte las políticas de permisos:
    - a. Busque y seleccione la política que creó anteriormente.
    - b. Elija Next (Siguiente).
  8. Etiquete, revise y cree el rol:
    - a. Introduzca el nombre de un rol (por ejemplo, AccessRole «S3»).
    - b. En el paso 3, selecciona Añadir etiqueta y, a continuación, introduce la clave y el valor siguientes:
      - Clave: res:Resource
      - Valor: s3-bucket-iam-role
    - c. Revisa el rol y selecciona Crear rol.
  9. Utilice el IAM rol en RES:
    - a. Copia el IAM rol ARN que creaste.
    - b. Inicie sesión en la RES consola.
    - c. En el panel de navegación izquierdo, selecciona S3 Bucket.
    - d. Seleccione Añadir depósito y rellene el formulario con el depósito de S3 ARN multicuenta.
    - e. Seleccione el menú desplegable Configuración avanzada (opcional).
    - f. Introduzca el rol ARN en el ARN campo del IAM rol.
    - g. Seleccione Añadir depósito.

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

1. Inicie sesión en la consola AWS de administración de la cuenta B.
2. Abra la consola S3:
  - a. Navegue hasta el panel de control de S3.
  - b. Seleccione el depósito al que quiere conceder acceso.
3. Edita la política de buckets:
  - a. Seleccione la pestaña Permisos y elija la política de buckets.
  - b. Añada la siguiente política para conceder al IAM rol de la cuenta A acceso al bucket (sustituya `<AccountA_ID>` con el ID de cuenta real de la cuenta A y `<BUCKET-NAME>` (con el nombre del depósito de S3):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountA_ID:role/S3AccessRole"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource": [
        "arn:aws:s3:::<BUCKET-NAME>",
        "arn:aws:s3:::<BUCKET-NAME>/*"
      ]
    }
  ]
}
```

- c. Seleccione Guardar.

## Evitar la exfiltración de datos en un entorno privado VPC

Para evitar que los usuarios extraigan datos de depósitos de S3 seguros y los depositen en sus propios depósitos de S3 de su cuenta, puedes conectar un VPC punto de conexión para proteger tu información privada. VPC En los siguientes pasos se muestra cómo crear un VPC punto de conexión para el servicio de S3 que permita el acceso a los buckets de S3 de su cuenta, así como a cualquier otra cuenta que tenga depósitos multicuenta.

1. Abre la Amazon VPC Console:
  - a. Inicie sesión en la consola AWS de administración.
  - b. Abre la VPC consola de Amazon en <https://console.aws.amazon.com/vpc/>.
2. Cree un VPC punto final para S3:
  - a. En el panel de navegación izquierdo, seleccione Puntos de conexión.
  - b. Elija Crear punto de conexión.
  - c. En Service category (Categoría de servicio), asegúrese de que se seleccionó AWS services (Servicios de AWS ).
  - d. En el campo Nombre del servicio, introduzca `com.amazonaws.<region>.s3` (`<region>` sustitúyalo por su AWS región) o busque «S3».
  - e. Seleccione el servicio S3 de la lista.
3. Configure los ajustes del punto final:
  - a. Para VPC, seleccione el VPC lugar en el que desea crear el punto final.
  - b. En el caso de las subredes, seleccione las dos subredes privadas utilizadas para las VDI subredes durante la implementación.
  - c. En Habilitar DNS nombre, asegúrese de que la opción esté marcada. Esto permite que el DNS nombre de host privado se resuelva en las interfaces de red de los puntos finales.
4. Configure la política para restringir el acceso:
  - a. En Política, elija Personalizado.
  - b. En el editor de políticas, introduce una política que restrinja el acceso a los recursos de tu cuenta o de una cuenta específica. A continuación, se muestra un ejemplo de política (sustituya `mybucket` con el nombre de su bucket de S3 y `111122223333` y `444455556666` con la AWS cuenta adecuada a la IDs que quieres acceder):

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

5. Cree el punto final:
  - a. Revise la configuración.
  - b. Seleccione Crear punto de conexión.
6. Verifique el punto final:
  - a. Una vez creado el punto final, vaya a la sección Puntos finales de la VPC consola.
  - b. Seleccione el punto final recién creado.
  - c. Compruebe que el estado esté disponible.

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

## Resolución de problemas

¿Cómo comprobar si un depósito no se monta en un VDI

Si un cucharón no se monta en unVDI, hay algunos lugares en los que puede comprobar si hay errores. Siga los pasos que se indican a continuación.

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

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

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

Además, consulte el `/etc/message` registro para obtener más información.

2. Compruebe los registros CloudWatch Lambda personalizados de Credential Broker:
  - a. Inicie sesión en la consola de AWS administración.
  - b. Abra la CloudWatch consola y vaya a Grupos de registros.
  - c. Busque el grupo de registros `aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`.
  - d. Examine el primer grupo de registros disponible y localice cualquier error en los registros. Estos registros contendrán detalles sobre posibles problemas y proporcionarán credenciales personalizadas temporales para el montaje de depósitos de S3.
3. Consulte los registros personalizados de Credential Broker API Gateway CloudWatch :
  - a. Inicie sesión en la consola AWS de administración.
  - b. Abra la CloudWatch consola y vaya a Grupos de registros.
  - c. Busque el grupo de registros `<stack-name>-vdc-custom-credential-broker-lambda vdc custom credential broker api gateway access logs <nonce>`.
  - d. Examine el primer grupo de registros disponible y localice cualquier error en los registros. Estos registros contendrán detalles sobre cualquier solicitud y respuesta a la API puerta de

enlace para obtener las credenciales personalizadas necesarias para montar los depósitos de S3.

¿Cómo editar la configuración de IAM roles de un bucket después de la incorporación

1. Inicie sesión en la consola de [AWS DynamoDB](#).
2. Seleccione la tabla:
  - a. En el panel de navegación izquierdo, elija Tables (Tablas).
  - b. Busque y seleccione `<stack-name>.cluster-settings`.
3. Escanea la tabla:
  - a. Elija Explorar elementos de la tabla.
  - b. Asegúrese de que esté seleccionada la opción Escanear.
4. Añadir un filtro:
  - a. Elija Filtros para abrir la sección de entrada de filtros.
  - b. Configure el filtro para que coincida con su clave
    - Atributo: introduce la clave.
    - Condición: seleccionar Empieza por.
    - Valor: Introduzca la opción de `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn` sustitución `<filesystem_id>` con el valor del sistema de archivos que se debe modificar.
5. Ejecute el escaneo:

Seleccione Ejecutar para ejecutar el escaneo con el filtro.
6. Compruebe el valor:

Si la entrada existe, asegúrese de que el valor esté establecido correctamente con el IAM rol correctoARN.

Si la entrada no existe:

  - a. Seleccione Crear elemento.
  - b. Introduzca los detalles del artículo:

- Para el atributo clave, introduzca `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`.
  - Añada el IAM rol correctoARN.
- c. Seleccione Guardar para añadir el elemento.
7. Reinicie las VDI instancias:

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

## Habilitando CloudTrail

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

# Usa el producto

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

## Temas

- [SSHacceder](#)
- [Escritorios virtuales](#)
- [Escritorios compartidos](#)
- [Explorador de archivos](#)

## SSHacceder

Para SSH usar el servidor del bastión:

1. En el RES menú, selecciona SSHacceso.
2. Sigue las instrucciones que aparecen en pantalla para usar SSH Pu TTY para acceder.

## Escritorios virtuales

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

### Sistemas operativos compatibles

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

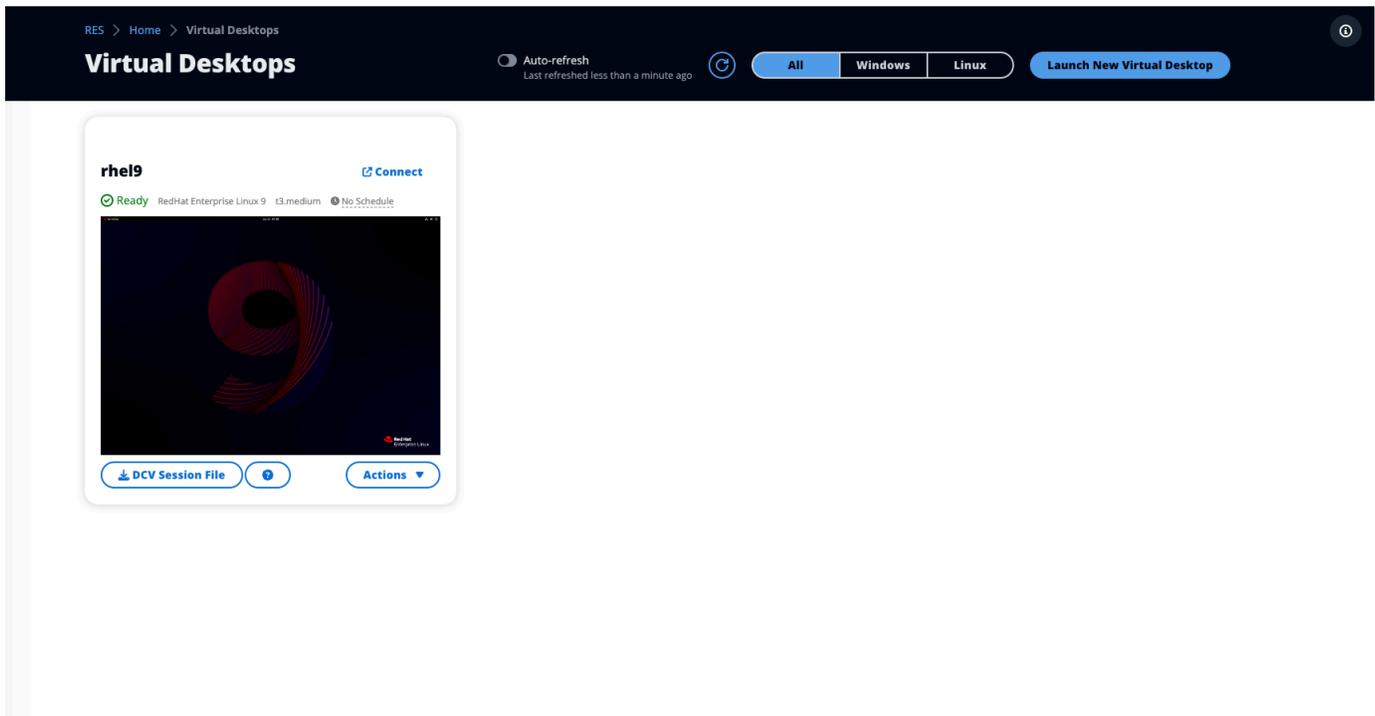
- Amazon Linux 2 (x86 yARM64)
- Ubuntu 22.04.03 (x86)
- RHEL8 (x86) y 9 (x86)
- Windows 2019, 2022 (x86)

## Temas

- [Lanza un escritorio nuevo](#)
- [Acceda a su escritorio](#)
- [Controle el estado de su escritorio](#)
- [Modifica un escritorio virtual](#)
- [Recupere la información de la sesión](#)
- [Programe escritorios virtuales](#)
- [Interfaz de escritorio virtual: parada automática](#)

## Lanza un escritorio nuevo

1. En el menú, elija Mis escritorios virtuales.
2. Seleccione Lanzar un nuevo escritorio virtual.



3. Introduzca los detalles de su nuevo escritorio.
4. Elija Enviar.

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

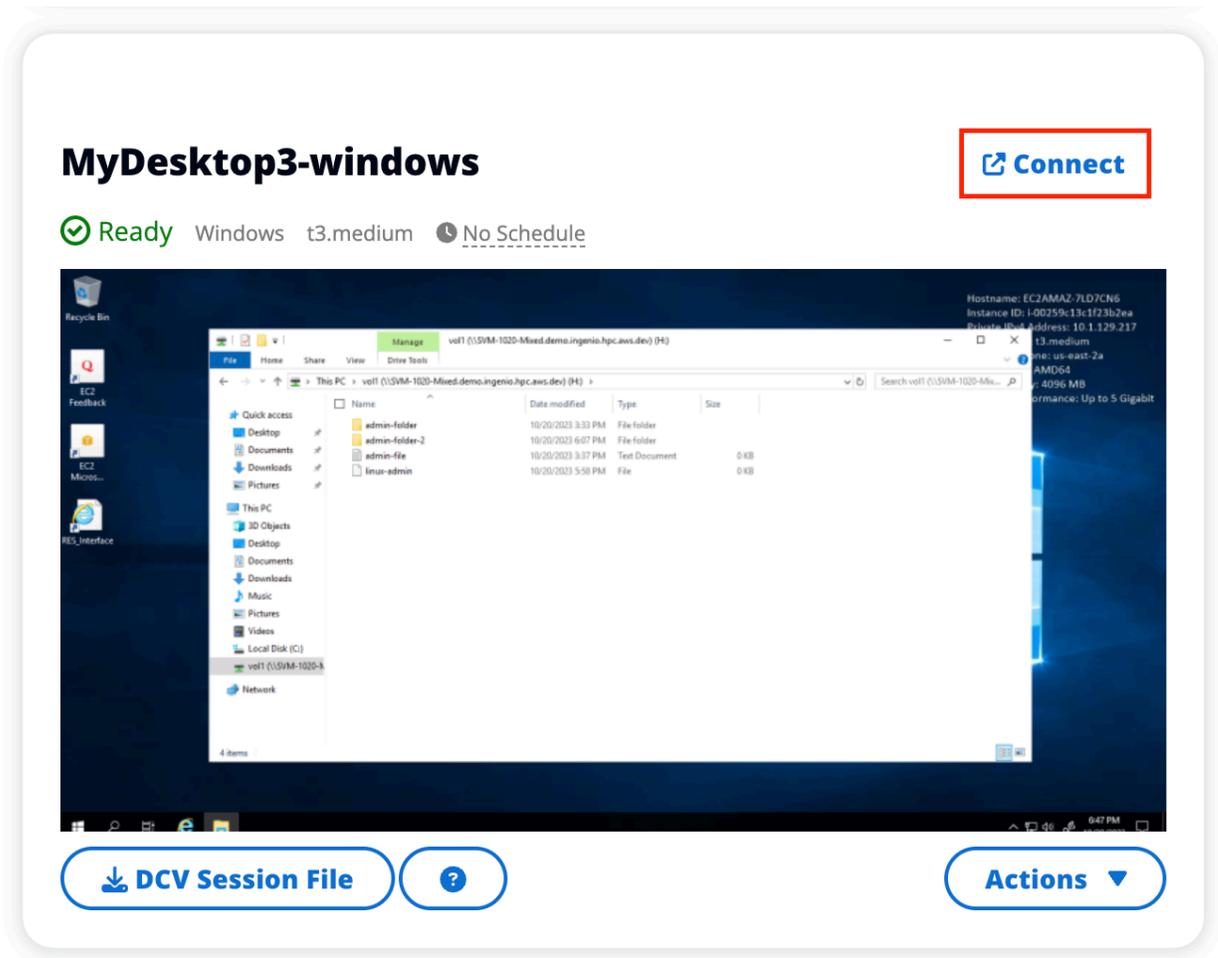
## Acceda a su escritorio

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

### Web connection

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

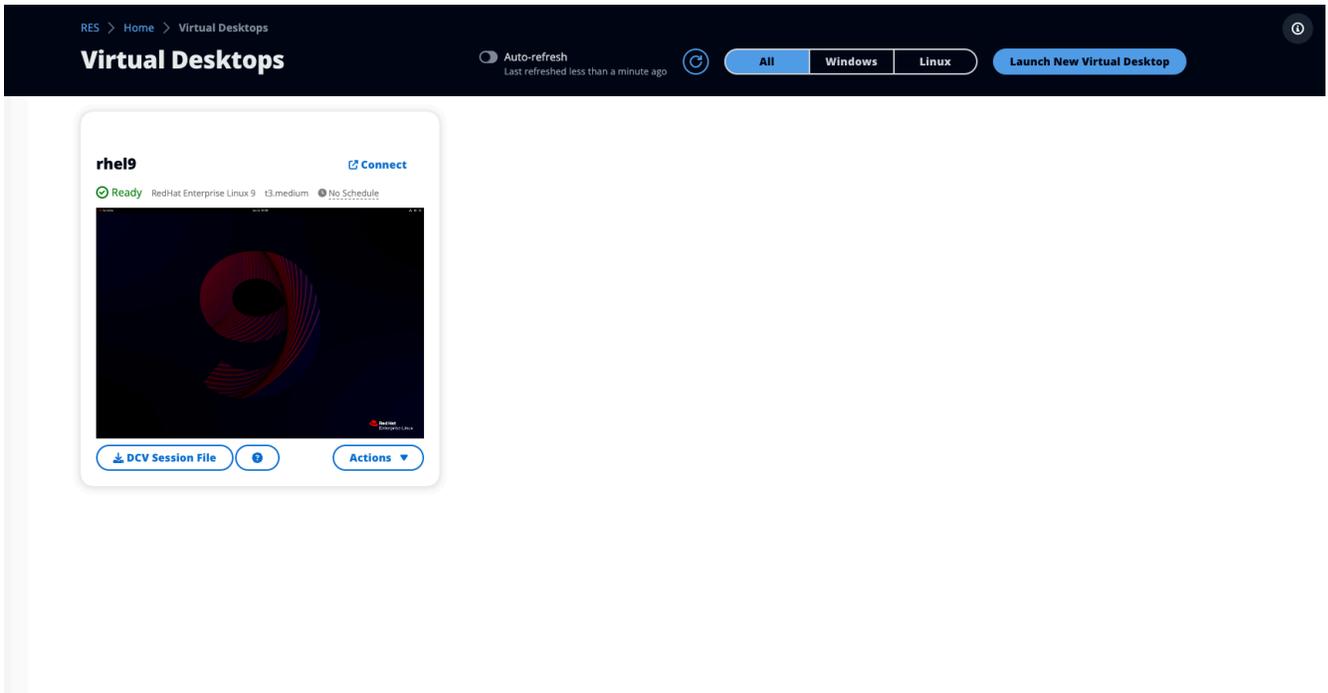
- Selecciona Connect o elige la miniatura para acceder al escritorio directamente a través del navegador.



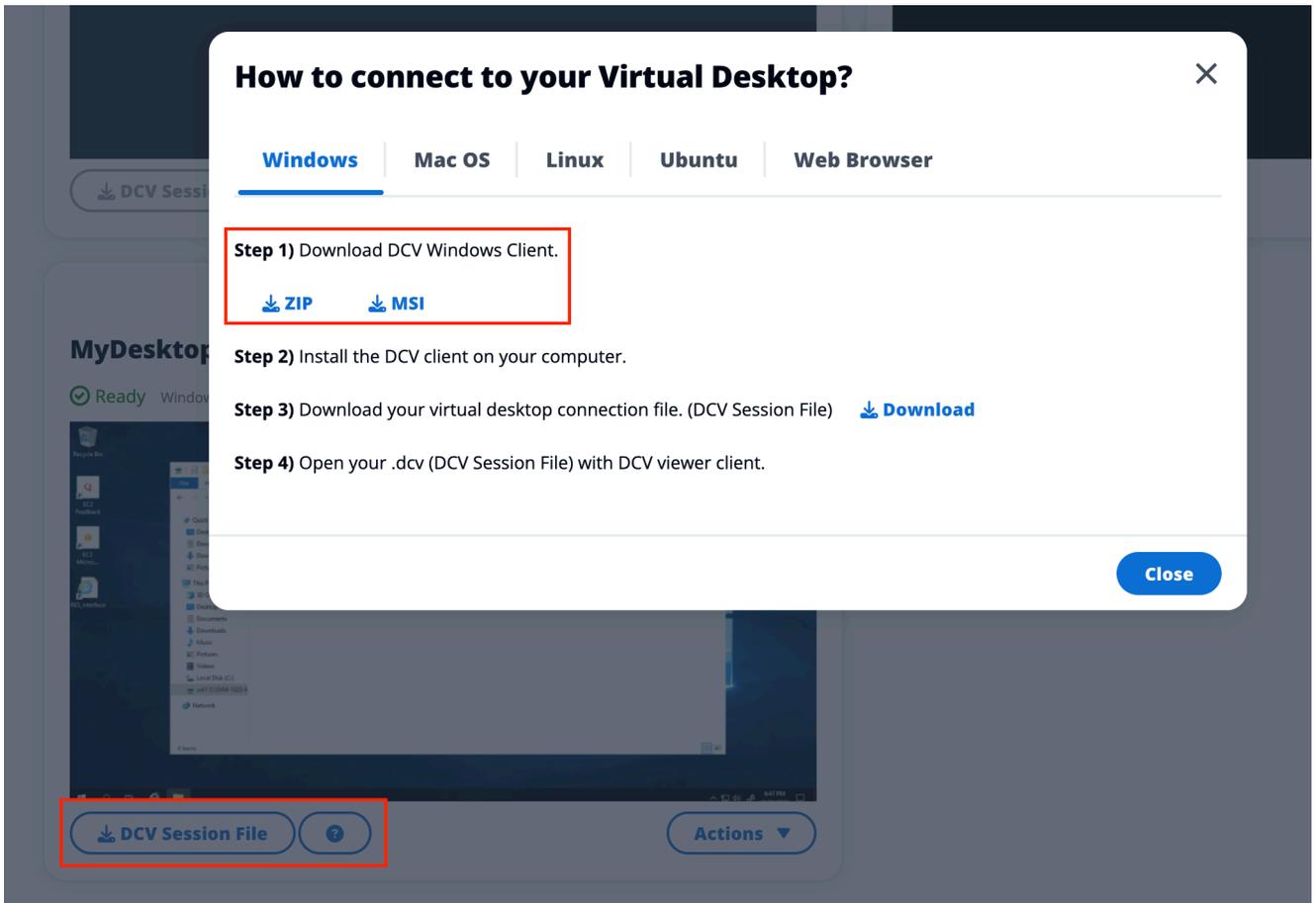
### DCV connection

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

1. Seleccione Archivo de DCV sesión para descargar el .dcv archivo. Necesitará tener un DCV cliente instalado en su sistema.



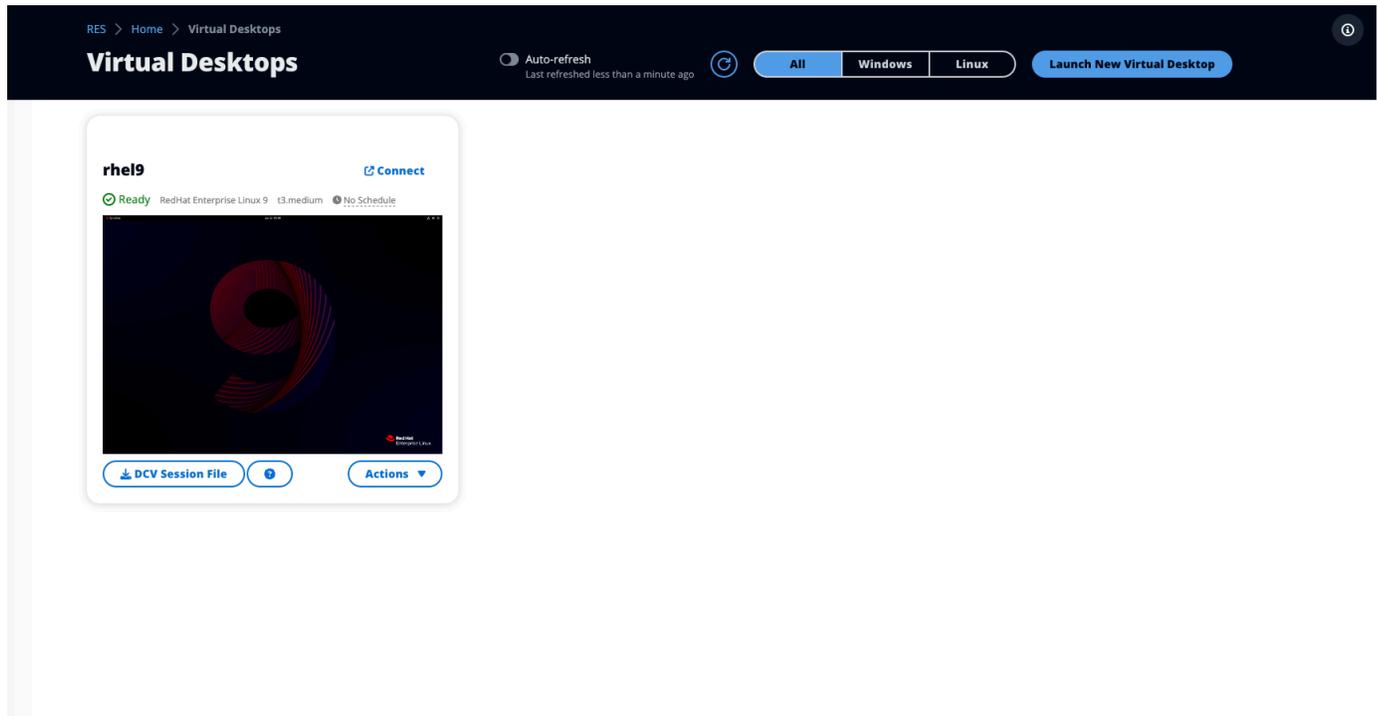
2. Para ver las instrucciones de instalación, elija la opción? icono.



## Controle el estado de su escritorio

Para controlar el estado del escritorio:

1. Elija Actions.



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

- 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 RES archivos antes de finalizar.

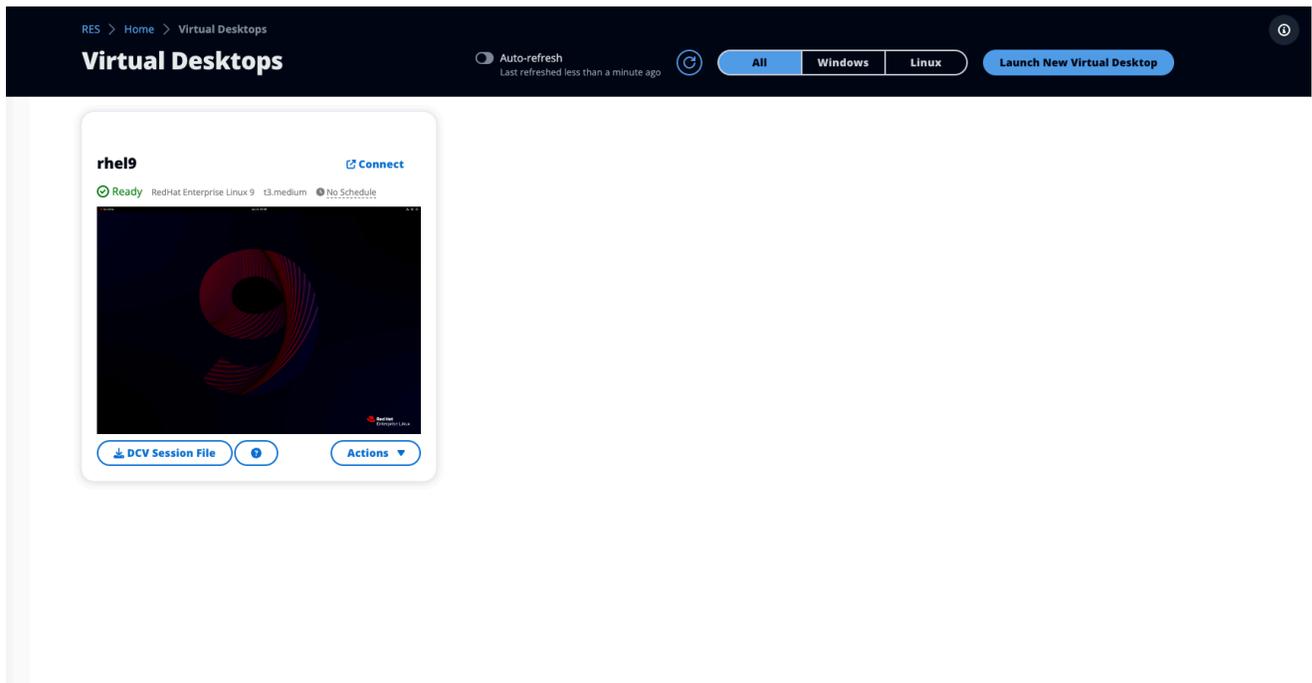
- Hibernar

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

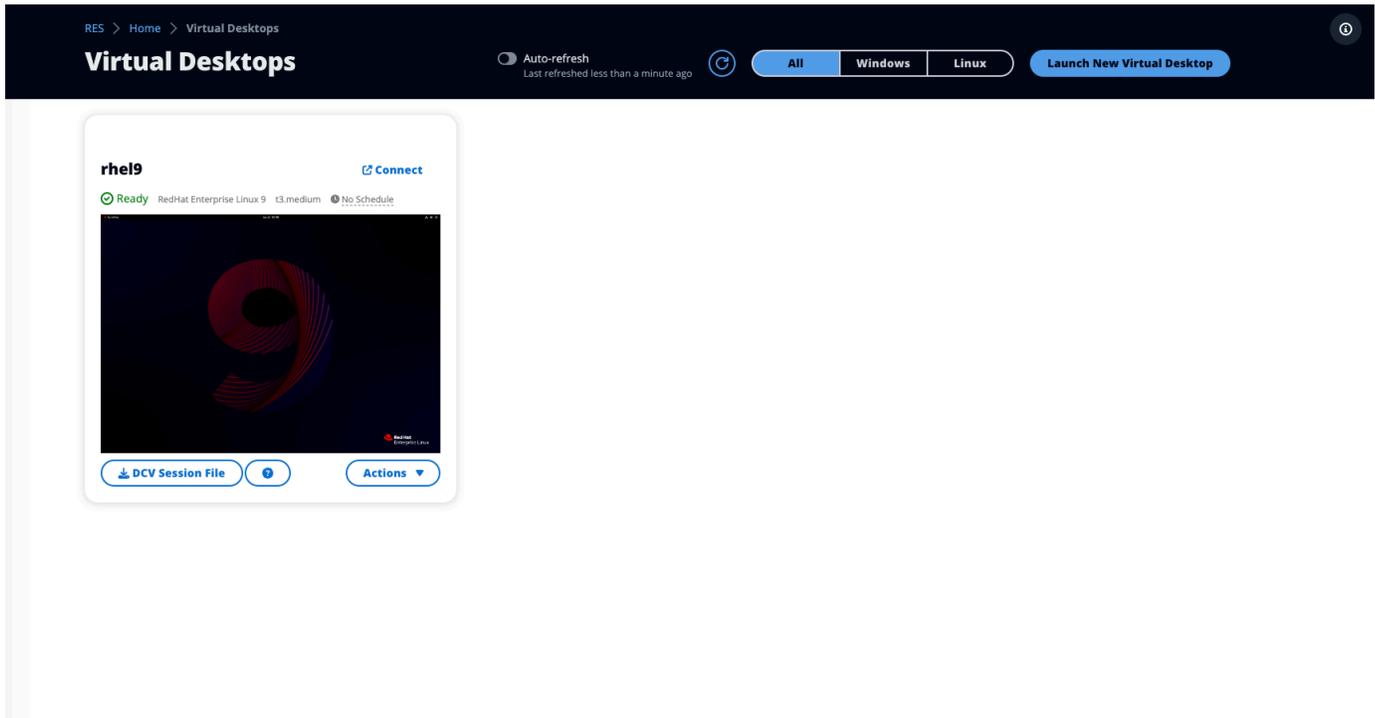
No puede actualizar el tamaño del escritorio para las sesiones en hibernación.

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. Elija 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.

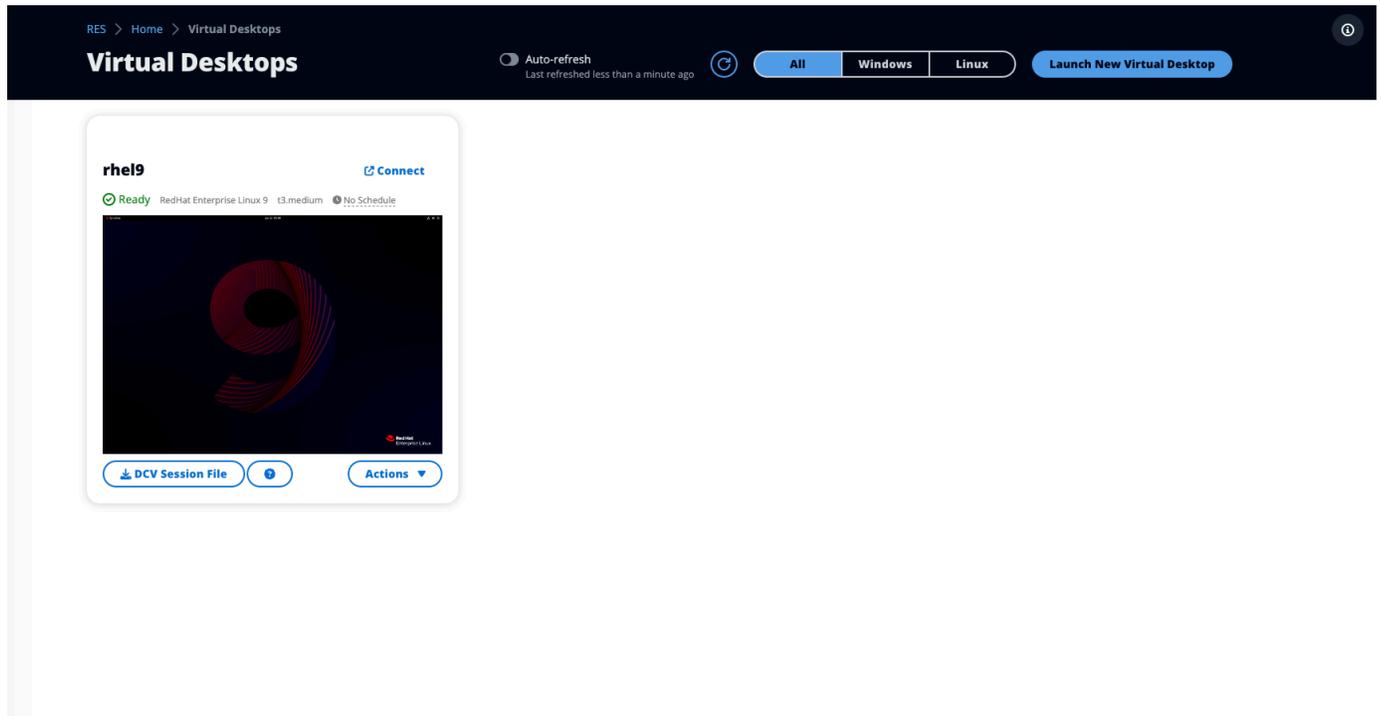


2. Selecciona Mostrar información.

## 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 CPU uso es inferior al 15% durante al menos 15 minutos. Puede configurar un horario 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

## Interfaz de escritorio virtual: parada automática

Los administradores pueden configurar los ajustes para permitir detener o finalizar la inactividadVDIs. Hay 4 ajustes configurables:

1. Tiempo de espera de inactividad: se agotará el tiempo de espera de las sesiones inactivas durante este tiempo con un CPU uso inferior al umbral.
2. CPUUmbral de utilización: las sesiones sin interacción y por debajo de este umbral se consideran inactivas. Si se establece en 0, las sesiones nunca se considerarán inactivas.
3. Estado de transición: una vez transcurrido el tiempo de espera de inactividad, las sesiones pasarán a este estado (detenidas o terminadas).
4. Hacer cumplir la programación: si se selecciona, una sesión que se haya detenido por estar inactiva se puede reanudar según su programación diaria.

## Update Session Settings ✕

**Idle Timeout (minutes)**

Sessions idle for this time with CPU utilization below the threshold will time out

**CPU Utilization Threshold (%)**

Sessions under this threshold are considered idle

**Transition State**

Sessions will transition to this state after idle timeout

**Enforce Schedule**

Enable to allow schedule to resume a session that has been stopped for being idle

**Allowed Sessions Per User**

Maximum sessions allowed per user

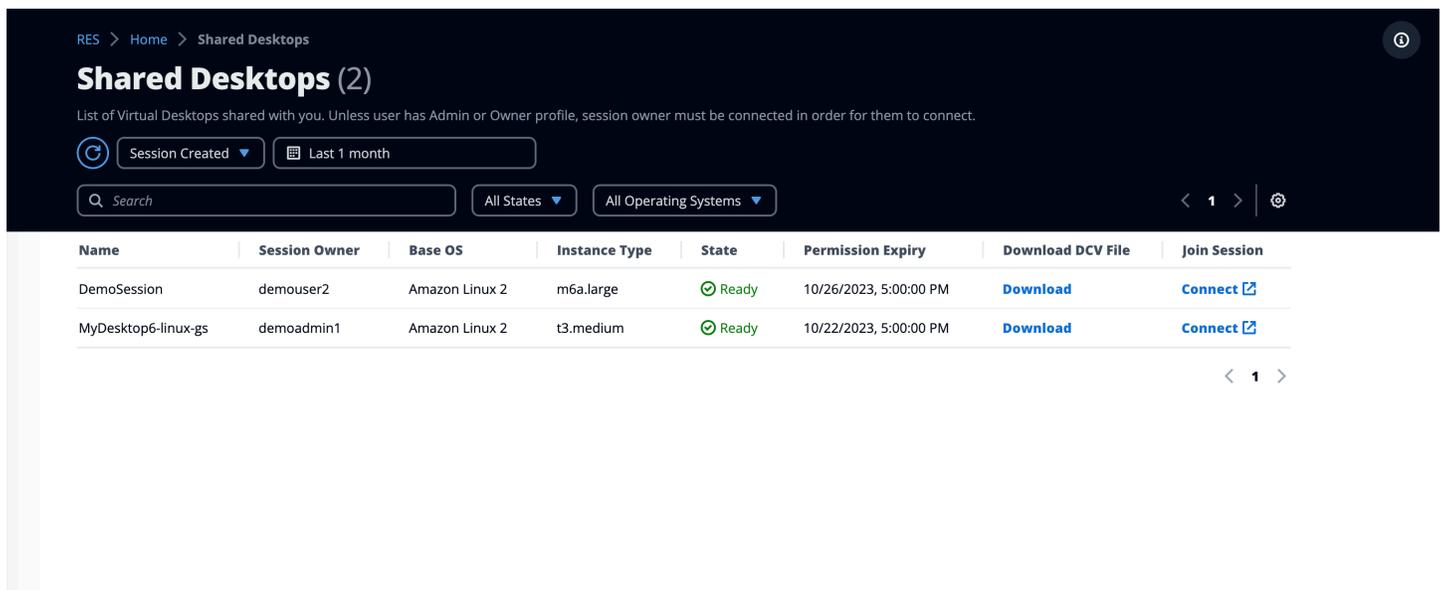
[Cancel](#) [Submit](#)

Estos ajustes están presentes en la página de configuración del escritorio, en la pestaña Servidor. Una vez que actualice la configuración de acuerdo con sus requisitos, haga clic en Enviar para guardar la configuración. Las nuevas sesiones utilizarán la configuración actualizada, pero tenga en cuenta que las sesiones existentes seguirán utilizando la configuración que tenían cuando se lanzaron.

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

## Escritorios compartidos

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



The screenshot shows the 'Shared Desktops' interface. At the top, there is a breadcrumb 'RES > Home > Shared Desktops' and a title 'Shared Desktops (2)'. Below the title, a subtitle reads: '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' (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 columns: Name, Session Owner, Base OS, Instance Type, State, Permission Expiry, Download DCV File, and Join Session. Two rows are visible: 'DemoSession' and 'MyDesktop6-linux-gs'. Both are in a 'Ready' state. The 'Join Session' column contains 'Connect' links with external icons.

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	<a href="#">Download</a>	<a href="#">Connect</a>
MyDesktop6-linux-gs	demoadmin1	Amazon Linux 2	t3.medium	Ready	10/22/2023, 5:00:00 PM	<a href="#">Download</a>	<a href="#">Connect</a>

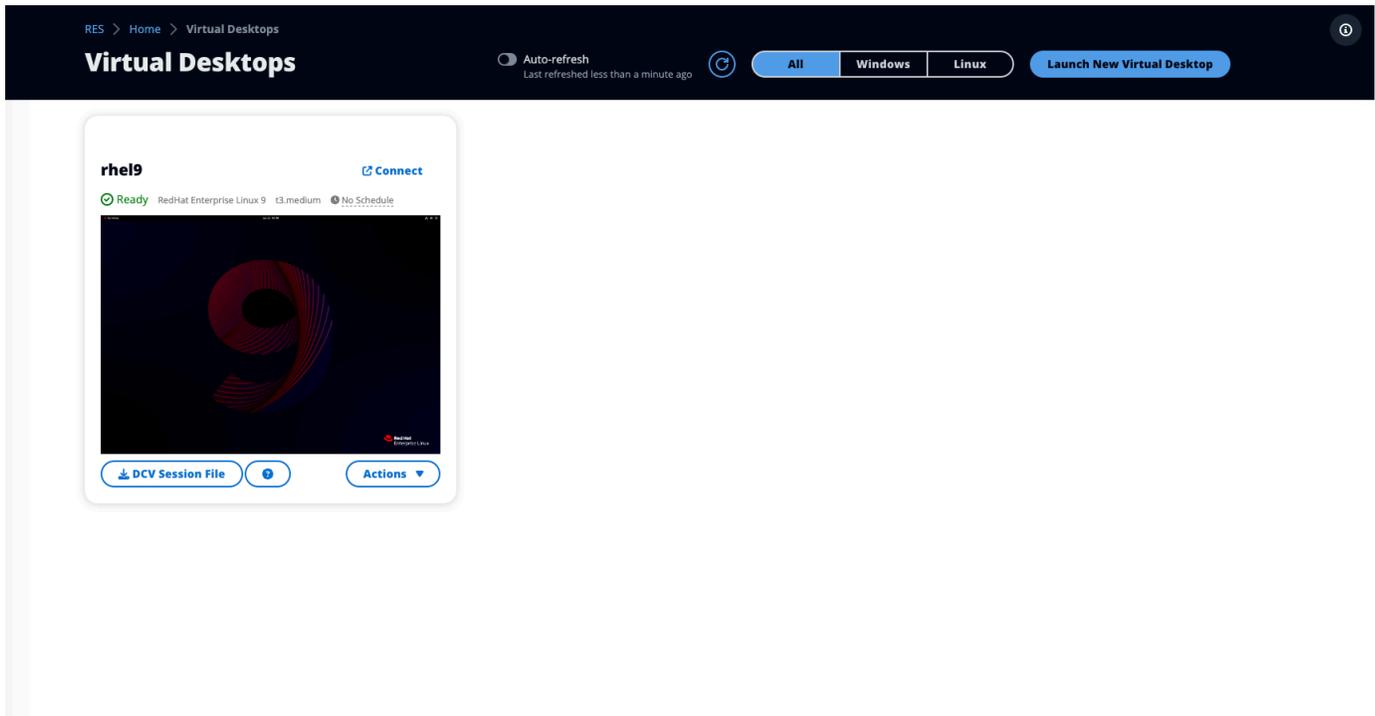
Al compartir una sesión, puede configurar los permisos para sus colaboradores. Por ejemplo, puedes conceder acceso de solo lectura a un compañero de equipo con el que estés colaborando.

### Temas

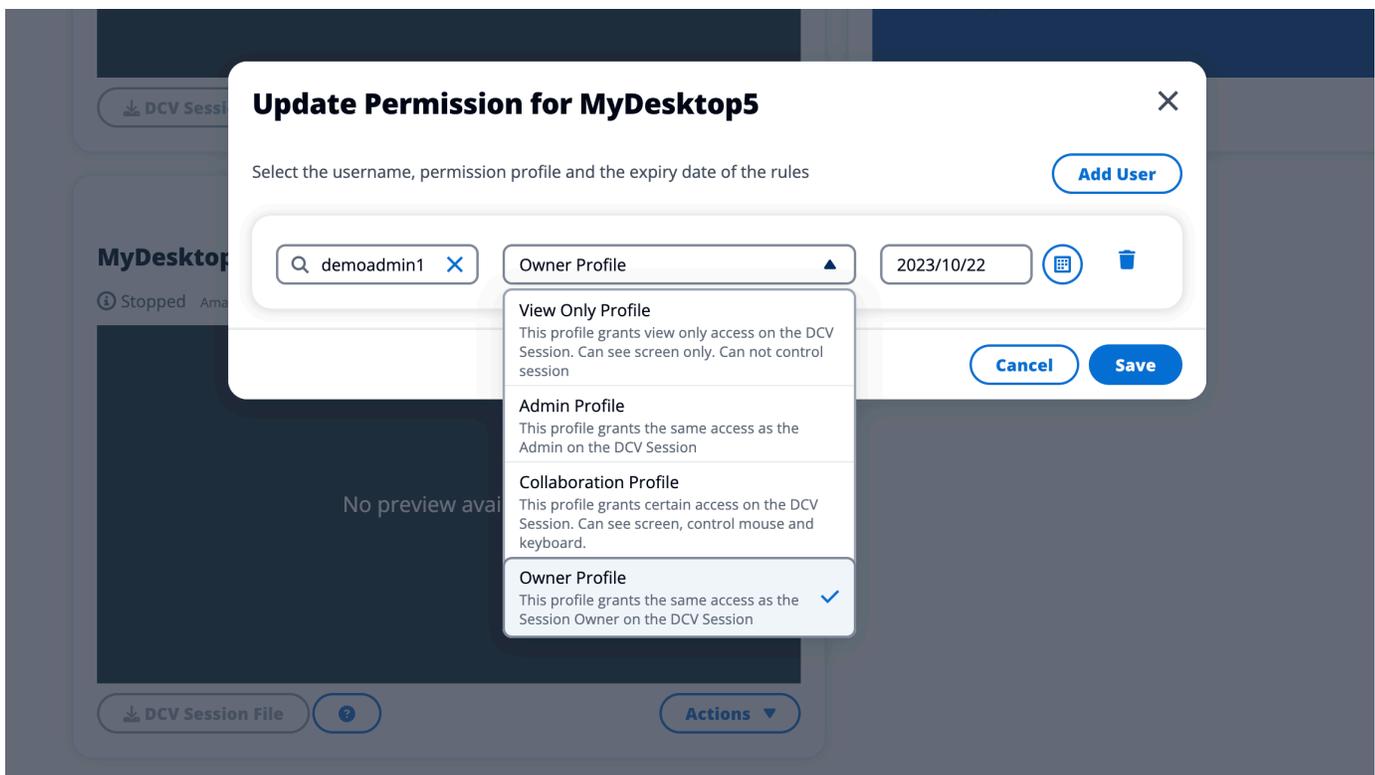
- [Comparte un escritorio](#)
- [Acceda a un escritorio compartido](#)

## Comparte un escritorio

1. En tu sesión de escritorio, selecciona Acciones.



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



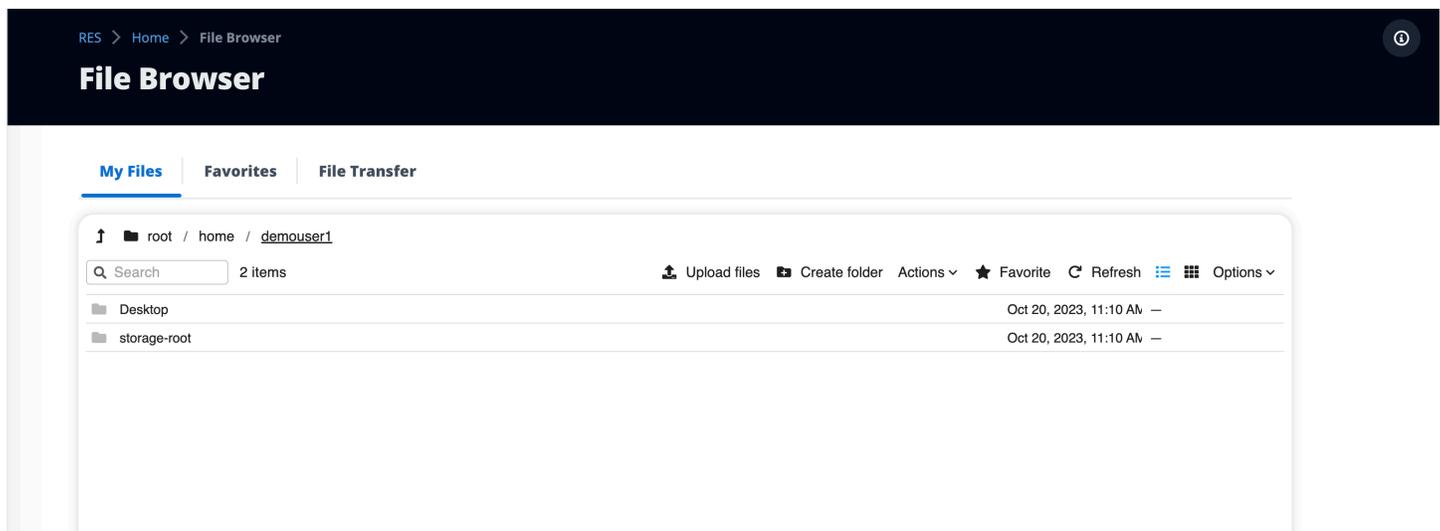
Para obtener más información sobre los permisos, consulte [the section called “Política de permisos”](#).

## 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 conectarte, sigue las instrucciones que aparecen en [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 backend (AmazonEFS) está disponible para todos los nodos de Linux. Para los nodos de Linux y Windows, ONTAP está disponible FSx para. Actualizar los archivos en el escritorio virtual es lo mismo que actualizar un archivo a través del terminal o del explorador de archivos basado en la web.

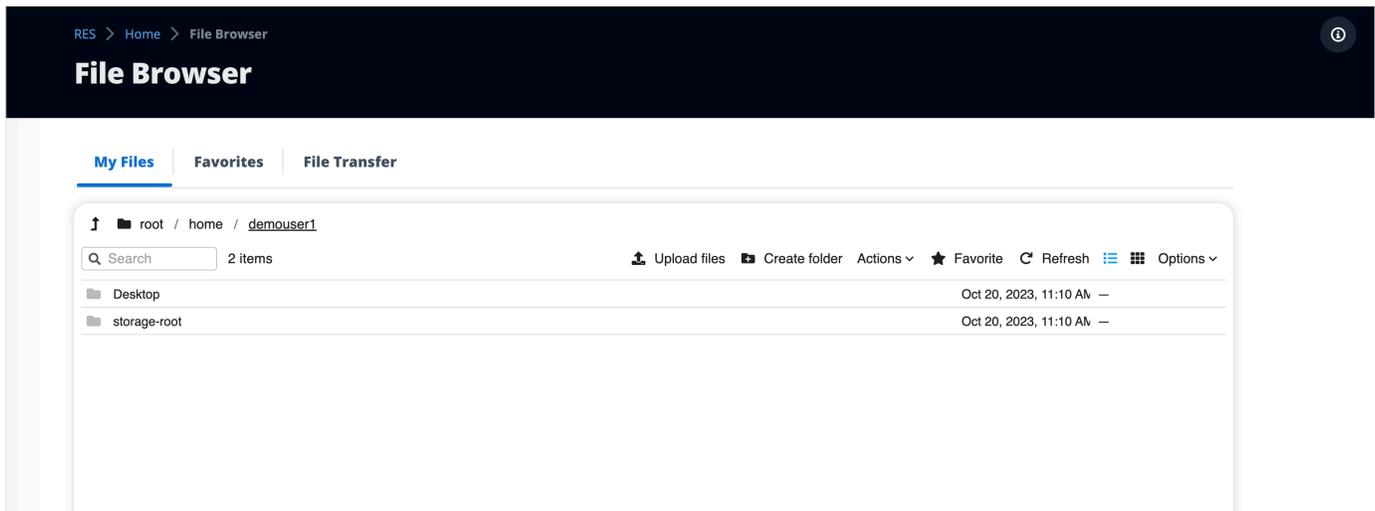


### Temas

- [Cargar archivo \(s\)](#)
- [Eliminar archivo \(s\)](#)
- [Administra los favoritos](#)
- [Edita archivos](#)
- [Transferencia de archivos](#)

## Cargar archivo (s)

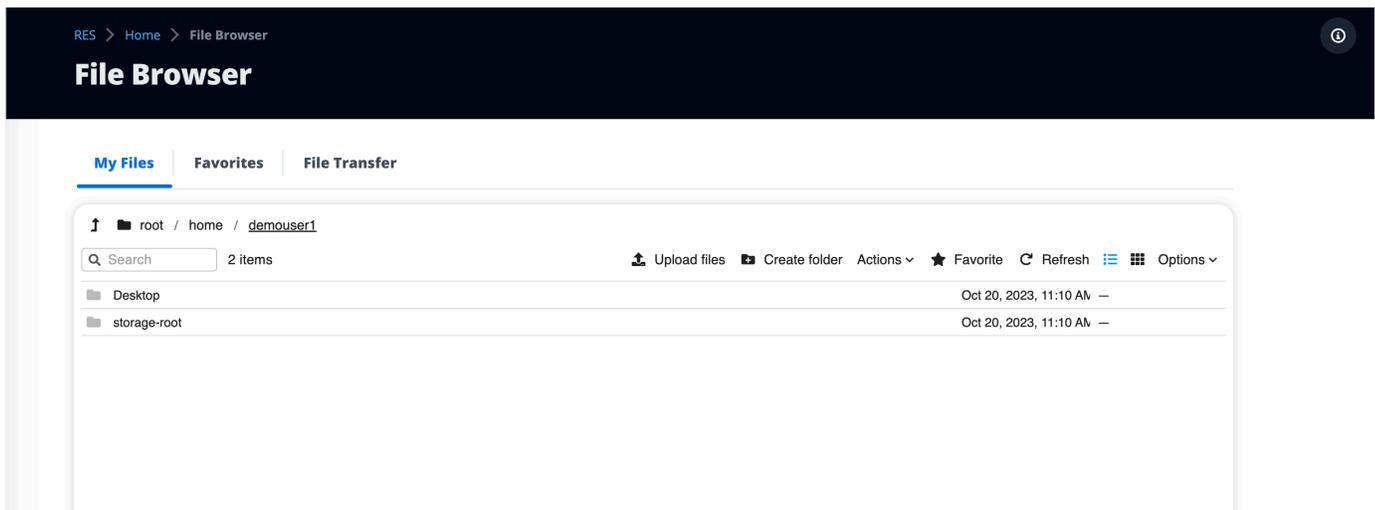
1. Selecciona Cargar archivos.



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

## Eliminar archivo (s)

1. Seleccione los archivos que desee eliminar.



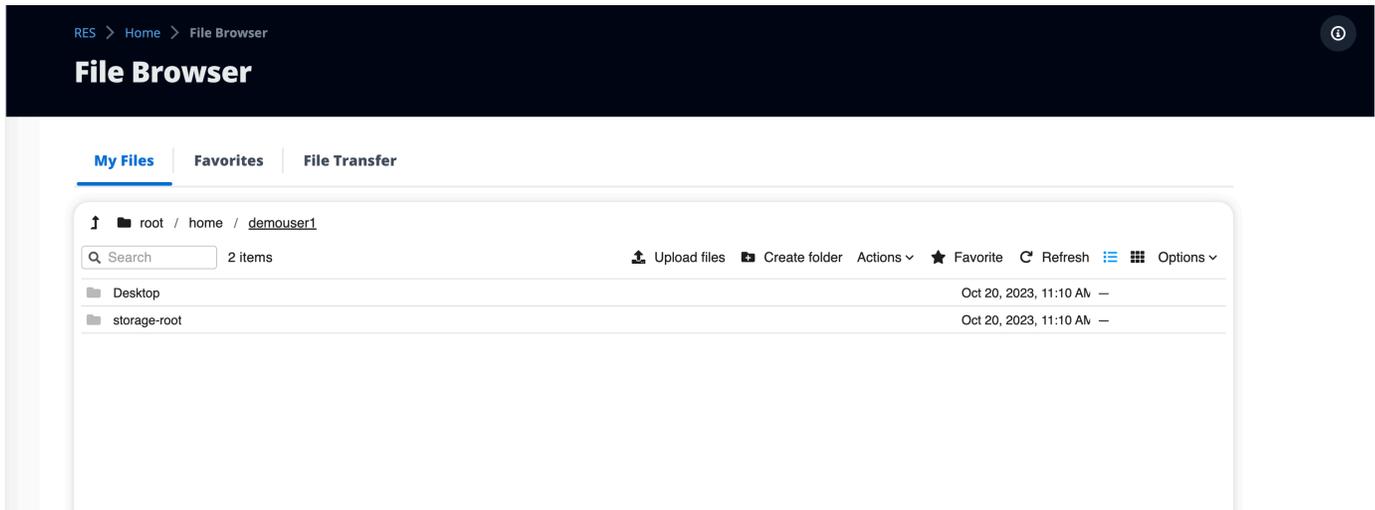
2. Elija Actions.
3. Selecciona Eliminar archivos.

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.

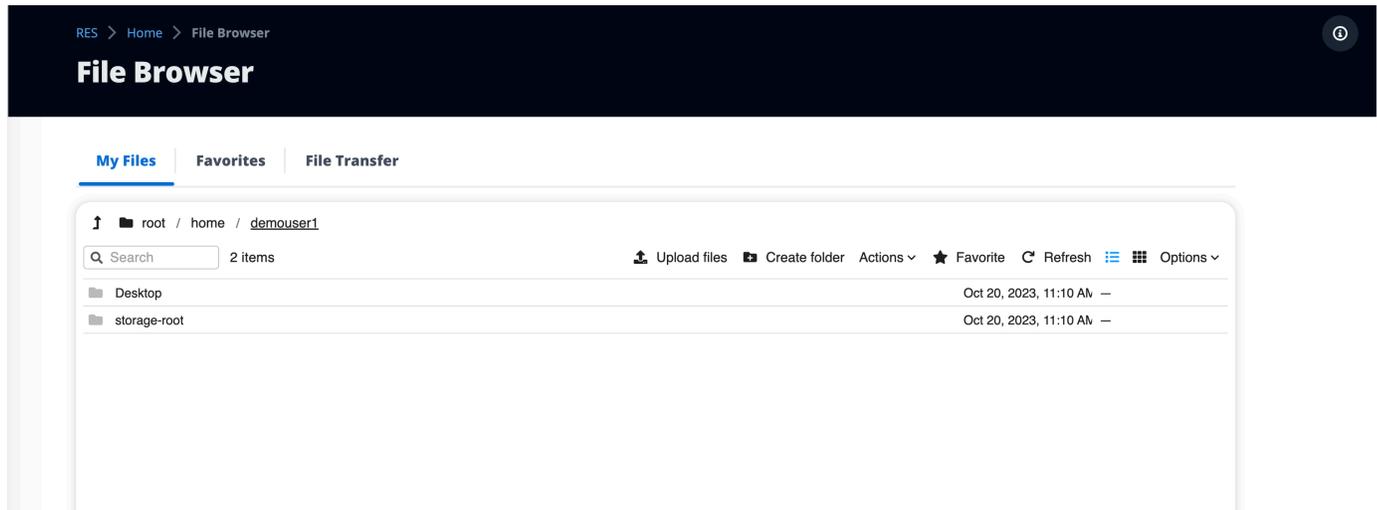
### Note

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



2. Realice las actualizaciones y seleccione Guardar.

## Transferencia de archivos

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

- FileZilla (Windows, macOS, Linux)
- Win SCP (Windows)
- AWS Transfer for FTP (AmazonEFS)

RES &gt; Home &gt; 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:

<b>Host</b> [Redacted]	<b>Port</b> [Redacted]
<b>Protocol</b> SFTP	<b>Logon Type</b> Key File
<b>User</b> demouser3	<b>Key File</b> /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.

# Solución de problemas

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

## Temas

- [Depuración y supervisión generales](#)
- [Problema RunBooks](#)
- [Problemas conocidos](#)

## Contenido detallado:

- [Depuración y supervisión generales](#)
  - [Fuentes útiles de información sobre registros y eventos](#)
    - [Archivos de registro en el entorno Amazon EC2 instances](#)
    - [CloudFormation Pilas](#)
    - [Fallos del sistema debidos a un problema y reflejados en la actividad grupal de Amazon EC2 Auto Scaling](#)
  - [Apariencia típica de Amazon EC2 Console](#)
    - [Hosts de infraestructura](#)
    - [Hosts de infraestructura y escritorios virtuales](#)
    - [Se aloja en un estado terminado](#)
    - [Comandos útiles relacionados con Active Directory \(AD\) como referencia](#)
  - [DCVDepuración de Windows](#)
  - [Encuentra información sobre DCV la versión de Amazon](#)
- [Problema RunBooks](#)
  - [Problemas de instalación](#)
    - [Quiero configurar dominios personalizados después de la instalación RES](#)
    - [AWS CloudFormation la pila no se puede crear con el mensaje «WaitCondition recibió un mensaje fallido». Error: estados. TaskFailed»](#)
    - [No se recibió la notificación por correo electrónico después de que las AWS CloudFormation pilas se crearan correctamente](#)

- [Instancias cíclicas o controladora de vdc en estado fallido](#)
- [La CloudFormation pila de entornos no se puede eliminar debido a un error en el objeto dependiente](#)
- [Se detectó un error en el parámetro de CIDR bloque durante la creación del entorno](#)
- [CloudFormation error al crear la pila durante la creación del entorno](#)
- [La creación de la pila de recursos externos \(demostración\) falla con \\_ AdDomainAdminNode CREATE FAILED](#)
- [Problemas de administración de identidades](#)
  - [No estoy autorizado a realizar iam: PassRole](#)
  - [Quiero permitir que personas ajenas a mi AWS cuenta accedan a los AWS recursos de mi Estudio de Investigación e Ingeniería](#)
  - [Al iniciar sesión en el entorno, vuelvo inmediatamente a la página de inicio de sesión](#)
  - [Se produjo el error «Usuario no encontrado» al intentar iniciar sesión](#)
  - [El usuario se agregó en Active Directory, pero no aparece en RES](#)
  - [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](#)
- [Almacenamiento](#)
  - [Creé el sistema de archivos por completo RES, pero no se monta en los hosts VDI](#)
  - [He incorporado un sistema de archivos, RES pero no se monta en los hosts VDI](#)
  - [No puedo leer ni escribir desde los hosts VDI](#)
    - [Ejemplo de casos de uso de la gestión de permisos](#)
  - [He creado Amazon FSx para NetApp ONTAP RES, pero no se ha unido a mi dominio](#)
- [Instantáneas](#)
  - [Una instantánea tiene el estado Fallido](#)
  - [No se puede aplicar una instantánea y los registros indican que las tablas no se pudieron importar.](#)
- [Infraestructura](#)
  - [Grupos objetivo del balanceador de carga sin instancias en buen estado](#)
- [Lanzamiento de escritorios virtuales](#)
  - [Un escritorio virtual que funcionaba anteriormente ya no se puede conectar correctamente](#)

- [Solo puedo iniciar 5 escritorios virtuales](#)
- [Los intentos de conexión a Windows desde un escritorio fallan y muestran el mensaje «Se ha cerrado la conexión». «Error de transporte»](#)
- [VDIsatascado en estado de aprovisionamiento](#)
- [VDIspasar al estado de error después de iniciarlo](#)
- [Componente de escritorio virtual](#)
  - [La EC2 instancia de Amazon aparece repetidamente finalizada en la consola](#)
  - [La instancia de vdc-controller está en ciclo debido a que no se pudo unir al VDI módulo AD/e muestra Failed Health Check API](#)
  - [El proyecto no aparece en el menú desplegable al editar la pila de software para añadirla](#)
  - [El registro de CloudWatch Amazon del administrador de clústeres muestra «user-home-init< > la cuenta aún no está disponible. En espera de que se sincronice el usuario» \(donde la cuenta es un nombre de usuario\)](#)
  - [Al intentar iniciar sesión en el escritorio de Windows, aparece el mensaje «Tu cuenta ha sido deshabilitada». Consulte a su administrador»](#)
  - [DHCPProblemas de opciones con la configuración de AD externa o de cliente](#)
  - [Error de Firefox MOZILLA PKIX \\_ ERROR \\_ REQUIRED \\_ TLS \\_ FEATURE \\_ MISSING](#)
- [Eliminación de Env](#)
  - [res-xxx-cluster se apilan en el estado FAILED "DELETE\\_" y no se pueden eliminar manualmente debido al error «El rol no es válido o no se puede asumir»](#)
  - [Recopilación de registros](#)
  - [Descargando VDI registros](#)
  - [Descargar registros de EC2 instancias de Linux](#)
  - [Descargar registros de EC2 instancias de Windows](#)
  - [Recopilando ECS los registros del WaitCondition error](#)
- [Entorno de demostración](#)
  - [Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad](#)
- [Problemas conocidos de la versión 2024.x](#)
  - [Problemas conocidos de la versión 2024.x](#)
  - [\(2024.08\) Los escritorios virtuales no pueden montar un bucket de Amazon S3 de lectura/escritura con ARN un bucket raíz y un prefijo personalizado](#)

- [\(2024.06\) Se produce un error al aplicar la instantánea cuando el nombre del grupo de AD contiene espacios](#)
- [\(2024.04-2024.04.02\) El límite de permisos proporcionado no está asociado a la función de las instancias IAM VDI](#)
- [\(2024.04.02 y versiones anteriores\) Las instancias de Windows NVIDIA en ap-southeast-2 \(Sídney\) no se inician](#)
- [\(2024.04 y 2024.04.01\) elimine el error en RES GovCloud](#)
- [\(2024.04 - 2024.04.02\) Es posible que el escritorio virtual Linux se quede atascado en el estado «" al reiniciarse RESUMING](#)
- [\(04.02 de abril de 2020 y versiones anteriores\) No se sincronizan los usuarios de AD cuyo SAMAccountName atributo incluye letras mayúsculas o caracteres especiales](#)
- [\(02 de abril de 2020 y versiones anteriores\) La clave privada para acceder al host del bastión no es válida](#)
- [\(2024.06 y versiones anteriores\) Los miembros del grupo no se sincronizaron durante la sincronización de AD RES](#)
- [\(2024.06 y versiones anteriores\) CVE -2024-6387, egreSSHion R, vulnerabilidad de seguridad en Ubuntu RHEL9 VDIs](#)

## Depuración y supervisión generales

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

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

- [Encuentra información sobre DCV la versión de Amazon](#)

## Fuentes útiles de información sobre registros y eventos

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

### Archivos de registro en el entorno Amazon EC2 instances

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

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

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

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

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

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

- PS C:\ProgramData\ n ice\ dcv\ log
- PS C:\\ ProgramData n ice\\ log DCVSessionManagerAgent

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

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

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

- C:\Windows\System32\config\systemprofile\AppData\ Local\NICE\ dcv\

## Grupos de Amazon CloudWatch Log

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

Estos grupos se denominan de la siguiente manera:

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

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

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

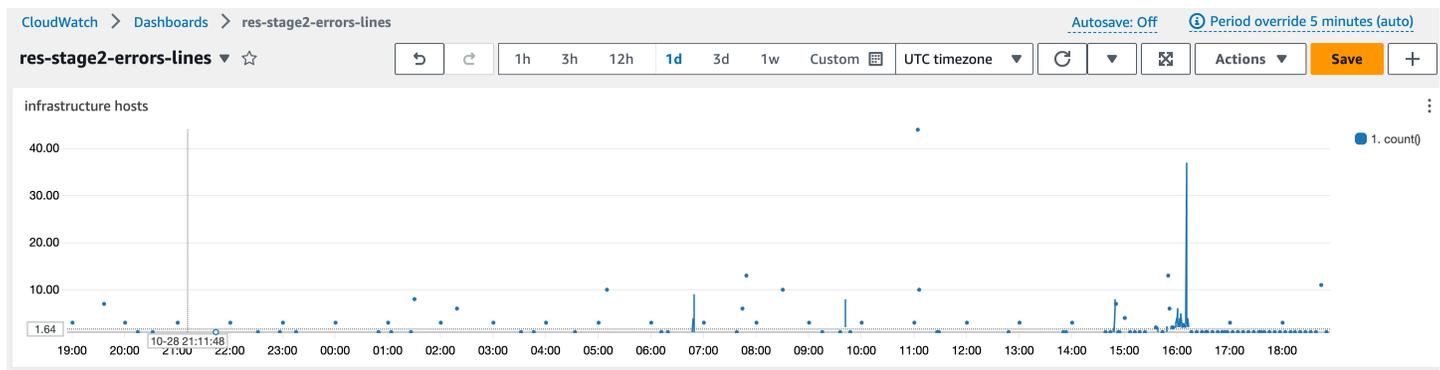
Otro método de supervisión de los problemas consiste en crear Amazon CloudWatch Dashboards que contengan widgets que muestren los datos de interés.

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

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

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

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



## CloudFormation Pilas

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

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

RESpilas:

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

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

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

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

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

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

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

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

The screenshot shows the Amazon EC2 console interface for a target group. The breadcrumb navigation at the top indicates the path: EC2 > Target groups > res-bicfn3-web-portal-e2958adc. The main content area displays the details for the target group 'res-bicfn3-web-portal-e2958adc'. A summary bar shows the following health metrics: Total targets: 1, Healthy: 1 (indicated by a green checkmark icon), Unhealthy: 0 (indicated by a red X icon), Unused: 0, Initial: 0, and Draining: 0. Below this, there is a section for 'Distribution of targets by Availability Zone (AZ)'. The 'Registered targets' section is expanded, showing a table with one entry:

Instance ID	Name	Port	Zone	Health status	Health status details
i-Oba5d508631f20043	res-bicfn3-cluster-manager	8443	eu-central-1c	healthy	

## Apariencia típica de Amazon EC2 Console

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

### Hosts de infraestructura

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

EC2 Dashboard ×

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

**Instances (5) Info**

Find Instance by attribute or tag (case-sensitive)

res-stage2 × Instance state = running × Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

## Hosts de infraestructura y escritorios virtuales

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

EC2 Dashboard ×

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

**Instances (7) Info**

Find Instance by attribute or tag (case-sensitive)

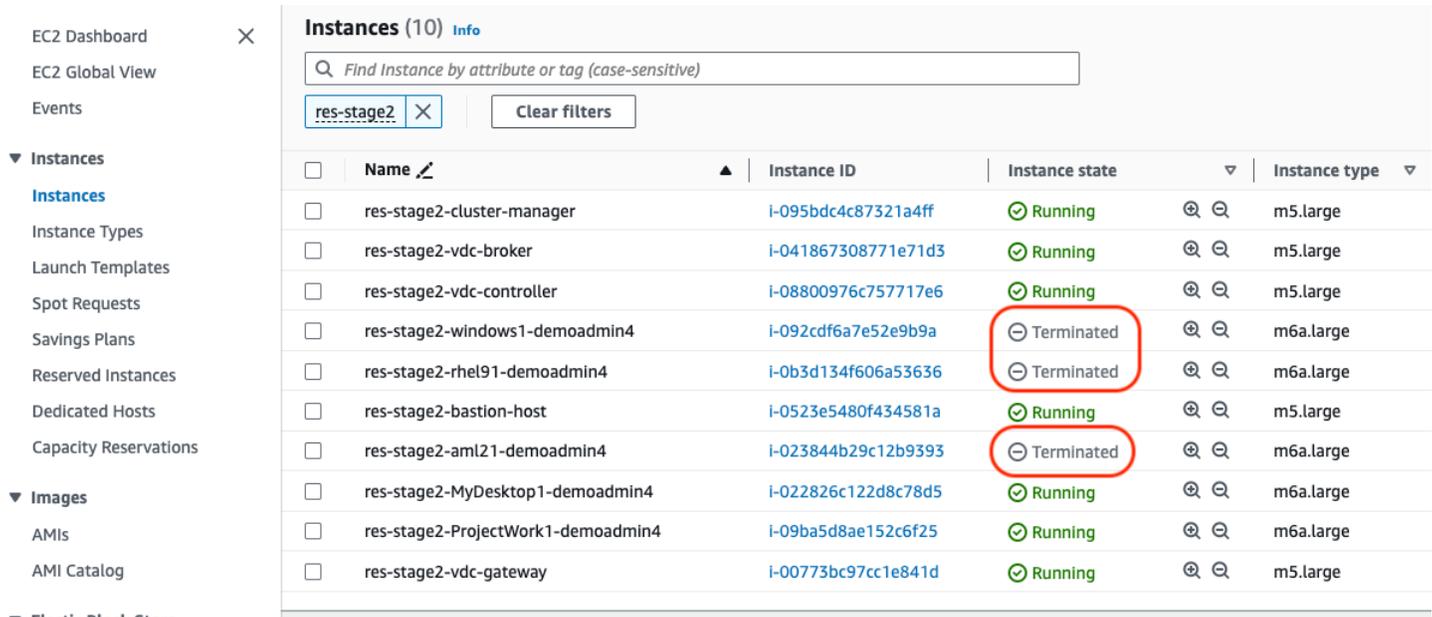
res-stage2 × Instance state = running × Clear filters

<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
<input type="checkbox"/>	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
<input type="checkbox"/>	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

## Se aloja en un estado terminado

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

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



<input type="checkbox"/>	Name <a href="#">↗</a>	Instance ID	Instance state	Instance type
<input type="checkbox"/>	res-stage2-cluster-manager	i-095bdc4c87321a4ff	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-broker	i-041867308771e71d3	Running	m5.large
<input type="checkbox"/>	res-stage2-vdc-controller	i-08800976c757717e6	Running	m5.large
<input type="checkbox"/>	res-stage2-windows1-demoadmin4	i-092cdf6a7e52e9b9a	Terminated	m6a.large
<input type="checkbox"/>	res-stage2-rhel91-demoadmin4	i-0b3d134f606a53636	Terminated	m6a.large
<input type="checkbox"/>	res-stage2-bastion-host	i-0523e5480f434581a	Running	m5.large
<input type="checkbox"/>	res-stage2-aml21-demoadmin4	i-023844b29c12b9393	Terminated	m6a.large
<input type="checkbox"/>	res-stage2-MyDesktop1-demoadmin4	i-022826c122d8c78d5	Running	m6a.large
<input type="checkbox"/>	res-stage2-ProjectWork1-demoadmin4	i-09ba5d8ae152c6f25	Running	m6a.large
<input type="checkbox"/>	res-stage2-vdc-gateway	i-00773bc97cc1e841d	Running	m5.large

## Comandos útiles relacionados con Active Directory (AD) como referencia

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

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

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

## DCVDepuración de Windows

En un escritorio de Windows, puede enumerar la sesión asociada a él de la siguiente manera:

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

## Encuentra información sobre DCV la versión de Amazon

Amazon DCV se utiliza para sesiones de escritorios virtuales. [AWS Amazon DCV](#). Los siguientes ejemplos muestran cómo determinar la versión del DCV software instalado.

### Linux

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

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

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

### Windows

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

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

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

## Problema RunBooks

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

- [Problemas de instalación](#)
  - [Quiero configurar dominios personalizados después de la instalación RES](#)
  - [AWS CloudFormation la pila no se puede crear con el mensaje «WaitCondition recibió un mensaje fallido». Error: estados. TaskFailed»](#)
  - [No se recibió la notificación por correo electrónico después de que las AWS CloudFormation pilas se crearan correctamente](#)

- [Instancias cíclicas o controladora de vdc en estado fallido](#)
- [La CloudFormation pila de entornos no se puede eliminar debido a un error en el objeto dependiente](#)
- [Se detectó un error en el parámetro de CIDR bloque durante la creación del entorno](#)
- [CloudFormation error al crear la pila durante la creación del entorno](#)
- [La creación de la pila de recursos externos \(demostración\) falla con \\_ AdDomainAdminNode CREATE FAILED](#)
- [Problemas de administración de identidades](#)
  - [No estoy autorizado a realizar iam: PassRole](#)
  - [Quiero permitir que personas ajenas a mi AWS cuenta accedan a los AWS recursos de mi Estudio de Investigación e Ingeniería](#)
  - [Al iniciar sesión en el entorno, vuelvo inmediatamente a la página de inicio de sesión](#)
  - [Se produjo el error «Usuario no encontrado» al intentar iniciar sesión](#)
  - [El usuario se agregó en Active Directory, pero no aparece en RES](#)
  - [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](#)
- [Almacenamiento](#)
  - [Creé el sistema de archivos por completo RES, pero no se monta en los hosts VDI](#)
  - [He incorporado un sistema de archivos, RES pero no se monta en los hosts VDI](#)
  - [No puedo leer ni escribir desde los hosts VDI](#)
    - [Ejemplo de casos de uso de la gestión de permisos](#)
  - [He creado Amazon FSx para NetApp ONTAP RES, pero no se ha unido a mi dominio](#)
- [Instantáneas](#)
  - [Una instantánea tiene el estado Fallido](#)
  - [No se puede aplicar una instantánea y los registros indican que las tablas no se pudieron importar.](#)
- [Infraestructura](#)
  - [Grupos objetivo del balanceador de carga sin instancias en buen estado](#)
- [Lanzamiento de escritorios virtuales](#)
  - [Un escritorio virtual que funcionaba anteriormente ya no se puede conectar correctamente](#)
- [Solo puedo iniciar 5 escritorios virtuales](#)

- [Los intentos de conexión a Windows desde un escritorio fallan y muestran el mensaje «Se ha cerrado la conexión». «Error de transporte»](#)
- [VDIsatascado en estado de aprovisionamiento](#)
- [VDIspasar al estado de error después de iniciarlo](#)
- [Componente de escritorio virtual](#)
  - [La EC2 instancia de Amazon aparece repetidamente finalizada en la consola](#)
  - [La instancia de vdc-controller está en ciclo debido a que no se pudo unir al VDI módulo AD/e muestra Failed Health Check API](#)
  - [El proyecto no aparece en el menú desplegable al editar la pila de software para añadirla](#)
  - [El registro de CloudWatch Amazon del administrador de clústeres muestra «user-home-init< > la cuenta aún no está disponible. En espera de que se sincronice el usuario» \(donde la cuenta es un nombre de usuario\)](#)
  - [Al intentar iniciar sesión en el escritorio de Windows, aparece el mensaje «Tu cuenta ha sido deshabilitada». Consulte a su administrador»](#)
  - [DHCPProblemas de opciones con la configuración de AD externa o de cliente](#)
  - [Error de Firefox MOZILLA PKIX \\_ ERROR \\_ REQUIRED \\_ TLS \\_ FEATURE \\_ MISSING](#)
- [Eliminación de Env](#)
  - [res-xxx-cluster se apilan en el estado FAILED "DELETE\\_" y no se pueden eliminar manualmente debido al error «El rol no es válido o no se puede asumir»](#)
  - [Recopilación de registros](#)
  - [Descargando VDI registros](#)
  - [Descargar registros de EC2 instancias de Linux](#)
  - [Descargar registros de EC2 instancias de Windows](#)
  - [Recopilando ECS los registros del WaitCondition error](#)
- [Entorno de demostración](#)
  - [Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad](#)

## Problemas de instalación

### Temas

- [Quiero configurar dominios personalizados después de la instalación RES](#)

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

.....

Quiero configurar dominios personalizados después de la instalación RES

 Note

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

Agregue certificados al cliente web

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

- a. Busque la tabla de configuración del clúster en DynamoDB -> Tablas -> *<env-name>.cluster-settings*
  - b. Vaya a Explorar elementos y filtre por atributo: nombre «clave», tipo «cadena», condición «contiene» y valor «external\_alb».
  - c. Establézcalo en True.  
`cluster.load_balancers.external_alb.certificates.provided`
  - d. Actualice el valor  
`decluster.load_balancers.external_alb.certificates.custom_dns_name`.  
Este es el nombre de dominio personalizado para la interfaz de usuario web.
  - e. Actualice el valor  
`decluster.load_balancers.external_alb.certificates.acm_certificate_arn`.  
Es el nombre del recurso de Amazon (ARN) del certificado correspondiente almacenado en Amazon Certificate Manager (ACM).
3. Actualice el registro de subdominio de Route53 correspondiente que creó para su cliente web para que apunte al DNS nombre del balanceador de cargas de laboratorio externo. `<env-name>-external-alb`
  4. Si ya SSO está configurado en el entorno, vuelva a configurarlo SSO con las mismas entradas que utilizó inicialmente en el botón Configuración general > Proveedor de identidad > Inicio de sesión único > Estado > Editar del portal web. RES

### Añada certificados al VDI

1. Conceda permiso a la RES aplicación para realizar una GetSecret operación en el secreto añadiendo las siguientes etiquetas a los secretos:
  - `res:EnvironmentName : <env-name>`
  - `res:ModuleName : virtual-desktop-controller`
2. En la tabla de configuración del clúster:
  - a. Busque la tabla de configuración del clúster en DynamoDB -> Tablas -> *<env-name>.cluster-settings*
  - b. Vaya a Explorar elementos y filtre por atributo: nombre «clave», tipo «cadena», condición «contiene» y valor «dcv\_connection\_gateway».
  - c. Establézcalo en True. `vdc.dcv_connection_gateway.certificate.provided`

- d. Actualice el valor `devdc.dcv_connection_gateway.certificate.custom_dns_name`. Este es el nombre de dominio personalizado para el VDI acceso.
  - e. Actualice el valor `devdc.dcv_connection_gateway.certificate.certificate_secret_arn`. Este es ARN el secreto que contiene el contenido del certificado.
  - f. Actualice el valor `devdc.dcv_connection_gateway.certificate.private_key_secret_arn`. Este es el ARN secreto que contiene el contenido de la clave privada.
3. Actualice la plantilla de lanzamiento utilizada para la instancia de puerta de enlace:
    - a. Abra el grupo Auto Scaling en la AWS consola, en EC2> Auto Scaling > Auto Scaling Groups.
    - b. Seleccione el grupo de escalado automático de la puerta de enlace que corresponda al RES entorno. El nombre sigue la convención de nomenclatura `<env-name>-vdc-gateway-asg`.
    - c. Busque y abra la plantilla de lanzamiento en la sección de detalles.
    - d. En Detalles > Acciones > selecciona Modificar plantilla (Crear nueva versión).
    - e. Desplázate hacia abajo hasta Detalles avanzados.
    - f. Desplázate hasta el final, hasta Datos de usuario.
    - g. Busca las palabras `CERTIFICATE_SECRET_ARN` y `PRIVATE_KEY_SECRET_ARN`. Actualice estos valores con lo ARNs indicado en los secretos que contienen el contenido del certificado (consulte el paso 2.c) y la clave privada (consulte el paso 2.d).
    - h. Asegúrese de que el grupo Auto Scaling esté configurado para usar la versión recientemente creada de la plantilla de lanzamiento (de la página del grupo Auto Scaling).
  4. Actualice el registro de subdominio de Route53 correspondiente que creó para sus escritorios virtuales para que apunte al DNS nombre del balanceador de cargas nlb externo: `<env-name>-external-nlb`
  5. Finalice la instancia `dcv-gateway` existente `<env-name>-vdc-gateway` y espere a que se active una nueva.

.....

AWS CloudFormation la pila no se puede crear con el mensaje «WaitCondition recibió un 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 recibió la notificación por correo electrónico después de que las AWS CloudFormation pilas se crearan correctamente

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

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

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

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

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

3. Si implementaste las fórmulas informáticas de AWS alto rendimiento para crear tus recursos externos, confirma que la VPC pila haya creado las subredes públicas y privadas y otros parámetros seleccionados.

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

- 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:

- Desde la línea de comandos, inicie una sesión con la instancia SSM en ejecución del vdc-controller.
- Ejecute `sudo su -`.
- 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-10-3-144-194 ~]# 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 2
```

Might see errors highlighted in RED here

## SSMregistro de errores

Para resolver el problema:

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

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

Causa principal 1: se ingresaron detalles de conexión LDAP incorrectos

Revise los registros. Si ve que lo siguiente se repite varias veces, 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 RES pila.
  - `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, abra Secrets Manager.
2. Busque la opción `directoryserviceServiceAccountUsername`. El secreto debería ser `<stack name>-directoryservice-ServiceAccountUsername`.
3. Abra el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y selecciona Texto sin formato.
4. Si el valor se actualizó, elimine las instancias del entorno con el administrador de clústeres y el controlador de vdc que se estén ejecutando actualmente. El escalado automático iniciará nuevas instancias con el valor más reciente de Secrets Manager.

Causa principal 3: se ingresó ServiceAccount una contraseña incorrecta

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

1. Desde la AWS consola, abra Secrets Manager.
2. Busque la opción `directoryserviceServiceAccountPassword`. El secreto debería ser `<stack name>-directoryservice-ServiceAccountPassword`.
3. Abra 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 de su RES directorio y elija Acciones.

- iii. Seleccione Restablecer contraseña de usuario.
  - iv. Ingresa el ServiceAccount nombre de usuario.
  - v. Introduce una contraseña nueva y selecciona Restablecer contraseña.
- b. Para restablecer la contraseña en Secrets Manager:
- i. Abre la AWS consola y ve a Secrets Manager.
  - ii. Busque la opción `directoryserviceServiceAccountPassword`. El secreto debería ser `<stack name>-directoryservice-ServiceAccountPassword`.
  - iii. Abre el secreto para ver la página de detalles. En Valor secreto, selecciona Recuperar valor secreto y, a continuación, selecciona Texto sin formato.
  - iv. Elija Editar.
  - v. Establece una nueva contraseña para el ServiceAccount usuario y selecciona Guardar.
5. Si actualizó el valor, elimine las instancias `cluster-manager` y `vdc-controller` del entorno que se estén ejecutando actualmente. El escalado automático iniciará nuevas instancias con el valor más reciente.

.....

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

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

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

.....

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

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

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 la pila de recursos externos (demostración) falla con `AddDomainAdminNode CREATE FAILED`

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

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

Para determinar la causa del error:

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

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

.....

## Problemas de administración de identidades

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

- [the section called “Configuración SSO con Identity Center IAM”](#)
- [the section called “Configurar su proveedor de identidad para SSO”](#)

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

### Temas

- [No estoy autorizado a realizar iam: PassRole](#)
- [Quiero permitir que personas ajenas a mi AWS cuenta accedan a los AWS recursos de mi Estudio de Investigación e Ingeniería](#)
- [Al iniciar sesión en el entorno, vuelvo inmediatamente a la página de inicio de sesión](#)
- [Se produjo el error «Usuario no encontrado» al intentar iniciar sesión](#)
- [El usuario se agregó en Active Directory, pero no aparece en RES](#)
- [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](#)

.....

### No estoy autorizado a realizar iam: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la PassRole acción iam:, debes actualizar tus políticas para que puedas transferirle una función. RES

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

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

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

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

.....

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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para más información, consulte lo siguiente:

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

.....

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

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

Para comprobar los registros:

1. Abra la [CloudWatch consola](#).
2. En Grupos de registros, busque el grupo denominado `<environment-name>/cluster-manager`.
3. Abra el grupo de registros para buscar cualquier error en las secuencias de registros.

Para comprobar los ajustes de configuración:

1. Abra la consola de [DynamoDB](#)
2. En Tablas, busque la tabla denominada `<environment-name>.cluster-settings`
3. 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 SSO de configuración 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	<input type="text" value="identity-provider.cognito.sso_enabled"/>
value	<input type="radio"/> True <input checked="" type="radio"/> False 

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

.....

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

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

- Si el usuario no está presente en AD RES y usted lo agregó recientemente a AD
  - Es posible que el usuario aún no esté sincronizado con. RES RESse 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 sincronizarla inmediatamente, sigue los pasos que se indican. [El usuario se agregó en Active Directory, pero no aparece en RES](#)
- Si el usuario está presente en RES:
  1. Asegúrese de que la asignación de atributos esté configurada correctamente. Para obtener más información, consulte [Configurar tu proveedor de identidad para el inicio de sesión único \(\) SSO](#).
  2. Asegúrese de que tanto el SAML asunto como el SAML correo electrónico 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 al Active Directory pero no está en él RES, debe activarse la sincronización de AD. La sincronización de AD se realiza cada hora mediante una función Lambda que importa las entradas de AD al RES entorno. En ocasiones, se produce un retraso hasta que se ejecute el siguiente proceso de sincronización después de añadir nuevos usuarios o grupos. Puede iniciar la sincronización manualmente desde Amazon Simple Queue Service.

Inicie el proceso de sincronización manualmente:

1. Abre la [SQSconsola de Amazon](#).
2. En Colas, selecciona `<environment-name>-cluster-manager-tasks.fifo`.
3. Seleccione Enviar y recibir mensajes.

4. En Cuerpo del mensaje, introduzca:

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

5. Para el ID del grupo de mensajes, introduzca: **adsync.sync-from-ad**

6. En el campo ID de deduplicación de mensajes, introduce una cadena alfanumérica aleatoria. Esta entrada debe ser diferente de todas las llamadas realizadas en los cinco minutos anteriores o se ignorará la solicitud.

.....

## El usuario no estaba disponible al crear una sesión

Si es un administrador que está creando una sesión, pero descubre que un usuario que 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, aumenta el límite de resultados de búsqueda IDP de LDAP.

.....

## Almacenamiento

### Temas

- [Creé el sistema de archivos por completo RES, pero no se monta en los hosts VDI](#)
- [He incorporado un sistema de archivos, RES pero no se monta en los hosts VDI](#)
- [No puedo leer ni escribir desde los hosts VDI](#)
- [He creado Amazon FSx para NetApp ONTAP RES, pero no se ha unido a mi dominio](#)

.....

## Creé el sistema de archivos por completo RES, pero no se monta en los hosts VDI

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

### Amazon EFS

1. Ve a la [EFSconsola de Amazon](#).
2. Comprueba que el estado del sistema de archivos esté disponible.
3. Si el estado del sistema de archivos no está disponible, espere antes de iniciar los VDI hosts.

### Amazon FSx ONTAP

1. Ve a la [FSxconsola de Amazon](#).
2. Comprueba que el estado esté disponible.
3. Si el estado no está disponible, espere antes de lanzar los VDI hosts.

.....

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

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

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

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

.....

## No puedo leer ni escribir desde los hosts VDI

ONTAPsoportes UNIX NTFS y estilo MIXED de seguridad para los volúmenes. Los estilos de seguridad determinan el tipo de permisos que se ONTAP utilizan para controlar el acceso a los datos y qué tipo de cliente puede modificar estos permisos.

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

### Ejemplo de casos de uso de la gestión de permisos

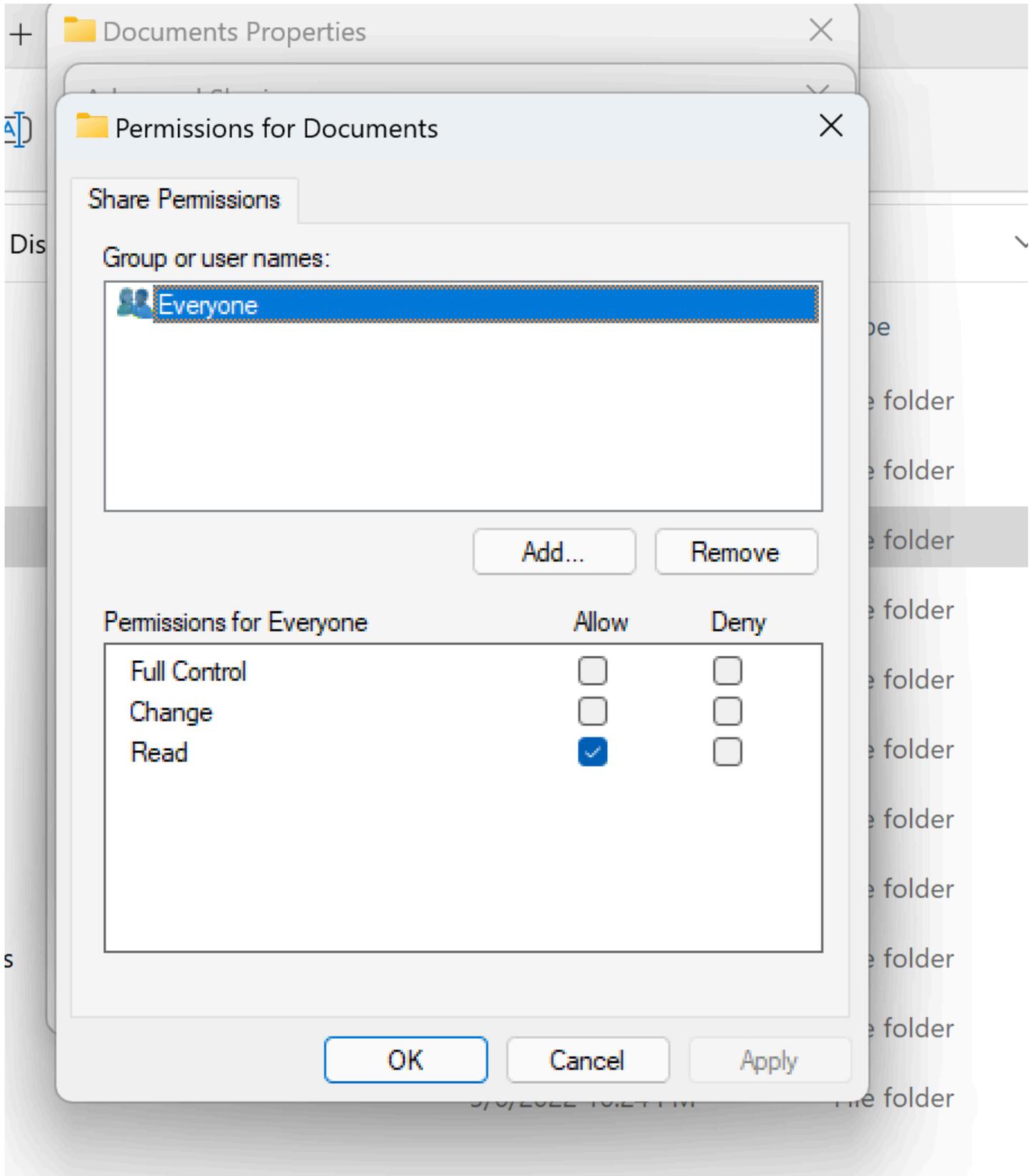
#### Uso del volumen UNIX de estilos con cargas de trabajo de Linux

El sudoer puede configurar los permisos para otros usuarios. Por ejemplo, lo siguiente daría a todos los miembros permisos <group-ID> completos de lectura y escritura en el directorio: /<project-name>

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

#### Uso de NTFS Style Volume con cargas de trabajo de Linux y Windows

Los permisos de uso compartido se pueden configurar mediante las propiedades de uso compartido de una carpeta concreta. Por ejemplo, en función de un usuario user\_01 y una carpetamyfolder, puedes configurar los permisos de Full ControlChange,, Allow o Read paraDeny:



Si el volumen lo van a utilizar clientes de Linux y Windows, necesitamos configurar una asignación de nombres SVM que asocie cualquier nombre de usuario de Linux al mismo nombre de usuario con el formato de nombre de BIOS dominio de red de dominio\ nombre de usuario. Esto es necesario para traducir entre usuarios de Linux y Windows. Como referencia, consulte [Habilitar cargas de trabajo multiprotocolo con Amazon FSx](#) for. NetApp ONTAP

.....

He creado Amazon FSx para NetApp ONTAPRES, pero no se ha unido a mi dominio

Actualmente, cuando creas Amazon FSx for NetApp ONTAP desde la RES consola, el sistema de archivos se aprovisiona pero no se une al dominio. Para unir el sistema de ONTAP archivos creado SVM a tu dominio, consulta [Cómo unirse SVMs a un Microsoft Active Directory](#) y sigue los pasos de la [FSxconsola de Amazon](#). Asegúrese de que [los permisos necesarios estén delegados a la cuenta de Amazon FSx Service](#) en AD. Una vez que SVM se haya unido al dominio correctamente, vaya a SVM Resumen > Puntos de enlace > SMB DNS nombre y copie el DNS nombre, ya que lo necesitará más adelante.

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

1. Vaya a la consola de [Amazon DynamoDB](#).
2. Seleccione Tablas y, a continuación, elija. <stack-name>-cluster-settings
3. En Explorar los elementos de la tabla, expanda Filtros e introduzca el siguiente filtro:
  - Nombre del atributo: clave
  - Condición: igual a
  - Valor - shared-storage.<file-system-name>.fsx\_netapp\_ontap.svm.smb\_dns
4. Selecciona el artículo devuelto y, a continuación, Acciones y Editar artículo.
5. Actualiza el valor con el SMB DNS nombre que copiaste anteriormente.
6. Elija Save and close.

Además, asegúrate de que el grupo de seguridad asociado al sistema de archivos permita el tráfico, tal y como se recomienda en [File System Access Control with Amazon VPC](#). VDI Los nuevos hosts que utilicen el sistema de archivos ahora podrán montar el sistema de archivos SVM y el sistema de archivos unidos al dominio.

Como alternativa, puede incorporar un sistema de archivos existente que ya esté unido a su dominio utilizando la función de sistema de archivos RES integrado; en Administración del entorno, elija Sistemas de archivos, Sistema de archivos integrado.

## Instantáneas

### Temas

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

### Una instantánea tiene el estado Fallido

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

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

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

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

1. Descargue el archivo metadata.json y compruebe que el estado de las ExportStatus distintas tablas es el siguiente. COMPLETED Asegúrese de que las distintas tablas tengan el

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

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

.....

## Infraestructura

### Temas

- [Grupos objetivo del balanceador de carga sin instancias en buen estado](#)

.....

### Grupos objetivo del balanceador de carga sin instancias en buen estado

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

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

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

A continuación se muestra un ejemplo de aspecto normal:

The screenshot displays the AWS Management Console interface for a Target Group named 'res-bicfn3-web-portal-e2958adc'. The 'Details' section shows the following information:

- Target type:** Instance
- Protocol:** Port HTTPS: 8443
- Protocol version:** HTTP1
- VPC:** vpc-011d10e23ad10cb8e
- Load balancer:** res-bicfn3-external-alb

The 'Status' section shows the following counts:

- Total targets: 1
- Healthy: 1 (circled in green)
- Unhealthy: 0 (circled in red)
- Unused: 0
- Initial: 0
- Draining: 0

The 'Registered targets' table is shown below:

Instance ID	Name	Port	Zone	Health status	Health status details
I-Oba5d508631f20043	res-bicfn3-cluster-manager	8443	eu-central-1-c	healthy	

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

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

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

.....

## Lanzamiento de escritorios virtuales

### Temas

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

- [VDI pasar al estado de error después de iniciarlo](#)

.....

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

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

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

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

.....

## Solo puedo iniciar 5 escritorios virtuales

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

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

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

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

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

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

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

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

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

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

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

Mode                LastWriteTime         Length Name
----                -
-a----             8/4/2022 12:59 PM         1704 dc.v.key
-a----             8/4/2022 12:59 PM         1265 dc.v.pem
```

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

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

.....

## VDIsatascado en estado de aprovisionamiento

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

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

Las posibles causas de este problema son las siguientes.

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

El script de aprovisionamiento de bootstrap no se completó porque Amazon Machine Image (AMI) no tiene la configuración o las herramientas necesarias esperadas. Los archivos de registro de la instancia, como `/root/bootstrap/logs/` los de una instancia de Linux, pueden contener información útil al respecto. AMIsEs posible que los identificadores tomados del AWS Marketplace no funcionen en las instancias RES de escritorio. Es necesario probarlas para confirmar si son compatibles.

- Los scripts de datos de usuario no se ejecutan cuando la instancia de escritorio virtual de Windows se lanza desde una instancia personalizadaAMI.

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

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

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

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

.....

## VDIspasar al estado de error después de iniciarlo

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

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

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

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

1. `SSMal host` del administrador del clúster.
2. `cd /home`.
3. `ls`- debería incluir directorios con nombres de directorio que coincidan con los nombres de usuario, como,.. y así sucesivamente `admin1`. `admin2`
4. Elimine los directorios,. `sudo rm -r 'dir_name'` No elimine los directorios `ssm-user` y `ec2-user`.
5. Si los usuarios ya están sincronizados con el nuevo entorno, elimine los del usuario de la tabla de usuarios (excepto `clusteradmin`). `DDB`

6. Inicie la sincronización de AD: `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad` ejecútela en el administrador de clústeres Amazon. EC2
7. Reinicia la VDI instancia en el `Error` estado desde la página web. RES Valide que VDI pase al `Ready` estado en unos 20 minutos.

.....

## Componente de escritorio virtual

### Temas

- [La EC2 instancia de Amazon aparece repetidamente finalizada en la consola](#)
- [La instancia de vdc-controller está en ciclo debido a que no se pudo unir al VDI módulo AD/e muestra Failed Health Check API](#)
- [El proyecto no aparece en el menú desplegable al editar la pila de software para añadirla](#)
- [El registro de CloudWatch Amazon del administrador de clústeres muestra «user-home-init< > la cuenta aún no está disponible. En espera de que se sincronice el usuario» \(donde la cuenta es un nombre de usuario\)](#)
- [Al intentar iniciar sesión en el escritorio de Windows, aparece el mensaje «Tu cuenta ha sido deshabilitada». Consulte a su administrador»](#)
- [DHCPProblemas de opciones con la configuración de AD externa o de cliente](#)
- [Error de Firefox MOZILLA PKIX \\_ ERROR \\_ REQUIRED \\_ TLS \\_ FEATURE \\_ MISSING](#)

.....

### La EC2 instancia de Amazon aparece repetidamente finalizada en la consola

Si una instancia de infraestructura aparece repetidamente como terminada en la EC2 consola de Amazon, la causa puede estar relacionada con su configuración y depender del tipo de instancia de infraestructura. Los siguientes son métodos para determinar la causa.

Si la instancia de vdc-controller muestra estados terminados repetidamente en la EC2 consola de Amazon, esto puede deberse a una etiqueta secreta incorrecta. Los secretos que mantienen RES tienen etiquetas que se utilizan como parte de las políticas de control de IAM acceso asociadas a la infraestructura de las EC2 instancias de Amazon. Si el controlador vdc está circulando y aparece el siguiente error en el grupo de CloudWatch registros, es posible que el secreto no se haya etiquetado correctamente. Tenga en cuenta que el secreto debe estar etiquetado con lo siguiente:

```
{  
  "res:EnvironmentName": "<envname>" # e.g. "res-demo"  
  "res:ModuleName": "virtual-desktop-controller"  
}
```

El mensaje de CloudWatch registro de Amazon correspondiente a este error tendrá un aspecto similar al siguiente:

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

Comprueba las etiquetas de la EC2 instancia de Amazon y confirma que coinciden con la lista anterior.

.....

La instancia de vdc-controller está en ciclo debido a que no se pudo unir al VDI módulo AD/e muestra Failed Health Check API

Si el VDI módulo e no pasa la comprobación de estado, mostrará lo siguiente en la sección Estado del entorno.

## Modules

Environment modules and status



Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	<a href="#">Config</a>	✔ Deployed	⊖ Not Applicable	-
Cluster	cluster	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Directory Service	directoryservice	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Analytics	analytics	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	<a href="#">App</a>	✔ Deployed	✔ Healthy	• default
eVDI	vdc	2023.10b1	<a href="#">App</a>	✔ Deployed	✘ Failed	• default
Bastion Host	bastion-host	2023.10b1	<a href="#">Stack</a>	✔ Deployed	⊖ Not Applicable	• default

En este caso, la ruta general para la depuración consiste en consultar los registros del administrador del clúster [CloudWatch](#). (Busque el nombre del grupo de registros). `<env-name>/cluster-manager`

Posibles problemas:

- Si los registros contienen el texto `Insufficient permissions`, asegúrese de que el `ServiceAccount` nombre de usuario indicado al crear la pila de resoluciones esté escrito correctamente.

Ejemplo de línea de registro:

```
Insufficient permissions to modify computer account:
CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
(CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
request will be retried in 30 seconds
```

- Puede acceder al `ServiceAccount` nombre de usuario proporcionado durante la RES implementación desde la [SecretsManager consola](#). Busca el secreto correspondiente en el administrador de secretos y selecciona Recuperar texto sin formato. Si el nombre de usuario es

incorrecto, selecciona Editar para actualizar el valor secreto. Finalice las instancias actuales de cluster-manager y vdc-controller. Las nuevas instancias aparecerán en un estado estable.

- El nombre de usuario debe ser ServiceAccount «» si utiliza los recursos creados por la [pila de recursos externos](#) proporcionada. Si el DisableADJoin parámetro se estableció en False durante la implementación de RES, asegúrese de que el usuario ServiceAccount «» tenga permisos para crear objetos informáticos en el AD.
- Si el nombre de usuario utilizado es correcto, pero los registros contienen el texto `Invalid credentials`, es posible que la contraseña que ingresó sea incorrecta o haya caducado.

Ejemplo de línea de registro:

```
{'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [], 'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error, data 532, v4563'}
```

- Puede leer la contraseña que ingresó durante la creación del entorno accediendo al secreto que almacena la contraseña en la [consola de Secrets Manager](#). Seleccione el secreto (por ejemplo `<env_name>directoryserviceServiceAccountPassword`) y elija Recuperar texto sin formato.
- Si la contraseña del secreto es incorrecta, selecciona Editar para actualizar su valor en el secreto. Finalice las instancias actuales de cluster-manager y vdc-controller. Las nuevas instancias usarán la contraseña actualizada y aparecerán en un estado estable.
- Si la contraseña es correcta, es posible que haya caducado en el Active Directory conectado. Primero tendrá que restablecer la contraseña en Active Directory y, a continuación, actualizar el secreto. Puede restablecer la contraseña del usuario en Active Directory desde la [consola de Directory Service](#):
  1. Elija el ID de directorio adecuado
  2. Seleccione Acciones, restablezca la contraseña del usuario y, a continuación, rellene el formulario con el nombre de usuario (por ejemplo, "ServiceAccount«») y la nueva contraseña.
  3. Si la contraseña recién establecida es diferente de la contraseña anterior, actualice la contraseña en el secreto de Secret Manager correspondiente (por ejemplo, `<env_name>directoryserviceServiceAccountPassword`).
  4. Finalice las instancias actuales de cluster-manager y vdc-controller. Las nuevas instancias aparecerán en un estado estable.

.....

El proyecto no aparece en el menú desplegable al editar la pila de software para añadirla

Este problema puede estar relacionado con el siguiente problema relacionado con la sincronización de la cuenta de usuario con AD. Si aparece este problema, busca el error `<user-home-init> account not available yet. waiting for user to be synced ""` en el grupo de registros de CloudWatch Amazon, administrador del clúster, para determinar si la causa es la misma o está relacionada.

.....

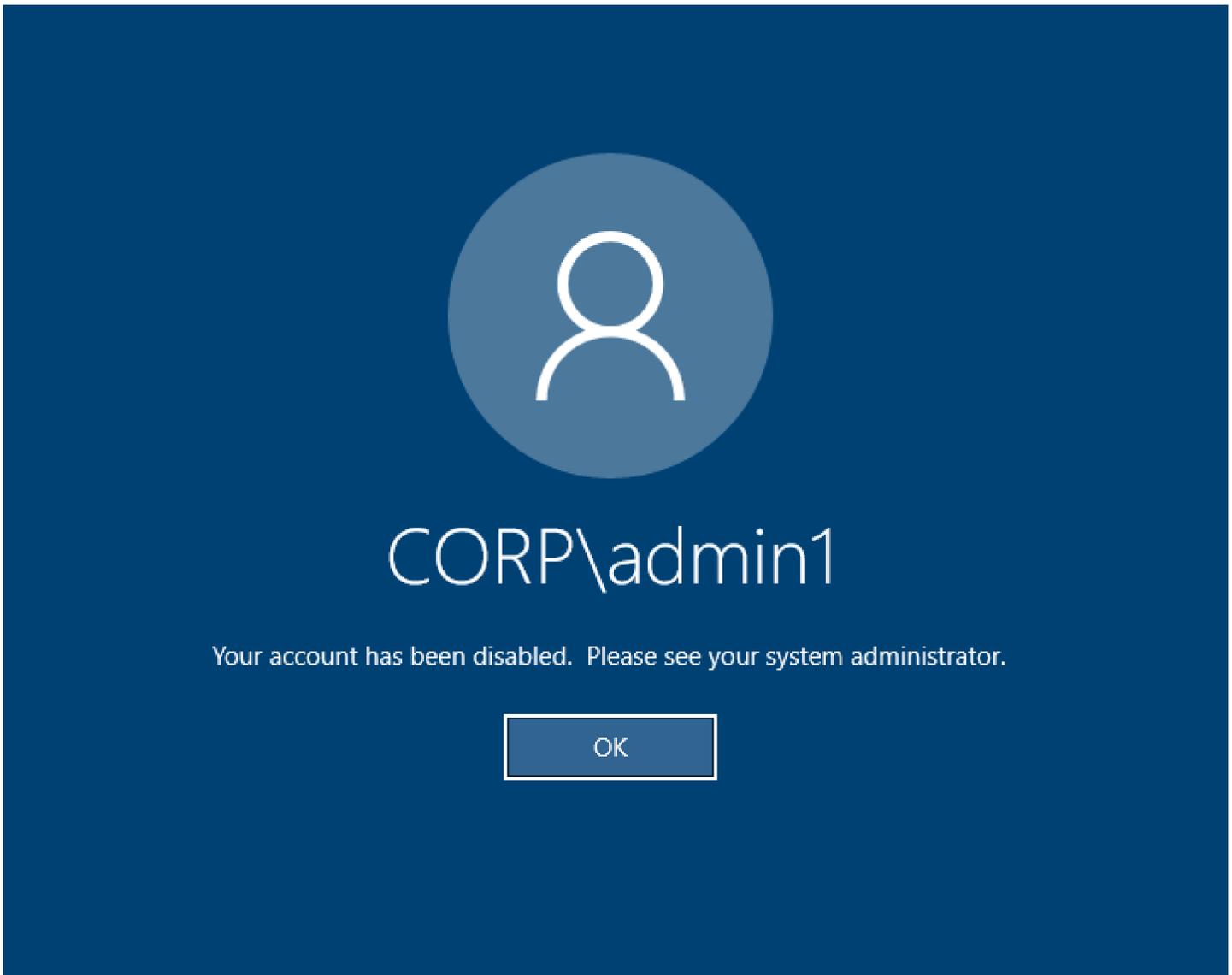
El registro de CloudWatch Amazon del administrador de clústeres muestra «user-home-init< > la cuenta aún no está disponible. En espera de que se sincronice el usuario» (donde la cuenta es un nombre de usuario)

El SQS suscriptor está ocupado y atrapado en un bucle infinito porque no puede acceder a la cuenta de usuario. Este código se activa cuando se intenta crear un sistema de archivos doméstico para un usuario durante la sincronización del usuario.

La razón por la que no puede acceder a la cuenta de usuario puede deberse a que no se RES configuró correctamente para el AD en uso. Un ejemplo podría ser que el `ServiceAccountCredentialsSecretArn` parámetro utilizado en la creación del RES entorno BI/ no fuera el valor correcto.

.....

Al intentar iniciar sesión en el escritorio de Windows, aparece el mensaje «Tu cuenta ha sido deshabilitada». Consulte a su administrador»



Si el usuario no puede volver a iniciar sesión en una pantalla bloqueada, esto puede indicar que el usuario se ha desactivado en el AD configurado RES después de haber iniciado sesión correctamente a través deSSO.

El SSO inicio de sesión debería fallar si la cuenta de usuario está deshabilitada en AD.

.....

## DHCPProblemas de opciones con la configuración de AD externa o de cliente

Si encuentra un error relacionado "The connection has been closed. Transport error" con los escritorios virtuales de Windows cuando los usa RES con su propio Active Directory, consulte el CloudWatch registro de dcv-connection-gateway Amazon para ver algo similar a lo siguiente:

```
Oct 28 00:12:30.626 INFO HTTP:Splicer Connection{id=263}:
WebSocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
lookup address information: Name or service not known" }

Oct 28 00:12:30.626 WARN HTTP:Splicer Connection{id=263}:
WebSocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
connection: Server unreachable: Server error: IO error: failed to lookup address
information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

Si utilizas un controlador de dominio de AD para tus DHCP opciones propiasVPC, debes:

1. AmazonProvidedDNS Añádalo a los dos controladores de dominioIPs.
2. Establezca el nombre de dominio en ec2.internal.

Aquí se muestra un ejemplo. Sin esta configuración, el escritorio de Windows generará un error de transporte, ya queRES/DCVbusca el nombre de host ip-10-0-x-xx.ec2.internal.

### Domain name

 ec2.internal

### Domain name servers

 10.0.2.168, 10.0.3.228,  
AmazonProvidedDNS

.....

Error de Firefox MOZILLA\_PKIX\_ERROR\_REQUIRED\_TLS\_FEATURE\_MISSING

Al utilizar el navegador web Firefox, es posible que aparezca un mensaje de error del tipo MOZILLA\_PKIX\_ERROR\_REQUIRED\_TLS\_FEATURE\_MISSING cuando intentes conectarte a un escritorio virtual.

[La causa es que el servidor RES web está configurado con TLS + Stapling activado, pero no responde con la validación de grapado \(consulta https://support.mozilla\). org/en-US/questions/1372483.](https://support.mozilla.org/en-US/questions/1372483)

[Para solucionarlo, sigue las instrucciones que se encuentran en: / mozilla\\_pkix\\_error\\_required\\_tls\\_feature\\_missing. https://really-simple-ssl.com](https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing)

.....

## Eliminación de Env

### Temas

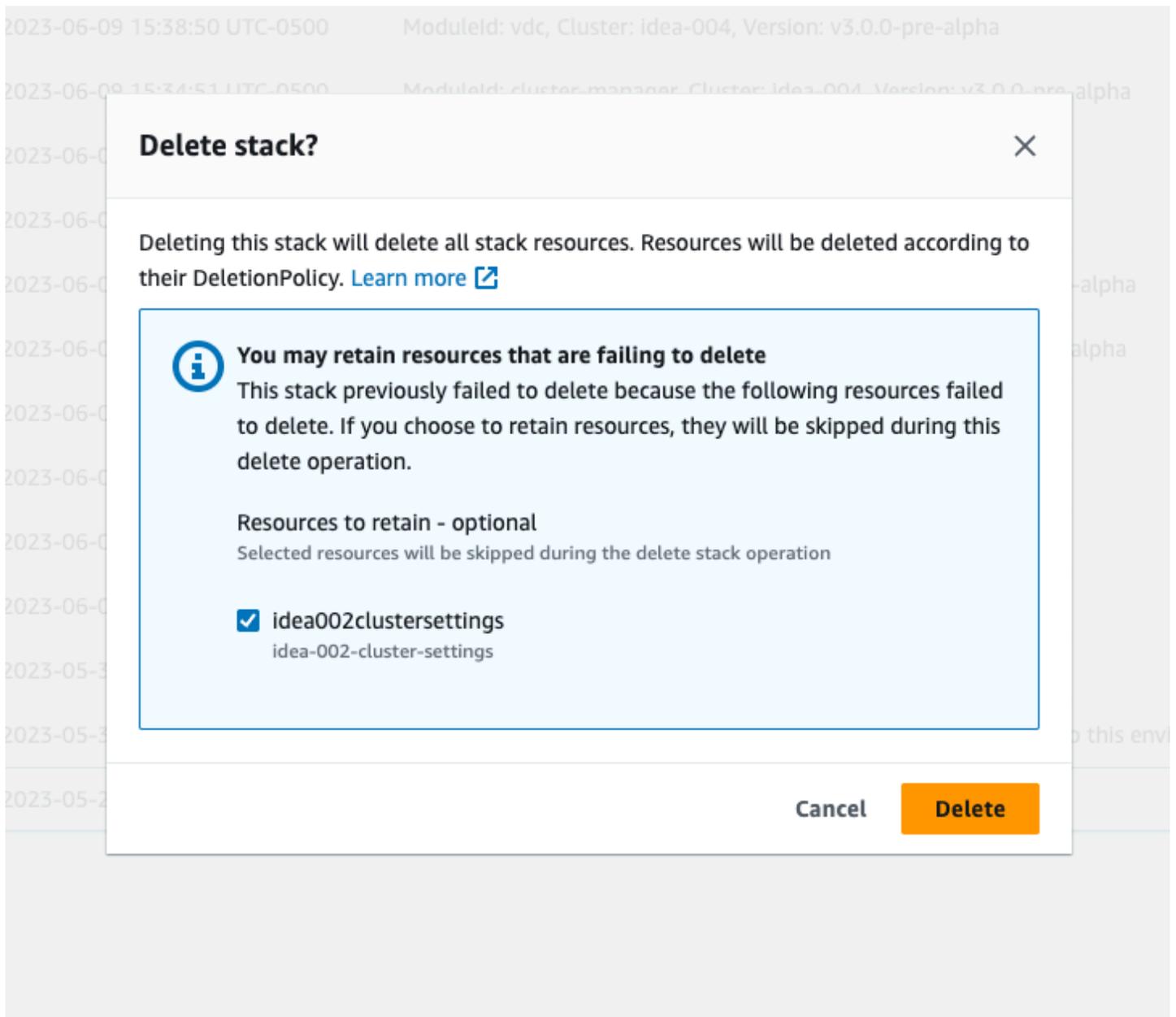
- [res-xxx-cluster se apilan en el estado FAILED "DELETE\\_" y no se pueden eliminar manualmente debido al error «El rol no es válido o no se puede asumir»](#)
- [Recopilación de registros](#)
- [Descargando VDI registros](#)
- [Descargar registros de EC2 instancias de Linux](#)
- [Descargar registros de EC2 instancias de Windows](#)
- [Recopilando ECS los registros del WaitCondition error](#)

.....

res-xxx-cluster se apilan en el estado FAILED "DELETE\_" y no se pueden eliminar manualmente debido al error «El rol no es válido o no se puede asumir»

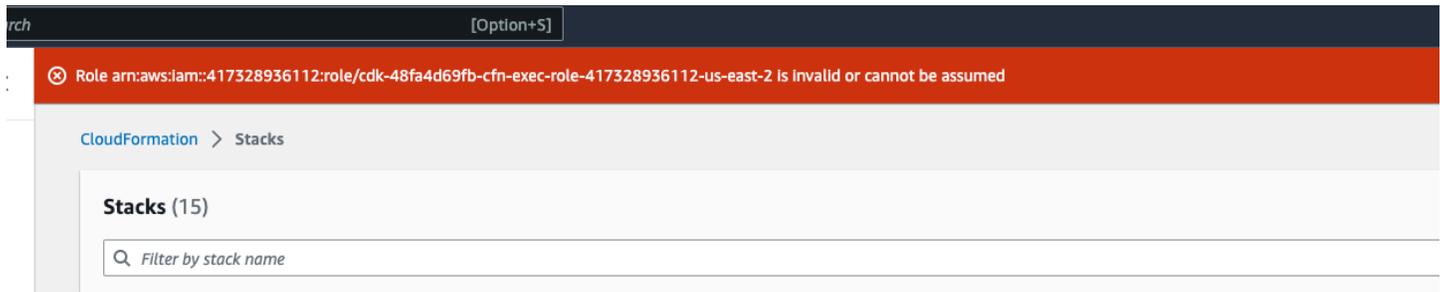
Si observa que la pila «res-xxx-cluster" está en el estado FAILED "DELETE\_" y no se puede eliminar manualmente, puede realizar los siguientes pasos para eliminarla.

Si ve la pila en un estado FAILED «DELETE\_», primero intente eliminarla manualmente. Es posible que aparezca un cuadro de diálogo confirmando la opción Eliminar pila. Elija Eliminar.



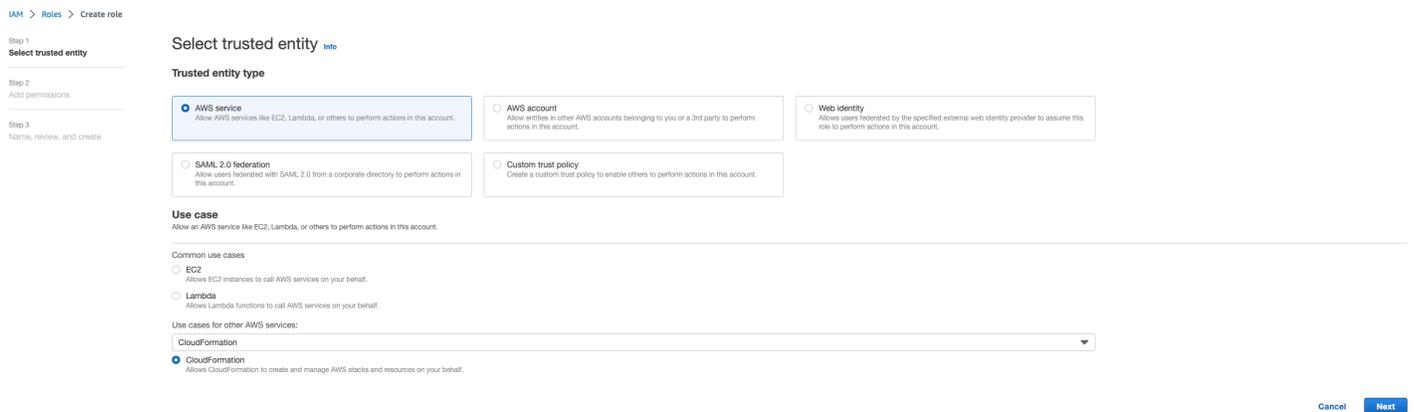
A veces, incluso si eliminas todos los recursos de la pila necesarios, es posible que sigas viendo el mensaje para seleccionar los recursos que deseas conservar. En ese caso, selecciona todos los recursos como «recursos a conservar» y selecciona Eliminar.

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



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

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



Elija Next (Siguiente). Asegúrese de conceder los permisos «**AWSCloudFormationFullAccess**» y «**AdministratorAccess**» al rol. Tu página de reseñas debería tener este aspecto:

## Name, review, and create

## Role details

## Role name

Enter a meaningful name to identify this role.

cdk-48fa4d69b-cfn-exec-role-417328936112-us-east-2

Maximum 64 characters. Use alphanumeric and '+,=,@,\_' characters.

## Description

Add a short explanation for this role.

Allows CloudFormation to create and manage AWS stacks and resources on your behalf.

Maximum 1000 characters. Use alphanumeric and '+,=,@,\_' characters.

## Step 1: Select trusted entities

Edit

```

1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Sid": "",
6-       "Effect": "Allow",
7-       "Principal": {
8-         "Service": "cloudformation.amazonaws.com"
9-       },
10-      "Action": "sts:AssumeRole"
11-    }
12-  ]
13- ]

```

## Step 2: Add permissions

Edit

## Permissions policy summary

Policy name	Type	Attached as
AWSCloudFormationFullAccess	AWS managed	Permissions policy
AdministratorAccess	AWS managed - job function	Permissions policy

## Tags

A continuación, vuelve a la CloudFormation consola y elimina la pila. Ahora deberías poder eliminarlo desde que creaste el rol. Por último, ve a IAM la consola y elimina el rol que creaste.

## Recopilación de registros

Iniciar sesión en una EC2 instancia desde la EC2 consola

- Sigue [estas instrucciones](#) para iniciar sesión en tu EC2 instancia de Linux.
- Sigue [estas instrucciones](#) para iniciar sesión en tu EC2 instancia de Windows. A continuación, abre Windows PowerShell para ejecutar cualquier comando.

## Recopilación de registros del host de Infraestructure

1. Administrador de clústeres: obtenga los registros para el administrador de clústeres de los siguientes lugares y adjúntelos al ticket.
  - a. Todos los registros del grupo de registros. CloudWatch <env-name>/cluster-manager
  - b. Todos los registros del /root/bootstrap/logs directorio de la <env-name>-cluster-manager EC2 instancia. Sigue las instrucciones que aparecen en el enlace «Iniciar sesión en

una EC2 instancia desde la EC2 consola» al principio de esta sección para iniciar sesión en tu instancia.

2. Controlador de VDC: Obtenga los registros del controlador de VDC de los siguientes lugares y adjúntelos al ticket.
  - a. Todos los registros del grupo de registros. CloudWatch <env-name>/vdc-controller
  - b. Todos los registros del /root/bootstrap/logs directorio de la <env-name>-vdc-controller EC2 instancia. Sigue las instrucciones que aparecen en el enlace «Iniciar sesión en una EC2 instancia desde la EC2 consola» al principio de esta sección para iniciar sesión en tu instancia.

Una de las maneras de obtener los registros fácilmente es seguir las instrucciones de la [Descargar registros de EC2 instancias de Linux](#) sección. El nombre del módulo sería el nombre de la instancia.

### Recopilación VDI de registros

Identifica la EC2 instancia de Amazon correspondiente

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

Recopile los VDI registros de Linux

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

Una de las formas de obtener los registros sería subirlos a s3 y luego descargarlos desde allí. Para ello, puedes seguir estos pasos para obtener todos los registros de un directorio y luego subirlos:

1. Siga estos pasos para copiar los registros dcv del /root/bootstrap/logs directorio:

```
sudo su -  
cd /root/bootstrap  
mkdir -p logs/dcv_logs  
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. Ahora, siga los pasos que se indican en la siguiente sección [Descargando VDI registros](#) para descargar los registros.

## Recopila los VDI registros de Windows

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

Una de las formas de obtener los registros sería subirlos a S3 y, a continuación, descargarlos desde allí. Para hacerlo, siga los pasos que se enumeran en la siguiente sección: [Descargando VDI registros](#).

.....

## Descargando VDI registros

1. Actualiza el IAM rol de la VDI EC2 instancia para permitir el acceso a S3.
2. Ve a la EC2 consola y selecciona tu VDI instancia.
3. Seleccione el IAM rol que está utilizando.
4. En la sección Políticas de permisos del menú desplegable Añadir permisos, selecciona Adjuntar políticas y, a continuación, selecciona la política de AmazonS3 FullAccess.
5. Seleccione Añadir permisos para adjuntar esa política.
6. Después, sigue los pasos que se indican a continuación según tu VDI tipo para descargar los registros. El nombre del módulo sería el nombre de la instancia.
  - a. [Descargar registros de EC2 instancias de Linux](#) para Linux.
  - b. [Descargar registros de EC2 instancias de Windows](#) para Windows.
7. Por último, edite el rol para eliminar la AmazonS3FullAccess política.

### Note

Todos VDIs usan el mismo IAM rol, que es `<env-name>-vdc-host-role-<region>`

.....

## Descargar registros de EC2 instancias de Linux

Inicia sesión en la EC2 instancia desde la que quieres descargar los registros y ejecuta los siguientes comandos para cargar todos los registros en un bucket de s3:

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

Después, vaya a la consola S3, seleccione el bucket con su nombre <environment\_name>-cluster-<region>-<aws\_account\_number> y descargue el <module\_name>\_logs.tar.gz archivo cargado anteriormente.

.....

## Descargar registros de EC2 instancias de Windows

Inicie sesión en la EC2 instancia desde la que desee descargar los registros y ejecute los siguientes comandos para cargar todos los registros en un bucket de S3:

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

Después, vaya a la consola S3, seleccione el bucket con su nombre `<environment_name>-cluster-<region>-<aws_account_number>` y descargue el `<module_name>_logs.zip` archivo cargado anteriormente.

.....

## Recopilando ECS los registros del WaitCondition error

1. Ve a la pila desplegada y selecciona la pestaña Recursos.
2. Expanda Implementar ResearchAndEngineeringStudio → Instalador → Tareas CreateTaskDef → CreateContainer → LogGroupy seleccione el grupo de registros para abrir CloudWatch los registros.
3. Obtenga el registro más reciente de este grupo de registros.

.....

## Entorno de demostración

### Temas

- [Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad](#)

.....

## Error de inicio de sesión en el entorno de demostración al gestionar la solicitud de autenticación al proveedor de identidad

### Problema

Si intentas iniciar sesión y aparece un «error inesperado al tramitar la solicitud de autenticación al proveedor de identidad», es posible que tus contraseñas estén caducadas. Puede ser la contraseña del usuario con el que intenta iniciar sesión o su cuenta de Active Directory Service.

### Mitigación

1. Restablezca las contraseñas del usuario y de la cuenta de servicio en la [consola de servicio de Directory](#).

2. Actualice las contraseñas de las cuentas de servicio en [Secrets Manager](#) para que coincidan con la nueva contraseña que ingresó anteriormente:
  - para la pila Keycloak: -... PasswordSecret - -... RESExternal - DirectoryService-... con descripción: Contraseña para Microsoft Active Directory
  - para RES: res- ServiceAccountPassword -... con descripción: contraseña de la cuenta de Active Directory Service
3. Ve a la [EC2consola](#) y termina la instancia del administrador de clústeres. Las reglas de Auto Scaling activarán automáticamente el despliegue de una nueva instancia.

## Problemas conocidos

- [Problemas conocidos de la versión 2024.x](#)
  - [\(2024.08\) Los escritorios virtuales no pueden montar un bucket de Amazon S3 de lectura/escritura con ARN un bucket raíz y un prefijo personalizado](#)
  - [\(2024.06\) Se produce un error al aplicar la instantánea cuando el nombre del grupo de AD contiene espacios](#)
  - [\(2024.04-2024.04.02\) El límite de permisos proporcionado no está asociado a la función de las instancias IAM VDI](#)
  - [\(2024.04.02 y versiones anteriores\) Las instancias de Windows NVIDIA en ap-southeast-2 \(Sídney\) no se inician](#)
  - [\(2024.04 y 2024.04.01\) elimine el error en RES GovCloud](#)
  - [\(2024.04 - 2024.04.02\) Es posible que el escritorio virtual Linux se quede atascado en el estado «" al reiniciarse RESUMING](#)
  - [\(04.02 de abril de 2020 y versiones anteriores\) No se sincronizan los usuarios de AD cuyo SAMAccountName atributo incluye letras mayúsculas o caracteres especiales](#)
  - [\(02 de abril de 2020 y versiones anteriores\) La clave privada para acceder al host del bastión no es válida](#)
  - [\(2024.06 y versiones anteriores\) Los miembros del grupo no se sincronizaron durante la sincronización de AD RES](#)
  - [\(2024.06 y versiones anteriores\) CVE -2024-6387, egreSSHion R, vulnerabilidad de seguridad en Ubuntu RHEL 9 VDIs](#)

## Problemas conocidos de la versión 2024.x

.....

(2024.08) Los escritorios virtuales no pueden montar un bucket de Amazon S3 de lectura/escritura con ARN un bucket raíz y un prefijo personalizado

### Descripción del error

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

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

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

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

### Versiones afectadas

2024.08

### Mitigación

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

- a. El parche solo se aplica a la versión RES 2024.08.
- b. [El script del parche requiere la AWS CLI versión 2, Python 3.9.16 o superior y Boto3.](#)
- c. Configure AWS CLI la cuenta y la región en las que RES se implementa y asegúrese de tener permisos de Amazon S3 para escribir en el bucket creado por RES.

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

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

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

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

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
  Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
  Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

#### Note

En el caso de VPC las configuraciones privadas, si aún no lo ha hecho, asegúrese de añadir a la <RES-EnvironmentName>-vdc-custom-credential-broker-lambda

función el Environment variable nombre `AWS_STS_REGIONAL_ENDPOINTS` y el valor `deRegional`. Para obtener más información, consulte [Requisitos previos del bucket de Amazon S3 para implementaciones aisladas VPC](#).

- Una vez que el grupo objetivo que comienza con el nombre `<RES-EnvironmentName>-vdc-ext` se recupere, VDI será necesario lanzar uno nuevo que tenga montados correctamente los buckets S3 de lectura/escritura con el bucket raíz ARN y el prefijo personalizado.

.....

(2024.06) Se produce un error al aplicar la instantánea cuando el nombre del grupo de AD contiene espacios

### Problema

RES La versión 2024.06 no puede aplicar las instantáneas de versiones anteriores si los grupos de AD contienen espacios en sus nombres.

Los registros del administrador de clústeres (del grupo de CloudWatch registros) incluirán el `<environment-name>/cluster-manager` siguiente error durante la sincronización de AD:

```
[apply-snapshot] authz.role-assignments/<Group name with spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_-.]{1,20}:(user|group)$
```

El error se debe a que RES solo se aceptan nombres de grupos que cumplen los siguientes requisitos:

- Solo puede contener ASCII letras minúsculas y mayúsculas, dígitos, guiones (-), puntos (.) y caracteres de subrayado (\_)
- No se permite usar un guión (-) como primer carácter
- No puede contener espacios.

### Versiones afectadas

2024.06

### Mitigación

1. Para descargar el script y el archivo del parche ([patch.py](#) y [groupname\\_regex.patch](#)), ejecute el siguiente comando y <output-directory> sustitúyalos por el directorio en el que desee colocar los archivos y por el nombre de su entorno: <environment-name> RES
  - a. El parche solo se aplica a la versión 2024.06 RES
  - b. [El script del parche requiere la AWS CLI versión 2, Python 3.9.16 o superior y Boto3.](#)
  - c. Configure AWS CLI la cuenta y la región en las que RES está implementado y asegúrese de tener permisos de S3 para escribir en el bucket creado por: RES

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
${OUTPUT_DIRECTORY}/groupname_regex.patch
```

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

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. Para reiniciar la instancia de Cluster Manager para su entorno, ejecute los siguientes comandos: También puede finalizar la instancia desde Amazon EC2 Management Console.

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
  Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
  Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

**Note**

El parche permite que los nombres de los grupos de AD contengan ASCII letras minúsculas y mayúsculas, dígitos, guiones (-), puntos (.), guiones bajos (\_) y espacios con una longitud total de entre 1 y 30, ambos inclusive.

.....

(2024.04-2024.04.02) El límite de permisos proporcionado no está asociado a la función de las instancias IAM VDI

¿El problema

Las sesiones de escritorios virtuales no heredan correctamente la configuración de límites de permisos de su proyecto. Esto se debe a que el límite de permisos definido por el IAMPermissionBoundary parámetro no se asignó correctamente a un proyecto durante su creación.

Versiones afectadas

2024.04 - 2024.04.02

Mitigación

Siga estos pasos para poder heredar correctamente VDIs el límite de permisos asignado a un proyecto:

1. Para descargar el script y el archivo del parche ([patch.py](#) y [vdi\\_host\\_role\\_permission\\_boundary.patch](#)), ejecute el siguiente comando y sustitúyalos por el directorio local en el que desee colocar los archivos: <output-directory>
  - a. El parche RES solo se aplica a la versión 2024.04.02. Si tiene la versión 2024.04 o 2024.04.01, puede seguir los [pasos que se indican en el documento público para las actualizaciones de las versiones menores a fin de actualizar su entorno a la versión 2024.04.02](#).
  - b. [El script del parche requiere \(AWS CLIv2\), Python 3.9.16 o superior y Boto3](#).
  - c. Configure la AWS CLI cuenta y la región en las que RES está desplegado y asegúrese de tener permisos de S3 para escribir en el bucket creado por él. RES

```
OUTPUT_DIRECTORY=<output-directory>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
--output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando patch y <environment-name> sustitúyalo por el nombre de su RES entorno:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. Reinicie la instancia del administrador de clústeres en su entorno ejecutando este comando, sustituyéndolo <environment-name> por el nombre de su entorno. RES También puede cancelar la instancia desde Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>
```

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
  Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
  Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 y versiones anteriores) Las instancias de Windows NVIDIA en ap-southeast-2 (Sídney) no se inician

¿El problema

Amazon Machine Images (AMIs) se utilizan para activar escritorios virtuales (VDIs) RES con configuraciones específicas. Cada uno AMI tiene un identificador asociado que varía según la región. El AMI ID configurado RES para lanzar instancias de Windows Nvidia en ap-southeast-2 (Sídney) es incorrecto actualmente.

AMI ID `ami-0e190f8939a996caf` de este tipo de configuración de instancia aparece incorrectamente en ap-southeast-2 (Sídney). AMI En su lugar, se debe usar un ID. `ami-027cf6e71e2e442f4`

Los usuarios recibirán el siguiente error al intentar lanzar una instancia con la configuración predeterminada `ami-0e190f8939a996caf` AMI.

```
An error occurred (InvalidAMIID.NotFound) when calling the RunInstances operation: The image id '[ami-0e190f8939a996caf]' does not exist
```

Pasos para reproducir el error, incluido un ejemplo de archivo de configuración:

- RES Despléguese en la región ap-southeast-2.
- Lance una instancia con la pila de software (ID) NVIDIA predeterminada de Windows. AMI `ami-0e190f8939a996caf`

## Versiones afectadas

Todas las RES versiones 2024.04.02 o anteriores se ven afectadas

## Mitigación

La siguiente mitigación se probó en la versión 2024.01.01: RES

- Registre una nueva pila de software con la siguiente configuración
  - AMIID: `ami-027cf6e71e2e442f4`
  - Sistema operativo: Windows
  - GPU Fabricante: NVIDIA
  - Mín. Tamaño de almacenamiento (GB): 30
  - Mín. RAM (GB): 4
- Utilice esta pila de software para lanzar NVIDIA instancias de Windows

.....

## (2024.04 y 2024.04.01) elimine el error en RES GovCloud

### ¿El problema

Durante el flujo de trabajo de RES eliminación, UnprotectCognitoUserPool Lambda desactiva la protección contra eliminación para los grupos de usuarios de Cognito que se eliminarán más adelante. La ejecución de Lambda se inicia con. InstallerStateMachine

Debido a las diferencias de AWS CLI versión predeterminadas entre las versiones comerciales y regionales, la `update_user_pool` llamada en la Lambda fallará en GovCloud las GovCloud regiones.

Los clientes recibirán el siguiente error cuando RES intenten eliminar en una GovCloud región:

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection\n\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,\nSmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,\nVerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,\nDeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,\nAdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

### Pasos para reproducir el error:

- Implemente RES en una GovCloud región
- Elimine la RES pila

### Versiones afectadas

RESversiones 2024.04 y 2024.04.01

### Mitigación

La siguiente mitigación se probó en la versión 2024.04: RES

- Abra la UnprotectCognitoUserPool Lambda
  - Convención de nomenclatura: `<env-name>-InstallerTasksUnprotectCognitoUserPool-...`
- Configuración del tiempo de ejecución -> Editar -> Seleccionar tiempo de ejecución Python 3.11 -> Guardar.

- Abrir CloudFormation.
- Eliminar RES pila -> salir de Retain Installer Resource UNCHECKED -> Eliminar.

.....

(2024.04 - 2024.04.02) Es posible que el escritorio virtual Linux se quede atascado en el estado «" al reiniciarse RESUMING

¿Cuál es el problema

Los escritorios virtuales Linux pueden quedarse atascados en el estado RESUMING «» al reiniciarse después de una parada manual o programada.

Una vez reiniciada la instancia, el AWS Systems Manager no ejecuta ningún comando remoto para crear una DCV sesión nueva y falta el siguiente mensaje de registro en los registros de vdc-controller (en el grupo de CloudWatch registros): <environment-name>/vdc/controller CloudWatch

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

Versiones afectadas

2024.04 - 2024.04.02

Mitigación

Para recuperar los escritorios virtuales que están atrapados en el estado «»: RESUMING

1. SSHa la instancia problemática desde la EC2 consola.
2. Ejecuta los siguientes comandos en la instancia:

```
sudo su -  
/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/  
configure_post_reboot.sh  
sudo reboot
```

3. Espera a que la instancia se reinicie.

Para evitar que los nuevos escritorios virtuales sufran el mismo problema, sigue estos pasos:

1. Para descargar el script y el archivo del parche ([patch.py](#) y [vdi\\_stuck\\_in\\_resuming\\_status.patch](#)), ejecute el siguiente comando y reemplácelo por el directorio en el que desee colocar los archivos: `<output-directory>`

 Note

- El parche RES solo se aplica a la versión 2024.04.02.
- [El script del parche requiere la AWS CLI versión 2, Python 3.9.16 o superior y Boto3.](#)
- Configure la AWS CLI cuenta y la región en las que RES está desplegado y asegúrese de tener permisos de S3 para escribir en el bucket creado por él. RES

```
OUTPUT_DIRECTORY=<output-directory>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando de parche y `<environment-name>` sustitúyalo por el nombre de su RES entorno y `<aws-region>` por la región en la que RES se implementa:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
--module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. Para reiniciar la instancia de VDC Controller de su entorno, ejecute los siguientes comandos y `<environment-name>` sustitúyalos por el nombre de su RES entorno:

```
ENVIRONMENT_NAME=<environment-name>
```

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
```

```
--output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(04.02 de abril de 2020 y versiones anteriores) No se sincronizan los usuarios de AD cuyo SAMAccountName atributo incluye letras mayúsculas o caracteres especiales

¿El problema

RES no sincroniza los usuarios de AD después SSO de configurarse durante al menos dos horas (dos ciclos de sincronización de AD). Los registros del administrador de clústeres (del grupo de CloudWatch registros) incluyen el <environment-name>/cluster-manager siguiente error durante la sincronización de AD:

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?![_.]$)
```

El error se debe a que RES solo se acepta un SAMAccount nombre de usuario que cumpla los siguientes requisitos:

- Solo puede contener ASCII letras minúsculas, dígitos, puntos (.) y caracteres de subrayado (\_).
- No se permite un punto o un guión bajo como primer o último carácter.
- No puede contener dos puntos o guiones bajos continuos (por ejemplo, .., \_\_, .\_, \_).

Versiones afectadas

2024.04.02 y versiones anteriores

Mitigación

1. Para descargar el script y el archivo del parche ([patch.py](#) y [samaccountname\\_regex.patch](#)), ejecute el siguiente comando y sustitúyalo por el directorio en el que desee colocar los archivos: <output-directory>

**Note**

- El parche RES solo se aplica a la versión 2024.04.02.
- [El script del parche requiere la AWS CLI versión 2, Python 3.9.16 o superior y Boto3.](#)
- Configure la AWS CLI cuenta y la región en las que RES está desplegado y asegúrese de tener permisos de S3 para escribir en el bucket creado por él. RES

```
OUTPUT_DIRECTORY=<output-directory>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
${OUTPUT_DIRECTORY}/samaccountname_regex.patch
```

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando patch y <environment-name> sustitúyalo por el nombre de su RES entorno:

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. Para reiniciar la instancia de Cluster Manager para su entorno, ejecute los siguientes comandos y <environment-name> sustitúyalos por el nombre de su RES entorno. También puede cancelar la instancia desde Amazon EC2 Management Console.

```
ENVIRONMENT_NAME=<environment-name>
```

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
  Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
  Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)
```

```
aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(02 de abril de 2020 y versiones anteriores) La clave privada para acceder al host del bastión no es válida

¿El problema

Cuando un usuario descarga la clave privada para acceder al servidor del bastión desde el portal RES web, la clave no tiene el formato correcto: se descargan varias líneas en una sola línea, lo que invalida la clave. El usuario recibirá el siguiente error cuando intente acceder al host del bastión con la clave descargada:

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic)
```

Versiones afectadas

2024.04.02 y versiones anteriores

Mitigación

Recomendamos usar Chrome para descargar las claves, ya que este navegador no se ve afectado.

Como alternativa, se puede volver a formatear el archivo clave creando una nueva línea después  
-----BEGIN PRIVATE KEY----- y otra línea nueva justo antes. -----END PRIVATE  
KEY-----

.....

(2024.06 y versiones anteriores) Los miembros del grupo no se sincronizaron durante la sincronización de AD RES

Descripción del error

Los miembros del grupo no se sincronizarán correctamente RES si el GroupOU es diferente del UserOU.

RES crea un filtro ldapsearch al intentar sincronizar los usuarios de un grupo de AD. El filtro actual utiliza incorrectamente el parámetro UserOU en lugar del parámetro GroupOU. El resultado es que

la búsqueda no devuelve ningún usuario. Este comportamiento solo se produce en los casos en que UserSou y GroupU son diferentes.

## Versiones afectadas

Este problema afecta a todas las RES versiones 2024.06 o anteriores

## Mitigación

Siga estos pasos para resolver el problema:

1. Para descargar el script patch.py y el archivo group\_member\_sync\_bug\_fix.patch, ejecute los siguientes comandos y <output-directory> sustitúyalos por el directorio local en el que desee descargar los archivos y por la versión que desee aplicar el parche: <res\_version>  
RES

### Note

- [El script del parche requiere la AWS CLI versión 2, Python 3.9.16 o superior y Boto3.](#)
- Configure la AWS CLI cuenta y la región en las que RES está desplegado y asegúrese de tener permisos de S3 para escribir en el bucket creado por él. RES
- El parche solo es compatible con RES las versiones 2024.04.02 y 2024.06. Si utiliza la 2024.04 o la 2024.04.01, puede seguir los pasos que se indican para actualizar primero su entorno [Actualizaciones de versiones menores](#) a la versión 2024.04.02 antes de aplicar el parche.

- RESVersión: 2024.04.02 RES

[Enlace de descarga del parche: 2024.04.02\\_group\\_member\\_sync\\_bug\\_fix.patch](#)

- RESVersiónRES: 2024.06

[Enlace de descarga del parche: 2024.06\\_group\\_member\\_sync\\_bug\\_fix.patch](#)

```
OUTPUT_DIRECTORY=<output-directory>  
RES_VERSION=<res_version>  
mkdir -p ${OUTPUT_DIRECTORY}
```

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

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

2. Navegue hasta el directorio en el que se descargaron el script y el archivo del parche. Ejecute el siguiente comando patch y <environment-name> sustitúyalo por el nombre de su RES entorno:

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>

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

3. Para reiniciar la instancia del administrador de clústeres de su entorno, ejecute los siguientes comandos:

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
  Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
  Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.06 y versiones anteriores) CVE -2024-6387, egreSSHion R, vulnerabilidad de seguridad en Ubuntu RHEL9 VDIs

#### Descripción del error

CVESe ha identificado [-2024-6387](#)regreSSHion, doblado, en el servidor Open. SSH Esta vulnerabilidad permite a atacantes remotos y no autenticados ejecutar código arbitrario en el servidor de destino, lo que supone un grave riesgo para los sistemas que utilizan Open para garantizar la seguridad de las comunicaciones. SSH

RESEn efecto, la configuración estándar consiste SSH en pasar por el host bastión hasta los escritorios virtuales, y el host bastión no se ve afectado por esta vulnerabilidad. Sin embargo, la versión predeterminada AMI (Amazon Machine Image) que proporcionamos RHEL9 y Ubuntu 2024 VDIs (infraestructura de escritorio virtual) en ALLRES las versiones utilizan una SSH versión abierta que es vulnerable a la amenaza de seguridad.

Esto significa que la versión existente RHEL9 y Ubuntu2024 VDIs podrían ser explotables, pero el atacante necesitaría acceder al servidor bastión.

[Puedes encontrar más detalles sobre el problema aquí.](#)

## Versiones afectadas

Este problema afecta a todas las RES versiones 2024.06 o anteriores.

## Mitigación

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

Si ya tienes Ubuntu RHEL9 o Ubuntu VDIs, te recomendamos que sigas las PATCHEXISTINGVDI instrucciones que aparecen a continuación. Para parchear future VDIs, te recomendamos seguir las PATCHFUTUREVDI instrucciones. Estas instrucciones describen cómo ejecutar un script para aplicar la actualización de la plataforma en su VDIs.

## PATCH EXISTING VDIs

1. Ejecute el siguiente comando que parcheará todos los Ubuntu existentes y RHEL9 VDIs:
  - a. El script del parche requiere la [AWS CLI versión 2](#).
  - b. Configure la AWS CLI cuenta y la región en las que RES está desplegado y asegúrese de tener permisos de administrador de AWS sistemas para enviar un comando de ejecución de Systems Manager.

```
aws ssm send-command \  
  --document-name "AWS-RunRemoteScript" \  
  --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \  
  --parameters '{"sourceType":["S3"],"sourceInfo":["{\\"path\\":\\"https://  
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
```

```
patch_scripts/scripts/patch_openssh.sh\"}], "commandLine": ["bash  
patch_openssh.sh"]}]'
```

2. Puede comprobar que el script se ha ejecutado correctamente en la [página Ejecutar comandos](#). Haga clic en la pestaña Historial de comandos, seleccione el ID de comando más reciente y compruebe que todas las instancias IDs tienen un SUCCESS mensaje.

## PATCH FUTURE VDIs

1. Para descargar el script y el archivo del parche ([patch.py](#) y [update\\_openssh.patch](#)), ejecute los siguientes comandos y <output-directory> sustitúyalos por el directorio en el que desee descargar los archivos y <environment-name> por el nombre de su entorno: RES

### Note

- El parche solo se aplica a la versión 2024.06. RES
- [El script del parche requiere \(AWS CLIv2\), Python 3.9.16 o superior y Boto3](#).
- Configure su copia AWS CLI para la cuenta y la región en las que RES está desplegado y asegúrese de tener permisos de S3 para escribir en el bucket creado por él. RES

```
OUTPUT_DIRECTORY=<output-directory>  
ENVIRONMENT_NAME=<environment-name>
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/  
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/  
releases/2024.06/patch_scripts/patches/update_openssh.patch --output  
${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. Ejecute el siguiente comando de parche:

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-  
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/  
update_openssh.patch
```

3. Reinicie la instancia de VDC Controller para su entorno con los siguientes comandos:

```
INSTANCE_ID=$(aws ec2 describe-instances \
  --filters \
  Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
  Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME} \
  --query "Reservations[0].Instances[0].InstanceId" \
  --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

### Important

La aplicación de parches en el futuro solo VDIs se admite en RES las versiones 2024.06 y posteriores. Para parchear el futuro VDIs en RES entornos con versiones anteriores a la 2024.06, primero actualice el RES entorno a la 2024.06 siguiendo las instrucciones de: [Actualizaciones de versiones principales](#)

.....

## Avisos

Cada EC2 instancia de Amazon incluye dos licencias de Servicios de Escritorio Remoto (Terminal Services) para fines de administración. Esta [información](#) está disponible para ayudarle a aprovisionar estas licencias a sus administradores. También puede usarlo [AWS Systems Manager Session Manager](#), lo que permite el acceso remoto a EC2 las instancias de Amazon sin RDP y sin necesidad de RDP licencias. Si se necesitan licencias adicionales de Remote Desktop Services, el usuario de Remote Desktop CALs debe adquirirse en Microsoft o en un distribuidor de licencias de Microsoft. Los usuarios de escritorios remotos CALs con Software Assurance activo tienen las ventajas de la movilidad de licencias y pueden trasladarse a entornos de inquilinos AWS predeterminados (compartidos). Para obtener información sobre cómo adquirir licencias sin las ventajas de Software Assurance o License Mobility, consulte [esta sección](#) delFAQ.

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 implica 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 [CHANGELOGarchivo.md](#) del GitHub repositorio.

Date	Cambio
Octubre de 2024	<ul style="list-style-type: none"> <li>• Versión de lanzamiento 2024.10: Se agregó soporte para:               <ul style="list-style-type: none"> <li>• <a href="#">Límites del entorno</a>.</li> <li>• <a href="#">Perfiles para compartir escritorios</a>.</li> <li>• <a href="#">Interfaz de escritorio virtual: parada automática</a>.</li> </ul> </li> </ul>
Agosto de 2024	<ul style="list-style-type: none"> <li>• Versión de lanzamiento 2024.08: Se agregó soporte para —               <ul style="list-style-type: none"> <li>• montar buckets de Amazon S3 en instancias de Linux Virtual Desktop Infrastructure (VDI). Consulte <a href="#">Buckets de Amazon S3</a>.</li> <li>• permisos de proyectos personalizados, un modelo de permisos mejorado que permite personalizar las funciones existentes y añadir funciones personalizadas. Consulte <a href="#">Política de permisos</a>.</li> </ul> </li> <li>• Guía del usuario: se amplió la <a href="#">Solución de problemas</a> sección.</li> </ul>
Junio de 2024	<ul style="list-style-type: none"> <li>• Versión de lanzamiento 2024.06: compatibilidad con Ubuntu, permisos de propietario del proyecto.</li> <li>• Guía del usuario: agregada <a href="#">Cree un entorno de demostración</a></li> </ul>

Date	Cambio
Abril de 2024	Versión de lanzamiento 2024.04: plantillas listas para el lanzamiento de RES proyectos AMIs y listas para el lanzamiento
Marzo de 2024	Temas adicionales de solución de problemas, retención de CloudWatch registros y desinstalación de versiones secundarias
Febrero de 2024	Versión de lanzamiento 2024.01.01: plantilla de despliegue actualizada
Enero de 2024	Versión de lanzamiento 2024.01
Diciembre de 2023	GovCloud instrucciones y plantillas añadidas
Noviembre de 2023	Versión inicial

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.