

S4: Laboratorio: Introducción a la gestión de identidades

Introducción a AWS Identity and Access Management (IAM) (Spanish)

En muchos entornos de negocios, el acceso involucra un inicio de sesión único en un equipo o una red de sistemas que proporciona al usuario acceso a todos los recursos de la red. Este acceso incluye los derechos a los archivos personales y compartidos en un servidor de red, intranet de empresas, impresoras y otros recursos y dispositivos de red. Los usuarios no autorizados pueden explotar rápidamente estos mismos recursos si el control de acceso y los procedimientos de autenticación asociados no están configurados correctamente.

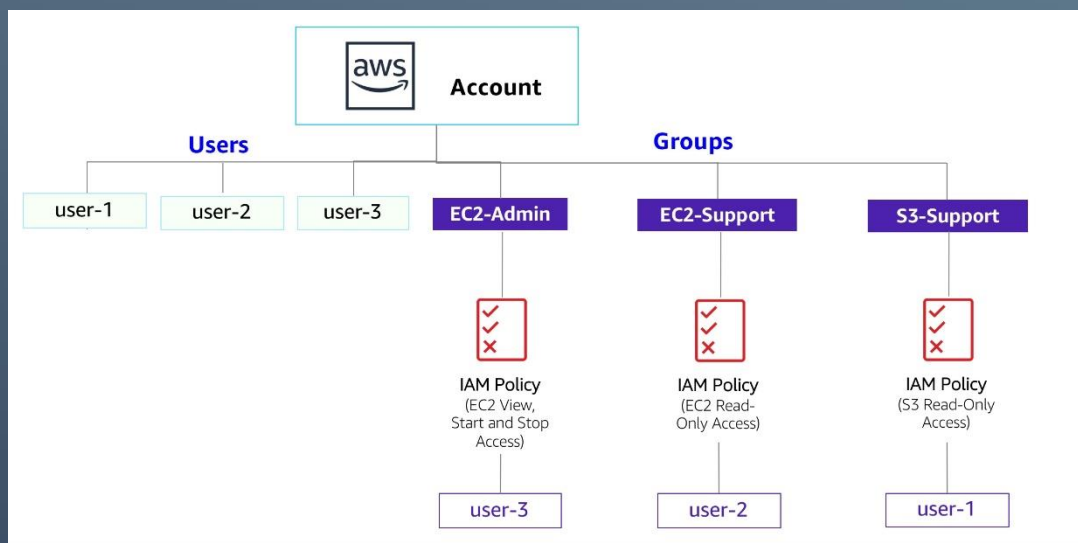
En este laboratorio, explorará los usuarios, grupos de usuarios y políticas en el servicio AWS Identity and Access Management (IAM).

OBJETIVOS

Después de completar este laboratorio, podrá realizar lo siguiente:

- Crear y aplicar una política de contraseñas de IAM
- Analizar usuarios y grupos de usuarios de IAM creados previamente
- Inspeccionar políticas de IAM según se apliquen a los grupos de usuarios creados previamente
- Agregar usuarios a grupos de usuario con capacidades específicas activas
- Ubicar y usar la URL de inicio de sesión de la IAM
- Probar los efectos de las políticas en el acceso a los servicios

Este es un diagrama del entorno actual con los usuarios de IAM y los grupos de IAM.



Otros servicios de AWS

Durante el laboratorio, es posible que aparezcan mensajes de error cuando intente realizar acciones que no se ajusten a los pasos incluidos en este laboratorio. Los mensajes no afectarán su capacidad para completar el laboratorio.

IAM

IAM se puede usar para lo siguiente:

- **Administrar usuarios de IAM y su acceso:** puede crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos con Multi-Factor Authentication). Puede administrar los permisos para controlar qué operaciones puede realizar cada usuario.
- **Administrar roles de IAM y sus permisos:** un rol de IAM es similar a un usuario, ya que un rol es una identidad de AWS con políticas de permisos que establecen qué puede hacer o no la identidad en Amazon Web Services (AWS). Sin embargo, en lugar de estar asociado únicamente a una persona, el objetivo es que cualquiera que necesite el rol pueda asumirlo.

Administrar usuarios federados y sus permisos: puede activar la identidad federada a fin de permitir que los usuarios existentes de su empresa puedan acceder a la Consola de administración de AWS, llamar a las interfaces de programación de aplicaciones (API) de AWS y acceder a los recursos sin necesidad de crear un usuario de IAM para cada identidad.

Tarea 1: Crear una política de contraseña de cuenta

En esta tarea, creará una política de contraseña personalizada para su cuenta de AWS. Esta política afecta a todos los usuarios asociados con la cuenta.

1. Primero, anote la región en la que se encuentra; por ejemplo, **Oregon** [Oregón]). La esquina superior derecha de la página de la consola muestra su región.
2. En la Consola de administración de AWS, en el cuadro de búsqueda , ingrese IAM y selecciónelo.
3. En el panel de navegación izquierdo, elija **Account settings** (Configuración de la aplicación).

Aquí puede ver la política de contraseña predeterminada que está en vigencia actualmente. La empresa en la que está trabajando tiene requisitos mucho más estrictos y tiene que actualizar esta política.

4. Seleccione **Change password policy** (Cambiar política de contraseñas).
5. En **Select your account password policy requirements** (Seleccionar los requisitos de políticas de contraseñas de su cuenta), configure las siguientes opciones:
 - En **Enforce minimum password length** (Aplicar longitud de contraseña mínima), cambie 8 a 10 caracteres.
 - Seleccione todas las casillas excepto la casilla para **Password expiration requires administrator reset** (El vencimiento de contraseña requiere un restablecimiento por el administrador).
 - En **Enable password expiration** (Habilitar vencimiento de contraseña), deje la opción predeterminada de **90** días.
 - En **Prevent password reuse** (Prevenir reutilización de contraseña), deje la opción predeterminada de **5** contraseñas.
6. Seleccione **Save changes** (Guardar los cambios).

Estos cambios se aplican en el nivel de cuenta de AWS y se aplican a todos los usuarios asociados con la cuenta.

RESUMEN DE LA TAREA 1

En esta tarea, fortaleció los requisitos de la contraseña al crear una política de contraseñas predeterminada. Las varias opciones de contraseña que seleccionó ahora han hecho que las contraseñas que los usuarios crearán sean mucho más difíciles de vulnerar.

Editar política de contraseñas [Información](#)

Política de contraseñas

☐ Valores predeterminados de IAM
Aplique los requisitos de contraseña predeterminados.

☒ Personalizada
Aplique requisitos de contraseña personalizados.

Longitud mínima de la contraseña.
Exija una longitud mínima de caracteres.

caracteres

Debe tener entre 6 y 128 caracteres.

Seguridad de la contraseña

- ☐ Exigir al menos un carácter en mayúscula del alfabeto latino (A-Z)
- ☐ Exigir al menos un carácter en minúscula del alfabeto latino (a-z)
- ☐ Exigir al menos un número
- ☐ Exija al menos un carácter que no sea alfanumérico (! @ # \$ % ^ & * () _ + - = [] { } | ')

Otros requisitos

☒ Habilitar el vencimiento de contraseñas

La contraseña caduca en días

Debe estar comprendido entre 1 y 1095 días.

☐ El vencimiento de la contraseña requiere un restablecimiento por parte del administrador

☐ Permitir que los usuarios cambien sus propias contraseñas

☒ Evitar la reutilización de contraseñas

Tarea 2: Analizar los usuarios y los grupos de usuarios

En esta tarea, analizará los usuarios y grupos de usuarios que ya se crearon para usted en IAM.

7. En el panel de navegación izquierdo, haga clic en **Users** (Usuarios).

Ya se crearon los siguientes usuarios de IAM para usted:

- user-1
- user-2
- user-3

8. Elija **user-1**.

Esta opción lo llevará a una página **Summary** (Resumen) para **user-1**. Se muestra la pestaña **Permissions** (Permisos).

Observe que user-1 no tiene permisos.

9. Seleccione la pestaña **Groups** (Grupos).

user-1 tampoco es miembro de ningún grupo de usuarios.

Un grupo de usuarios consta de varios usuarios que necesitan acceder a los mismos datos. Los privilegios se pueden distribuir al grupo de usuarios completo en lugar de a cada individuo. Esta opción es mucho más eficaz cuando aplica permisos y proporciona un mayor control general del acceso a los recursos que aplicar permisos a los individuos.

user-1

Info

Delete

Summary

ARN

arn:aws:iam::520940006427:user/spl66/user-1

Created

January 31, 2024, 00:24 (UTC-03:00)

Console access

Enabled without MFA

Last console sign-in

Never

Access key 1

Create access key

Permissions

Groups

Tags (1)

Security credentials

Access Advisor

User groups membership (0)

Remove

Add user to groups

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name

Attached policies

No resources

This user does not belong to any groups.

10. Elija la pestaña **Security credentials** (Credenciales de seguridad).

user-1 tiene asignada una **Console password** (Contraseña de consola).

11. En el panel de navegación de la izquierda, elija **User groups** (Grupos de usuarios).

Los siguientes grupos de usuarios ya están creados:

- EC2-Admin
- EC2-Support
- S3-Support

12. Elija el grupo **EC2-Support**.

Esta opción le muestra la página **Summary** (Resumen) del grupo **EC2-Support**.

13. Seleccione la pestaña **Permissions** (Permisos).

Este grupo se encuentra asociado a una política administrada que se llama **AmazonEC2ReadOnlyAccess**. Las políticas administradas son políticas prediseñadas (que creó AWS o sus administradores) que se pueden adjuntar a grupos o grupos de usuarios de IAM. Cuando la política se actualiza, los cambios se implementan inmediatamente en los usuarios y grupos de usuarios adjuntos a ella.

14. Junto a la política **AmazonEC2ReadOnlyAccess**, seleccione el signo más para mostrar la política.

Una política define qué acciones se permiten o niegan para determinados recursos de AWS. Esta política concede permiso para listar y describir información sobre Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudWatch y Amazon EC2 Auto Scaling. Esta capacidad para ver recursos, pero no para modificarlos, es ideal para asignar a la función de soporte.

A continuación está la estructura básica de la statements de una política de IAM:

- **Effect** (Efecto) indica si **Allow** (Permitir) o **Deny** (Denegar) los permisos.
- **Action** (A acción) especifica las llamadas de API que se pueden realizar contra un servicio AWS (por ejemplo, *cloudwatch:ListMetrics*).
- **Resource** (Recurso) define el alcance de las entidades cubiertas por la regla de política (por ejemplo, un bucket de Amazon Simple Storage Service [Amazon S3], una instancia de EC2, o * que significa *cualquier recurso*).

15. En el panel de navegación de la izquierda, elija **User groups** (Grupos de usuarios).

16. Elija el grupo **S3-Support**.

17. Seleccione la pestaña **Permissions** (Permisos).

El grupo S3-Support está asociado a la política **AmazonS3ReadOnlyAccess**.

18. Junto a la política **AmazonS3ReadOnlyAccess**, seleccione el signo más para mostrar la política.

La política tiene permisos para obtener y hacer una lista de recursos en Amazon S3.

19. En el panel de navegación de la izquierda, elija **User groups** (Grupos de usuarios).
20. Elija el grupo **EC2-Admin**.
21. Seleccione la pestaña **Permissions** (Permisos).

Este grupo difiere levemente de los otros dos. En lugar de tener una política administrada, tiene una política **insertada de cliente**, que es una política asignada a un único usuario o grupo. Las políticas insertadas, generalmente, se usan para asignar permisos a situaciones aisladas.

22. Junto a la política **EC2-Admin-Policy**, seleccione el signo más para mostrar la política.

La política concede permiso para ver (describir) información acerca de Amazon EC2 y también la capacidad de iniciar o detener instancias.

RESUMEN DE LA TAREA 2

En esta tarea, pudo ver usuarios creados previamente, junto con los grupos de usuarios creados previamente. Aprendió acerca de las políticas adjuntas a los grupos de usuarios y cuáles son las diferencias entre los grupos de usuarios y sus permisos.

Permissions policies (1) Info

🔄

Simulate

Remove

Add permissions


You can attach up to 10 managed policies.

🔍 Search

Filter by Type

All types

< 1 > ⚙️

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	 AmazonEC2ReadOnlyAccess	AWS managed	1

AmazonEC2ReadOnlyAccess

Copy JSON

Provides read only access to Amazon EC2 via the AWS Management Console.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "ec2:Describe*",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "elasticloadbalancing:Describe*",
12      "Resource": "*"
13    },
14    {
15      "Effect": "Allow",
16      "Action": [
17        "cloudwatch:ListMetrics",
18        "cloudwatch:GetMetricStatistics",
19        "cloudwatch:Describe*"
20      ]
21    }
22  ]
23 }
```

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Simulate](#)

Remove

Add permissions ▾

Filter by Type

All types ▾

< 1 > ⚙

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	1

AmazonS3ReadOnlyAccess

[Copy JSON](#)

Provides read only access to all buckets via the AWS Management Console.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*",
9         "s3:Describe*",
10        "s3-object-lambda:Get*",
11        "s3-object-lambda:List*"
12      ],
13       "Resource": "*"
14     }
15   ]
16 }
```

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

[Simulate](#)

Remove

Add permissions ▾

Filter by Type

All types ▾

< 1 > ⚙

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	EC2-Admin-Policy	Customer inline	0

EC2-Admin-Policy

[Copy JSON](#) [Edit](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "ec2:Describe*",
7         "ec2:StartInstances",
8         "ec2:StopInstances"
9       ],
10      "Resource": [
11        "*"
12      ],
13      "Effect": "Allow"
14    }
15  ]
16 }
```


Tarea 3: Agregar usuarios a los grupos de usuarios

Recientemente contrató a **user-1** para un rol que brindará soporte a Amazon S3. Lo agregará al grupo **S3-Support** para que pueda heredar los permisos necesarios mediante la política AmazonS3ReadOnlyAccess adjunta.

Puede ignorar los errores **no autorizados** que aparezcan durante esta tarea. Se provocan porque su cuenta de laboratorio tiene permisos limitados, pero esto no debería afectar su capacidad para completar el laboratorio.

AGREGAR A USER-1 AL GRUPO S3-SUPPORT.

23. En el panel de navegación de la izquierda, elija **User groups** (Grupos de usuarios).
24. Elija el grupo **S3-Support**.
25. Seleccione la pestaña **Users** (Usuarios).
26. En la pestaña **Users** (Usuarios), elija **Add users** (Agregar usuarios).
27. En la ventana **Add users to S3-Support** (Agregar usuarios a S3-Support), configure las siguientes opciones:
 - Seleccione la casilla que corresponde a **user-1**.
 - Seleccione **Add users** (Agregar usuarios).

En la pestaña **Users** (Usuarios), verá que user-1 se agregó al grupo.

AGREGAR A USER-2 AL GRUPO EC2-SUPPORT.

Contrató a **user-2** con el rol de brindar soporte a Amazon EC2.

28. Usando los pasos anteriores en esta tarea, agregue **user-2** al grupo **EC2-Support**.

Ahora, user-2 debería formar parte del grupo **EC2-Support**.

AGREGAR A USER-3 AL GRUPO EC2-ADMIN

Contrató a **user-3** como administrador de Amazon EC2 para que administre sus instancias EC2.

29. Usando los pasos anteriores en esta tarea, agregue **user-3** al grupo **EC2-Admin**.

Ahora, user-3 debería formar parte del grupo **EC2-Admin**.

30. En el panel de navegación de la izquierda, elija **User groups** (Grupos de usuarios).

Cada grupo debería tener un **1** en la columna **Users** (Usuarios) como representación de la cantidad de usuarios de cada grupo.

Si no hay un **1** junto a cada grupo, revise las instrucciones anteriores en esta tarea para confirmar que cada usuario se encuentre asignado a un grupo, como se muestra en la tabla al principio de la sección **Business scenario** (Situación empresarial).

RESUMEN DE LA TAREA 3

En esta tarea, agregó todos los usuarios asociados a los grupos de usuarios.

Add users to S3-Support

Other users in this account (1/3)

Search

< 1 > ⚙

<input checked="" type="checkbox"/>	User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	user-1	0	None	27 minutes ago
<input type="checkbox"/>	user-2	0	None	27 minutes ago
<input type="checkbox"/>	user-3	0	None	27 minutes ago

Cancel

Add users

EC2-Support

Delete

Summary

Edit

User group name

EC2-Support

Creation time

January 31, 2024, 00:24 (UTC-03:00)

ARN

arn:aws:iam::520940006427:group/spl66/EC2-Support

Users (1)

Permissions

Access Advisor

Users in this group (1)

Refresh

Remove

Add users

Search

< 1 > ⚙

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	user-2	1	None	29 minutes ago

EC2-Admin

Info

Delete

Summary

Edit

User group name

EC2-Admin

Creation time

January 31, 2024, 00:24 (UTC-03:00)

ARN

arn:aws:iam::520940006427:group/spl66/EC2-Admin

Users (1)

Permissions

Access Advisor

Users in this group (1)

Remove

Add users

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

< 1 > ⚙

☐

User name

▲

Groups

Last activity

▼

Creation time

▼

☐

[user-3](#)

1

None

30 minutes ago

User groups (3)

Info

Delete

Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

< 1 > ⚙

☐

Group name

▲

Users

▼

Permissions

▼

Creation time

▼

☐

[EC2-Admin](#)

1

Defined

31 minutes ago

☐

[EC2-Support](#)

1

Defined

31 minutes ago

☐

[S3-Support](#)

1

Defined

31 minutes ago

Tarea 4: Iniciar sesión y probar permisos de usuarios

En esta tarea, probará los permisos de cada usuario de IAM.

31. En el panel de navegación izquierdo, seleccione **Dashboard** (Panel).

La sección **AWS Account** (Cuenta de AWS) incluye una **URL de inicio de sesión para los usuarios de IAM en esta cuenta**. Este enlace debe tener un aspecto similar al siguiente: **<https://123456789012.signin.aws.amazon.com/console>**

Puede usar este enlace para iniciar sesión en la cuenta de AWS que está usando.

32. Copie la **URL de inicio de sesión para usuarios de IAM en esta cuenta** a un editor de texto.

33. Abra una ventana privada usando las siguientes instrucciones para su navegador web.

Mozilla Firefox

- Elija las barras de menú de la parte superior derecha de la pantalla.
- Seleccione **New Private Window** (Nueva ventana privada).

Google Chrome

- Elija los puntos suspensivos de la parte superior derecha de la pantalla.
- Elija **New incognito window** (Nueva ventana de incógnito).

Microsoft Edge

- Elija los puntos suspensivos de la parte superior derecha de la pantalla.
- Elija **New InPrivate window** (Nueva ventana InPrivate).

Microsoft Internet Explorer

- Elija la opción de menú **Tools** (Herramientas).
- Elija **InPrivate Browsing** (Navegación InPrivate).

34. Pegue la **URL de inicio de sesión para usuarios de IAM en esta cuenta** en la ventana privada y presione Intro.

Ahora iniciará sesión como **user-1**, a quien se contrató como personal de soporte para el almacenamiento de Amazon S3.

35. Inicie sesión con las siguientes credenciales:

- **IAM user name (Nombre de usuario AIM):** Ingrese user-1
- **Password (Contraseña):** Ingrese Lab-Password1

36. Seleccione **Sign in** (Iniciar sesión).

Si ve un cuadro de diálogo que le indica que debe cambiar al inicio de la nueva consola, seleccione **Switch to the new Console Home** (Cambiar al inicio de la nueva consola).

37. En el menú **Services** (Servicios), elija **S3**.

38. Haga clic en el nombre de uno de los buckets y busque el contenido.

Debido a que el usuario forma parte del grupo **S3-Support** en IAM, tiene permiso para ver una lista de buckets de S3 y su contenido.

Ahora, pruebe si tienen acceso a Amazon EC2.

39. En el menú **Services** (Servicios), seleccione **EC2**.

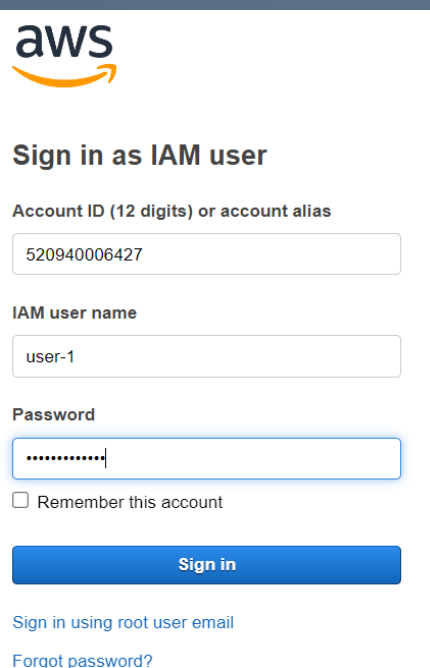
40. En el panel de navegación izquierdo, elija **Instances** (Instancias).

No puede ver ninguna instancia. En su lugar, verá un mensaje que dice **You are not authorized to perform this operation** (No está autorizado para realizar esta operación). Este mensaje aparece ya que el usuario no tiene ningún permiso para utilizar Amazon EC2.

Ahora, iniciará sesión como **user-2**, a quien se contrató como personal de soporte para Amazon EC2.

41. Cierre la sesión de user-1 en la **Consola de administración de AWS** mediante los siguientes pasos:

- En la parte superior de la pantalla, elija **user-1**.
- Seleccione **Sign out** (Cerrar sesión).



The screenshot shows the AWS IAM console sign-in page. At the top is the AWS logo. Below it is the heading "Sign in as IAM user". There are three input fields: "Account ID (12 digits) or account alias" with the value "520940006427", "IAM user name" with the value "user-1", and "Password" with masked characters. Below the password field is a checkbox labeled "Remember this account". At the bottom is a blue "Sign in" button. Below the button are two links: "Sign in using root user email" and "Forgot password?".

[Alt+S]

Global

user-1 @ 5209-4000

Amazon S3

▼ Instantánea de la cuenta

Ver panel de Storage Lens

Última actualización: 29 Jan 2024 por Storage Lens. Las métricas se generan cada 24 horas. Las métricas no incluyen los buckets de directorio. [Más información](#)

Almacenamiento total

25.9 KB

Recuento de objetos

4

Tamaño medio de los objetos

6.5 KB

Puede habilitar las métricas avanzadas en la Configuración de "default-account-dashboard".

Buckets de uso general

Buckets de directorio

Buckets de uso general (3) Información

Copiar ARN

Vaciar

Eliminar

Crear bucket

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

Q Buscar buckets por nombre

< 1 >

	Nombre ▲	Región de AWS ▼	Acceso ▼	Fecha de creación ▼
<input type="radio"/>	awslabs-resources-krxqqla59sui8d-us-east-1-520940006427	EE. UU. Este (Norte de Virginia) us-east-1	Error	30 May 2023 1:48:32 PM -04
<input type="radio"/>	awslabs-resources-r5b3y6ojjszcap-	EE. UU. Este (Norte de Virginia) us-	Error	23 Jan 2024 3:02:55 PM -03

Instancias Información

Conectar

Estado de la instancia ▼

Acciones ▼

Lanzar instancias ▼

Q Buscar Instance por atributo o etiqueta (case-sensitive)

Any state ▼

< 1 ... >

	Name ↗ ▼	ID de la instancia	Estado de la i... ▼	Tipo de inst... ▼	Comprobación de	Estado de la al	Zona de dispon... ▼	DNS de IPv4 públi
You are not authorized to perform this operation. User: arn:aws:iam::520940006427:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action								

42.Pegue la **URL de inicio de sesión para usuarios de IAM en esta cuenta** en la ventana privada y presione Intro.

Este enlace debe estar en su editor de texto.

43. Inicie sesión con las siguientes credenciales:

- **IAM user name (Nombre de usuario AIM):** Ingrese user-2
- **Password (Contraseña):** Ingrese Lab-Password2

44. Seleccione **Sign in** (Iniciar sesión).

Si ve un cuadro de diálogo que le indica que debe cambiar al inicio de la nueva consola, seleccione **Switch to the new Console Home** (Cambiar al inicio de la nueva consola).

45. En el menú **Services** (Servicios), seleccione **EC2**.

46. En el panel de navegación izquierdo, elija **Instances** (Instancias).

Ahora puede ver una instancia de EC2 porque tiene permisos de solo lectura. Sin embargo, no podrá realizar ninguna modificación en los recursos de Amazon EC2.

La instancia de EC2 debe estar seleccionada. Si no lo está, selecciónela .

47. Desde la lista desplegable **Instance state** (Estado de la instancia), seleccione **Stop instance** (Detener instancia).

48. En la ventana **Stop instance?** (¿Detener instancia?), elija **Stop** (Detener).

No se pudo detener la instancia i-0851e7a6f9c110f8a

You are not authorized to perform this operation. User: aws:iam::520940006427:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-west-2:520940006427:instance/i-0851e7a6f9c110f8a because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: _Jk4aEv5aUEhTHsSJPLSz1y_t-YD_IT3PzwameJh4D3Cz-EMjGaDfOGF-KHK_ys07Gd8J-ZWkIAsz3O7t6bYttrjyXkKPJwQ8ow3-Dalh9ToFRORsMEKcwlq37UE8E3UX7N3Qb_eVe6z_7AZMq6hFSo3xaeWAARVIAmSjvGoP4GjA2OnhRK4LvoCdOCTZE7ISRIJJs9gvv2sg-bJStuyutLtl1xvoHaWC84NOgu7v8WgTO6S0MRldiWyhBEYtTtXK7Jw-uEJIAheFPQOsqUVDI07Q3KEakZyGrVj8udae1-8LWhtSYW7pj80v4stybsVIZMlmVzoIRD3ALOrxxX6A1_YFEv908z7zhs5ozVpOhro1ONFZNJsLH9V-t4JlNjqy_Tlh4U03FQ-SMaDysTv9M6kNC5ZL9MMoVHL6io1F7I26qicAulbgBUXvBAe1FHgyRMAaZa2757bHordFildqJWzKzxfGICvptkIH780FFqxo5MTBeQs7y5XWkoSGOcdQle5E2BMBISIX_7D_Rtsa1v8H-hX7WKRtEVSH73qQJA7L4IB-TaWY7LK0hsvO8wY82D9PGTy8MjEAXXgOoQ964p57PYVBbufoMitsowez_5NqDdTCpQfWdQJBDDX2XyVoJ6CxdHU3ZLrDIMsQH84RvmHOus3ZaanJYKmpPGF8pD66yl_a6RoSVct_uouppoGuY5ivAWuxoNLUx4QTNsrdGVZa9uFLp39790lb8-5ojxtHdndmlW55NK2CUXSulN8fbdEp8ld3F4CqslchdHJC-NaVes10CqKAGS2RD_skaR6jwUaugu6-5mV9VCCUHRailUOgdgt-ctk85nraKfa_q8MxIKzyRE_6Uq8hNswpkhnmPYfBROGAjilR8cwpdkpwTjXNxFJ1PwWZvEal-J154mYthYIP2ZJC_03j0Zdox_QCf8wu_mzlexLmQkw1XOR1_H1REwgHctKCBOK1QK8mwgNVjGiSE6-H1ECMu-JSFTu2K57b5Y1

Instancias (1/1) Información

Buscar Instance por atributo o etiqueta (case-sensitive) Any state

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al...	Zona de dispon...	DNS de IPv4 pública	Dirección IP...	IP elástica	Direcciones l...
<input checked="" type="checkbox"/>	Web Server	i-0851e7a6f9c110f8a	En ejecución	t2.micro	2/2 comprobador	View alarms	us-west-2a	ec2-54-202-249-138.us...	54.202.249.138	-	-

Instancia: i-0851e7a6f9c110f8a (Web Server)

Detalles

Status and alarms New

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

Resumen de instancia Información

ID de la instancia
i-0851e7a6f9c110f8a (Web Server)

Dirección IPv6
-

Tipo de nombre de anfitrión
Nombre de IP: ip-10-1-11-86.us-west-2.compute.internal

Responder al nombre DNS de recurso privado
-

Dirección IP asignada automáticamente
54.202.249.138 [IP pública]

Dirección IPv4 pública
54.202.249.138 [dirección abierta](#)

Estado de la instancia
En ejecución

Nombre DNS de IP privada (solo IPv4)
ip-10-1-11-86.us-west-2.compute.internal

Tipo de instancia
t2.micro

ID de VPC
vpc-0a04b045427073b3a (Lab VPC)

Direcciones IPv4 privadas
10.1.11.86

DNS de IPv4 pública
ec2-54-202-249-138.us-west-2.compute.amazonaws.com [dirección abierta](#)

Direcciones IP elásticas
-

Hallazgo de AWS Compute Optimizer

► **Instantánea de la cuenta**






Storage Lens ofrece visibilidad sobre el uso del almacenamiento y las tendencias de la actividad. [Más información](#)

Ver panel de Storage Lens


Buckets de uso general

Buckets de directorio

Buckets de uso general [Información](#)

  Copiar ARN  Vaciar  Eliminar  Crear bucket

Los buckets son contenedores de datos almacenados en S3. [Más información](#)


< 1 > 


Nombre ▲

Región de AWS ▼

Acceso ▼

Fecha de creación ▼

 **No tiene permisos para obtener una lista de los buckets**
Una vez que usted o el administrador de AWS hayan actualizado los permisos para permitir la acción s3:ListAllMyBuckets, actualice la página. Más información acerca de [Identity and Access Management en Amazon S3](#)

 Troubleshoot with Amazon Q

Recibirá un error que dice, **Failed to stop the instance. You are not authorized to perform this operation** (No se pudo detener la instancia. No está autorizado a realizar la operación). Este mensaje demuestra que la política le otorga el permiso solo para ver información y no para realizar cambios.

49. En la ventana **Stop instances** (Detener instancias), elija **Cancel** (Cancelar).

Luego, verifique si user-2 puede acceder a Amazon S3.

50. En el menú **Services** (Servicios), elija **S3**.

Recibirá el mensaje **You don't have permissions to list buckets** (No tiene permisos para listar buckets) porque user-2 no tiene permiso para usar Amazon S3.

Ahora, iniciará sesión como **user-3**, a quien se contrató como administrador de Amazon EC2.

51. Cierre la sesión de user-2 en la **Consola de administración de AWS** mediante los siguientes pasos:

- En la parte superior de la pantalla, elija **user-2**.
- Seleccione **Sign out** (Cerrar sesión).
-

52. Pegue la **URL de inicio de sesión para usuarios de IAM en esta cuenta** en la ventana privada y presione Intro.

Si este enlace no está en el portapapeles, recupérela del editor de texto en el que lo pegó anteriormente.

53. Inicie sesión con las siguientes credenciales:

- **IAM user name (Nombre de usuario AIM):** Ingrese user-3
- **Password (Contraseña):** Ingrese Lab-Password3

54. Seleccione **Sign in** (Iniciar sesión).

Si ve un cuadro de diálogo que le indica que debe cambiar al inicio de la nueva consola, seleccione **Switch to the new Console Home** (Cambiar al inicio de la nueva consola).

55. En el menú **Services** (Servicios), seleccione **EC2**.

56. En el panel de navegación izquierdo, elija **Instances** (Instancias).

Como administrador de EC2, debería tener permisos para detener la instancia de EC2.

Se debe seleccionar la instancia de EC2. Si no lo está, selecciónela .

Si la instancia de EC2 no es visible, es posible que la región sea incorrecta. En la parte superior derecha de la pantalla, seleccione el menú **Region** (Región) y seleccione la región que anotó al principio del laboratorio (por ejemplo, **Oregon** [Oregón]).

57. Desde la lista desplegable **Instance state** (Estado de la instancia), seleccione **Stop instance** (Detener instancia).

58. En la ventana **Stop instance?** (¿Detener instancia?), elija **Stop** (Detener).

La instancia ingresará al estado **Stopping** (Deteniéndose) y se cerrará.

59. Cierre la ventana privada.

RESUMEN DE LA TAREA 4

En esta tarea, pudo iniciar sesión como los tres usuarios. Comprobó que user-1 pudo ver los buckets S3 pero no pudo ver las instancias de EC2. Luego inició sesión como user-2 y comprobó que pudo ver las instancias de EC2 pero no pudo realizar la acción de detención de instancia. user-2 tampoco pudo ver los buckets S3. Después de iniciar sesión como user-3, pudo ver las instancias de EC2 y realizar la acción de detención de instancia.

Conclusión

¡Felicitaciones! Aprendió a realizar correctamente las siguientes tareas:

- Crear y aplicar una política de contraseñas de IAM
- Analizar usuarios y grupos de IAM creados previamente
- Inspeccionar políticas de IAM según se apliquen a los grupos creados previamente
- Agregar usuarios a grupos de usuario con capacidades específicas activas
- Ubicar y utilizar la dirección URL de inicio de sesión de IAM
- Probar los efectos de las políticas en el acceso a los servicios

Iniciar sesión como usuario de IAM

ID de cuenta (12 dígitos) o alias de cuenta

520940006427

Nombre de usuario:

user-3

Contraseña:

.....

☐ Recordar esta cuenta

Iniciar sesión

[Iniciar sesión con el email del usuario raíz](#)

[¿Olvidó la contraseña?](#)

Se ha detenido correctamente i-0851e7a6f9c110f8a

Instancias (1/1) Información

Buscar Instance por atributo o etiqueta (case-sensitive)

Any state



Conectar

Estado de la instancia

Acciones

Lanzar instancias

<input checked="" type="checkbox"/>	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al...	Zona de dispon...	DNS de IPv4 pública	Dirección IP...	IP elástica	Direcciones I...
<input checked="" type="checkbox"/>	Web Server	i-0851e7a6f9c110f8a	Deteniéndose	t2.micro	2/2 comprobador	User: am:aws3	us-west-2a	ec2-54-202-249-138.us...	54.202.249.138	-	-