

AWS Academy Cloud Foundations

Módulo 4: Seguridad en la nube de AWS



Información general sobre el módulo



Temas

- Modelo de responsabilidad compartida de AWS
- AWS Identity and Access Management (IAM)
- Protección de una cuenta nueva de AWS
- Protección de cuentas
- Protección de datos en AWS
- Trabajo para garantizar la conformidad

Actividades

- Actividad sobre el modelo de responsabilidad compartida de AWS

Demostración

- Demostración grabada de IAM

Laboratorio

- Introducción a AWS IAM



Revisión de conocimientos

Después de completar este módulo, debería ser capaz de lo siguiente:

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS

Módulo 4: Seguridad en la nube de AWS

Sección 1: Modelo de responsabilidad compartida de AWS

Modelo de responsabilidad compartida de AWS



Responsabilidad de AWS: seguridad de la nube



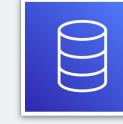
Servicios de AWS



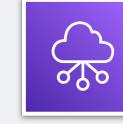
Informática



Almacenamiento

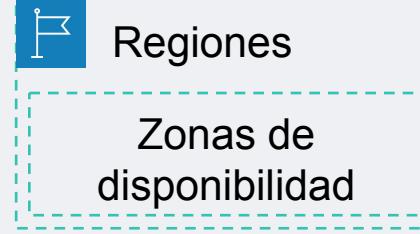


Base de datos



Redes

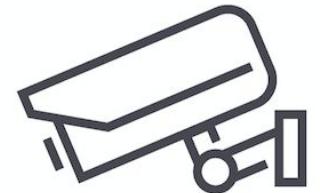
Infraestructura global de AWS

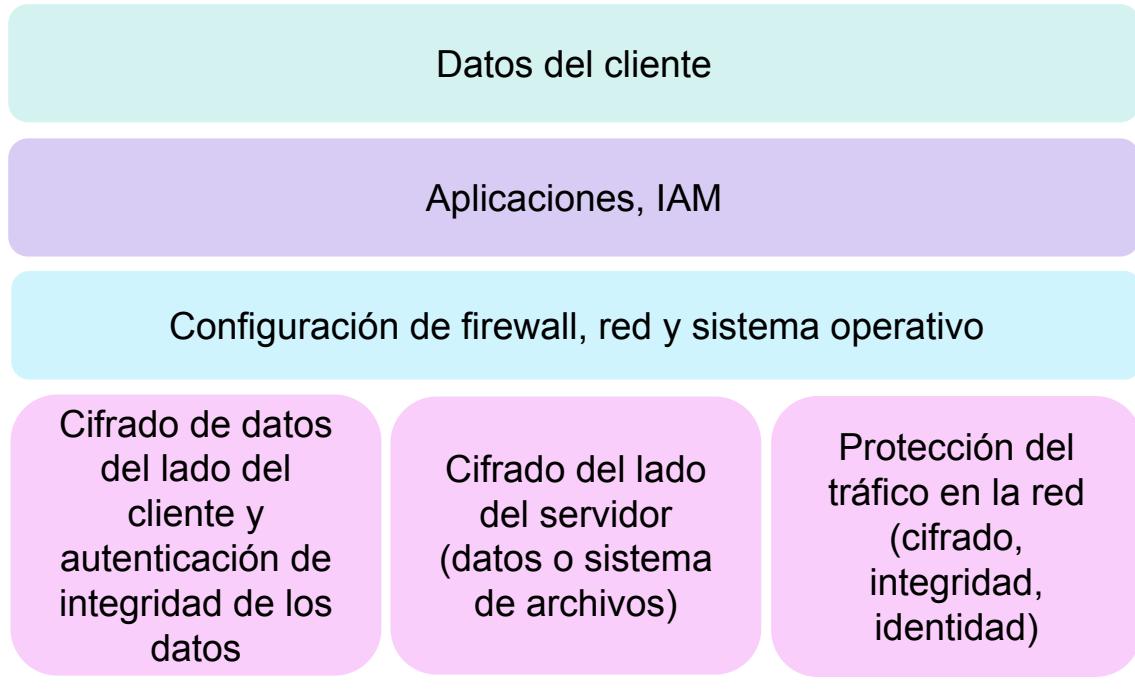


Ubicaciones
de borde

Responsabilidades de AWS:

- Seguridad física de los centros de datos
 - Acceso controlado basado en las necesidades
- Infraestructura de hardware y software
 - Baja de recursos de almacenamiento, registro de acceso del sistema operativo (SO) del host y auditoría
- Infraestructura de red
 - Detección de intrusiones
- Infraestructura de virtualización
 - Aislamiento de instancias





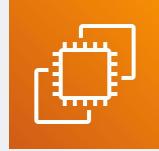
Responsabilidades de los clientes:

- **Sistema operativo** de la instancia de Amazon Elastic Compute Cloud (Amazon EC2)
 - Incluidos los parches y el mantenimiento
- **Aplicaciones**
 - Contraseñas, acceso basado en roles, etc.
- Configuración **del grupo de seguridad**
- SO o **firewalls** basados en host
 - Incluidos los sistemas de detección o prevención de intrusiones
- Configuraciones **de red**
- Administración de cuentas
 - Configuración de inicio de sesión y permisos para cada usuario

Características del servicio y responsabilidad en materia de seguridad



Servicios de ejemplo administrados por el cliente



Amazon
EC2



Amazon Elastic
Block Store
(Amazon EBS)



Amazon Virtual
Private Cloud
(Amazon VPC)

Servicios de ejemplo administrados por AWS



AWS Lambda



Amazon Relational
Database Service
(Amazon RDS)



AWS Elastic
Beanstalk

Infraestructura como servicio (IaaS)

- El cliente tiene más flexibilidad en lo que respecta a la configuración de redes y almacenamiento.
- El cliente es responsable de administrar más aspectos de la seguridad.
- El cliente configura los controles de acceso.

Plataforma como servicio (PaaS)

- El cliente no necesita administrar la infraestructura subyacente.
- AWS gestiona el sistema operativo, la implementación de parches a la base de datos, la configuración del firewall y la recuperación de desastres.
- El cliente puede centrarse en la administración de código o datos.

Características del servicio y responsabilidad en materia de seguridad (continuación)



Ejemplos de SaaS



AWS Trusted
Advisor



AWS Shield



Amazon Chime

Software como servicio (SaaS)

- El software está alojado de forma centralizada.
- Cuenta con licencia según un modelo de suscripción o de pago por uso.
- Normalmente, el acceso a los servicios se realiza a través de un navegador web, una aplicación móvil o una interfaz de programación de aplicaciones (API).
- Los clientes no necesitan administrar la infraestructura que respalda el servicio.

Actividad: Modelo de responsabilidad compartida de AWS



Foto de Pixabay de Pexels

Actividad: escenario 1 de 2



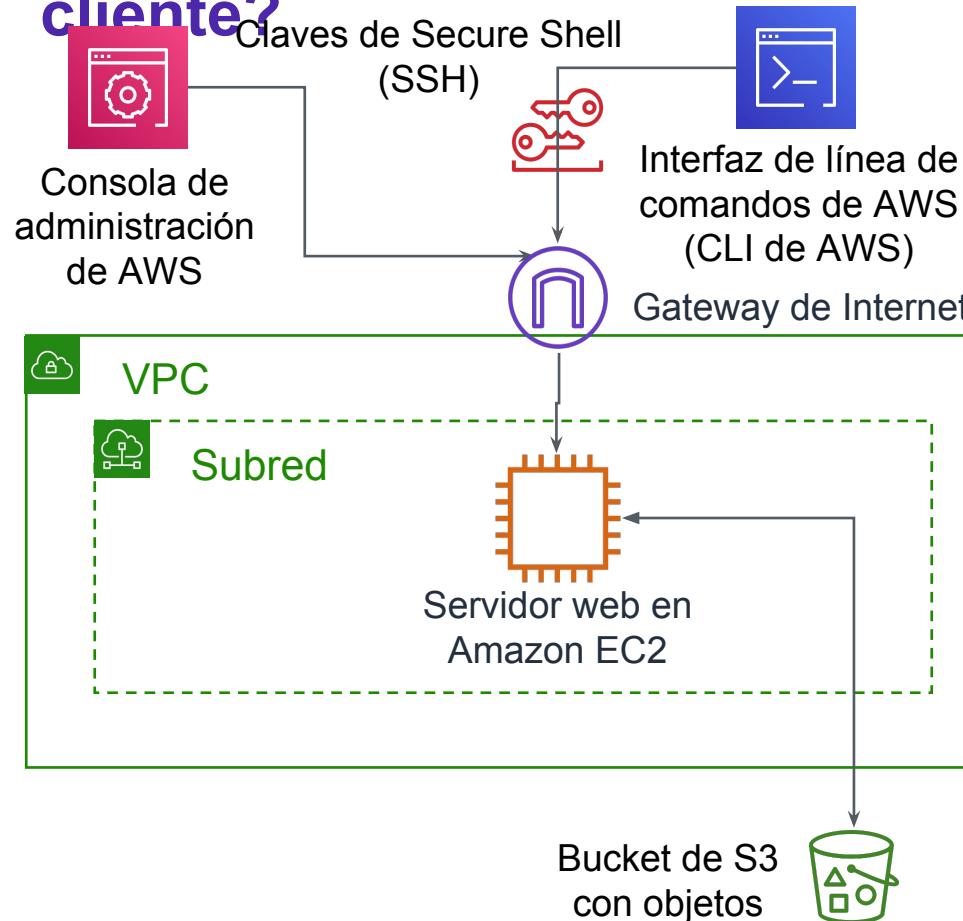
Considere esta implementación. ¿Quién es responsable? ¿AWS o el cliente?



1. ¿Actualizaciones y parches en el sistema operativo en la instancia EC2?
 - **RESPUESTA:** el cliente
2. ¿Seguridad física del centro de datos?
 - **RESPUESTA:** AWS
3. ¿Infraestructura de virtualización?
 - **RESPUESTA:** AWS
4. ¿Configuración de grupos de seguridad de EC2?
 - **RESPUESTA:** el cliente
5. ¿Configuración de las aplicaciones que se ejecutan en la instancia EC2?
 - **RESPUESTA:** el cliente
6. ¿Actualizaciones o parches de Oracle si la instancia de Oracle se ejecuta como una instancia de Amazon RDS?
 - **RESPUESTA:** AWS
7. ¿Actualizaciones o parches de Oracle si Oracle se ejecuta en una instancia EC2?
 - **RESPUESTA:** el cliente
8. ¿Configuración de acceso al bucket de S3?
 - **RESPUESTA:** el cliente

Actividad: escenario 2 de 2

Consideré esta implementación. ¿Quién es responsable? ¿AWS o el cliente?



1. ¿Garantizar que la consola de administración de AWS no sea pirateada?
 - **RESPUESTA:** AWS
2. ¿Configurar la subred?
 - **RESPUESTA:** el cliente
3. ¿Configurar la VPC?
 - **RESPUESTA:** el cliente
4. ¿Proteger frente a interrupciones de red en las regiones de AWS?
 - **RESPUESTA:** AWS
5. ¿Proteger las claves SSH?
 - **RESPUESTA:** el cliente
6. ¿Garantizar el aislamiento de red entre los datos de los clientes de AWS?
 - **RESPUESTA:** AWS
7. ¿Garantizar una conexión de red de baja latencia entre el servidor web y el bucket de S3?
 - **RESPUESTA:** AWS
8. ¿Requerir la autenticación multifactor para todos los inicios de sesión de los usuarios?
 - **RESPUESTA:** el cliente

Aprendizajes clave de la sección 1



- AWS y el cliente comparten responsabilidades en materia de seguridad:
 - AWS es responsable de la seguridad **de** la nube.
 - El cliente es responsable de la seguridad **en** la nube.
- **AWS es responsable de proteger la infraestructura** (incluido el hardware, el software, las redes y las instalaciones) que ejecuta los servicios en la nube de AWS.
- En el caso de los servicios clasificados como infraestructura como servicio (IaaS), el **cliente es responsable de realizar las tareas de configuración y administración de seguridad necesarias**.
 - Por ejemplo, actualizaciones del sistema operativo invitado y configuraciones de parches de seguridad, firewall y grupos de seguridad.

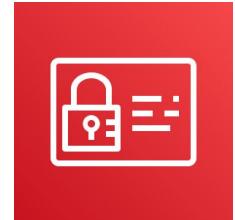
Módulo 4: Seguridad en la nube de AWS

Sección 2: AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)



- Utilice **IAM** para administrar el acceso a los **recursos de AWS**:
 - Un recurso es una entidad en una cuenta de AWS con la que puede trabajar.
 - Recursos de ejemplo: una instancia de Amazon EC2 o un bucket de Amazon S3
- *Por ejemplo:* controle quién puede terminar instancias de Amazon EC2
- Defina los derechos de acceso detallados:
 - **Quién** puede obtener acceso al recurso
 - **A qué** recursos se puede obtener acceso y qué puede hacer el usuario con el recurso
 - **Cómo** se puede obtener acceso a los recursos
- IAM es una característica de cuenta de AWS gratuita



AWS Identity and
Access Management
(IAM)

IAM: componentes esenciales



Usuario de IAM



Grupo de IAM



Política de IAM



Rol de IAM

Persona o aplicación que se puede autenticar con una cuenta de AWS

Colección de usuarios de IAM a los que se concede una autorización idéntica

El documento que define **a qué recursos se puede obtener acceso** y el **nivel de acceso** a cada recurso

Mecanismo útil para conceder un conjunto de permisos a fin de realizar solicitudes de servicios de AWS

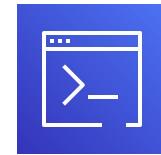
Autenticarse como usuario de IAM para obtener acceso



Cuando define un **usuario de IAM**, selecciona qué **tipos de acceso** puede utilizar el usuario.

• **Acceso mediante programación**

- Se autentica con lo siguiente:
 - ID de clave de acceso
 - Clave de acceso secreta
- Proporciona acceso a la CLI de AWS y al SDK de AWS.



CLI de AWS Herramientas y
SDK de AWS



Acceso a la consola de administración de AWS

- Se autentica con lo siguiente:
 - ID de cuenta o alias de 12 dígitos
 - Nombre de usuario de IAM
 - Contraseña de IAM
- Si está habilitada, **Multi-Factor Authentication (MFA)** solicita un código de autenticación.



Consola de
administración de AWS

- MFA proporciona más seguridad.
- Además del **nombre de usuario** y la **contraseña**, MFA requiere un **código de autenticación** único para acceder a los servicios de AWS.

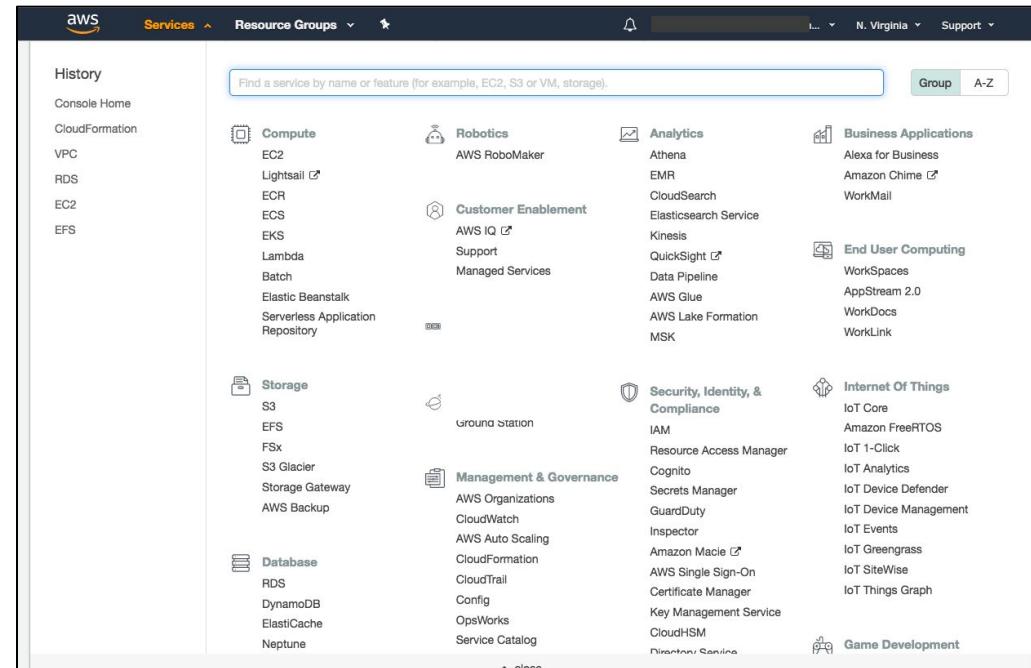
Account: [REDACTED]

User Name: [REDACTED]

Password: [REDACTED]

MFA users, enter your code on the next screen.

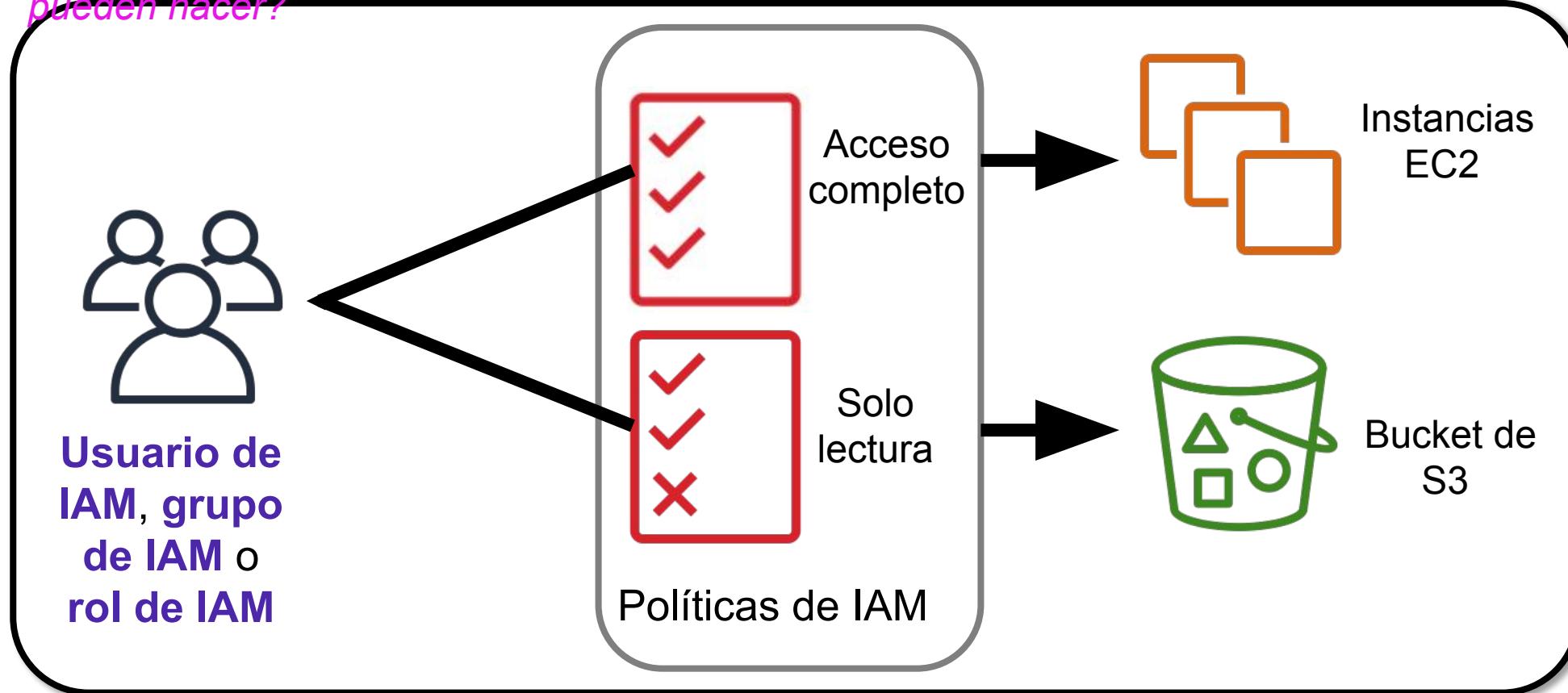
Sign In



Consola de administración de AWS

Autorización: qué acciones están permitidas

Una vez que el usuario o la aplicación se haya conectado a la cuenta de AWS, ¿qué pueden hacer?



- Asigna permisos mediante la creación de una política de IAM.
- Los permisos determinan **qué recursos y operaciones** están permitidas:
 - De forma predeterminada, todos los permisos están denegados implícitamente.
 - Si algo está denegado explícitamente, nunca se permite.



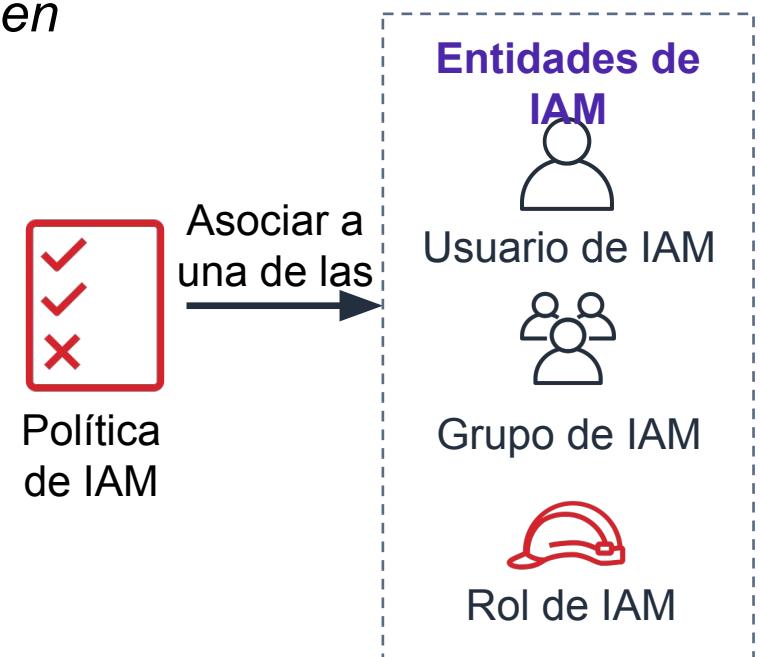
Permisos de IAM

Práctica recomendada: seguir el **principio de mínimo privilegio**.

Nota: El alcance de las configuraciones de servicios de IAM es **global**. Las configuraciones se aplican a todas las regiones de AWS.

Políticas de IAM

- Una política de IAM es un documento que define permisos.
 - Habilita el control de acceso detallado.
- Existen dos tipos de políticas: *basadas en identidad* y *basadas en recursos*
- Políticas **basadas en identidad**:
 - Asocian una política a cualquier entidad de IAM.
 - Un **usuario de IAM**, un **grupo de IAM**, o un **rol de IAM**
 - Las políticas especifican lo siguiente:
 - Acciones que **puede** realizar la entidad
 - Acciones que la entidad **no puede** realizar
 - Una sola *política* se puede asociar a varias *entidades*.
 - Una sola *entidad* puede tener varias *políticas* asociadas a ella.
- Políticas **basadas en recursos**
 - Están asociadas a un recurso (como un bucket de S3).



Ejemplo de política de IAM

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": ["DynamoDB:*", "s3:*"],  
    "Resource": [  
      "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",  
      "arn:aws:s3:::bucket-name",  
      "arn:aws:s3:::bucket-name/*"]  
    ],  
    {  
      "Effect": "Deny",  
      "Action": ["dynamodb:*", "s3:*"],  
      "NotResource": ["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",  
                     "arn:aws:s3:::bucket-name",  
                     "arn:aws:s3:::bucket-name/*"]  
    }  
  }]  
}
```

El permiso explícito concede a los usuarios acceso a una tabla específica de DynamoDB y a...

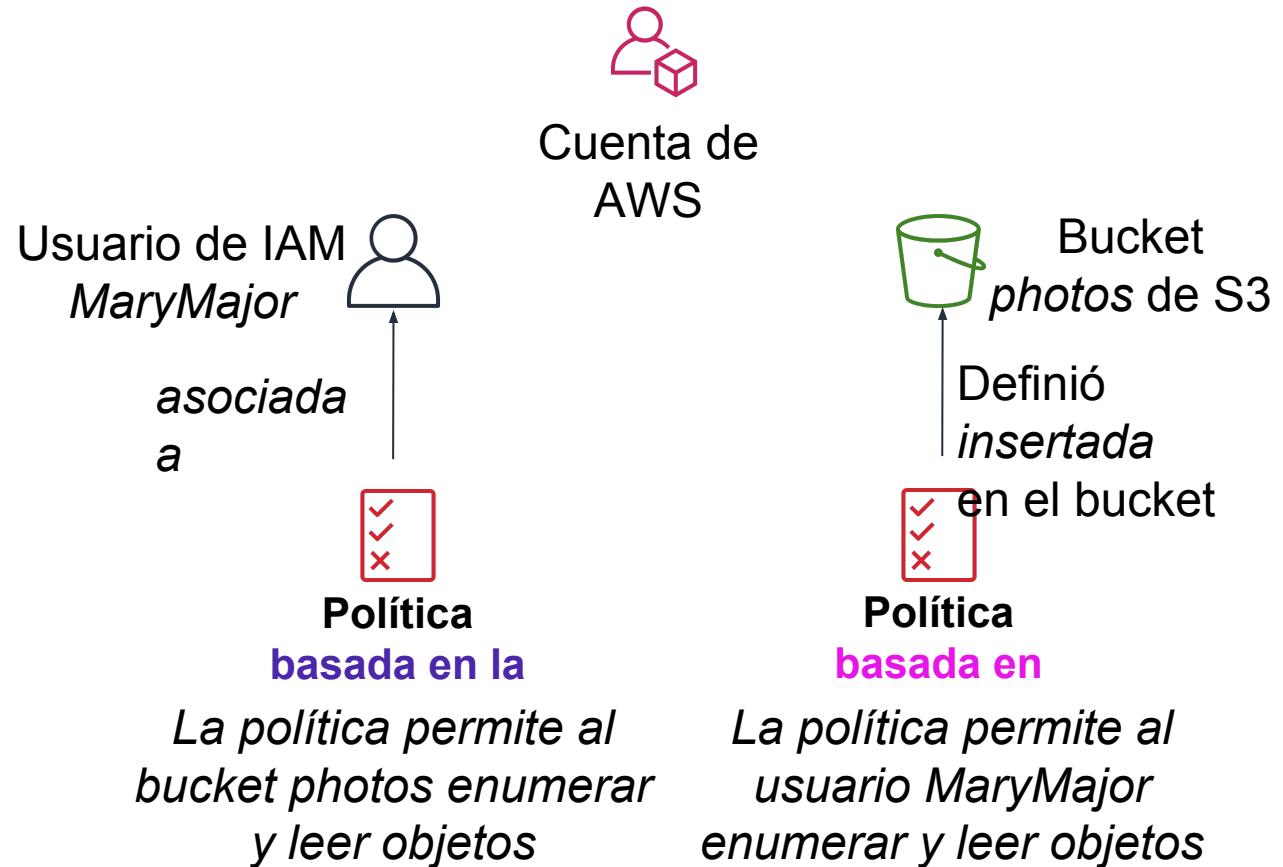
...buckets de Amazon S3.

Explicit deny (denegación explícita) garantiza que los usuarios no puedan usar otras acciones o recursos de AWS que no sean esa tabla y esos buckets.

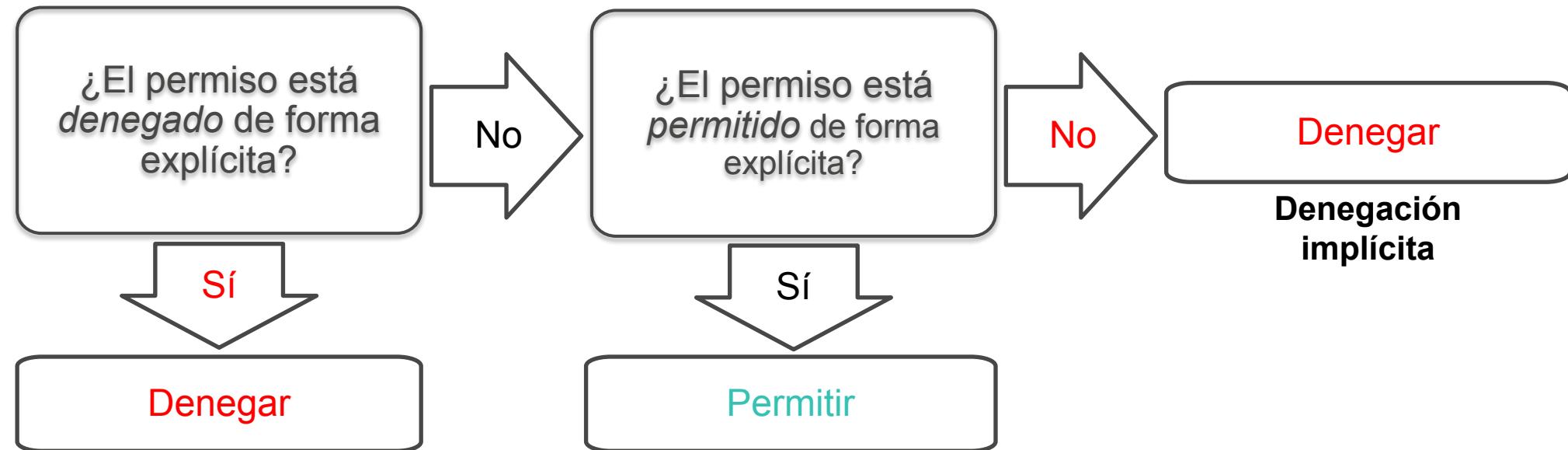
Una instrucción de denegación explícita **prevalece** sobre una instrucción de permiso.

Políticas basadas en recursos

- Las políticas *basadas en identidad* se asocian a un usuario, grupo o rol.
- Las **políticas basadas en recursos** se asocian a un recurso (*no* a un usuario, grupo o rol)
- Características de las políticas basadas en recursos:
 - Especifican quién tiene acceso al recurso y qué acciones se pueden realizar en él.
 - Las políticas son *insertadas* solamente, no se administran.
- Las políticas basadas en recursos solo se admiten en algunos servicios de AWS

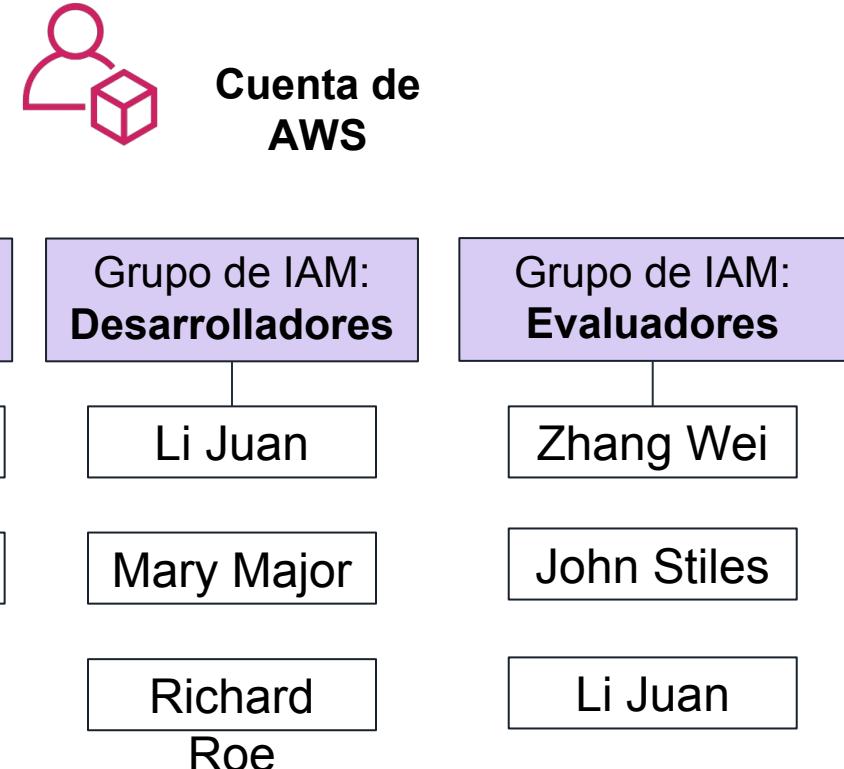


Modo en que IAM determina los permisos:



Grupos de IAM

- Un **grupo de IAM** es un conjunto de usuarios de IAM.
- Un grupo se utiliza para conceder los mismos permisos a varios usuarios.
 - Se conceden los permisos cuando se asocia la *política* o las políticas de IAM al grupo.
- Un usuario puede pertenecer a varios grupos.
- No hay grupo predeterminado.
- Los grupos no pueden estar anidados.



- Un **rol de IAM** es una identidad de IAM con permisos específicos.
- Es similar a un usuario de IAM
 - Asocia políticas de permisos a él.
- Es diferente a un usuario de IAM.
 - No está asociado de forma exclusiva a una persona.
 - Está diseñado para *que lo pueda asumir* una **persona**, una **aplicación** o un **servicio**.
- El rol proporciona credenciales de seguridad *temporales*.
- Ejemplos de cómo se utilizan los roles de IAM para **delegar** el acceso:
 - Utilizado por un usuario de IAM en la misma cuenta de AWS que utiliza el rol
 - Utilizado por un servicio de AWS, como Amazon EC2, en la misma cuenta que utiliza el rol
 - Utilizado por un usuario de IAM en una cuenta de AWS diferente a la que utiliza el rol



Rol de IAM

Ejemplo de uso de un rol de IAM

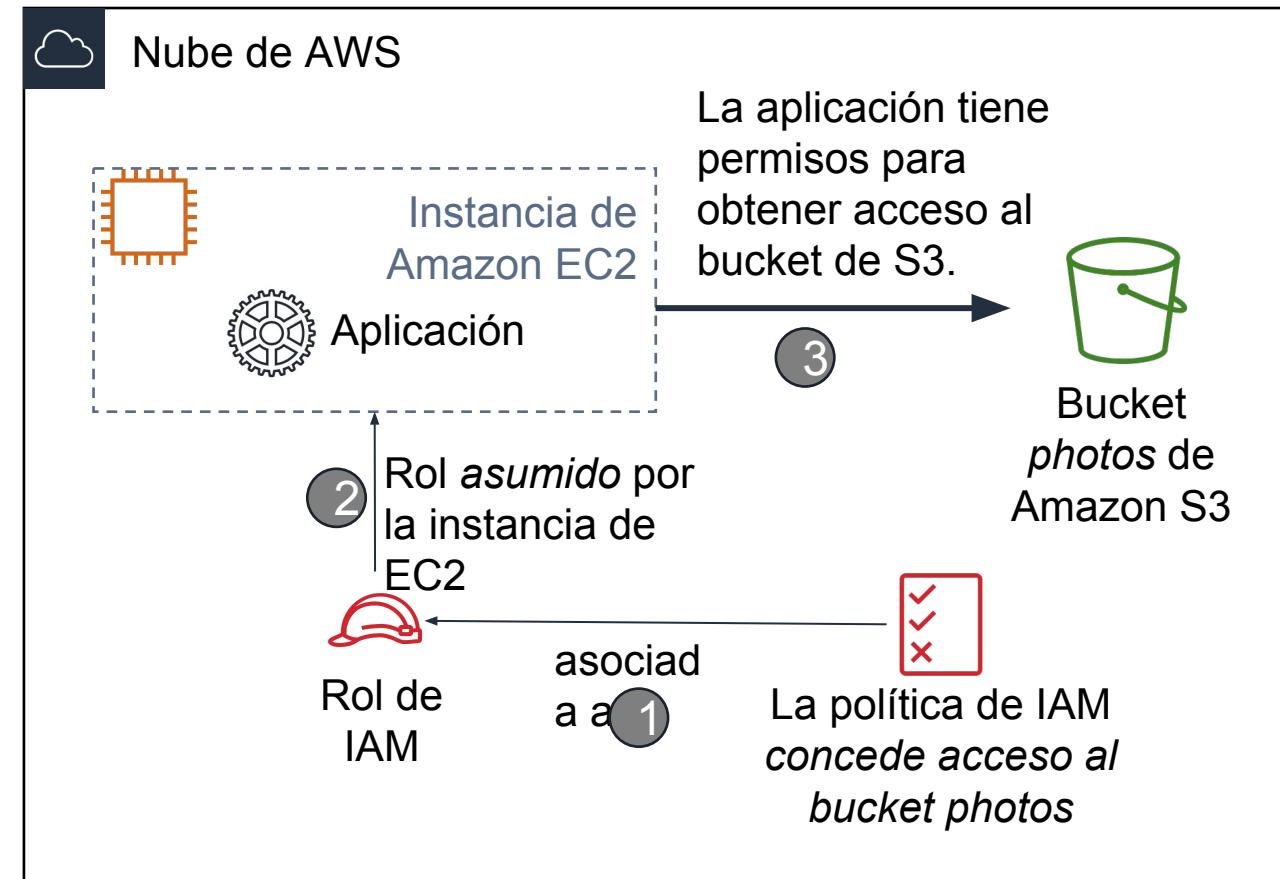


Situación:

- Una aplicación que se ejecuta en una instancia EC2 necesita acceso a un bucket de S3

Solución:

- Definir una política de IAM que conceda acceso al bucket de S3
- Asociar la política a un rol
- Permitir que la instancia EC2 asuma el rol



Aprendizajes clave de la sección 2



- Las **políticas de IAM** se crean con la notación de objetos JavaScript (JSON) y definen permisos.
 - Las políticas de IAM se pueden asociar a cualquier **entidad de IAM**.
 - Las entidades son usuarios de IAM, grupos de IAM y roles de IAM.
- Un **usuario de IAM** permite que una persona, aplicación o servicio pueda autenticarse en AWS.
- Un **grupo de IAM** permite asociar las mismas políticas a varios usuarios de una manera sencilla.
- Un **rol de IAM** puede tener asociadas políticas de permisos y se puede utilizar para delegar acceso temporal a usuarios o aplicaciones.

Demostración grabada: IAM



Módulo 4: Seguridad en la nube de AWS

Sección 3: Protección de una cuenta nueva de AWS

Acceso de usuario raíz de la cuenta de AWS frente al acceso de IAM



- **Práctica recomendada:** **no utilice el usuario raíz de la cuenta de AWS, excepto cuando sea necesario.**
 - Para acceder al **usuario raíz de la cuenta**, se requiere iniciar sesión con la *dirección de email* (y la contraseña) que utilizó para crear la cuenta.
- Ejemplos de acciones que solo se pueden realizar con el **usuario raíz de la cuenta**:
 - Actualizar la contraseña del usuario raíz de la cuenta
 - Cambiar el plan de AWS Support
 - Restaurar los permisos de un usuario de IAM
 - Cambiar la configuración de la cuenta (por ejemplo, la información de contacto o las regiones permitidas)

Protección de una nueva cuenta de AWS: usuario raíz de la cuenta



Paso 1: Deje de utilizar el usuario raíz de la cuenta tan pronto como sea posible.

- El usuario raíz de la cuenta tiene acceso ilimitado a todos sus recursos.
- Pasos a seguir para dejar de utilizar el usuario raíz de la cuenta:
 1. Inicie sesión como usuario raíz de la cuenta y **cree un usuario de IAM** para usted. Guarde las claves de acceso si es necesario.
 2. Cree un grupo de IAM, otórguele permisos totales de administrador y agregue el usuario de IAM al grupo.
 3. Deshabilite y **elimine las claves de acceso de usuario raíz de la cuenta**, en caso de que existan.
 4. **Habilite una política de contraseñas** para los usuarios.
 5. Inicie sesión con sus nuevas credenciales de usuario de IAM.
 6. Guarde las credenciales de usuario raíz de la cuenta en un lugar seguro.

Protección de una nueva cuenta de AWS: MFA



Paso 2: Habilite Multi-Factor Authentication (MFA).

- Exija MFA para su [usuario raíz de la cuenta](#) y para [todos los usuarios de IAM](#).
- También puede usar MFA para controlar el acceso a las API de servicio de AWS.
- Opciones para recuperar el token de MFA:
 - Aplicaciones virtuales compatibles con MFA:
 - Google Authenticator
 - Authy Authenticator (aplicación de Windows Phone)
 - Dispositivos de clave de seguridad U2F:
 - Por ejemplo, YubiKey.
 - Opciones de MFA de hardware:
 - Llavero o tarjeta de visualización ofrecida por [Gemalto](#).



Token de MFA

Protección de una nueva cuenta de AWS: AWS CloudTrail



Paso 3: Utilice AWS CloudTrail.

- CloudTrail realiza un seguimiento de la actividad de los usuarios en su cuenta.
 - Registra todas las solicitudes API para los recursos de todos los servicios admitidos de su cuenta.
- El historial básico de eventos de AWS CloudTrail está habilitado de forma predeterminada y es gratuito.
 - Contiene todos los datos de eventos de administración de los últimos 90 días de actividad de la cuenta.
- Pasos a seguir para obtener acceso a CloudTrail:
 1. Inicie sesión en la **consola de administración de AWS** y seleccione el servicio **CloudTrail**.
 2. Haga clic en **Event history** (Historial de eventos) para ver, filtrar y buscar los últimos 90 días de eventos.
- **Para habilitar los registros de más de 90 días y las alertas de eventos especificados, cree un registro de seguimiento.**
 1. En la página de registros de seguimiento de la consola de CloudTrail, haga clic en **Create trail** (Crear registro de seguimiento).
 2. Asígnele un nombre, aplíquelo a todas las regiones y cree un nuevo bucket de Amazon S3 para el almacenamiento de registros.
 3. Configure las restricciones de acceso en el bucket de S3 (por ejemplo, solo los usuarios administradores deben tener acceso).

Protección de una nueva cuenta de AWS: informes de facturación



Paso 4: Habilite un informe de facturación, como el informe de uso y costo de AWS.

- Los informes de facturación proporcionan información sobre el uso de los recursos de AWS y los costos estimados de dicho uso.
- AWS entrega los informes en el bucket de Amazon S3 que especifique.
 - El informe se actualiza al menos una vez al día.
- **El Informe de uso y costo de AWS** hace un seguimiento del uso que hace de AWS y proporciona cargos estimados asociados con su cuenta de AWS, ya sea por hora o por día.

Módulo 4: Seguridad en la nube de AWS

Opcional: Protección de una nueva cuenta de AWS
(explicación completa)

Revisión del estado de seguridad de IAM



Custom Sign In Link

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists navigation options: Search IAM, Dashboard (which is selected and highlighted in orange), Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. A red arrow points from the text 'Custom Sign In Link' to the 'Dashboard' option. To the right, the main content area has a header 'Welcome to Identity and Access Management'. It features an 'IAM users sign-in link:' section with a URL <https://signin.aws.amazon.com/console> enclosed in a red box. Below this are sections for 'IAM Resources' (Users: 0, Roles: 0, Groups: 0, Identity Providers: 0, Customer Managed Policies: 0) and 'Security Status' (1 out of 5 complete). The security status is represented by a progress bar with a blue segment and a grey background. Under 'Security Status', there are five items with dropdown arrows: 'Delete your root access keys' (green checkmark icon), 'Activate MFA on your root account' (orange warning icon), 'Create individual IAM users' (orange warning icon), 'Use groups to assign permissions' (orange warning icon), and 'Apply an IAM password policy' (orange warning icon).

Activar MFA en el usuario raíz de la cuenta



**Enlace
de inicio
de
sesión
personalizado**

Activación
de MFA

Welcome to Identity and Access Management

IAM users sign-in link:
<https://.signin.aws.amazon.com/console>

Customize | Copy Link

IAM Resources

Users: 0 Roles: 0

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status

1 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

Activar MFA en el usuario raíz de la cuenta



Search IAM

Dashboard Groups Users Roles Policies Identity providers Account settings Credential reports

Encryption keys

Manage MFA device

If your virtual MFA application supports scanning QR codes, scan the following QR code with your smartphone's camera.



Show secret key for manual configuration

After the application is configured, enter two consecutive authentication codes in the boxes below and choose **Activate virtual MFA**.

Authentication code 1

Authentication code 2

Cancel Previous Activate virtual MFA

MFA en el usuario raíz de la cuenta está activado



Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

MFA activada

Welcome to Identity and Access Management

IAM users sign-in link:
<https://raysinut.signin.aws.amazon.com/console>

Customize | Copy Link

IAM Resources

Users: 0 Roles: 0

Groups: 0 Identity Providers: 0

Customer Managed Policies: 0

Security Status 2 out of 5 complete.

- Delete your root access keys ▾
- Activate MFA on your root account ▾
- Create individual IAM users ▾
- Use groups to assign permissions ▾
- Apply an IAM password policy ▾

Crear un usuario individual de IAM (1)



Search IAM

Dashboard

- Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Credential report

Encryption keys

Creación de usuario de IAM

Welcome to Identity and Access Management

IAM users sign-in link:
<https://raysinut.signin.aws.amazon.com/console> Customize | Copy Link

IAM Resources

Users: 0	Roles: 0
Groups: 0	Identity Providers: 0
Customer Managed Policies: 0	

Security Status 2 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users** !
- Use groups to assign permissions
- Apply an IAM password policy

Crear un usuario individual de IAM (2)



Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* [Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

- Console password* Autogenerated password
 Custom password

- Require password reset User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Crear un usuario individual de IAM (3)



Add user

1

Details

2

Permissions

3

Review

4

Complete

Set permissions for M



Add user to group



Copy permissions from
existing user



Attach existing policies
directly

i Get started with groups

You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

[Create group](#)

[Cancel](#)

[Previous](#)

[Next: Review](#)

Crear un usuario individual de IAM (4)



Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name Administrators

[Create policy](#) [Refresh](#)

	Policy name	Type	Attachments	Description
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to relat...
<input type="checkbox"/>	AlexaForBusinessGatewayEx...	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessReadOnlyA...	AWS managed	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdminist...	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gatew...
<input type="checkbox"/>	AmazonAPIGatewayInvokeFu...	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushToC...	AWS managed	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAccess	AWS managed	0	Provides full access to Amazon AppStream via the AWS Managemen...
<input type="checkbox"/>	AmazonAppStreamReadOnly...	AWS managed	0	Provides read only access to Amazon AppStream via the AWS Mana...

Showing 313 results

[Cancel](#) [Create group](#)

Crear un usuario individual de IAM (5)



Add user

1 Details 2 Permissions 3 Review 4 Complete

Set permissions for N

Permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Create group Refresh

Search Showing 1 result

Group	Attached policies
Administrators	AdministratorAccess

Cancel Previous Next: Review

Creación exitosa de usuario de IAM



Add user

1

Details

2

Permissions

3

Review

4

Complete

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://raysia.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
	Mi...	AKI...	***** Show	***** Show	<input checked="" type="checkbox"/> Send email

Close

Estado de seguridad del panel de IAM



Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Creación de política de contraseñas

Welcome to Identity and Access Management

IAM users sign-in link:
<https://raysinut.signin.aws.amazon.com/console>

Customize | Copy Link

IAM Resources

Users: 1 Roles: 0

Groups: 1 Identity Providers: 0

Customer Managed Policies: 0

Security Status 4 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
<input checked="" type="checkbox"/> Activate MFA on your root account	▼
<input checked="" type="checkbox"/> Create individual IAM users	▼
<input checked="" type="checkbox"/> Use groups to assign permissions	▼
⚠ Apply an IAM password policy	▼

Establecer una política de contraseñas de IAM

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Password Policy

You have unsaved changes to your password policy.

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Currently, this AWS account does not have a password policy. Specify a password policy below.

Minimum password length:

Require at least one uppercase letter i

Require at least one lowercase letter i

Require at least one number i

Require at least one non-alphanumeric character i

Allow users to change their own password i

Enable password expiration i

Password expiration period (in days):

Prevent password reuse i

Number of passwords to remember:

Password expiration requires administrator reset i

Apply password policy **Delete password policy**

Comprobaciones de estado de seguridad completadas



Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
<https://raysinut.signin.aws.amazon.com/console>

Customize | Copy Link

IAM Resources

Users: 1	Roles: 0
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

Security Status

5 out of 5 complete.

<input checked="" type="checkbox"/> Delete your root access keys	▼
<input checked="" type="checkbox"/> Activate MFA on your root account	▼
<input checked="" type="checkbox"/> Create individual IAM users	▼
<input checked="" type="checkbox"/> Use groups to assign permissions	▼
<input checked="" type="checkbox"/> Apply an IAM password policy	▼

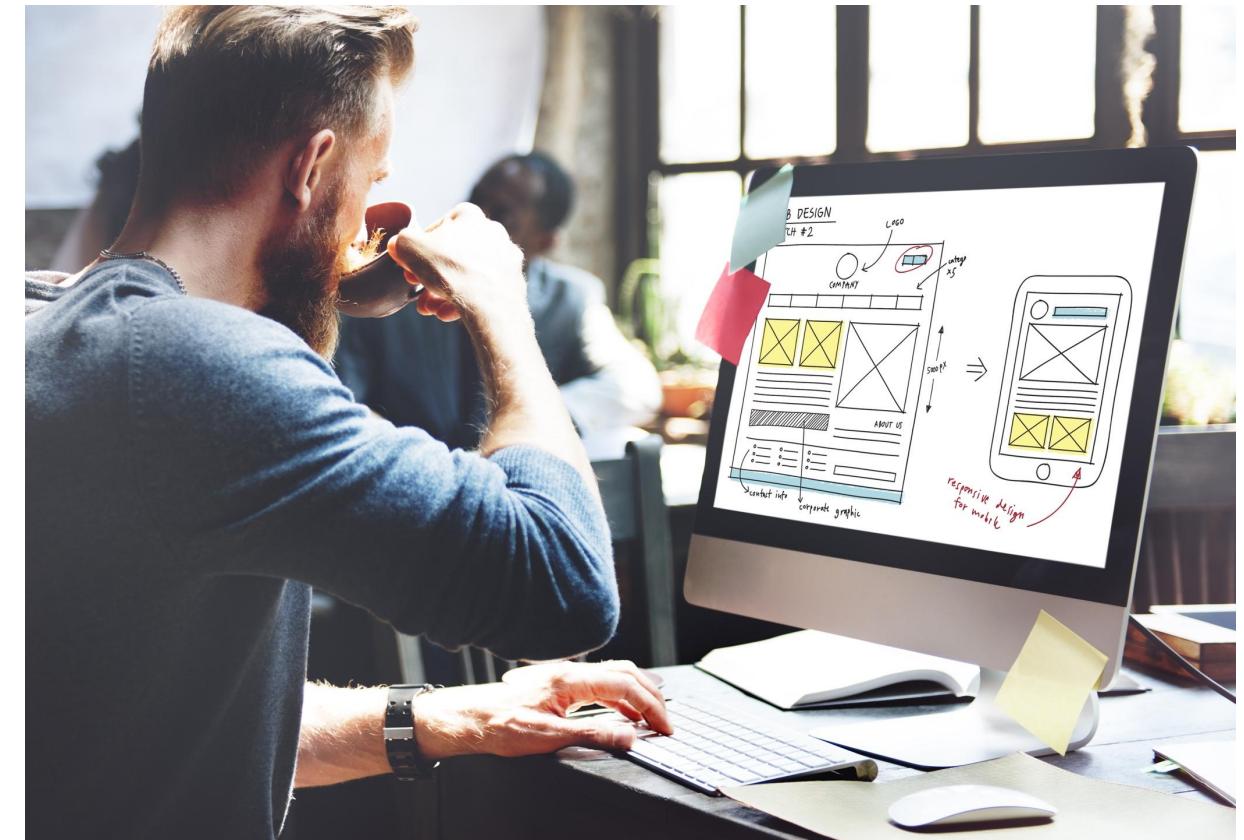
Aprendizajes clave de la sección 3



Prácticas recomendadas para proteger una cuenta de AWS:

- **Proteja** los inicios de sesión con Multi-Factor Authentication (MFA).
- **Elimine** las **claves de acceso** de usuario raíz de la cuenta.
- **Cree** **usuarios de IAM** individuales y otorgue permisos de acuerdo con el principio de mínimo privilegio.
- **Utilice grupos** para asignar permisos a usuarios de IAM.
- **Configure** una **política de contraseñas sólida**.
- **Delegue** el uso de **roles** en lugar del uso compartido de credenciales.
- **Monitoree** la actividad de la cuenta mediante AWS CloudTrail.

Laboratorio 1: Introducción a IAM



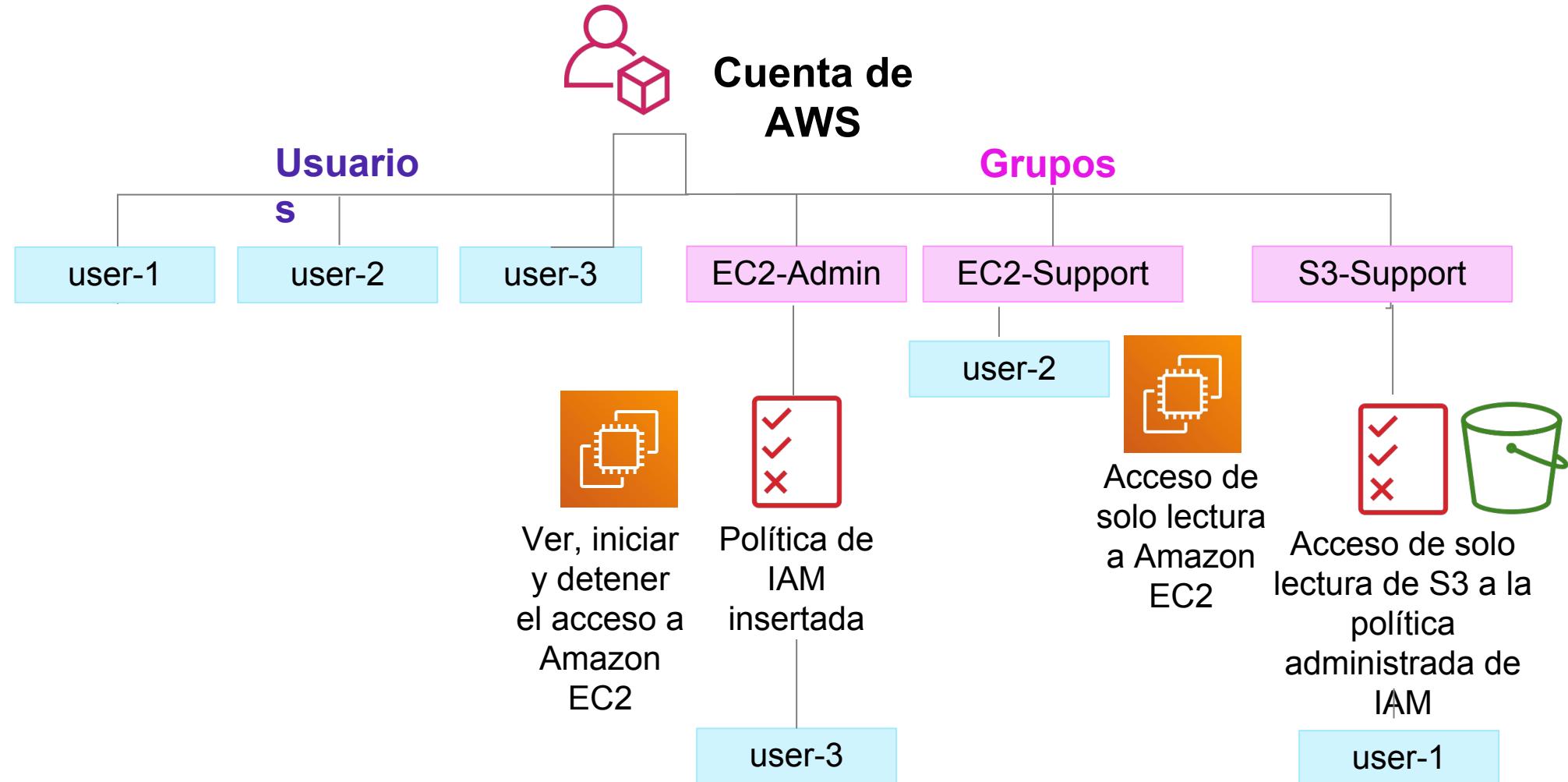
Laboratorio 1: tareas

- Tarea 1: analizar los usuarios y los grupos
- Tarea 2: agregar usuarios a los grupos
- Tarea 3: iniciar sesión y probar los usuarios



AWS Identity and
Access Management
(IAM)

Laboratorio 1: producto final





~ 40 minutos



Comience el laboratorio 1: Introducción a AWS IAM

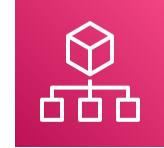
Análisis posterior del laboratorio: aprendizajes clave



Módulo 4: Seguridad en la nube de AWS

Sección 4: Protección de cuentas

- **AWS Organizations** le permite consolidar varias cuentas de AWS para que las administre de forma centralizada.



AWS Organizations

- **Características de seguridad** de AWS Organizations:

- Agrupa las cuentas de AWS en unidades organizativas (OU) y asocian las diferentes políticas de acceso a cada una de ellas.
- Permite integración y compatibilidad con IAM.
 - Los permisos para un usuario son la intersección de lo que AWS Organizations permite y lo que IAM concede en esa cuenta.
- Utiliza políticas de control de servicios para establecer el control sobre las acciones de API y los servicios de AWS a los que cada cuenta de AWS puede obtener acceso.

- Las **políticas de control de servicios (SCP)** ofrecen control centralizado sobre las cuentas.
 - Limita los permisos disponibles en una cuenta que forma parte de la organización.
- Garantiza que las cuentas cumplan con las directrices de control de acceso.
- Las SCP son *similares* a las políticas de permisos de IAM:
 - Utilizan una sintaxis similar.
 - Sin embargo, una SCP nunca concede permisos.
 - En su lugar, las SCP **especifican los permisos máximos** para una organización.

AWS Key Management Service (AWS KMS)



Características de AWS Key Management Service (AWS KMS):

- Le permite **crear y administrar claves de cifrado**.
- Le permite controlar el uso del cifrado en los servicios de AWS y en sus aplicaciones.
- Se integra con AWS CloudTrail para registrar el uso de todas las claves.
- Utiliza módulos de seguridad de hardware (HSM) validados por *Federal Information Processing Standards* (FIPS, Estándar de procesamiento de la información federal) 140-2 para proteger las claves.



AWS Key Management Service (AWS KMS)

Características de **Amazon Cognito**:

- Incorpora control de acceso, inicio de sesión y registro de usuarios a sus aplicaciones web y móviles.
- Escala a millones de usuarios.
- Admite el inicio de sesión con proveedores de identidad social, como Facebook, Google y Amazon; y proveedores de identidades empresariales, como Microsoft Active Directory a través del lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0.



Amazon Cognito

- Características de **AWS Shield**:

- Es un servicio administrado de protección contra ataques de denegación de servicio distribuidos (DDoS).
- Protege las aplicaciones que se ejecutan en AWS.
- Proporciona detección permanente y mitigaciones directas automáticas.
- Se puede habilitar *AWS Shield Standard* sin costo adicional. *AWS Shield Advanced* es un servicio de pago opcional.
- Utilícelo para **minimizar el tiempo de inactividad y la latencia de la aplicación**.



AWS Shield

Módulo 4: Seguridad en la nube de AWS

Sección 5: Protección de datos en AWS

Cifrado de datos *en reposo*



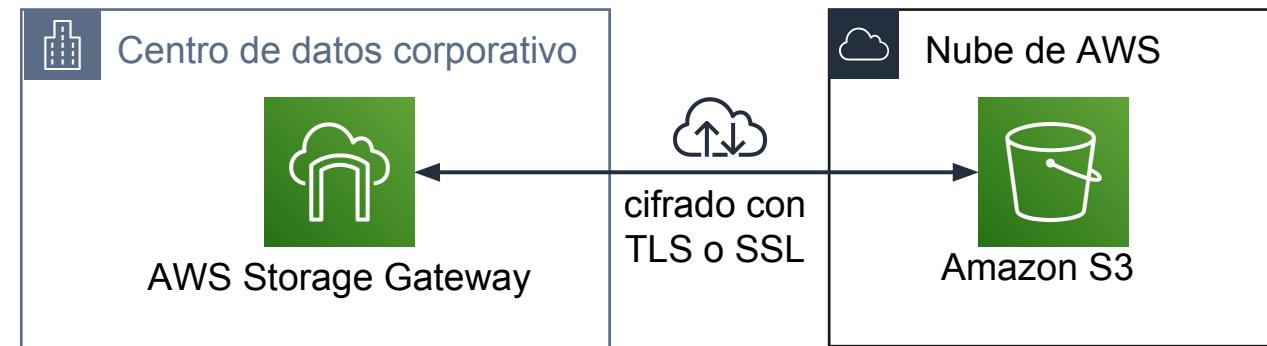
- El **cifrado** codifica los datos con una **clave secreta**, lo que hace que sean ilegibles.
 - Solo aquellos que tienen la clave secreta pueden descodificar los datos.
 - **AWS KMS** puede administrar sus claves secretas.
- AWS admite el cifrado de **datos en reposo**.
 - Datos en reposo = datos almacenados físicamente (en disco o en cinta)
 - Puede cifrar los datos almacenados en cualquier servicio compatible con AWS KMS, como los siguientes:
 - Amazon S3
 - Amazon EBS
 - Amazon Elastic File System (Amazon EFS)
 - Bases de datos administradas de Amazon RDS



Cifrado de datos en tránsito



- Cifrado de **datos en tránsito** (datos que migran a través de una red)
 - **Transport Layer Security (TLS)**, anteriormente SSL, es un protocolo estándar abierto.
 - **AWS Certificate Manager** ofrece una forma de administrar, implementar y renovar certificados TLS o SSL
- HTTP seguro (HTTPS) crea un túnel seguro.
 - Utiliza TLS o SSL para el intercambio bidireccional de datos.
- **Los servicios de AWS admiten el cifrado de datos en tránsito.**
 - Dos ejemplos:



- Los buckets y objetos de S3 recientemente creados son **privados** y están **protegidos** de forma predeterminada.
- Cuando los casos de uso requieren compartir objetos de datos en Amazon S3:
 - Es fundamental administrar y controlar el acceso a los datos.
 - Siga los **permisos que siguen el principio de privilegio mínimo** y considere la posibilidad de utilizar el cifrado de Amazon S3.
- Entre las herramientas y opciones para controlar el acceso a los datos de S3 se incluyen las siguientes:
 - [Característica de Amazon S3 Block Public Access](#): es fácil de usar.
 - Políticas de IAM: son una buena opción cuando el usuario puede autenticarse con IAM.
 - [Políticas de buckets](#)
 - [Listas de control de acceso](#) (ACL): son un mecanismo de control de acceso heredado.
- Comprobación de permisos del bucket de [AWS Trusted Advisor](#): es una característica gratuita.

Módulo 4: Seguridad en la nube de AWS

Sección 6: Trabajo para garantizar la conformidad

Programas de conformidad de AWS



- Los clientes están sujetos a diferentes reglamentos y requisitos de seguridad y conformidad.
- **AWS colabora con organismos de certificación y auditores independientes para ofrecer a los clientes información detallada sobre las políticas, los procesos y los controles que establece y aplica AWS.**
- Los programas de conformidad pueden clasificarse en las siguientes categorías generales:
 - **Certificaciones y acreditaciones**
 - Evaluadas por un auditor de terceros independiente
 - Ejemplos: ISO 27001, 27017, 27018 e ISO/IEC 9001
 - **Leyes, regulaciones y privacidad**
 - AWS ofrece características de seguridad y acuerdos legales para respaldar la conformidad
 - Ejemplos: Reglamento General de Protección de Datos (GDPR) de la UE, HIPAA
 - **Alineaciones y marcos de trabajo**
 - Requisitos de conformidad o seguridad específicos de cada sector o función
 - Ejemplos: Centro de seguridad en Internet (CIS), certificado por el Escudo de la privacidad UE-EE. UU.





AWS Config

Ejemplo de la vista del panel de AWS Config

The screenshot shows the AWS Config Dashboard with the following data:

Resource Type	Total Count
EC2 SecurityGroup	8
Lambda Function	7
S3 Bucket	6
EC2 Subnet	6
CloudWatch Alarm	3
EC2 InternetGateway	2
EC2 Instance	2
EC2 VPC	2
EC2 NetworkInterface	2
EC2 RouteTable	2

Config rule compliance: 1 Noncompliant rule(s)

Resource compliance: 35 Noncompliant resource(s)

Noncompliant rules:

Rule name	Compliance
required-tags	25+ noncompliant resource(s)

- **Evalúe, audite y analice las configuraciones de sus recursos de AWS.**
- Utilícelo para el monitoreo continuo de las configuraciones.
- Evalúe automáticamente las configuraciones *registradas* frente a las configuraciones deseadas.
- Revise los cambios de configuración.
- Consulte históricos de configuración detallados.
- **Simplifique la auditoría de conformidad y el análisis de seguridad.**



AWS Artifact

- **Es un recurso destinado a la información relacionada con la conformidad.**
- Proporciona acceso a informes de seguridad y conformidad, así como también a acuerdos en línea seleccionados.
- Puede obtener acceso a descargas de ejemplo:
 - Certificaciones ISO de AWS
 - Informes del sector de tarjetas de pago (PCI) y del control de organizaciones de servicios (SOC)
- Puede acceder a AWS Artifact directamente desde la consola de administración de AWS
 - En **Security, Identify & Compliance** (Seguridad, identidad y conformidad), haga clic en **Artifact**.

Aprendizajes clave de la sección 6



- Los **programas de conformidad de seguridad de AWS** proporcionan información acerca de las políticas, los procesos y los controles que establece y opera AWS.
- **AWS Config** se utiliza para analizar, auditar y evaluar las configuraciones de los recursos de AWS.
- **AWS Artifact** proporciona acceso a informes de seguridad y conformidad.

Módulo 4: Seguridad en la nube de AWS

Sección 7: Servicios y recursos de seguridad adicionales



AWS Service
Catalog

- **Cree y administre catálogos de servicios de TI aprobados por su organización.**
 - Ayuda a los empleados a encontrar e implementar servicios de TI *aprobados*.
 - Un servicio de TI puede incluir uno o varios recursos de AWS.
 - Ejemplo:
 - Instancias EC2, volúmenes de almacenamiento, bases de datos y componentes de red
- Controle el uso de los servicios de AWS a través de la especificación de restricciones:
 - Restricciones de ejemplo:
 - La región de AWS en la cual se puede lanzar un producto
 - Rangos de direcciones IP permitidos
- Administre de forma centralizada el ciclo de vida de los servicios de TI.
- Ayude a cumplir los requisitos de conformidad.

Servicios de seguridad adicionales seleccionados



Amazon
Macie

Proteja información de identificación personal (PII) de forma proactiva y entérese cuando se modifique su ubicación.



Amazon
Inspector

Defina estándares y prácticas recomendadas para sus aplicaciones y **valide su conformidad** con estos **estándares**.



Amazon
GuardDuty

Brinda **detección de amenazas** inteligente y monitoreo continuo para proteger sus cargas de trabajo y cuentas de AWS.

Módulo 4: Seguridad en la nube de AWS

Conclusión del módulo

Resumen del módulo



En resumen, en este módulo, aprendió a hacer lo siguiente:

- Reconocer el modelo de responsabilidad compartida
- Identificar la responsabilidad del cliente y de AWS
- Reconocer usuarios, grupos y roles de IAM
- Describir los diferentes tipos de credenciales de seguridad en IAM
- Identificar los pasos para proteger una nueva cuenta de AWS
- Explorar los usuarios y los grupos de IAM
- Reconocer cómo proteger los datos de AWS
- Reconocer los programas de conformidad de AWS

Complete la revisión de conocimientos



Pregunta del examen de muestra



¿Cuál de las siguientes opciones es responsabilidad de AWS según el modelo de responsabilidad compartida de AWS?

- A. Configuración de aplicaciones de terceros
- B. Mantenimiento del hardware físico
- C. Protección del acceso a la aplicación y de los datos de esta
- D. Administración de las Imágenes de Amazon Machine (AMI) personalizadas

Recursos adicionales



- Página de inicio de [Seguridad en la nube de AWS](#)
- [Recursos de seguridad de AWS](#)
- [Blog de seguridad de AWS](#)
- [Boletines de seguridad](#)
- [Pruebas de intrusión y vulnerabilidad](#)
- Marco de Buena Arquitectura de AWS: [pilar de seguridad](#)
- Documentación de AWS: [prácticas recomendadas de IAM](#)

Gracias

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. Este contenido no puede reproducirse ni redistribuirse, total ni parcialmente, sin el permiso previo por escrito de Amazon Web Services, Inc. Queda prohibida la copia, el préstamo o la venta de carácter comercial. Envíenos sus correcciones o comentarios relacionados con el curso a: aws-course-feedback@amazon.com. Si tiene cualquier otra duda, contacte con nosotros en: <https://aws.amazon.com/contact-us/aws-training/>. Todas las marcas comerciales pertenecen a sus propietarios.

