Arquitecturas de nube con AWS

Ing. Fernando Lichtschein
Ing. Mora Villa Abrille

9. Seguridad de usuarios, aplicaciones y datos

UNIVERSIDAD AUSTRAL

Objetivos

Administrar permisos mediante usuarios, grupos y roles de AWS IAM

Implementar federación de usuarios en una arquitectura para aumentar la seguridad

Describir cómo se manejan múltiples cuentas de AWS

Reconocer la función de las políticas de control de servicio (SCP) de AWS Organizations.

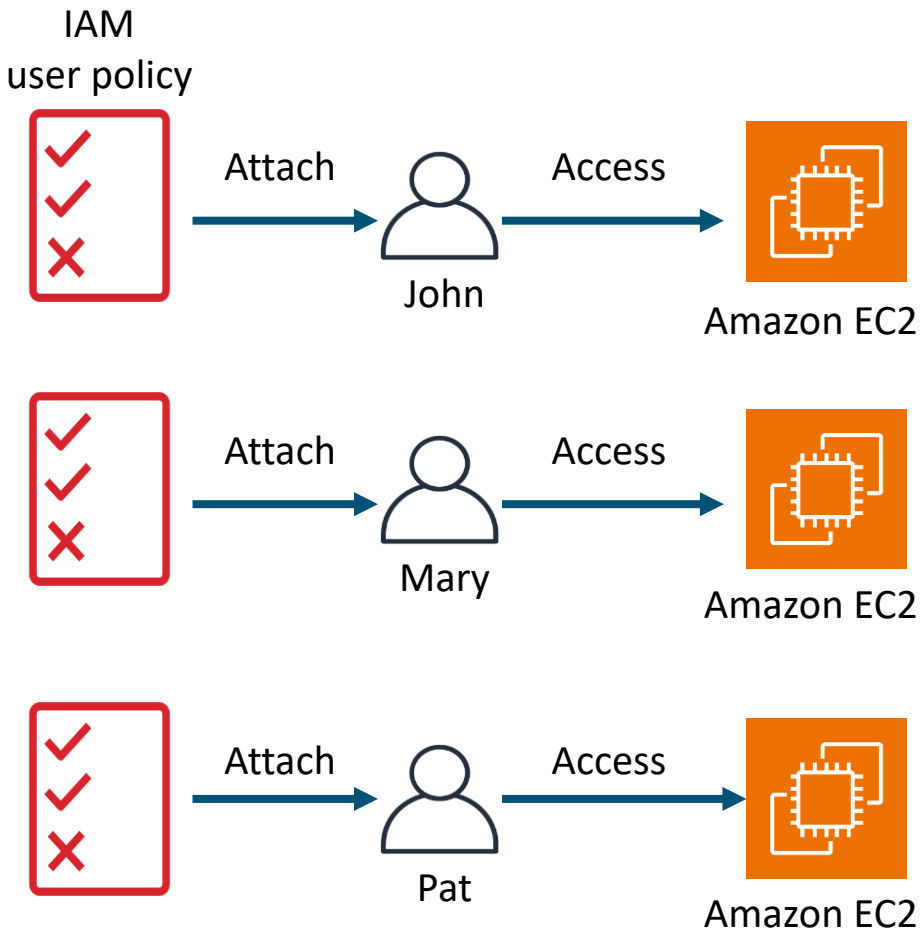
Cifrar datos en reposo usando AWS Key Management Service (AWS KMS).

Identificar los servicios de seguridad adecuados para ciertos casos de uso.

Administración de permisos

UNIVERSIDAD AUSTRAL

Gestión de permisos por usuarios



Configuración inicial

Cada desarrollador recibe acceso total a Amazon EC2 a través de políticas vinculadas con usuarios individuales.

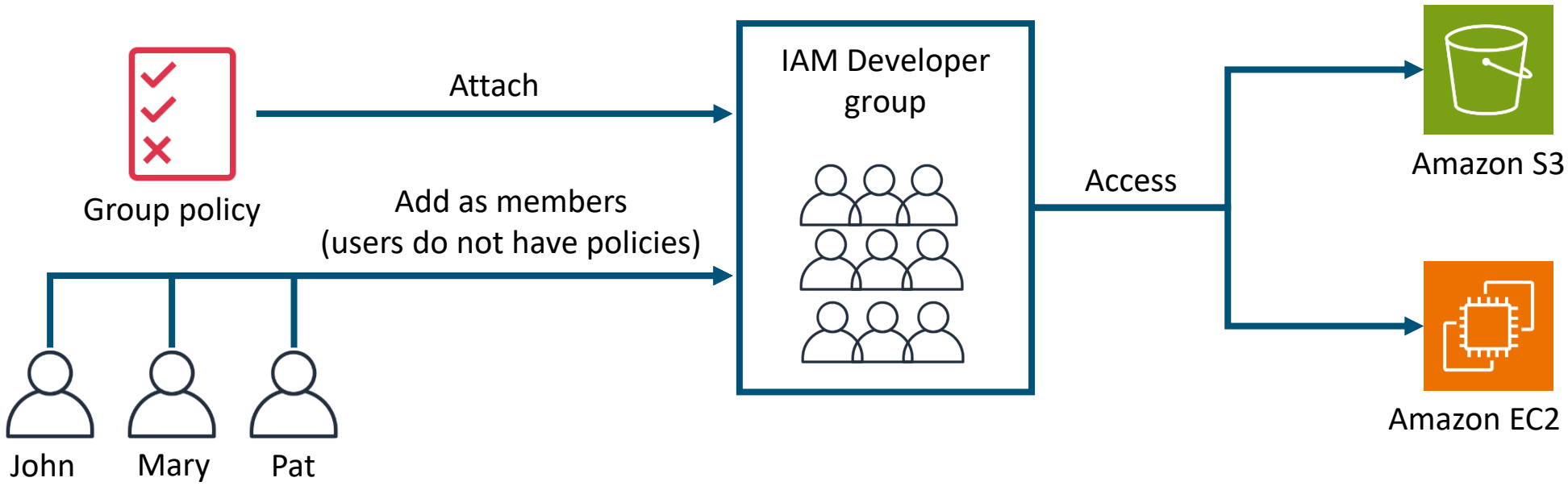
Se necesitan permisos adicionales

Cada desarrollador necesita acceso a Amazon S3. Para implementar el cambio, el administrador debe hacer tres modificaciones, una para cada política de usuario de IAM.

Crece la cantidad de usuarios

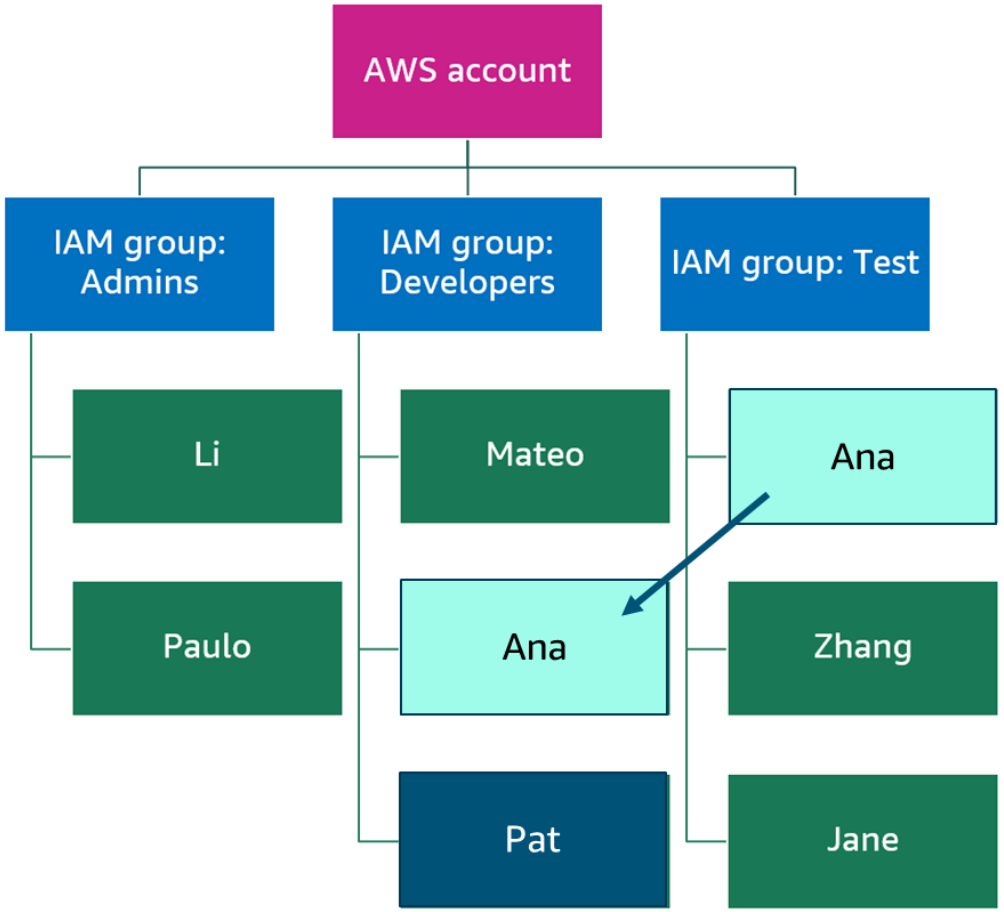
Este enfoque resulta inmanejable. ¿Cuál es la solución más apropiada?

Asignación de permisos por grupos



Ejemplo

Uso de grupos para reflejar la estructura organizacional



Al contratar un Nuevo desarrollador, se lo agrega en el grupo de desarrolladores. Inmediatamente, heredará los mismos accesos que tiene el resto del equipo.

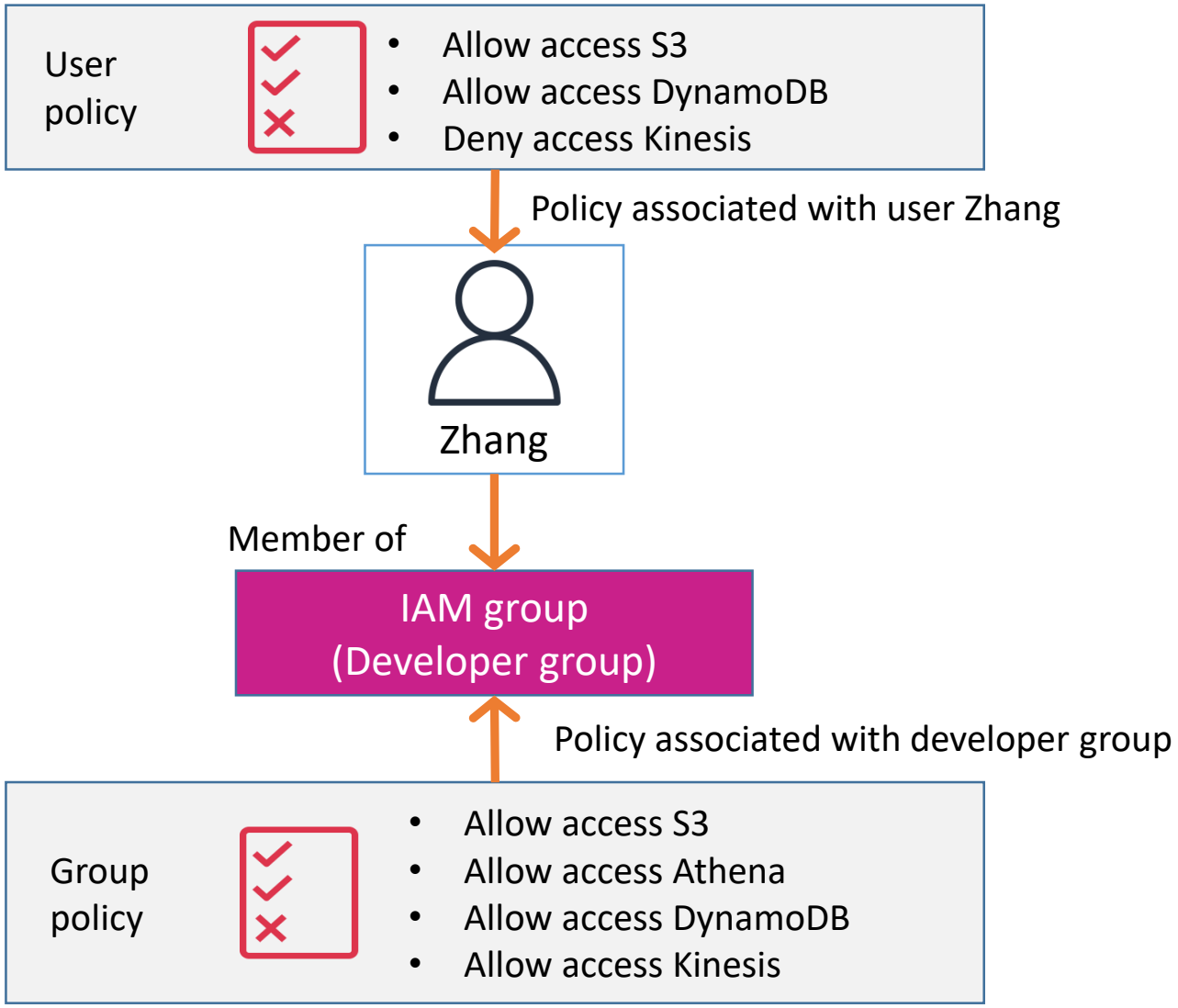
Si Ana cambia de rol, se hará lo siguiente:

- Quitarle los permisos del grupo de Test
- Agregarla al grupo de desarrollo.

Los usuarios pueden pertenecer a más de un grupo, pero los grupos no pueden anidarse.

Los permisos de las políticas asociadas a un usuario prevalecen sobre los del grupo **si son más restrictivos.**

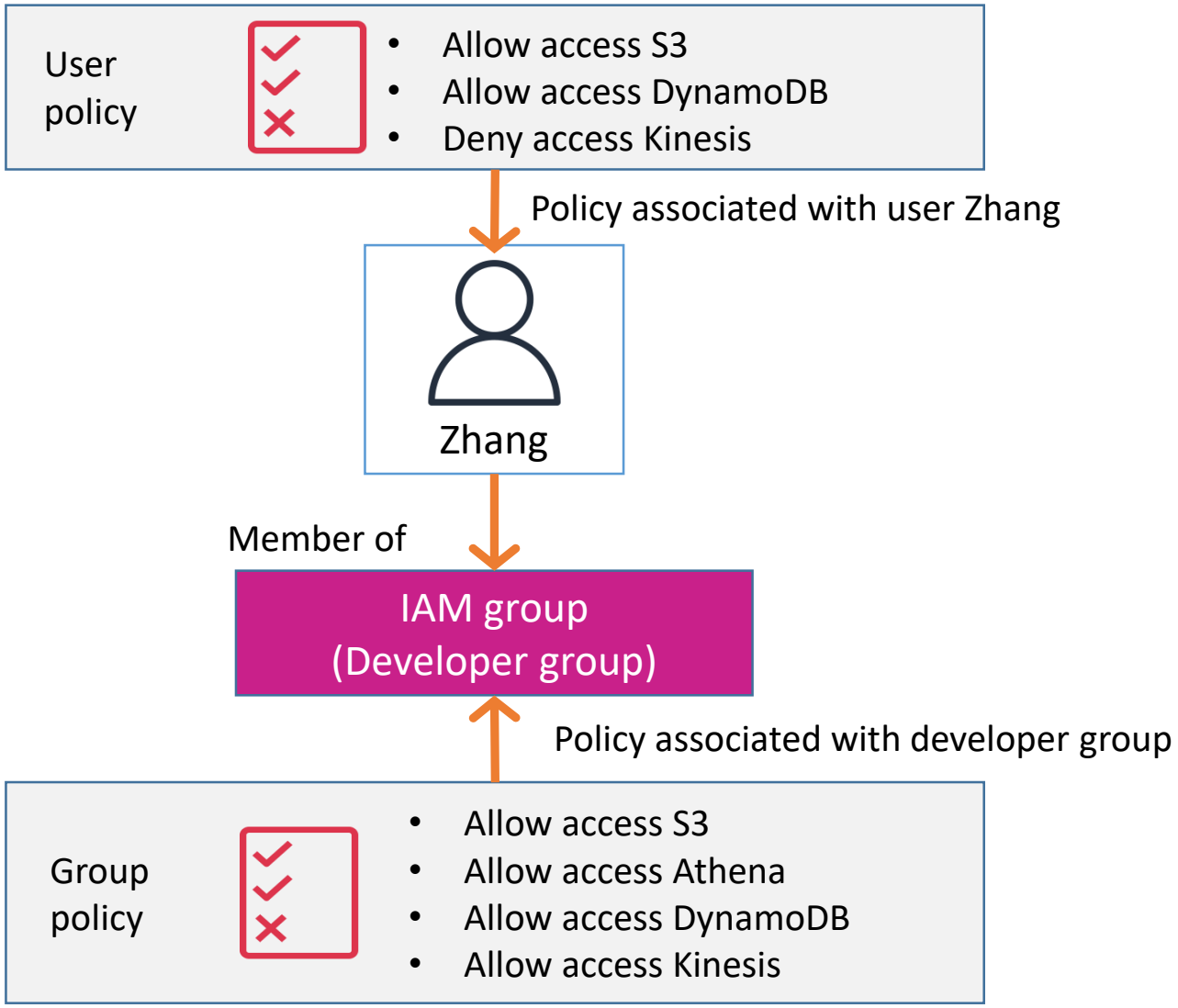
Ejemplo



¿Zhang puede acceder a Amazon Athena?

¿Zhang tiene acceso a Amazon Kinesis?

Ejemplo



Zhang puede acceder a Amazon Athena

Sí, por ser miembro del grupo, Zhang tiene acceso a Amazon Athena.

Zhang no tiene acceso a Amazon Kinesis

Aunque el grupo habilita el acceso a Kinesis, la política de usuario de Zhang niega explícitamente el acceso a Kinesis.

Escalamiento usando RBAC

UNIVERSIDAD AUSTRAL

Definición de roles

Crear una política IAM con los permisos del rol.

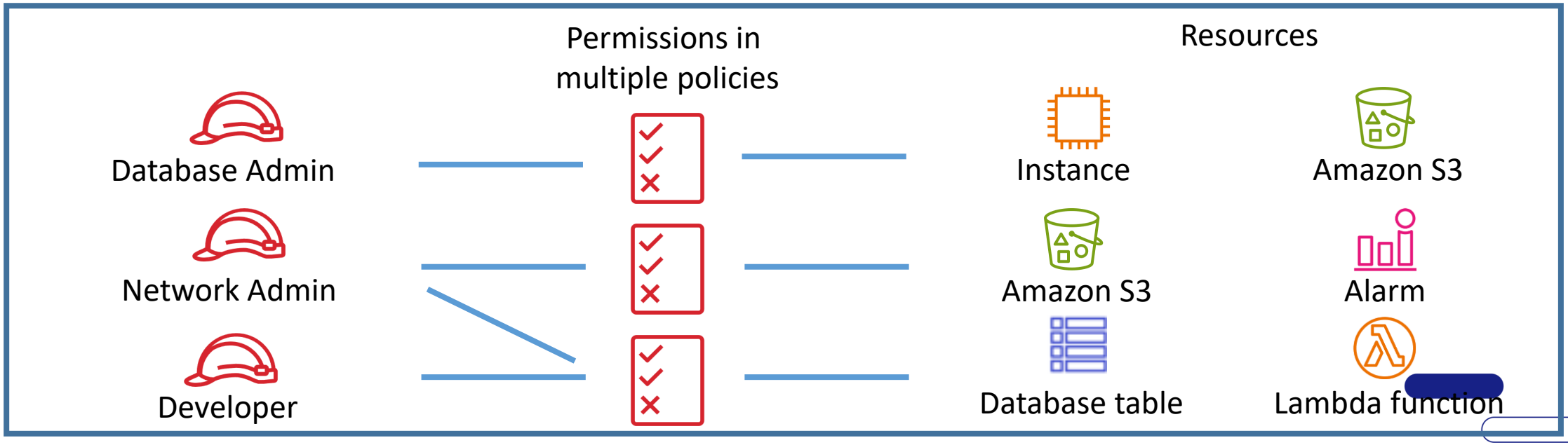
La política indica los recursos accesibles.

Asociar la política con una entidad de IAM (usuario, grupo o rol).

Actualización del rol

Actualizar la política.

Si el nuevo recurso es usado por varios roles, es necesario modificar múltiples políticas.



Uso de ABAC

¿Qué es?

Estrategia de autorización que define permisos en basados en atributos.

Los atributos son claves o pares de clave-valor.

En AWS, los atributos se llaman etiquetas (*tags*).

Las etiquetas se aplican a recursos de IAM y de AWS.

Ventajas

Es más flexible que las políticas en las que hay que identificar recursos individuales.

Permiten asignar permisos granulares sin actualizar las políticas cada vez que se agrega un recurso.

Es altamente escalable y auditable.

Etiquetas en AWS

Son metadatos conformados por un par (key/value).

Se pueden aplicar a recursos de las cuentas de AWS, y también a usuarios y roles de IAM.

Podemos crear nuestras propias etiquetas.

Muchas de las API de AWS devuelven datos de etiquetas.

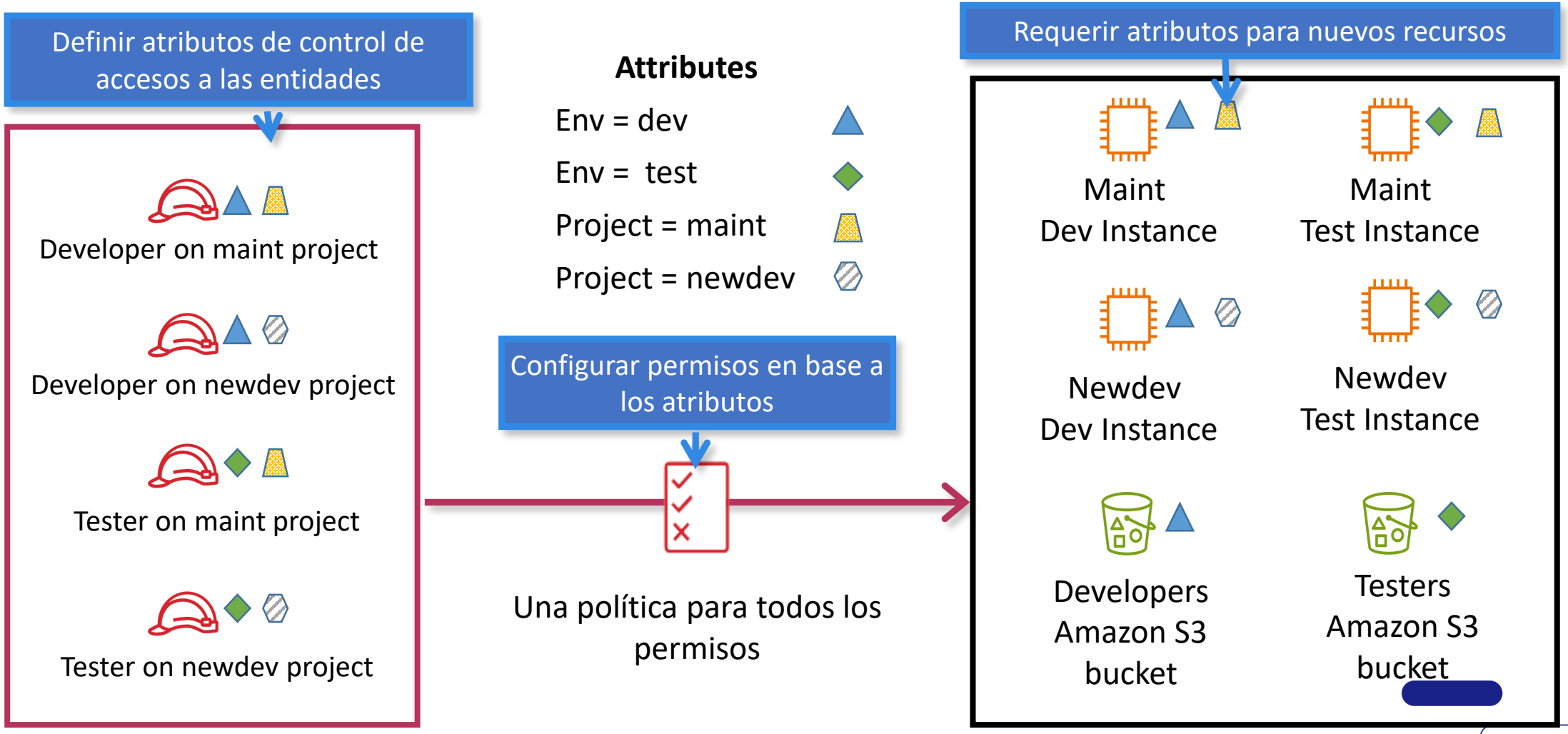
Se utilizan para facturación, control de accesos o aplicación de filtros a las vistas.

Ejemplos de etiquetas aplicadas a una instancia EC2

Key	Value
Name	Web server
Project	Unicorn
Env	Dev

Uso de ABAC para asignar permisos

Ejemplo



Resumen

Los grupos IAM permiten asignar los mismos derechos de acceso a múltiples usuarios. Los grupos deben reflejar las funciones de trabajo.

ABAC es más conveniente que RBAC para escalar mejor la gestión de permisos.

ABAC es una estrategia de autorización que define los permisos en base a ciertos atributos. Simplifica la gestión del control de acceso mediante la combinación de permisos en una única política.

Los atributos son pares key/value.

AWS permite asignar atributos a los recursos e identidades mediante la creación de etiquetas.

Federación

Seguridad de usuarios, grupos y datos

UNIVERSIDAD AUSTRAL

Federación de identidades

Generalidades

Es un sistema de confianza entre dos partes para autenticar usuarios y compartir información necesaria para autorizar el acceso a los recursos.

Proveedor de identidad (IdP)

Responsable de la autenticación del usuario.

Ejemplos

OpenID connect (OIDC), como Amazon, Facebook y Google

Security Assertion Markup Language (SAML), como Active Directory Federation Services

Proveedor del servicio

Responsable de controlar el acceso a sus recursos.

Ejemplos

AWS services
Redes sociales
Banco online

Servicios de AWS

Con soporte de federación de identidades

AWS Identity and Access Management (IAM)

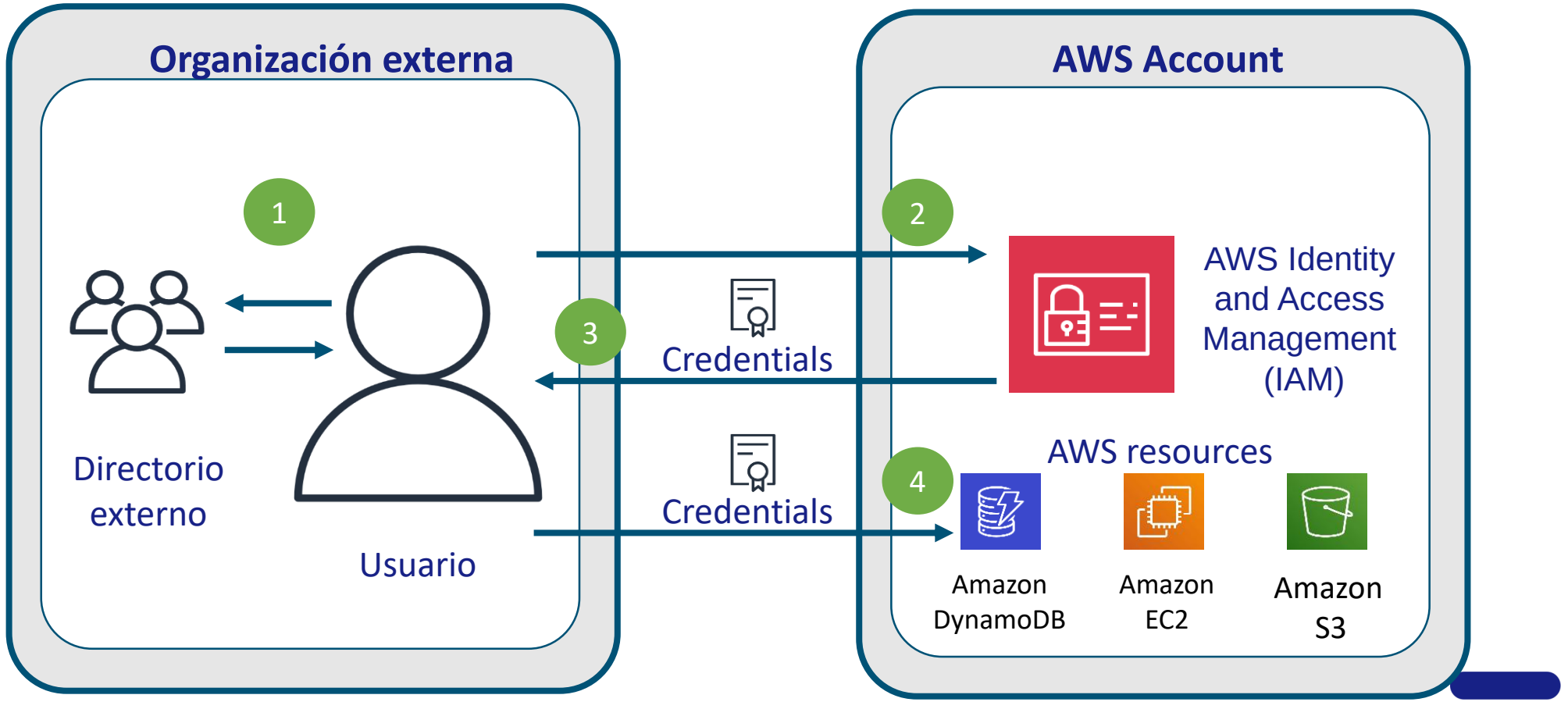
AWS IAM Identity Center (ex AWS Single Sign-On)

AWS Security Token Service (AWS STS)

Amazon Cognito

Federación de identidades

Ejemplo



IAM Identity Center

Sucesor de AWS Single Sign On

IAM Identity Center

Permite crear o conectar identidades únicas y manejar los accesos de manera centralizada en múltiples cuentas de AWS

Función de administración unificada para definir, personalizar y asignar accesos granulares

Proporciona un portal para acceder a todas las cuentas o aplicaciones de AWS

Se puede usar en conjunto con IAM

IAM Security Token Service (STS)

IAM STS

Es una API que permite solicitar credenciales transitorias con privilegios limitados.

Las credenciales pueden ser utilizadas por usuarios IAM, usuarios federados o aplicaciones.

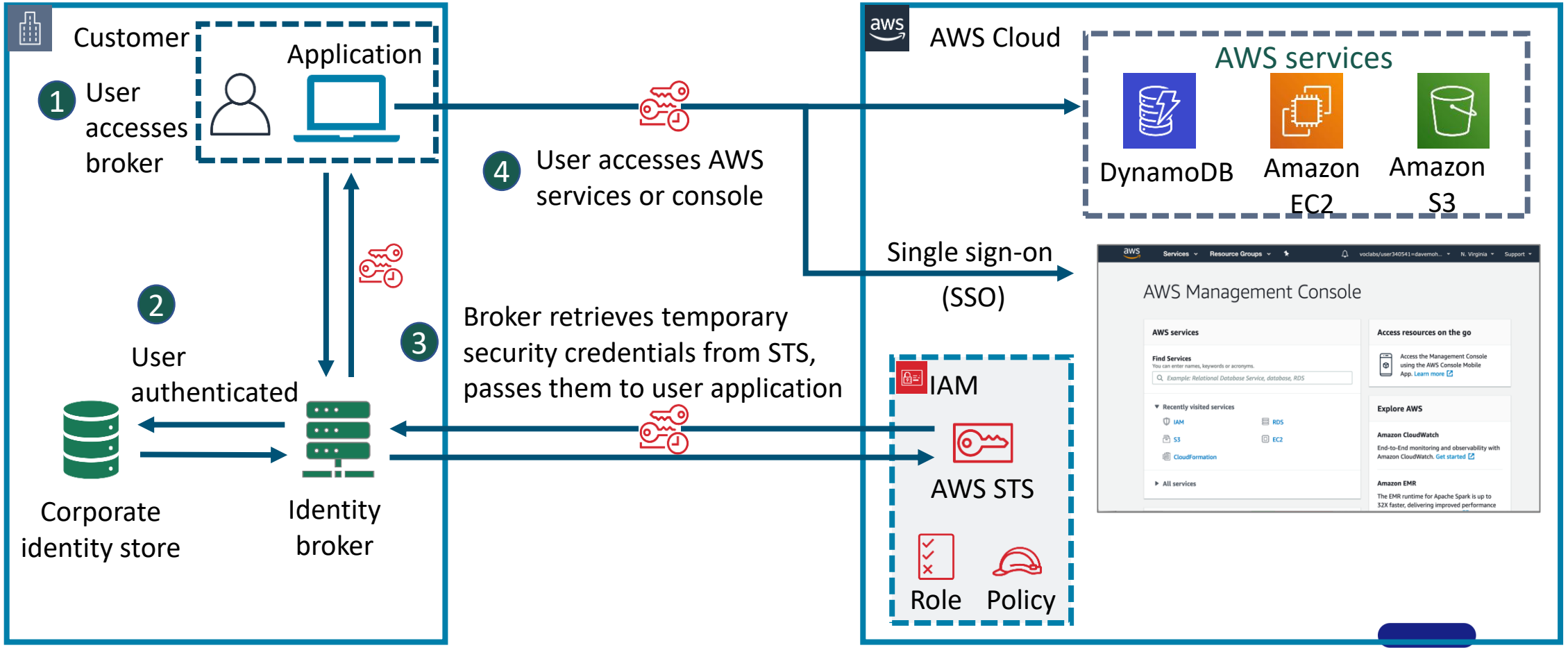
Federación de identidades

Identity brokers

El usuario accede con las credenciales que tiene en el IdP	Un *identity broker* funciona como intermediario entre los IdP y el SP	AWS STS genera credenciales temporales de manera dinámica	El *identity broker* le brinda las credenciales temporales a la aplicación
Por ejemplo, un *login* corporativo o su Amazon.com ID.	The identity broker requests temporary credentials from AWS STS.	Tienen un tiempo de expiración que puede variar entre minutos y horas.	AWS STS le transfiere las credenciales temporales al broker.

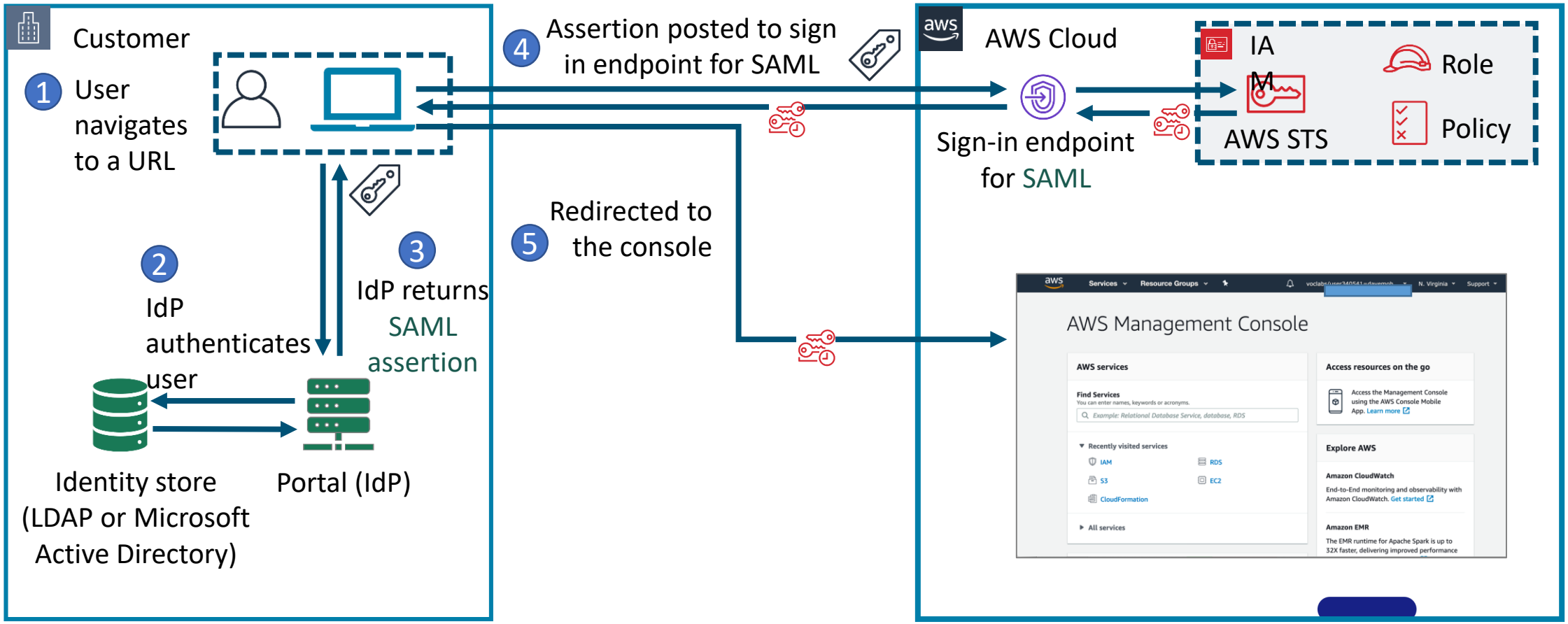
Federación de identidades

Para el acceso a la consola



Federación de identidades

Usando SAML (Windows / LDAP)



Amazon Cognito

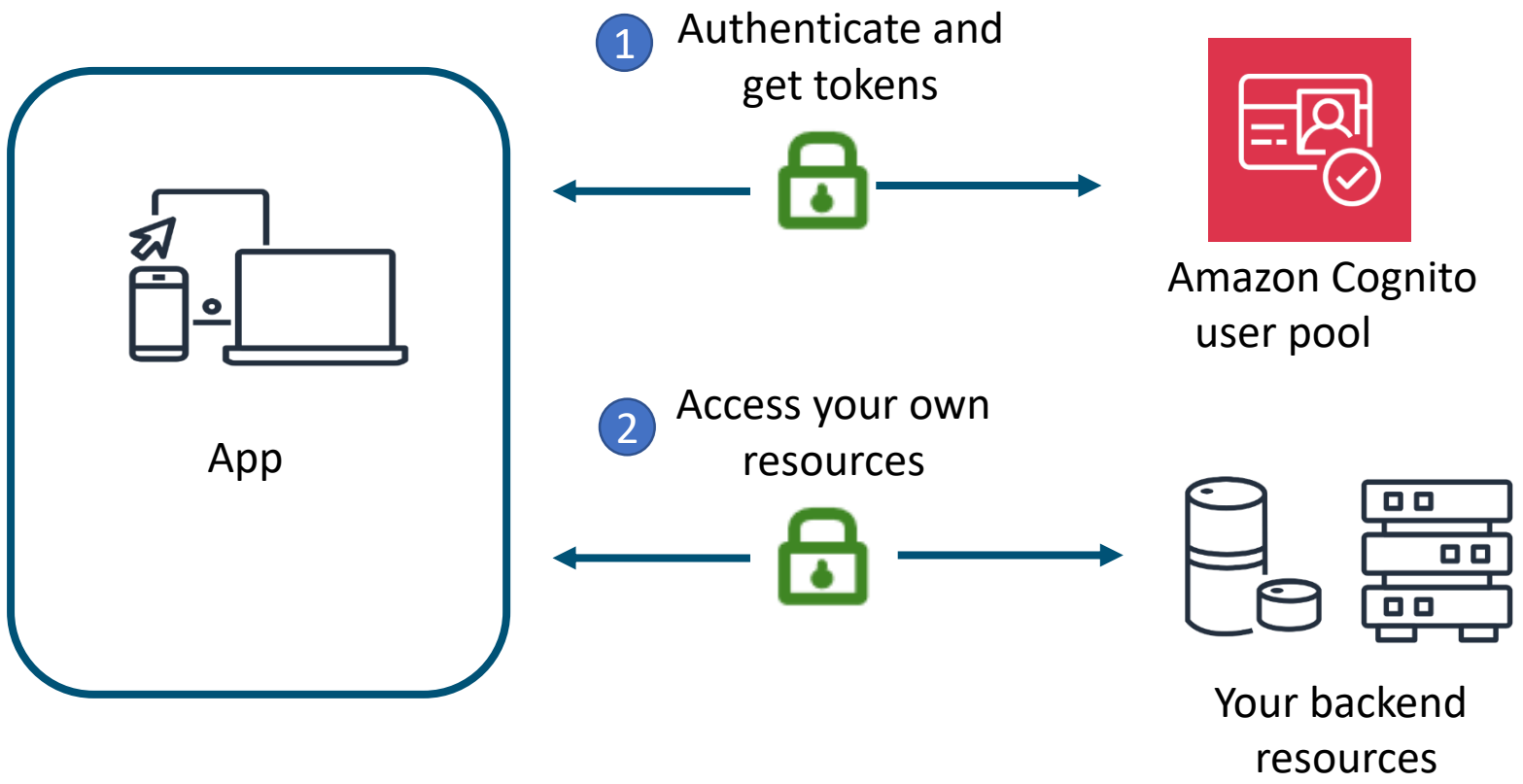
Es un servicio administrado que brinda:

Amazon Cognito

- Autenticación, autorización y gestión de usuarios para aplicaciones web y móviles
- Identidades federadas para accede por medio de terceros (Amazon, Facebook, Google) o SAML
- Grupos de usuarios (*user pools*) que mantienen un conjunto de perfiles de usuarios con *tokens* de autenticación
- Grupos de identidades (*identity pools*) que permiten crear identidades únicas y asignación de permisos para los usuarios

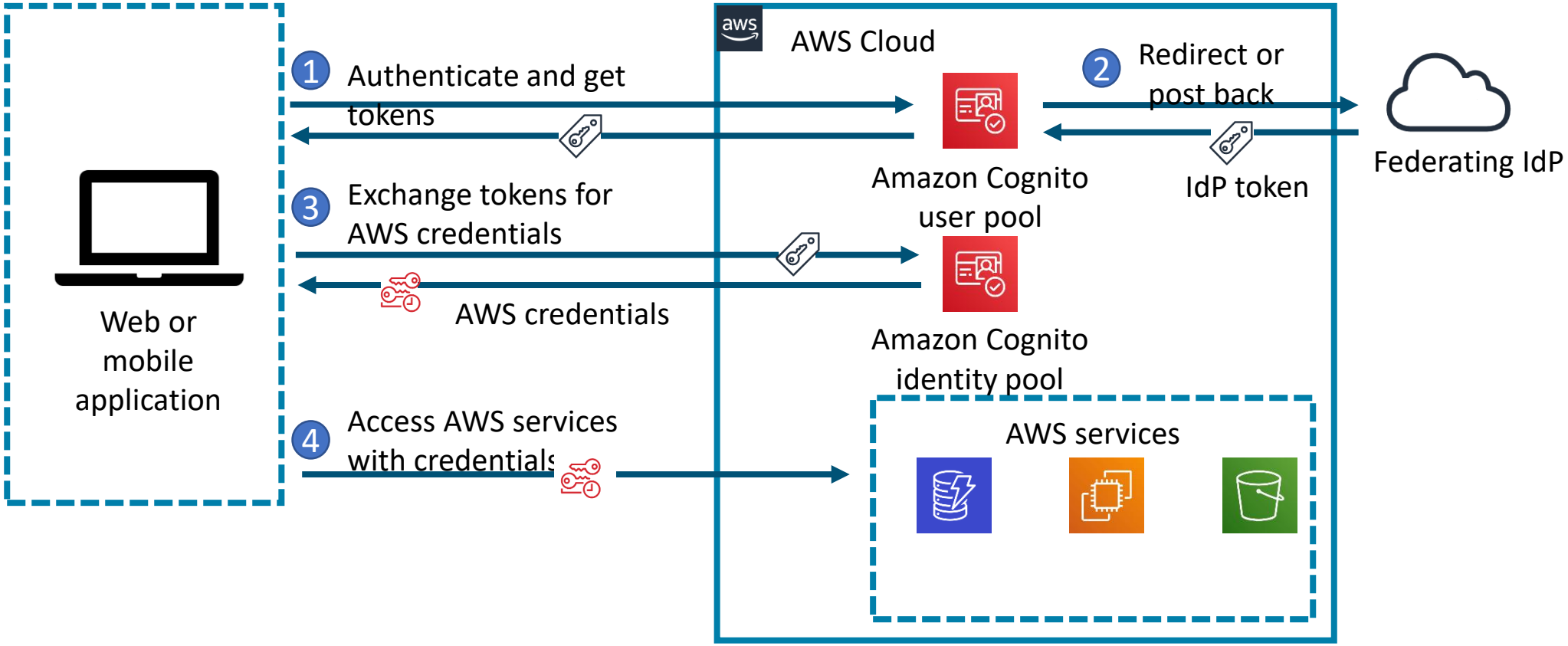
Federación de identidades

Para el acceso desde aplicaciones



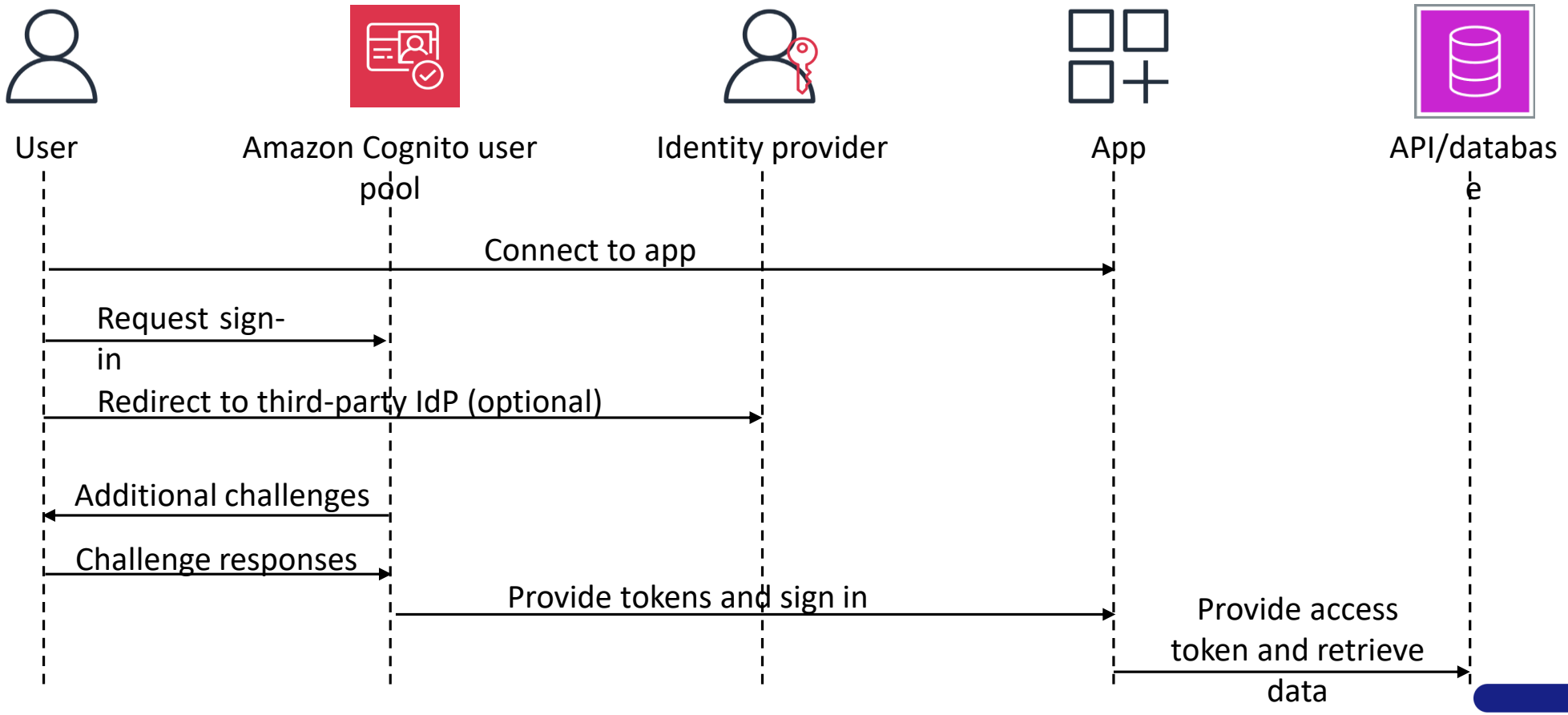
Federación de identidades

Ejemplo de Amazon Cognito



Federación de identidades

User pools



Amazon Cognito

User pools

Característica	Descripción
Sign-up	Los usuarios pueden ingresar su información en la aplicación y crear un perfil de usuario nativo para el *user pool.* Se puede redirigir a los usuarios a un IdP de terceros, el usuario autoriza pasar la información de autenticación a Amazon Cognito. Crear usuarios a partir de una fuente de datos o un esquema.
Sign-in	Se puede usar el pool de usuarios para brindar acceso o recurrir a un IdP.
Identidades federadas de terceros	El user pool permite gestionar los tokens recibidos de IdP que usan Open ID o SAML
UI propia para sign-up y sign-in	Se pueden personalizar las páginas web de Amazon Cognito (sign-up, sign-in, MFA, password reset).
JWTs	Permite usar tokens JWT para acceder a recursos del servidor o a otros servicios de AWS (con credenciales temporales).
Grupos de user pools	Los usuarios se pueden organizar en grupos para simplificar la gestión de permisos.

Federación de identidades

Resumen

La federación de identidades es un Sistema de confianza entre IdS y SPs.

AWS IAM Identity Center brinda funciones unificadas para definir, personalizar y asignar permisos granulares asociadas a las responsabilidades.

AWS STS es un servicio web que proporciona credenciales temporales de AWS y permite que un usuario (IAM, federado o de aplicación) asuma un rol de IAM.

Un *identity broker* permite la federación de usuarios que ya tienen una identidad fuera de AWS, como un directorio corporativo.

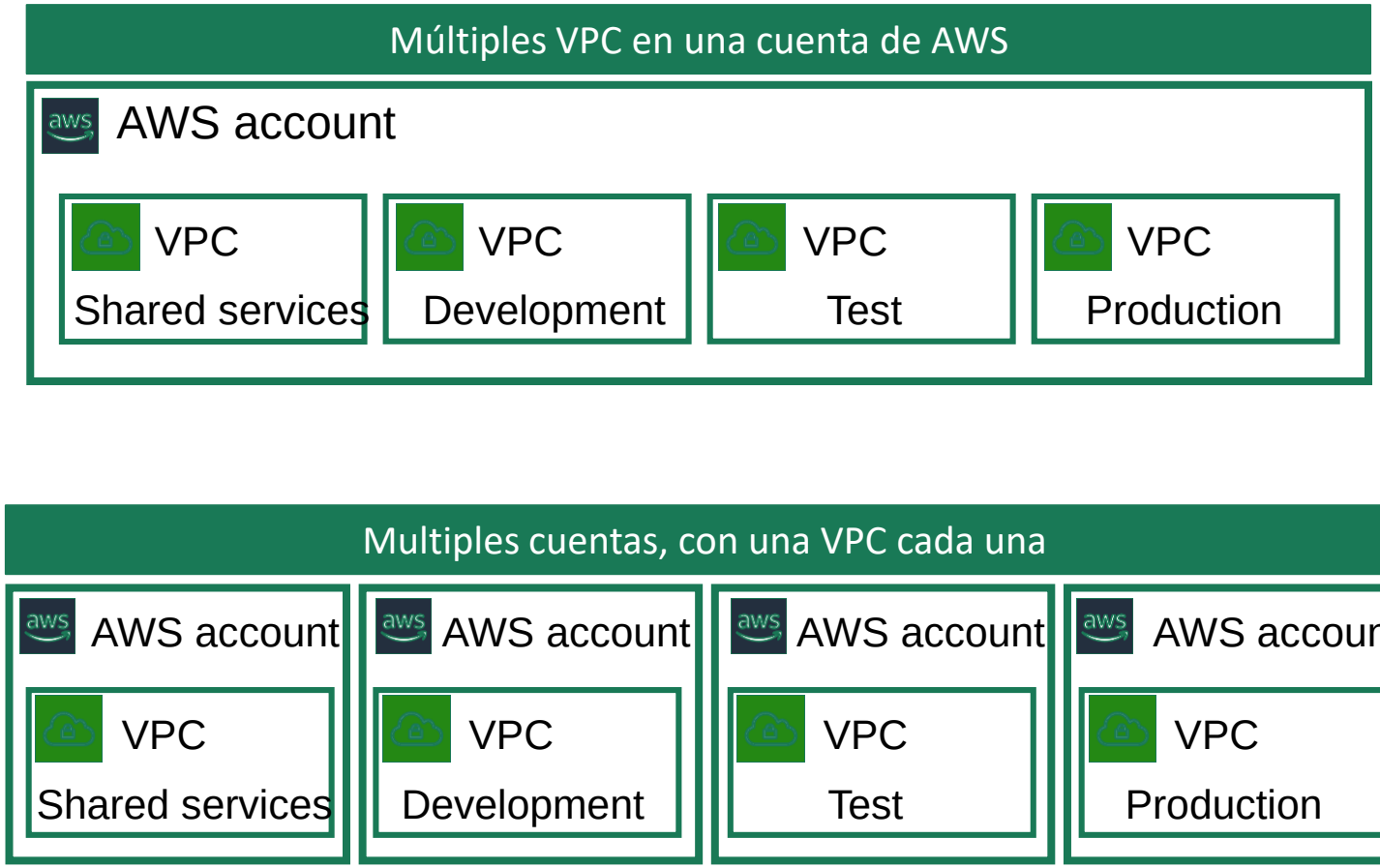
Amazon Cognito es un servicio gestionado que brinda autenticación, autorización y gestión de usuarios en aplicaciones web y móviles. Puede tener sus propios usuarios o integrarse con IdP de terceros.

Gestión de accesos a múltiples cuentas

UNIVERSIDAD AUSTRAL

Acceso a recursos

Patrones habituales



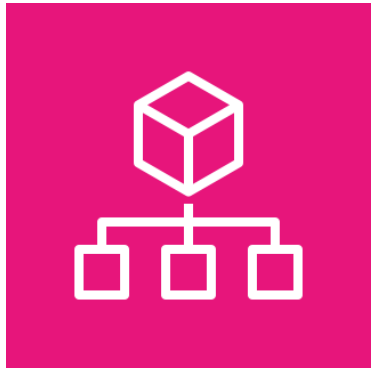
Uso de múltiples cuentas

Ventajas y desafíos

Ventajas
Separación de unidades de negocio o departamentos
Separación de ambientes
Aislamiento de datos de auditoria y recuperación
Segregación de cuentas para cargas de trabajo sujetas a regulación
Facilidad para la creación de alertas de costo por unidad de negocio
Ahorro de costos (hay precios preferenciales)

Desafíos
La gestión de seguridad en múltiples cuentas es más compleja
Es necesario aplicar procesos manuales en la creación de cada cuenta
Determinación de qué organización debe recibir la facturación
Necesidad de un gobierno centralizado que asegure la consistencia y el cumplimiento

AWS Organizations



AWS Organizations

Servicio de gestión de cuentas que permite consolidar múltiples cuentas de AWS en una única organización, que se administra de manera centralizada.

Permite aplicar descuentos

Permite la creación y gestión de cuentas

Tiene funciones para consolidar la facturación

Permite agrupar las cuentas jerárquicamente

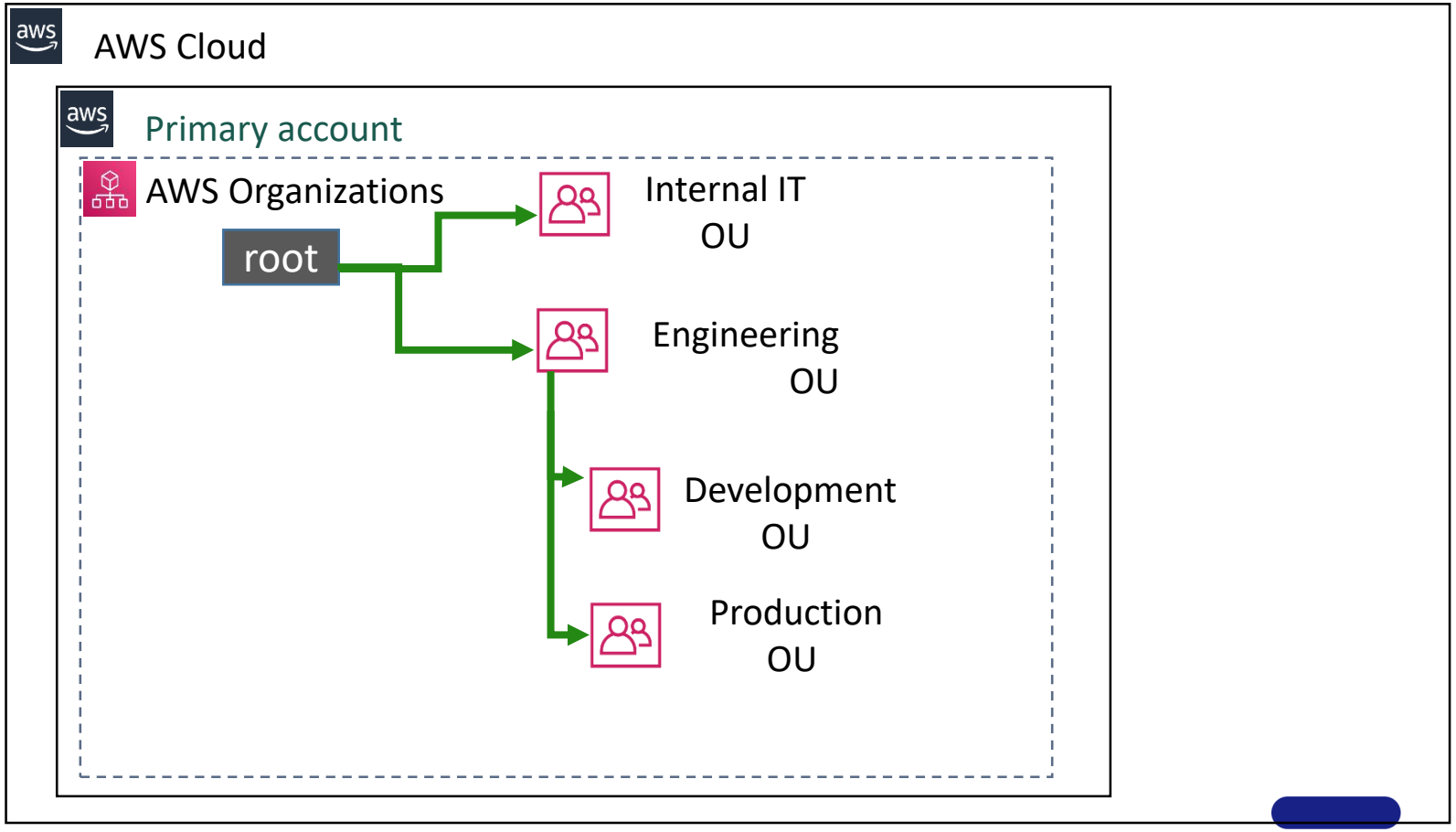
Permite aplicar controles centralizados sobre las políticas de los servicios de AWS, mediante *service control policies* (SCPs)

AWS Organizations

Creación de unidades organizativas

En la cuenta primaria de AWS Organizations:

1. Crear una jerarquía de unidades organizativas (OUs).

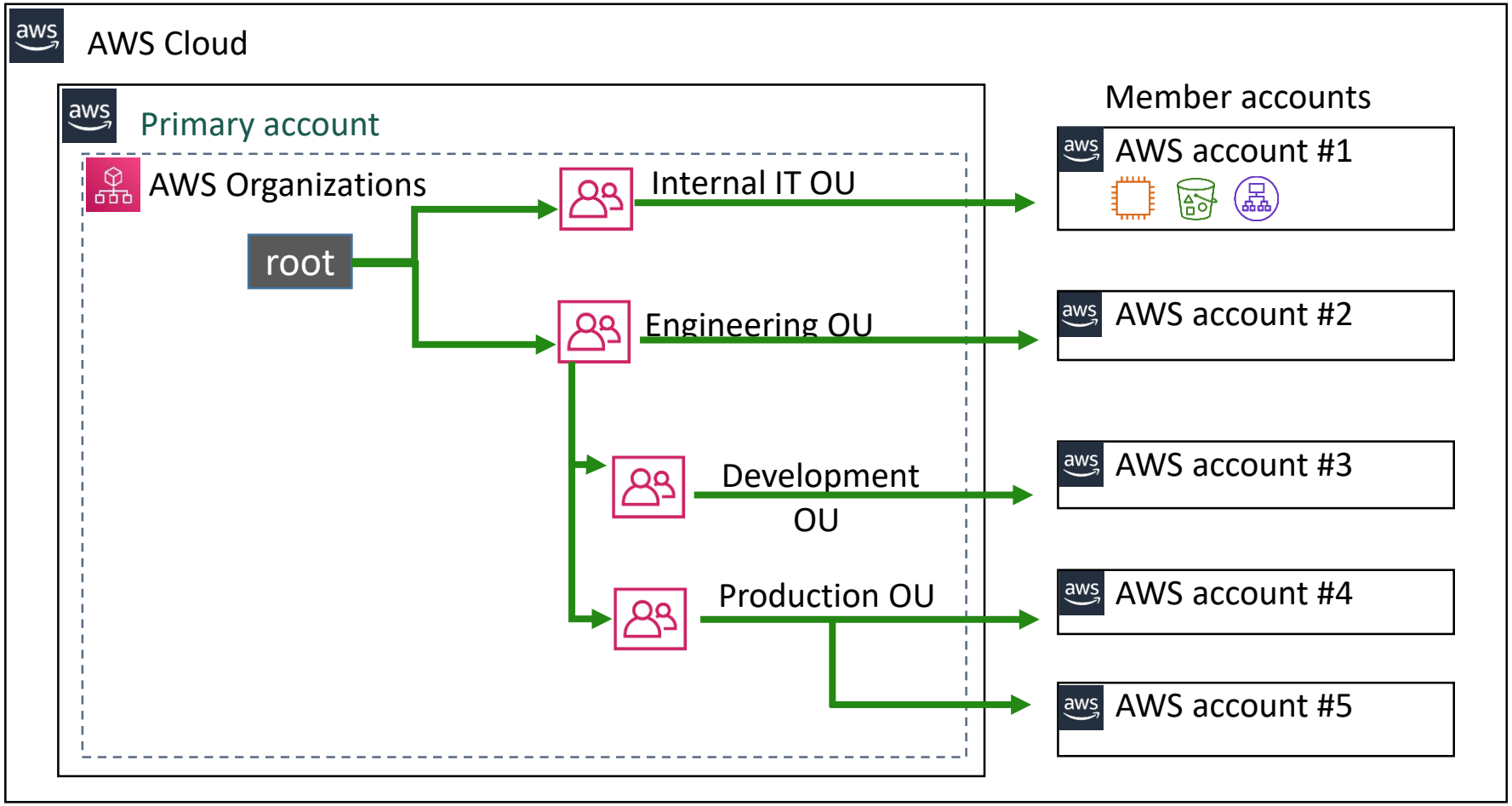


AWS Organizations

Creación de unidades organizativas

En la cuenta primaria de AWS Organizations:

1. Crear una jerarquía de unidades organizativas (OUs).
2. Asignar cuentas a las OU, como cuentas miembro.

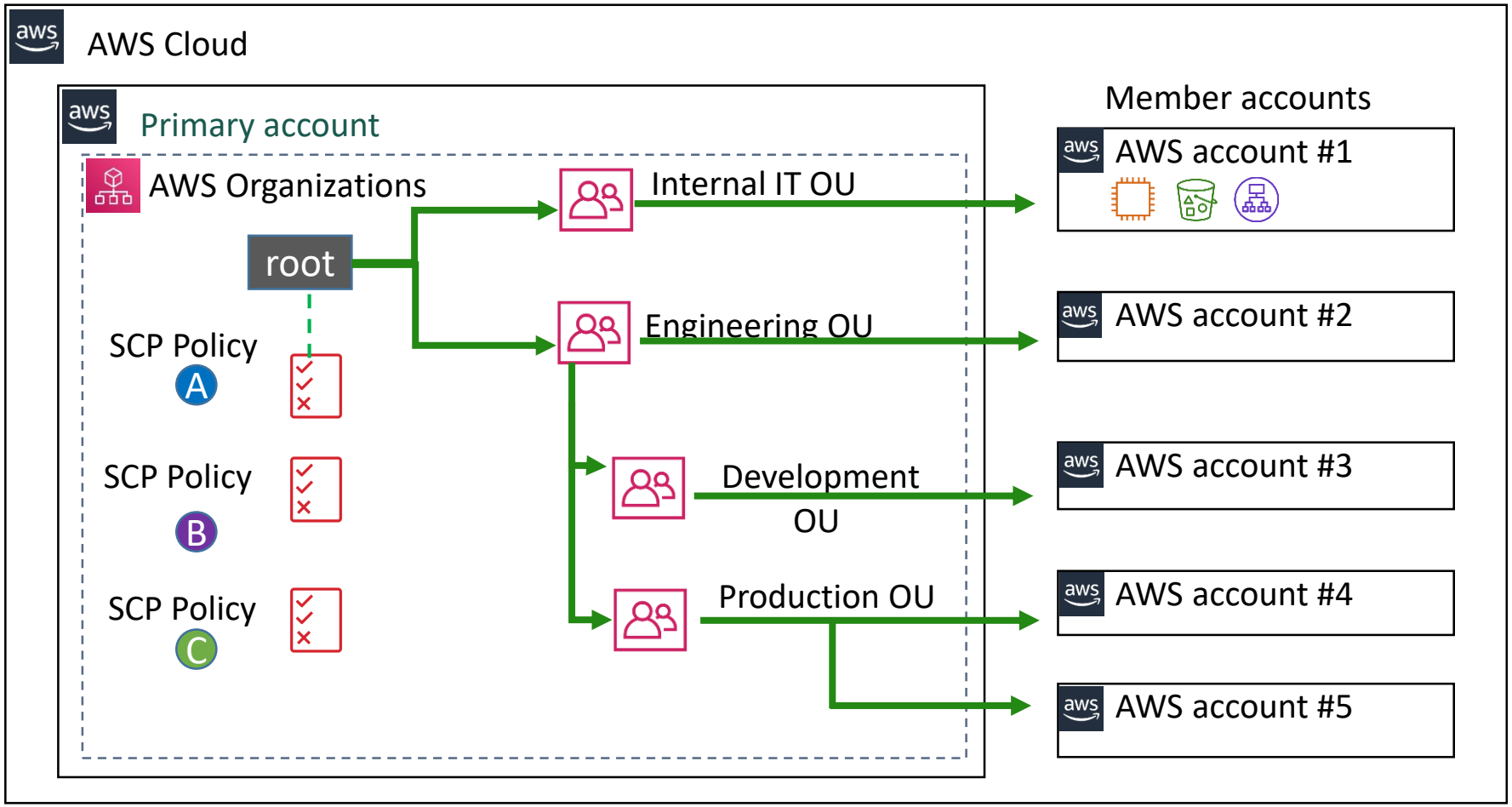


AWS Organizations

Creación de unidades organizativas

En la cuenta primaria de AWS Organizations:

1. Crear una jerarquía de unidades organizativas (OUs).
2. Asignar cuentas a las OU, como cuentas miembro.
3. Definir SCP que aplican restricciones a los permisos de cuentas específicas.

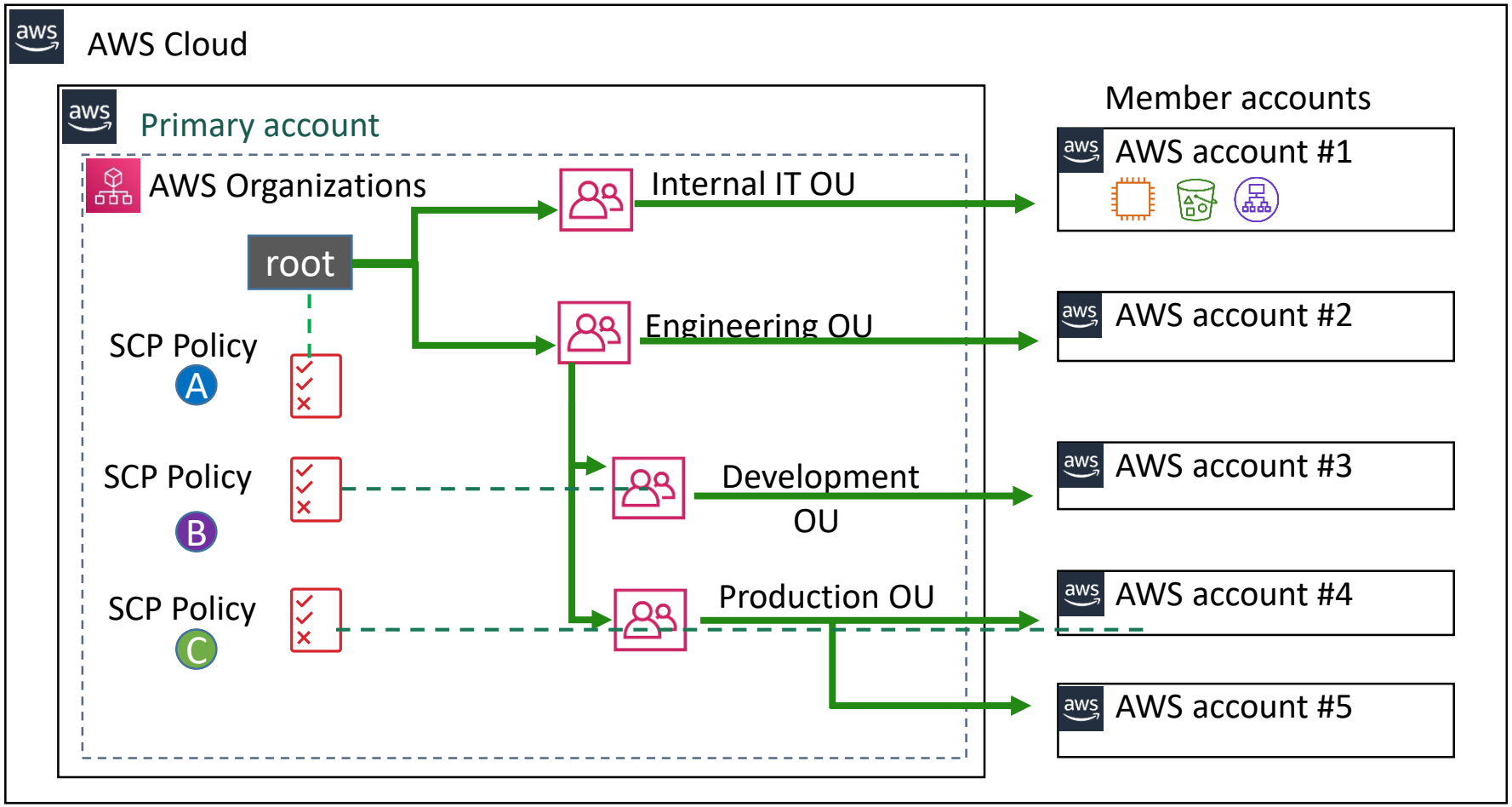


AWS Organizations

Creación de unidades organizativas

En la cuenta primaria de AWS Organizations:

1. Crear una jerarquía de unidades organizativas (OUs).
2. Asignar cuentas a las OU, como cuentas miembro.
3. Definir SCP que aplican restricciones a los permisos de cuentas específicas.
4. Asociar la SPCs a root, a las OUs o directamente a las cuentas.



AWS Organizations

Uso de SCP

Control centralizado de los permisos máximos disponibles para todas las cuentas de la organización

Permite controlar qué servicios son accesibles a los usuarios de IAM en las cuentas miembros.

Define permisos que afectan a una cuenta completa.

Define “guardrails”, o establece límites, sobre las acciones que puede delegar un administrador de una cuenta a los usuarios de esa cuenta. Las políticas de IAM que se definen en cada cuenta siguen siendo aplicables.

Las SCP no pueden ser modificadas por los administradores locales.

Buena práctica

Es más simple definir políticas en una SCP y aplicarlas a múltiples cuentas, que replicar los permisos en las políticas de IAM de cada una de las cuentas.

AWS Organizations

Uso de SCP

UNIVERSIDAD AUSTRAL

Ejemplos

Bloquear el acceso a servicios o acciones específicas. Por ejemplo, denegar el acceso a que los usuarios deshabiliten AWS CloudTrail en cualquiera de las cuentas.

Establecer la obligatoriedad de etiquetar los recursos. Por ejemplo, prohibir que se lancen instancias de EC2 sin un tag específico.

Evitar que las cuentas se desvinculen de la organización.

Gestión de permisos de acceso

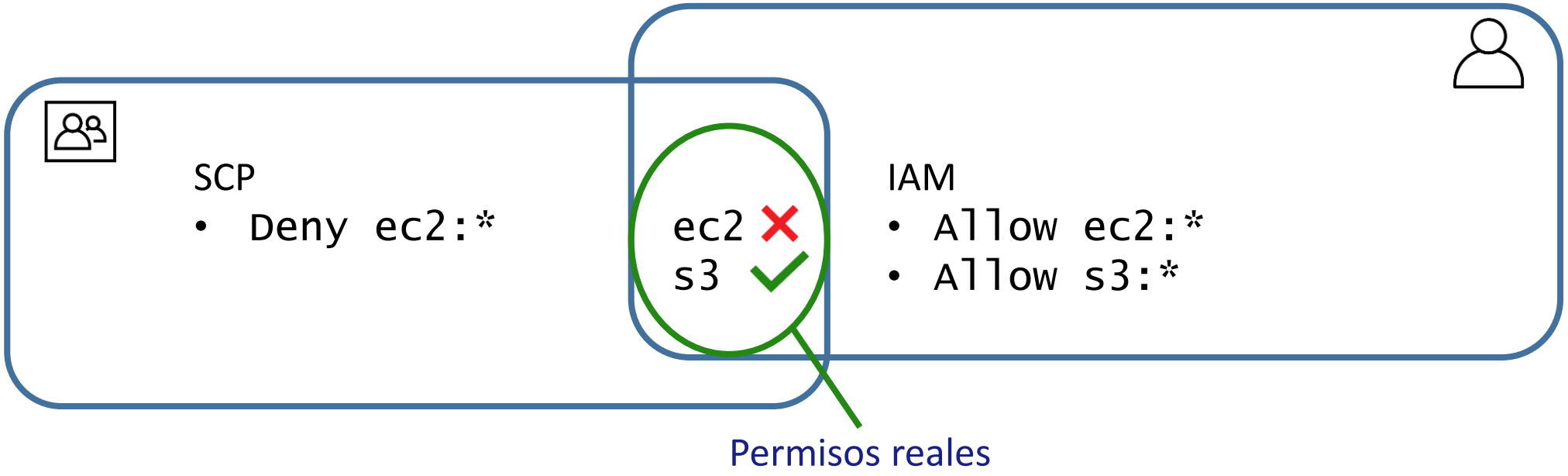
Uso de SCP - Ejemplos

UNIVERSIDAD AUSTRAL

```
{
    "Version": "2023-06-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [ "organizations:LeaveOrganization"],
            "Resource": "*"
        }
    ]
}
```

Gestión de permisos de acceso

SCP combinadas con permisos en IAM



Gestión de permisos de acceso

Permission boundaries

Este límite permite el acceso a S3, EC2 y Cloudwatch

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:*",
                "cloudwatch:*",
                "ec2:*"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM user

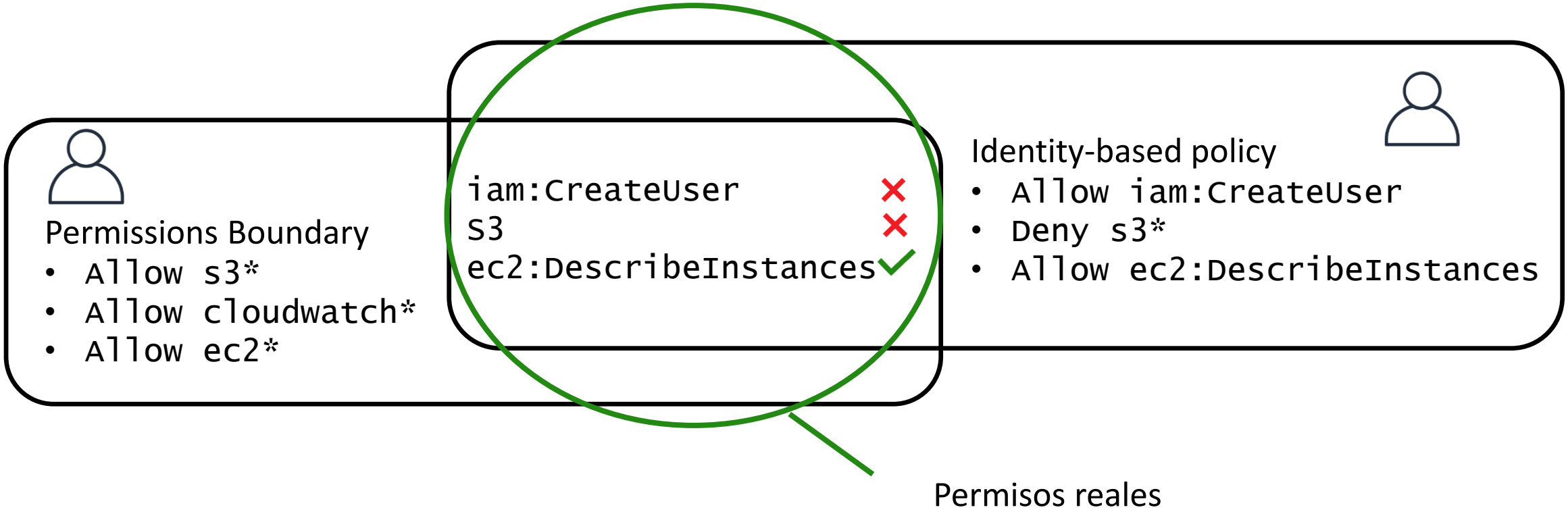
Esta política de IAM le da al usuario permiso para crear usuarios en IAM

```
{
    "Version": "2012-10-17",
    "Statement": {
      "Effect": "Allow",
      "Action":"iam:CreateUser",
      "Resource": "*"
    }
}
```

El límite no incluye el acceso a IAM, así que la política de identidades no podrá asignar al usuario el permiso iam:CreateUser.

AWS Organizations

Los permisos deben asignarse en ambas políticas



Gestión de permisos de acceso

Combinación de políticas

SCP asociada a la OU "Test"
- `Deny ec2*`
- `Deny sqs*`

Política IAM basada en identidades
- `Allow ec2:DescribeInstances`
- `Allow kms*`
- `Allow s3*`
- `Allow sqs:SendMessage`

Permission boundary
- `Allow s3*`
- `Allow sqs*`

IAM user in test OU

Recurso o acceso	¿Puede?	¿Por qué?
Describir las instancias de EC2	No	La SCP deniega el acceso a EC2. Esto prevalence sobre la política IAM
AWS Key Management Service (AWS KMS)	No	No está denegado explícitamente, pero el servicio no está incluido en el *permission boundary.*
Amazon S3	Yes	S3 está dentro del *permission boundary* y no está denegado explícitamente en la SCP. La política IAM asigna acceso al recurso.
Mandar un mensaje de Amazon SQS	No	El *deny* explícito en la SCP tiene prioridad sobre los otros dos permisos.

Gestión de permisos de acceso

Combinación de políticas

Permission boundaries	SCP organizacionales
Aplica a una entidad de IAM (rol o usuario)	Aplica a todos los miembros de una organización
Define los máximos permisos que se le podrían asignar a esa entidad	Define los máximos permisos que podrían asignarse en una organización, una OU o una cuenta dentro de la organización.
No asignan permisos	No asignan permisos
Se usan para definir los recursos habilitados para un usuario o rol	Se suelen usar para denegar el acceso a un conjunto de recursos
Ejemplo: permitir que el rol “Dev” acceda a EC2, S3 y CloudWatch. Resultado: el rol de desarrollador solo puede acceder a esos servicios, con independencia del resto de los permisos que tenga.	Ej: Denegar el acceso a RDS a todos los miembros de la OU “Internal IT” Resultado: todos los miembros de esa OU tendrán prohibido el acceso a RDS, aunque otras políticas les den permisos.

AWS Control Tower

AWS Control Tower

Facilita la implementación y la gestión de un entorno multi-cuentas seguro dentro de AWS.

Permite:

- Automatizar la implementación de un entorno multi-cuenta que aplique el WAF.
- Gestionar las reglas de seguridad, operación y *compliance* de las cuentas.
- Brinda guías para gobernar el entorno de AWS a escala.

Múltiples cuentas en AWS

Resumen

Es frecuente encontrar organizaciones que crean múltiples cuentas de AWS y definen una VPC en cada una.

Se pueden agrupar cuentas para consolidar la facturación.

Este esquema permite separar distintos recursos y establecer controles de seguridad.

AWS Organizations permite consolidar múltiples cuentas de AWS para gestionarlas centralizadamente.

Las SCPs permiten establecer límites de permisos en el nivel de la organización.

Los *permissions boundaries* permiten definir límites para las entidades de IAM (usuarios y roles)

Los grupos o usuarios pueden tener múltiples políticas asociadas. Se aplica la más restrictiva.

Cifrado de datos en reposo

Seguridad de usuarios, aplicaciones y datos

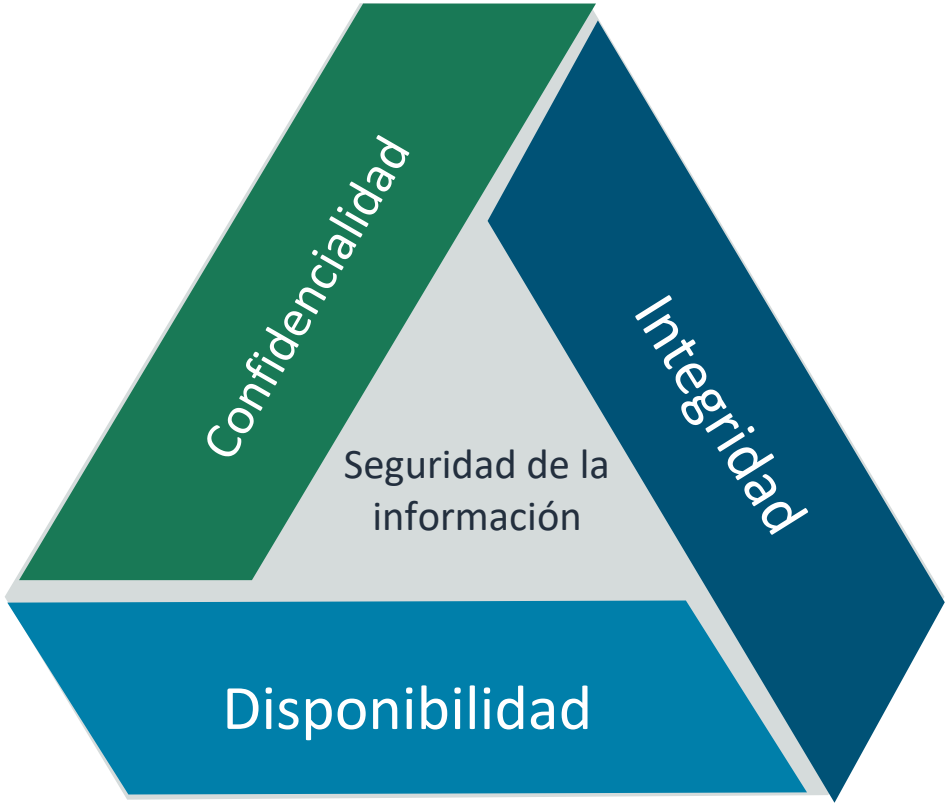
UNIVERSIDAD AUSTRAL

Protección de datos en reposo

Objetivos

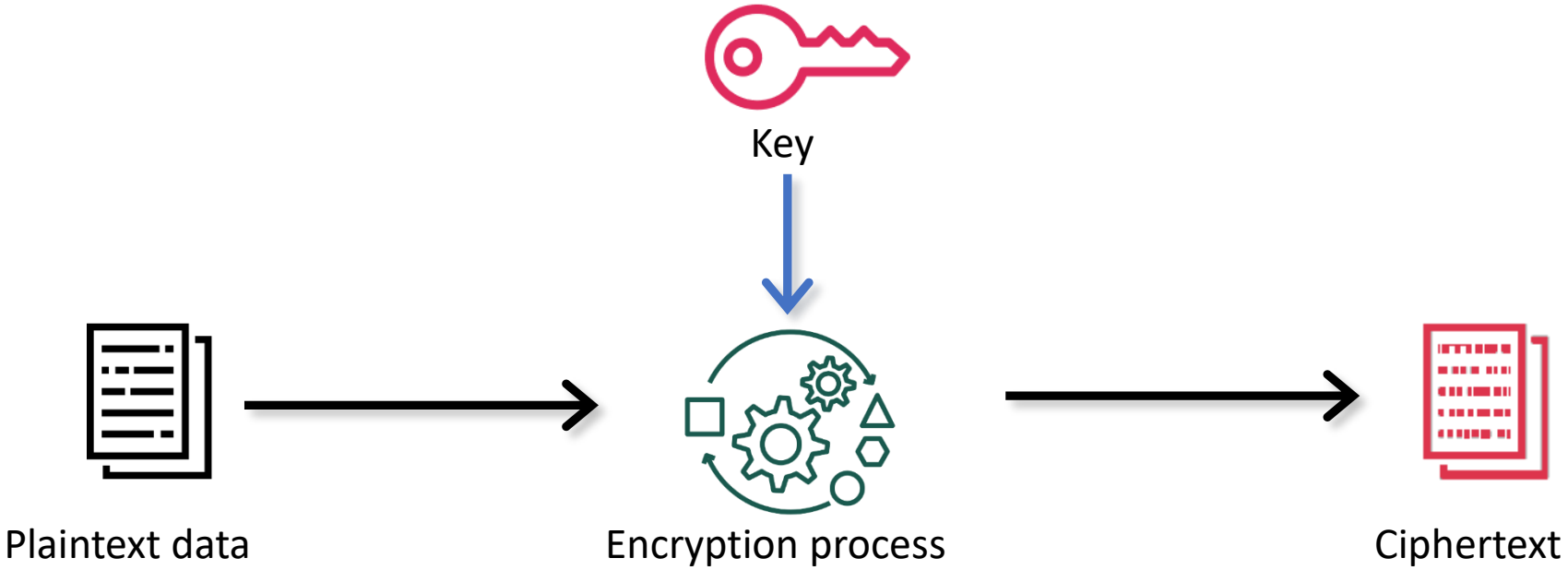
Asegurar la confidencialidad e integridad de la información

Brindar una capa extra de protección si un Sistema está comprometido



Cifrado de datos

Proceso



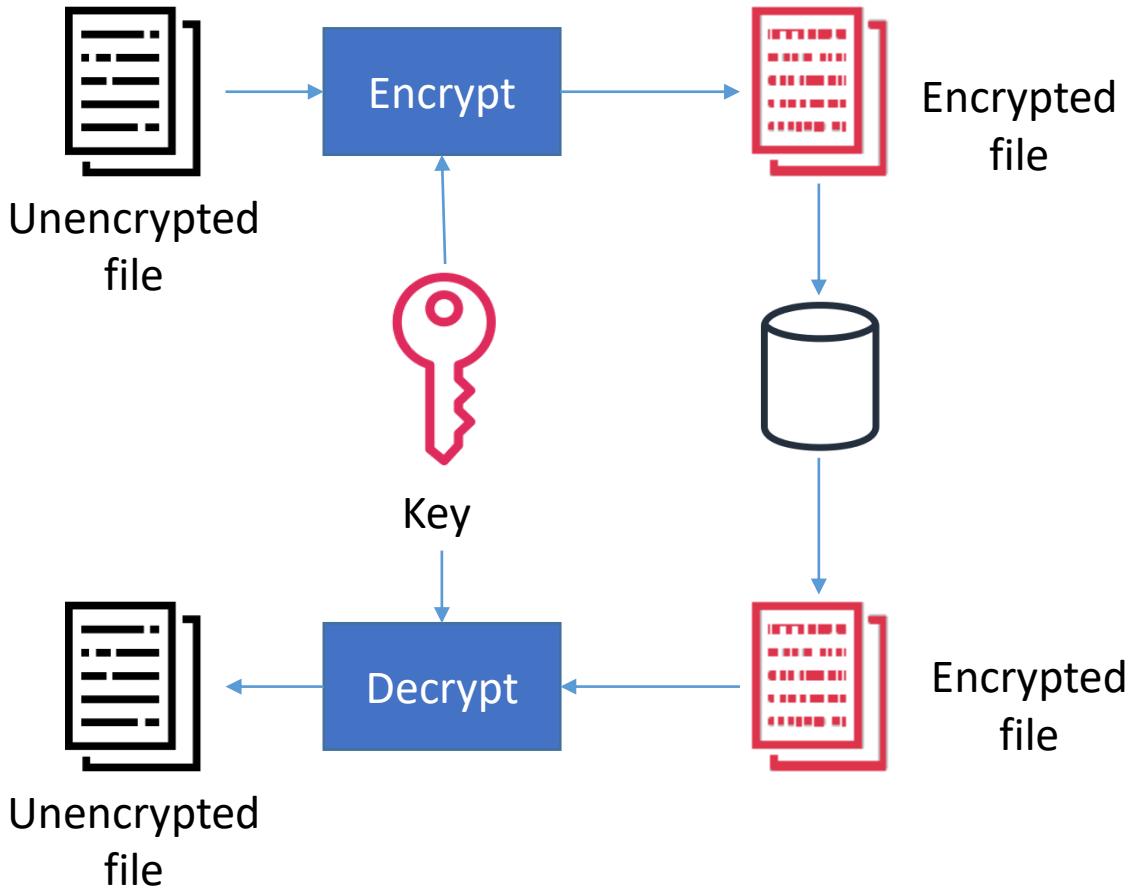
Cifrado de datos

Simétrico

Usa la misma clave para cifrar y descifrar los datos

Más rápido y eficiente para volúmenes grandes

Muy difundido y generalmente aceptado



Cifrado de datos

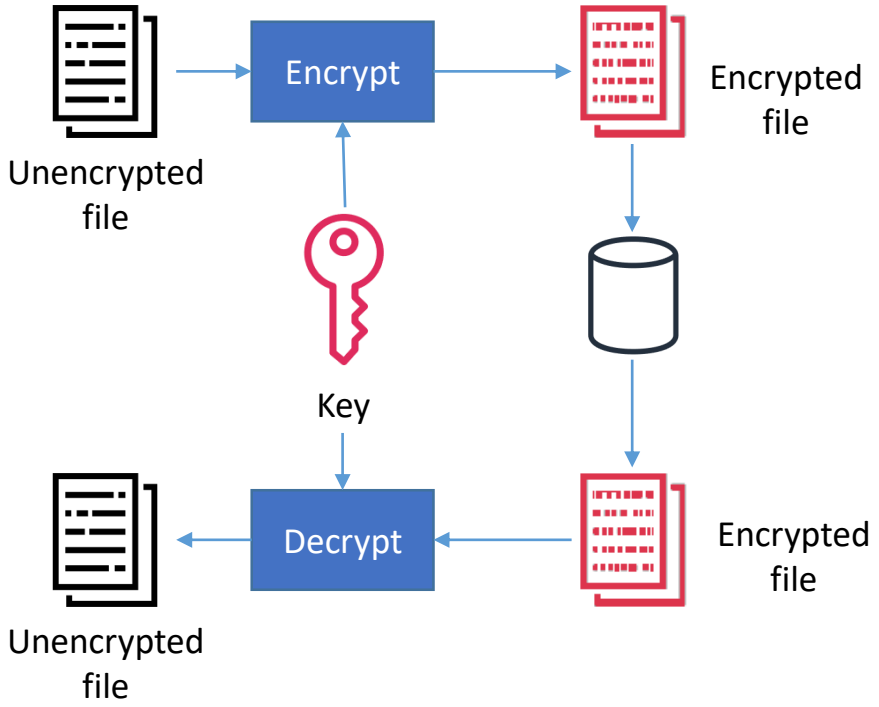
Simétrico

Casos de uso

Cuando se priorizan la velocidad y el costo.

Para cifrar grandes volúmenes.

Si los datos no salen de los límites de la organización.



Cifrado de datos

Asimétrico

Usa un par de claves (pública y privada).

Considerado más seguro.

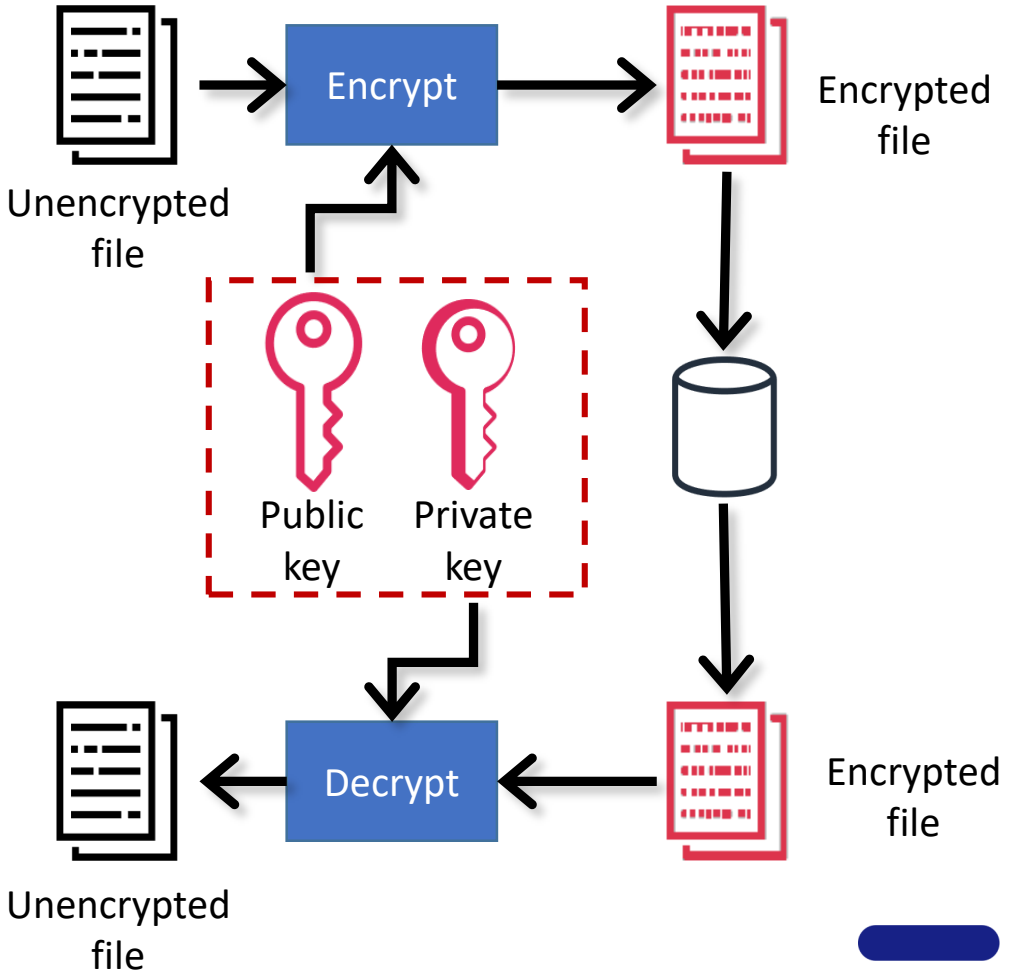
Más lento que el cifrado simétrico.

Casos de uso

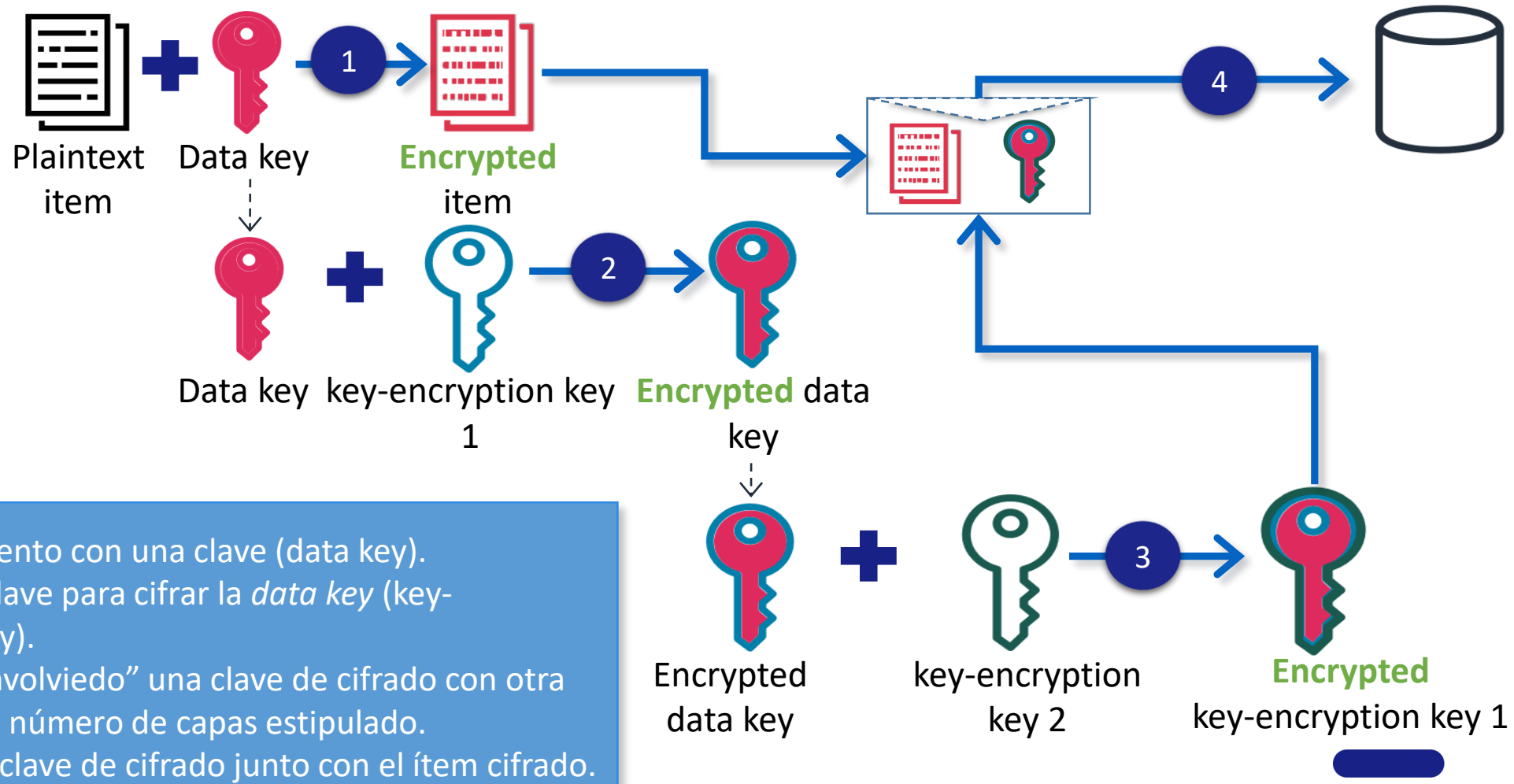
Cuando la información sale de la organización

No-repudio

Motivos regulatorios



Cifrado de datos



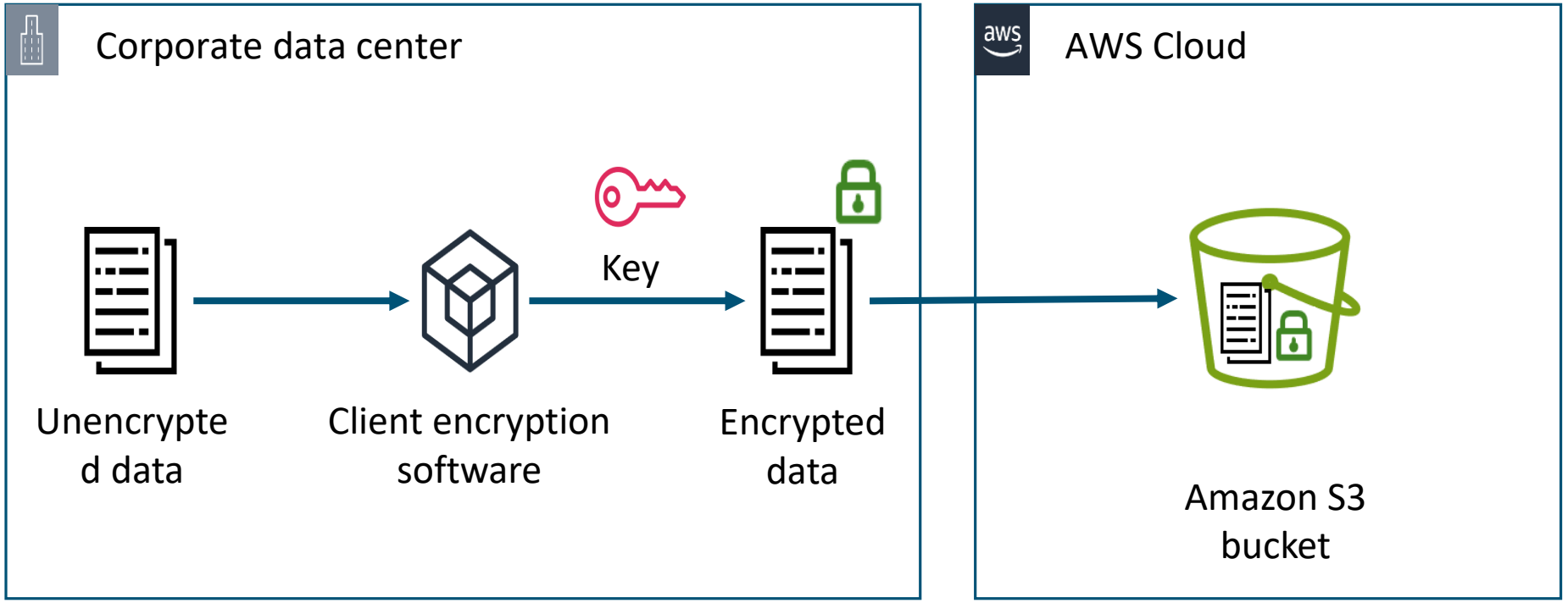
1. Cifrar el elemento con una clave (data key).
2. Utilizar otra clave para cifrar la *data key* (key-encryption key).
3. Continuar "envolviedo" una clave de cifrado con otra hasta llegar al número de capas estipulado.
4. Almacenar la clave de cifrado junto con el ítem cifrado.

Cifrado de datos en reposo

Cifrado del lado del cliente (CSE)	Cifrado del lado del servidor (SSE)
La aplicación cifra los datos antes de mandarlos a AWS.	AWS cifra los datos una vez que los recibe.
El cliente crea y administra sus propias claves de cifrado.	Los servicios cifran los datos antes de grabarlos en disco y los descifran de manera transparente en cada acceso.
Las claves y los algoritmos solo son conocidos por el cliente.	Las claves pueden ser administradas por AWS.

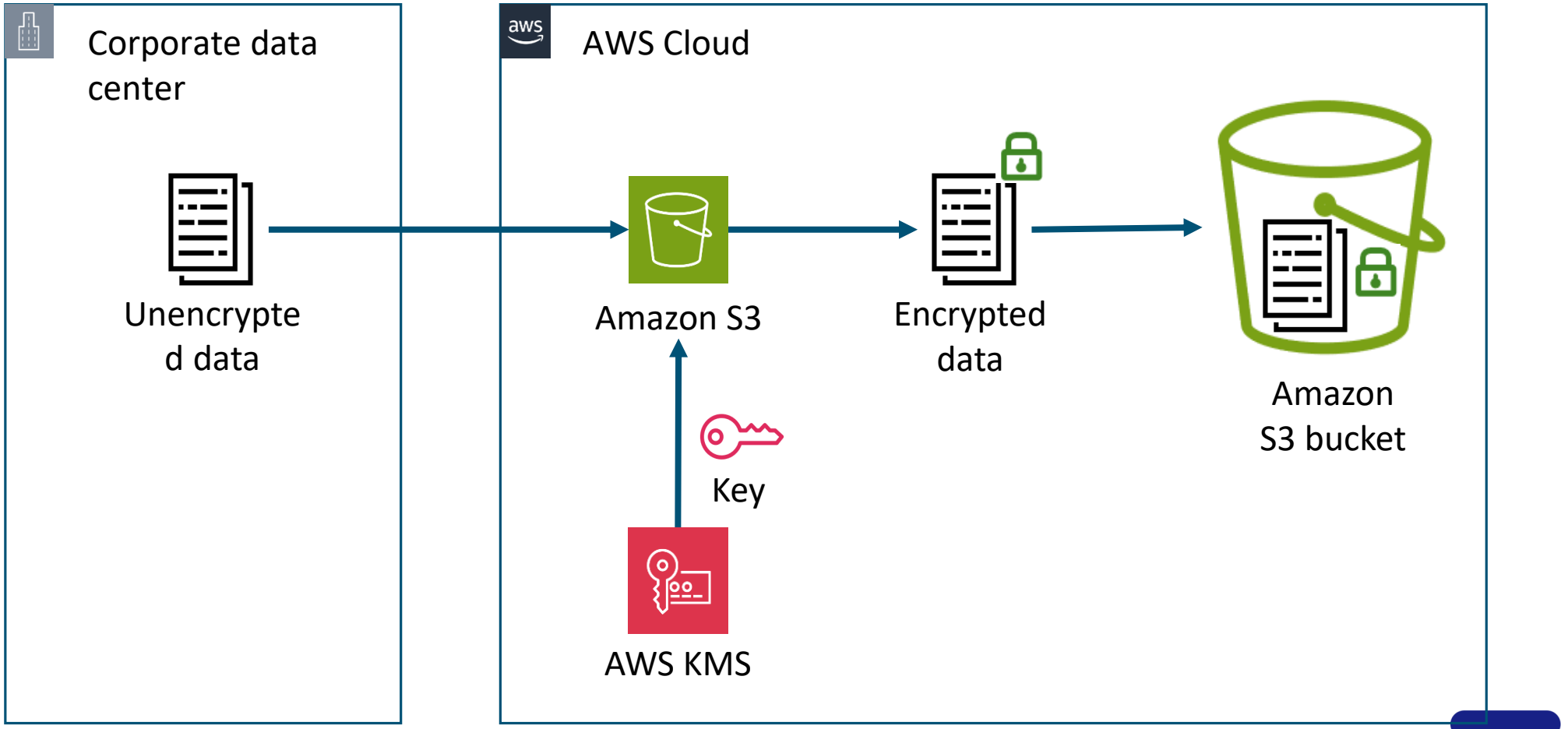
Cifrado de datos en reposo

Del lado del cliente



Cifrado de datos en reposo

Del lado del servidor



AWS Key Management System (KMS)

AWS KMS

Permite crear y administrar claves criptográficas.

Usa módulos de seguridad por hardware (HSM) para proteger las claves

Se integra con otros servicios de AWS

Permite establecer políticas de uso para determinar qué usuarios pueden emplear las claves.

AWS Key Management System (KMS)

UNIVERSIDAD AUSTRAL

Claves	Operaciones
Gestionadas por el cliente	Encrypt
Gestionadas por KMS	Decrypt
Data key (symmetric)	GenerateDataKey
Data key pair (asymmetric)	GenerateDataKeyPair

AWS Key Management System (KMS)

Integraciones

Amazon Simple Storage Service (Amazon S3)

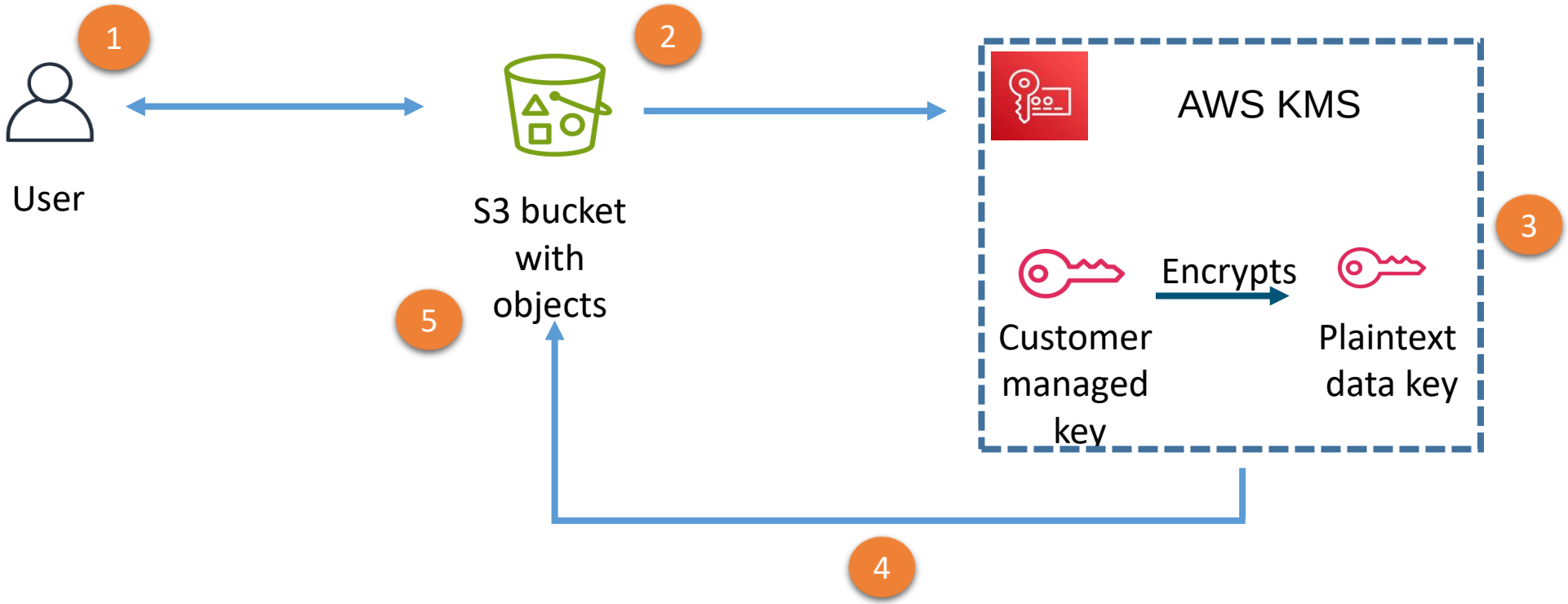
Amazon Elastic Block Store (Amazon EBS)

Importante

Los servicios integrados con AWS KMS solamente usan claves simétricas.

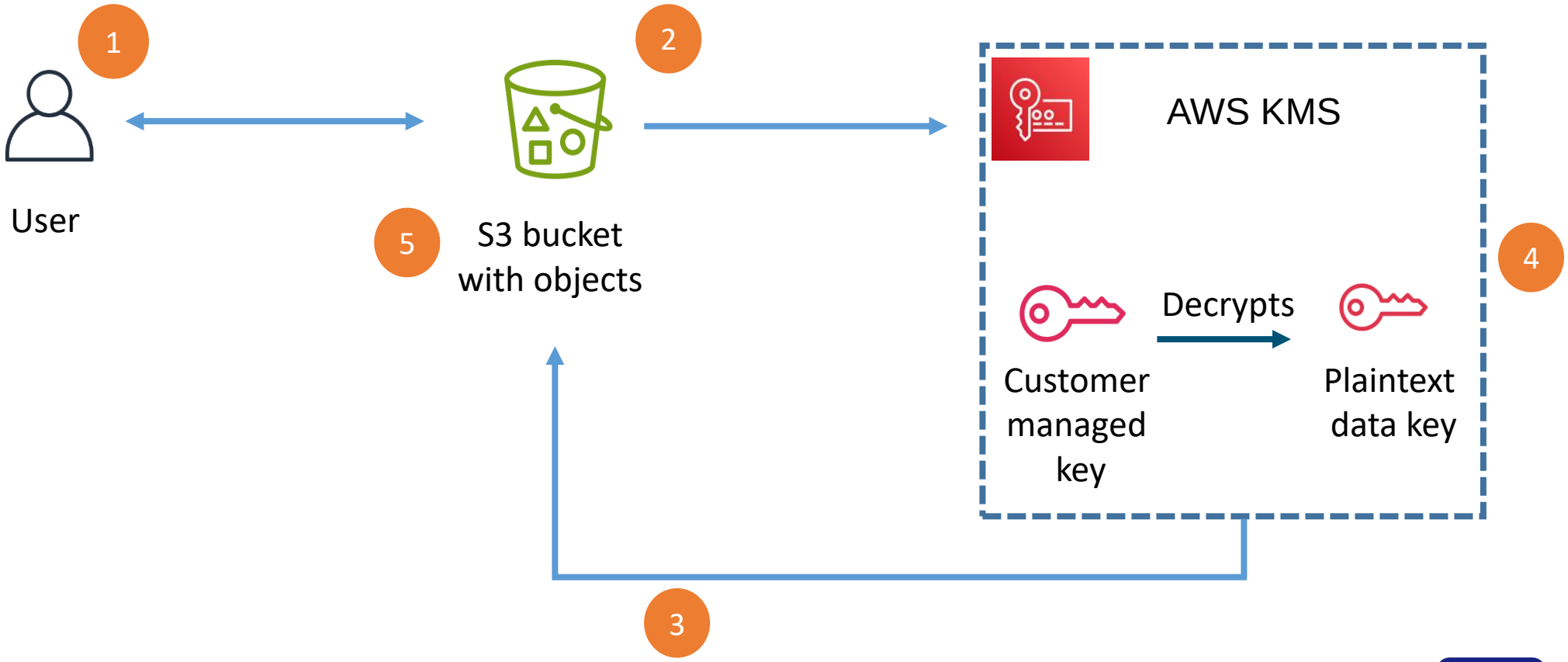
AWS Key Management System (KMS)

Ejemplo de cifrado con S3



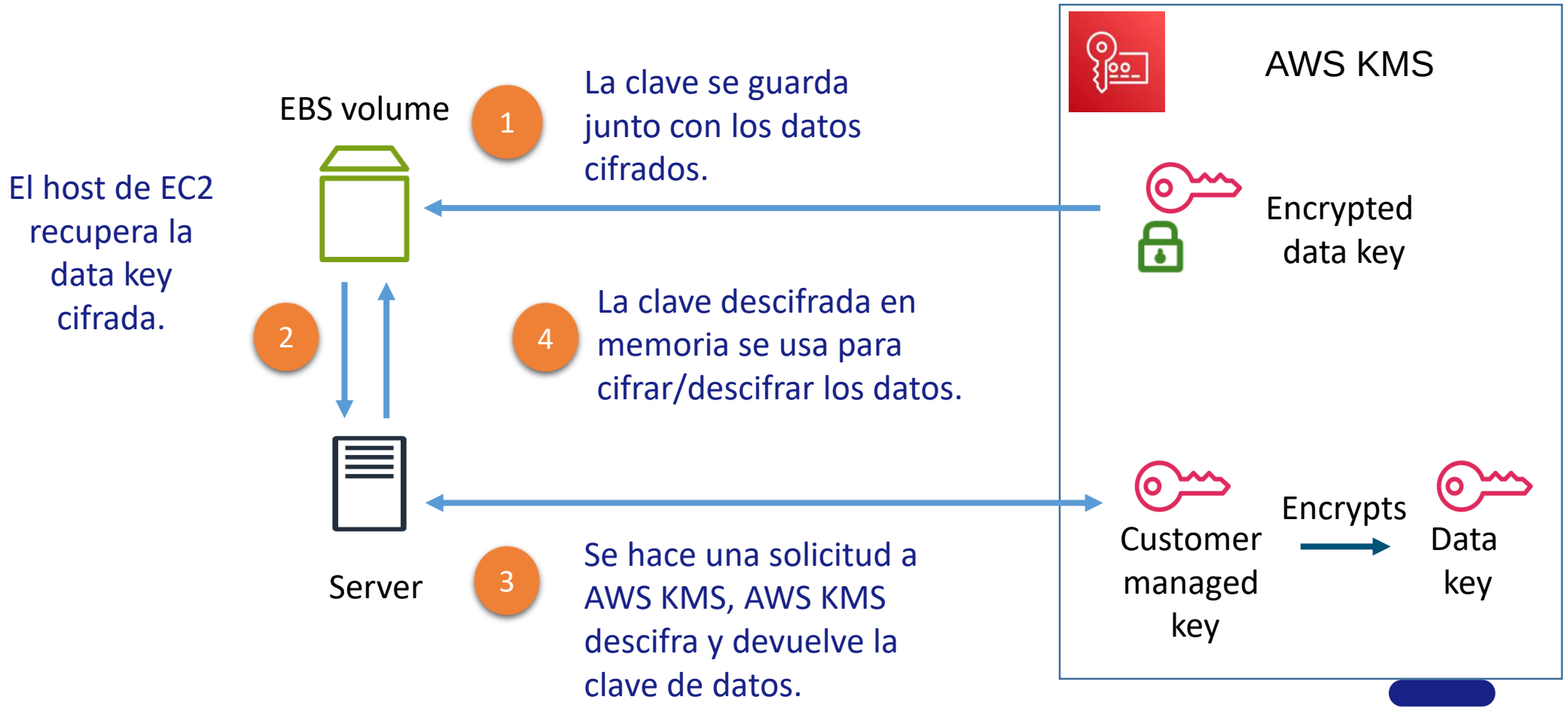
AWS Key Management System (KMS)

Ejemplo de descifrado con S3



AWS Key Management System (KMS)

Ejemplo de integración con Amazon EBS



Múltiples cuentas en AWS

Resumen

El cifrado de datos en reposo reduce los riesgos de compromiso de datos, incluso cuando un *endpoint* está comprometido.

El cifrado simétrico usa la misma clave para cifrar y descifrar los datos.

El cifrado asimétrico usa un par de claves: la pública para cifrar, la privada para descifrar.

El ensobrado es una práctica de cifrar texto plano con una clave de datos y luego cifrar la clave de datos con otra clave.

Con cifrado del lado del cliente, la aplicación cifra los datos localmente antes de enviarlos a AWS. La propia aplicación tiene que descifrarlos una vez que los recibe.

El cifrado del lado del servidor consiste en que la aplicación o el servicio que recibe los datos los cifra antes de grabarlos y los descifra cuando los recupera.

Las claves AWS KMS son el principal recurso de AWS KMS. Se usan para cifrar y descifrar datos.

Servicios de seguridad de AWS

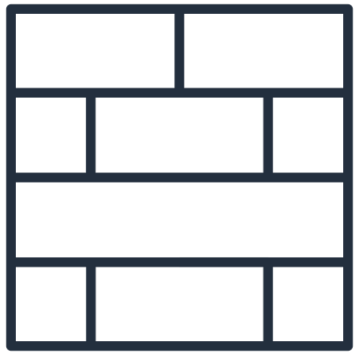
Seguridad de usuarios, aplicaciones y datos

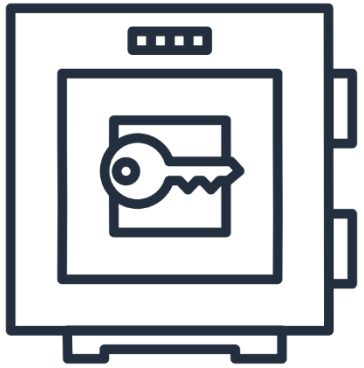
UNIVERSIDAD AUSTRAL

Servicios de AWS para seguridad

Categoría	Descripción	Ejemplos
Gestión de identidades y accesos	Administrar identidades, recursos y permisos.	AWS Identity and Access Management (IAM) AWS IAM Identity Center Amazon Cognito AWS Organizations
Detección y respuesta	Mejorar la postura de seguridad y aplicar las operaciones de seguridad en un entorno completo de AWS.	AWS CloudTrail Amazon Detective Amazon Inspector AWS Security Hub
Protección de redes y aplicaciones	Aplicar políticas de seguridad granulares y puntos de control de red en toda la organización.	AWS Network Firewall AWS Shield AWS WAF
Protección de datos	Proteger los datos, las cuentas y las cargas de trabajo para evitar accesos no autorizados.	AWS Key Management System (AWS KMS) AWS Secrets Manager Amazon Macie
Compliance	Obtener una visión general del cumplimiento y monitorear continuamente chequeos automáticos basados en buenas prácticas de AWS y estándares de la industria..	AWS Artifact AWS Audit Manager

Servicios de AWS para seguridad





Defender el perímetro	Proteger los datos	Detectar y responder a amenazas
AWS WAF and AWS Shield	Amazon Macie	Amazon Inspector
		Amazon Detective
		AWS Security Hub

AWS WAF

Descripción	Características	Ejemplos
Es un Web Application Firewall que permite monitorear las solicitudes de HTTP y HTTPS que se reenvían a los recursos protegidos de la aplicación del cliente.	Se pueden usar reglas administradas o gestionadas. Se pueden permitir o bloquear requerimientos en función de diversos criterios (dirección IP, país de origen, encabezados). AWS Shield permite reducir el impacto de ataques de (DDoS).	Bloquear los requerimientos que no tienen el encabezado User-Agent de HTTP. Detectar y administra intentos maliciosos de creación de cuentas en la página de sign-up de la aplicación.

AWS Macie

Descripción	Características	Ejemplos
Es servicio de seguridad que descubre los datos sensibles almacenados en Amazon S3. Aplica machine learning, provee visibilidad de los riesgos sobre los daos y permite protegerse de esos riesgos.	Automatizar el descubrimiento de datos Permite crear y ejecutar *jobs* de descubrimiento de datos Se pueden usar etiquetas estandarizadas o personalizadas. Permite revisar, analizar y gestionar los hallazgos.	*Macie* permite identificar datos sensibles cuando se los migra a Amazon S3. Esto permite notificar a un administrador y decidir si se permite que siga copiando datos a S3.

AWS Inspector

Descripción	Características	Ejemplos
Servicio de gestión de vulnerabilidades que escanea las cargas de trabajo para identificar vulnerabilidades y exposiciones no deseadas a la red. Detecta y escanea instancias de EC2, contenedores de ECR y funciones lambda.	Se puede usar AWS Organizations para centralizar la administración. Inspector Risk score permite evaluar vulnerabilidades El dashboard de Amazon Inspector permite identificar hallazgos de alto impacto. Los hallazgos se pueden publicar en Amazon EventBridge para integrarse con otros servicios	Escanear las AMI de EC2 y generar los reportes de hallazgos en AWS Inspector para asegurar que se actualice antes de la implementación.

AWS Detective

Descripción	Características	Ejemplos
Ayuda a analizar, investigar e identificar la causa raíz de los hallazgos o de las actividades sospechosas. Recolecta automáticamente datos de log de distintas fuentes. Usa *machine learning,* análisis estadístico y teoría de grafos para generar visualizaciones que mejoran las capacidades de investigación	Permite visualizar los datos en modo de grafo que resumen la información de contexto y datos de comportamiento. Validar, comparar y correlacionar los datos para hacer análisis Obtener y analizar automáticamente los datos relevantes de todas las cuentas habilitadas.	Investigación de incidente vinculado con una entidad IAM.

AWS Security Hub

Descripción	Características	Ejemplos
Recolecta datos de seguridad de todas las cuentas, servicios de AWS, y de productos de terceros soportados. Permite analizar las tendencias de seguridad e identificar problemas de seguridad de alta prioridad.	Soporta múltiples estándares de seguridad Recibe hallazgos de otros servicios, como Amazon Macie y Amazon Inspector. Se pueden aplicar reglas de automatización para actualizar automáticamente los hallazgos críticos.	Priorizar los esfuerzos de respuesta y remediación de los equipos de seguridad mediante la búsqueda, correlación y agregación de hallazgos de distintas cuentas y recursos.

AWS Trusted Advisor

Trusted Advisor

Genera recomendaciones basadas en 5 categorías de las buenas prácticas.

Evalúa la cuenta para sugerir mejoras y optimizaciones para los recursos.

Se accede desde la consola de AWS y está disponible para todos los niveles de soporte.

La consola de Trusted Advisor permite ver los controles y los hallazgos de seguridad si se habilita Security Hub.

Servicios de seguridad de AWS

Resumen

Los servicios de seguridad de AWS permiten implementar una estrategia de defensa en profundidad para las cargas de trabajo de AWS.

Los servicios de seguridad de AWS incluyen:

- AWS WAF. Monitoreo de requerimientos web
- Amazon Macie. Identificación de datos sensibles en Amazon S3
- Amazon Inspector. Identificación de vulnerabilidades en instancias EC2, contenedores y funciones lambda
- Amazon Detective. Análisis, investigación e identificación de la causa raíz de actividades sospechosas o hallazgos de seguridad
- AWS Security Hub. Consolidar automáticamente los hallazgos y monitorear la postura de seguridad respecto de las buenas prácticas.

AWS Trusted Advisor inspecciona el entorno de AWS y hace recomendaciones para cerrar los gaps de seguridad.

Módulo 9

Resumen

Uso de AWS Identity and Access Management (IAM) para administrar permisos.

Federación de identidades para aumentar la seguridad.

Describir cómo administrar múltiples cuentas de AWS.

Reconocer cómo contribuyen las *service control policies* (SCPs) a la seguridad.

Cifrar datos en reposo con AWS KMS.

Identificar los servicios de seguridad de AWS apropiados para cada caso.

Ejemplo de pregunta

A company has two separate AWS accounts for testing workloads: one for performance testing and the other for integration testing. The accounts are grouped into an AWS Organizations organizational unit, and each account has a Tester role defined. The company wants to enforce the following security rules on users in the Tester role (testers) in both accounts:

- Testers can only access the Amazon EC2 and Amazon RDS services.
- Testers can only start and stop EC2 instances.
- Testers have read and write permissions to RDS databases.

Which tasks does a system administrator need to perform to implement these requirements? (Select TWO).

A Create a service control policy (SCP) to deny all actions on all AWS services except for the Amazon EC2 and Amazon RDS services, and attach it to the Tester role in both accounts.

B Create an AWS Identity and Access Management (IAM) policy with the required EC2 and RDS permissions, and attach it to the organizational unit.

C Create a service control policy (SCP) to deny all actions on all AWS services except for the Amazon EC2 and Amazon RDS services, and attach it to the organizational unit.

D Create an AWS Identity and Access Management (IAM) policy in both accounts with the required EC2 and RDS permissions, and attach it to the Tester role.

E Create a service control policy (SCP) in both accounts with the required EC2 and RDS permissions, and attach it to the Tester role.

Ejemplo de pregunta

A company has two separate AWS accounts for testing workloads: one for performance testing and the other for integration testing. The accounts are grouped into an AWS Organizations organizational unit, and each account has a Tester role defined. The company wants to enforce the following security rules on users in the Tester role (testers) in both accounts:

- Testers can only access the Amazon EC2 and Amazon RDS services.
- Testers can only start and stop EC2 instances.
- Testers have read and write permissions to RDS databases.

Which tasks does a system administrator need to perform to implement these requirements? (Select TWO).

A Create a service control policy (SCP) to deny all actions on all AWS services except for the Amazon EC2 and Amazon RDS services, and attach it to the Tester role in both accounts.

B Create an AWS Identity and Access Management (IAM) policy with the required EC2 and RDS permissions, and attach it to the organizational unit.

C Create a service control policy (SCP) to deny all actions on all AWS services except for the Amazon EC2 and Amazon RDS services, and attach it to the organizational unit.

D Create an AWS Identity and Access Management (IAM) policy in both accounts with the required EC2 and RDS permissions, and attach it to the Tester role.

E Create a service control policy (SCP) in both accounts with the required EC2 and RDS permissions, and attach it to the Tester role.

Muchas gracias.

www.austral.edu.ar

UNIVERSIDAD AUSTRAL