COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 5

Varias cuentas

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

¿Una cuenta o varias cuentas?

Dos patrones de arquitectura

- La mayoría de las organizaciones optan por crear varias cuentas

Ventajas de varias cuentas

- Aislar unidades de negocio o departamentos
- Aislar entornos de desarrollo, prueba y producción
- Aislar datos de auditoría, datos de recuperación
- Cuentas independientes para cargas de trabajo reguladas
- Es más fácil activar alertas de costos para el consumo de cada unidad de negocio

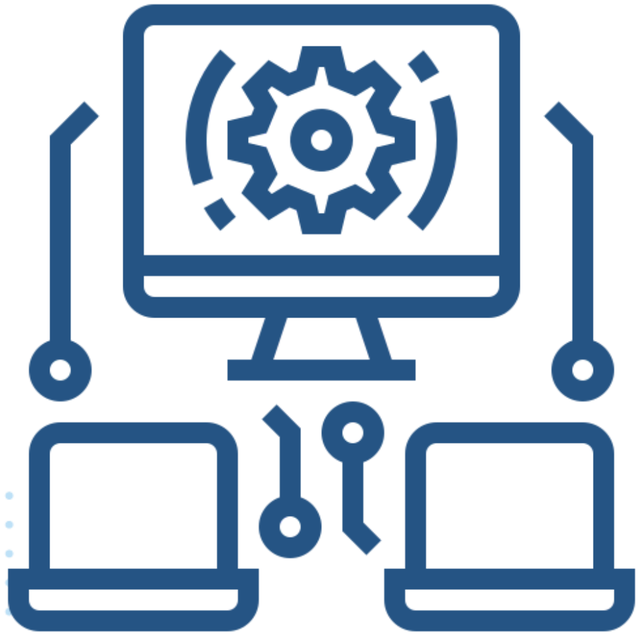
Múltiples VPC en una sola cuenta
Patrón de arquitectura

Varias cuentas, un VPC en cada cuenta
Patrón de arquitectura

Cuando utiliza AWS para brindar soporte a los diferentes equipos y departamentos de una organización, puede elegir entre dos patrones de arquitectura generales para aislar y separar los recursos que utiliza cada equipo.

El primer patrón consiste en definir varias nubes privadas virtuales (VPC) en una cuenta única de AWS. Si prefiere una administración de seguridad de la información centralizada con una sobrecarga mínima, puede optar por utilizar una cuenta única de AWS.

El segundo patrón consiste en crear varias cuentas de AWS y definir una VPC en cada una de ellas. En la práctica, las organizaciones grandes y pequeñas tienden a crear varias cuentas para sus organizaciones. Por ejemplo, podrían crear cuentas individuales para varias unidades de negocio. También podrían crear cuentas independientes para sus recursos de desarrollo, prueba y producción.



Cuando los clientes utilizan cuentas de AWS separadas (generalmente con facturación unificada) para los recursos de desarrollo y producción, les permite separar claramente diferentes tipos de recursos. También puede proporcionar algunos beneficios de seguridad.

Alternativamente, si su empresa mantiene entornos separados para producción, desarrollo y pruebas, puede configurar tres cuentas de AWS y tener una cuenta para cada entorno. Además, si tiene varios departamentos autónomos, también puede crear cuentas de AWS independientes para cada parte autónoma de la organización.

Cuando utiliza varias cuentas, una estrategia más eficiente es crear una cuenta de AWS única para los recursos comunes del proyecto. Los recursos comunes pueden incluir servicios del Sistema de nombres de dominio (DNS), Microsoft Active Directory y sistemas de administración de contenidos (CMS). También podría separar cuentas para los proyectos o departamentos autónomos. Esta estrategia le permite asignar permisos y políticas para cada departamento o cuenta de proyecto, y otorgar acceso a recursos entre cuentas.

Desafíos para administrar varias cuentas

Administración de seguridad entre cuenta
- Replicación de políticas de IAM

Creación de cuentas nuevas
- Implica muchos procesos manuales

Consolidación de facturación

Se necesita gobernanza centralizada para garantizar la coherencia

Aunque la mayoría de las organizaciones optan por utilizar varias cuentas de AWS, esa elección conlleva algunos desafíos.
Primero, debe determinar cómo administrar eficazmente la seguridad en todas sus cuentas. Si replica las políticas de IAM que definió en todas las cuentas para garantizar la coherencia, podría implicar automatización personalizada, esfuerzo manual o ambos.

Además, es posible que se le solicite constantemente que cree más cuentas. Se necesita tiempo para crear estas cuentas manualmente. También puede resultar difícil realizar un seguimiento de todas las cuentas y el propósito de cada cuenta.

También puede ser un desafío determinar a qué centro de costos de la organización se le debe facturar, por qué recursos y en qué cuentas. Y, por último, es posible que también desee lograr la gobernanza centralizada que se necesita para garantizar la coherencia.

Administra varias cuentas con AWS Organizations

Administrar y aplicar políticas de manera centralizada entre varias cuentas de AWS.

- Administración de cuentas basadas en grupos
- Acceso a los servicios de AWS basado en políticas
- Administración y creación automatizada de cuentas
- Facturación unificada
- Basado en API

AWS ofrece un servicio que está diseñado para abordar estos desafíos de administración.

AWS Organizations es un servicio administrado para la administración de cuentas. Una organización es una entidad que se crea para integrar, ver de forma centralizada y administrar todas las cuentas de AWS. Usted determina la funcionalidad de una organización a través del conjunto de funciones que habilita.

Organizations lo ayuda a administrar políticas para varias cuentas de AWS. Puede utilizar el servicio para crear grupos de cuentas. Para asegurarse de que se aplican las políticas correctas en toda la cuenta, adjunte políticas a un grupo.

Puede crear grupos de cuentas AWS y luego aplicar diferentes políticas a cada grupo.

Las API de Organizations pueden crear nuevas cuentas mediante programación y agregarlas a un grupo. Las políticas que se adjuntan al grupo se aplican de manera automática a la nueva cuenta.

También puede configurar un único método de pago para todas las cuentas de AWS de su empresa mediante la facturación unificada. Con la facturación unificada, puede ver una vista combinada de los cargos en los que incurren todas sus cuentas.

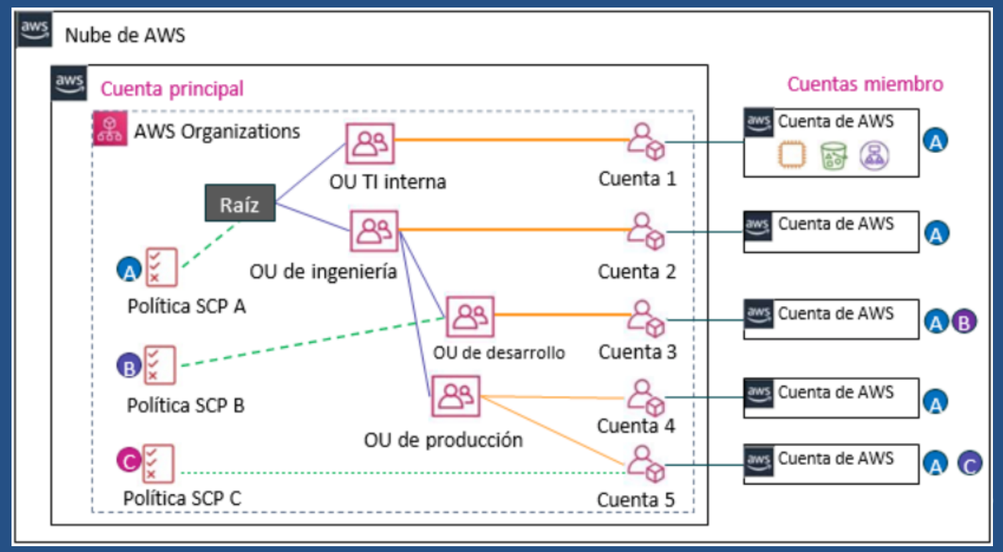
Finalmente, puede administrar el uso de los servicios de AWS a nivel de API. Por ejemplo, puede aplicar una política a un grupo de cuentas que solo permitirá a los usuarios de IAM de esas cuentas leer datos de buckets de S3.

AWS Organizatios: ilustradas

En la cuenta principal de AWS Organizations:

1. Crear una jerarquía de unidades organizativas (OU)
2. Asignar cuentas a OU como cuentas miembro
3. Definir políticas de control de servicios (SCP) que apliquen restricciones de permisos a cuentas miembro específicas
4. Adjuntar los SPC a la raíz, OU o cuentas

¿A qué cuentas se aplica cada SCP?



Este es un ejemplo de AWS organization. Se define dentro de una cuenta de AWS normal a la que se hace referencia en la diapositiva como la cuenta principal porque en ella se define la organización de AWS.

Cuando crea una organización en la cuenta principal, la organización crea automáticamente un contenedor principal que se denomina raíz. Debajo de cada raíz de la organización, puede definir unidades organizativas, que también se conocen como OU. Cada OU es un contenedor de cuentas miembro. Una OU también puede contener otras OU y esas OU pueden contener más cuentas. Esta función le permite crear una jerarquía en forma de árbol. Puede pensar en la raíz y OU como ramas que se extienden y terminan en cuentas, que son como las hojas de un árbol.

Para configurar controles de acceso entre cuentas, debe entonces definir políticas de control de servicios (SCP). Adjunte cada política al lugar adecuado en la jerarquía de OU y cuentas. La política se aleja de la raíz y afecta a todas las OU y cuentas debajo de ella.

Por lo tanto, si aplica una SCPa la raíz (como la Política A de SCP en el ejemplo), se aplicará a todas las OU y cuentas de la organización. Puede adjuntar la SCP a la raíz, a cualquier OU o una cuenta individual.

Recuerde que al igual que las políticas de IAM, las SCP solo otorgarán acceso si está permitido explícitamente y no está denegado explícitamente por cualquier otra SCP o política de IAM que se aplique al usuario. Por ejemplo, supongamos que la Política A de SCP, que se aplica a la raíz de la organización, establece más restricciones en un determinado servicio o conjunto de recursos que la Política C de SCP. Entonces, los usuarios en la Cuenta 5 están sujetos a los permisos más restrictivos establecidos por la Política A. Del mismo modo, si alguna política de IAM a nivel de cuenta individual deniega explícitamente cualquier acción para el usuario, estas políticas de IAM anulan cualquier permiso en las SCP que se otorgan a la cuenta.

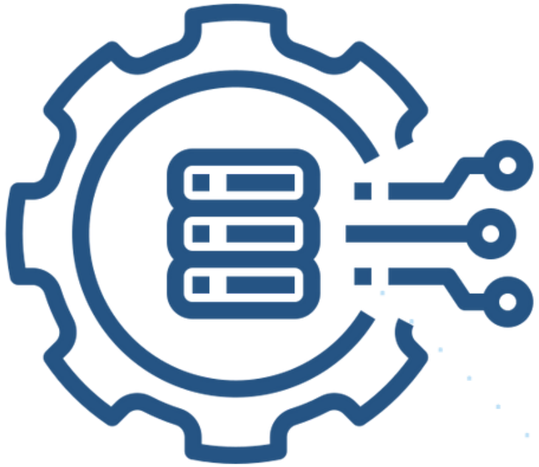
Ejemplos de usos de SCP

Características de las políticas de control de servicios (SCP)

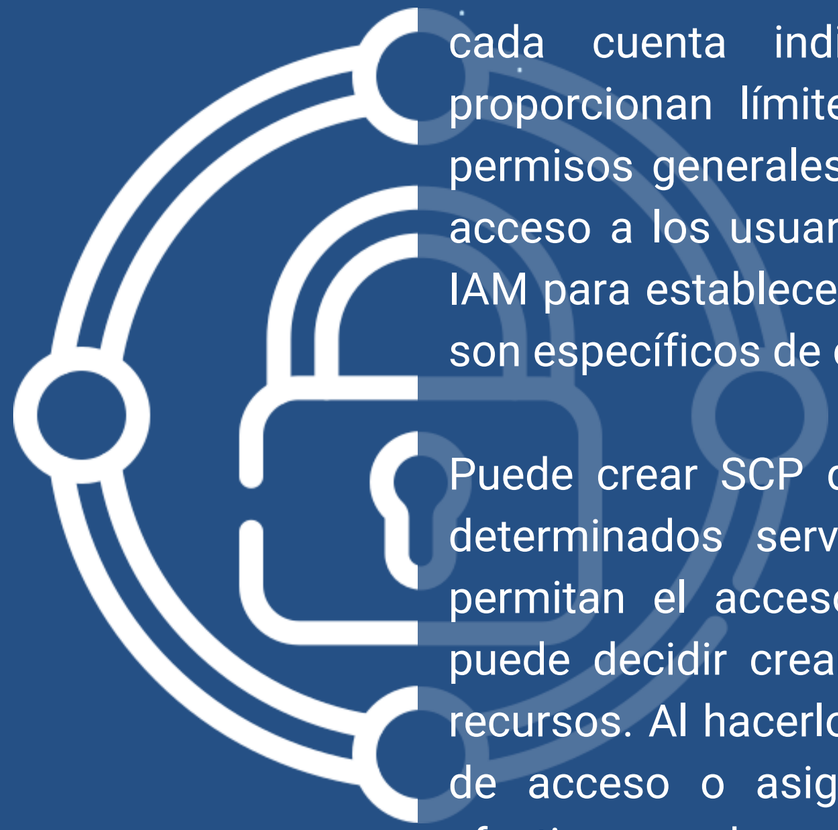
- Le permiten controlar a qué servicios pueden acceder los usuarios de IAM en cuentas miembro
- El administrador local no puede anular los SCP
- Las políticas de IAM definidas en cuentas individuales aún se aplican

Ejemplos de usos de SCP

- Crear una política que bloquee el acceso al servicio o acciones específicas
  - Ejemplo: impedir que los usuarios deshabiliten AWS CloudTrail en todas las cuentas miembro
- Crear un apoítica que permita el acceso completo a servicios específicos
  - Ejemplo: permitir el acceso completo a Amazon ec2 Y cloudWatch
- Crear una política que imponga el etiquetado de los recursos



Las políticas de control de servicios (SCP) le permiten controlar a qué servicios pueden acceder los usuarios de IAM en cuentas miembro. Supongamos que tiene políticas específicas que desea aplicar en varias cuentas. Es más fácil definir estas políticas en una SCP que replicar estas configuraciones de permisos en documentos de políticas de IAM en cada cuenta.



Se deben usar las SCP con políticas de IAM que se definen en cada cuenta individual. Puede pensar que las SCP proporcionan límites generales en torno a los servicios y permisos generales a los que se debe permitir o denegar el acceso a los usuarios. Luego, puede utilizar las políticas de IAM para establecer controles de acceso más detallados que son específicos de cuentas individuales.

Puede crear SCP que bloqueen (o denieguen) el acceso a determinados servicios. También puede definir SCP que permitan el acceso a determinados servicios. Finalmente, puede decidir crear un SCP que imponga el etiquetado de recursos. Al hacerlo, su estrategia de etiquetado para control de acceso o asignación de costos puede seguir siendo efectiva cuando se crean nuevos recursos en sus cuentas.

Entre los aprendizajes clave de esta lección de esta unidad, se incluyen los siguientes:

- Puede utilizar varias cuentas de AWS para aislar unidades de negocio, entornos de desarrollo y pruebas, cargas de trabajo reguladas y datos de auditoría
- AWS Organizations le permite configurar la creación automatizada de cuentas y la facturación unificada
- Puede configurar controles de acceso entre cuentas a través de políticas de control de servicios (SCP)

Ahora es el momento de revisar la unidad y concluir con una evaluación de conocimientos y una discusión sobre una pregunta del examen de certificación de práctica.

En resumen, en esta unidad aprendió a hacer lo siguiente:

- Explicar el propósito de los usuarios, los grupos y los roles de AWS Identity and Access Management (IAM).
- Describir cómo se permite la federación de usuarios dentro de una arquitectura para mejorar la seguridad
- Reconocer cómo las políticas de control de servicios (SCP) de AWS Organizations potencian la seguridad dentro de una arquitectura
- Describir cómo administrar varias cuentas de AWS
- Configurar usuarios de IAM

INICIO