Smart Data
DATA PARA TODOS

Arquitecto de Soluciones en aws

Gestión de la Identidad, Acceso y Gobernanza

Instructor: Jose Zamalloa

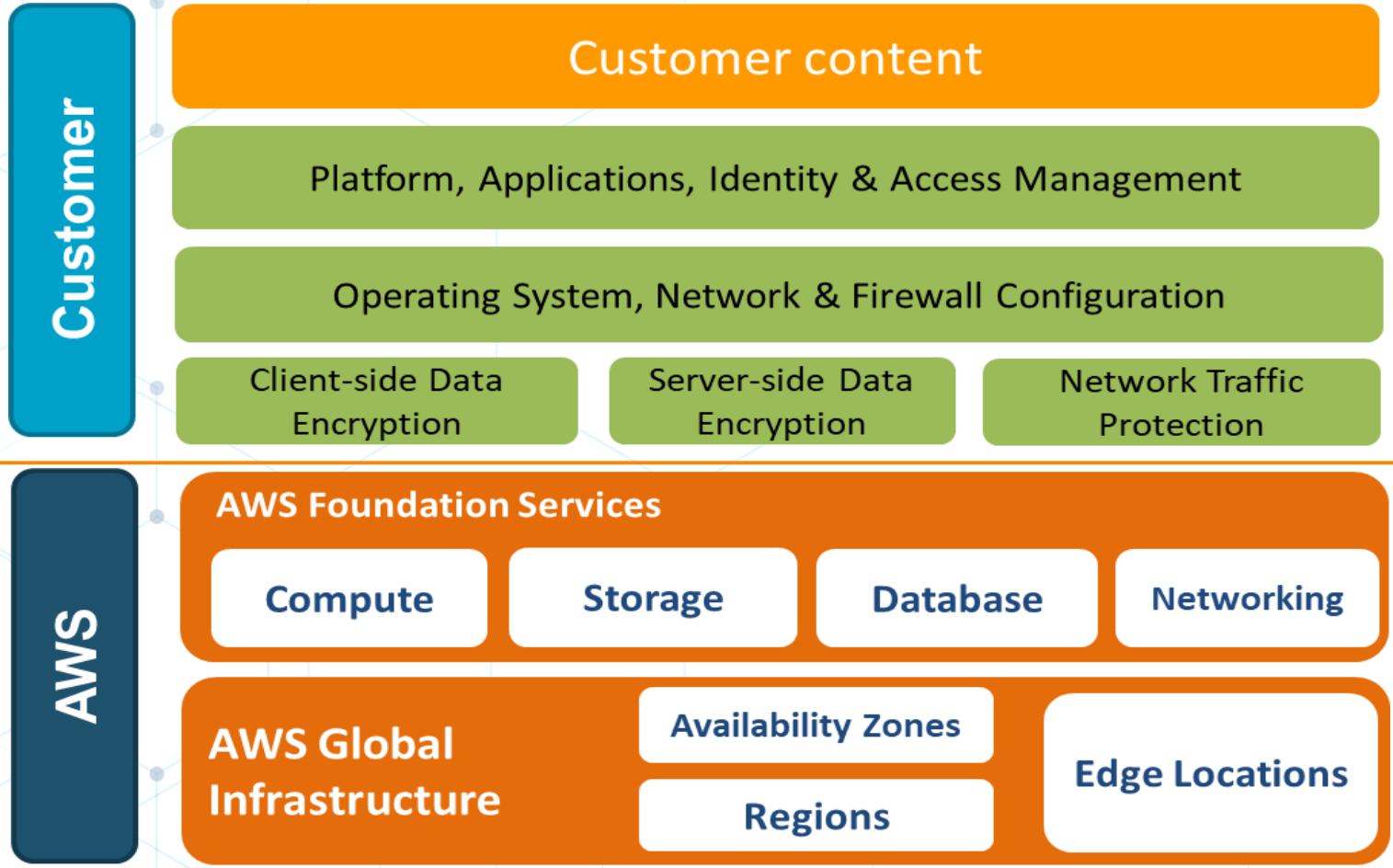
Diciembre de 2024

Agenda

- ❑ Modelo de Responsabilidad Compartida
- ❑ ¿Cómo se puede acceder a AWS?
- ❑ Gestión de Identidad y Acceso (IAM)
- ❑ Planes de Soporte
- ❑ Estrategias Multicuenta

Modelo de Responsabilidad Compartida

Responsabilidad Compartida



Los clientes son responsables de su seguridad y cumplimiento **EN** la Nube

AWS es responsable de la seguridad **DE** la Nube

https://aws.amazon.com/es/compliance/shared-responsibility-model/

Responsabilidad Compartida

Más Personalizable
+
Más Responsabilidad Del Cliente

Amazon EC2

CUSTOMER DATA	CUSTOMER IAM
PLATFORM & APPLICATION MANAGEMENT	
OS, NETWORK, FIREWALL CONFIGURATION	
NETWORK TRAFFIC PROTECTION	
SERVER-SIDE ENCRYPTION	
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY	
COMPUTE / STORAGE / DATABASE / NETWORK	AWS IAM
HARDWARE/AWS GLOBAL INFRASTRUCTURE	

Infrastructure Services

Amazon RDS

CUSTOMER DATA	CUSTOMER IAM
NETWORK TRAFFIC PROTECTION	
CLIENT-SIDEDATA ENCRYPTION	
FIREWALL CONFIGURATION	
PLATFORM & APPLICATION MANAGEMENT	AWS IAM
OS, NETWORK, FIREWALL CONFIGURATION	
COMPUTE / STORAGE / DATABASE / NETWORK	
HARDWARE/AWS GLOBAL INFRASTRUCTURE	

Container Services

AWS S3

AWS KMS

DynamoDB

CUSTOMER DATA	CUSTOMER IAM
CLIENT-SIDE DATA ENCRYPTION	
SERVER-SIDE ENCRYPTION	
NETWORK TRAFFIC PROTECTION	
PLATFORM & APPLICATION MANAGEMENT	
OS, NETWORK, FIREWALL CONFIGURATION	
COMPUTE / STORAGE / DATABASE / NETWORK	
HARDWARE/AWS GLOBAL INFRASTRUCTURE	

Abstracted Services

Menos Personalizable
+
Menos Responsabilidad del Cliente
+
Más prácticas recomendadas incorporadas

Smart Data

Responsabilidad de AWS

Seguridad Física del Centro de Datos

- **Amazon ha estado construyendo centros de datos a gran escala durante muchos años.**
- **Atributos importantes:**
  - Instalaciones no descriptas
  - Controles perimetrales robustos
  - Acceso físico estrictamente controlado
  - Dos o más niveles de autenticación de dos factores
- **Acceso controlado y basado en las necesidades.**
- **Todos los accesos se registra y se revisan.**
- **Separación de Deberes**
  - Los empleados con acceso físico no tienen privilegios lógicos.

Responsabilidad de AWS

Seguridad EC2

- **Sistema operativo host (hypervisor)**
  - Inicios de sesión individuales con clave SSH a través del host bastión para administradores de AWS
  - Todos los accesos se han registrado y auditado
- **Sistema operativo invitado (instancia EC2)**
  - Controlado por el cliente (el cliente posee root/admin)
  - Los administradores de AWS no pueden iniciar sesión
  - Pares de claves generados por el cliente
- **Firewall con estado**
  - Firewall de entrada obligatorio, modo de denegación predeterminado.
  - El cliente controla la configuración a través de grupos de seguridad

Seguridad de la red

- Prohibida la suplantación de IP a nivel de SO host.
- Escaneo de puertos no autorizados es una violación de TOS y se detecta/bloquea.
- Puertos entrantes bloqueados por defecto.

Responsabilidad de AWS

Administración de configuración

- La mayoría de las actualizaciones se realizan de tal manera que no impactarán al cliente.
- Los cambios son autorizados, registrados, probados, aprobados y documentados.
- AWS se comunicará con los clientes, ya sea por correo electrónico, el AWS Service Health Dashboard (http://status.aws.amazon.com/) o el panel de AWS Personal Health (https://health.aws.amazon.com) cuando existe la posibilidad de que el servicio se vea afectado.

Construido para "Disponibilidad Continua"

- **Servicios escalables y tolerantes a fallas.**
- **Todas las zonas de disponibilidad (AZ) están siempre encendida.**
  - No existe un "Centro de datos de recuperación ante desastres"
  - Todos manejados con los mismos estándares
- **Conectividad robusta a Internet**
  - Cada AZ tiene proveedores de servicios ISP redundantes
  - Infraestructura de red resiliente

Responsabilidad de AWS

Administración de discos

- La administración de discos patentada impide que los clientes accedan a los datos de los demás.
- Discos limpiados antes de su uso.
- Los discos también pueden ser encriptados por el cliente para mayor seguridad.

Desmantelamiento de dispositivos de almacenamiento

- Todos los dispositivos de almacenamiento pasan por proceso utilizando técnicas de:
  - DoD 5220.22-M (“Manual de Operación del Programa Nacional de Seguridad Industrial”).
  - NIST 800-88 (“Directrices para la desinfección de medios”).
- En última instancia, los dispositivos son:
  - Desmagnetizada.
  - Físicamente destruido.

Bajo el modelo de responsabilidad compartida de AWS

¿RESPONSABILIDAD DE AWS? o ¿RESPONSABILIDAD DEL CLIENTE?

Configuración de las reglas del grupo de seguridad que determinan qué puertos están abiertos en la instancia de Linux EC2

Parchear el sistema operativo con los últimos parches de seguridad

Instalación de sistemas de cámaras para monitorear los centros de datos físicos

Triturar unidades de disco antes de que salgan de un datacenter

Accionando la función de cifrado del lado del servidor para buckets S3

Prevención de la detección de paquetes a nivel de hipervisor

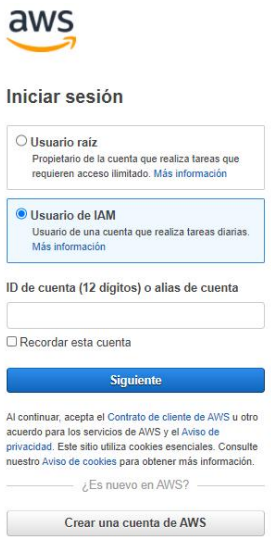
Asegurar la red interna dentro de los centros de datos de AWS

¿Cómo se puede acceder a AWS?

Acceso a AWS

Para acceder a AWS, tenemos tres opciones:

- Consola de Administración de AWS (Password + MFA)
- Interfaz de Linea de Comandos (CLI) (Access keys)
- Kits de Desarrollo de Software (SDK) (Access keys)



Access Keys son generadas a través de la Consola de AWS.
Usuarios administran sus propias Access Keys.
Access Keys son secretas. **No deben compartirse.**

Ejemplo Access Keys

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. Learn more

Create access key

Access key ID	Created	Last used	Status	
AKIASK4E37PV4TU3RD6C	2020-05-25 15:13 UTC+0100	N/A	Active | Make inactive	✖

- Access key ID: AKIASK4E37PV4983d6C
- Secret Access Key: AZPN3zojWozWCndIjhB0Unh8239a1bzbzO5fqqkZq

¿Qué es la CLI?

- ✓ Una herramienta que le permite interactuar con los servicios de AWS mediante comandos en su shell de línea de comandos
- ✓ Acceso directo a las API públicas de los servicios de AWS
- ✓ Puedes desarrollar scripts para gestionar tus recursos.
- ✓ Es de código abierto https://github.com/aws/aws-cli
- ✓ Alternativa al uso de la Consola de administración de AWS

```
➜  ~ aws s3 cp myfile.txt s3://ccp-mybucket/myfile.txt
upload: ./myfile.txt to s3://ccp-mybucket/myfile.txt
➜  ~ aws s3 ls s3://ccp-mybucket
2021-05-14 03:22:52          0 myfile.txt
➜  ~
```

¿Qué es el SDK?

- ✓ Kit de desarrollo de software de AWS (SDK de AWS)
- ✓ API específicas del lenguaje de programación(conjunto de bibliotecas)
- ✓ Le permite acceder y administrar los servicios de AWS mediante programación
- ✓ Integrado dentro de su aplicación
- ✓ Soporta:
  - ✓ SDK (JavaScript, Python, PHP, .NET, Ruby, Java, Go, Node.js, C++)
  - ✓ SDK móviles (Android, iOS,...)
  - ✓ SDK de dispositivos IoT (C integrado, Arduino,...)
- ✓ Ejemplo: AWS CLI se basa en AWS SDK para Python

Your Application

Gestión de Identidad y Acceso (IAM)

AAA con AWS

Authenticate	Authorize	Audit
IAM Username/Password Access Key (+ MFA) Federation	IAM Policies	CloudTrail

Principales de AWS

ID de propietario de cuenta (cuenta raíz)

- Acceso a todos los servicios suscritos.
- Acceso a la facturación.
- Cambiar la configuración de la cuenta, cambiar el plan de soporte de AWS, cerrar la cuenta de AWS.
- Regístrate como vendedor, regístrate en GovCloud.

Usuarios, grupos y roles de IAM

- Acceso a servicios específicos.
- Acceso a consola y/o APIs.
- Acceso a Atención al Cliente (Business y Enterprise).

Credenciales de Seguridad Temporales

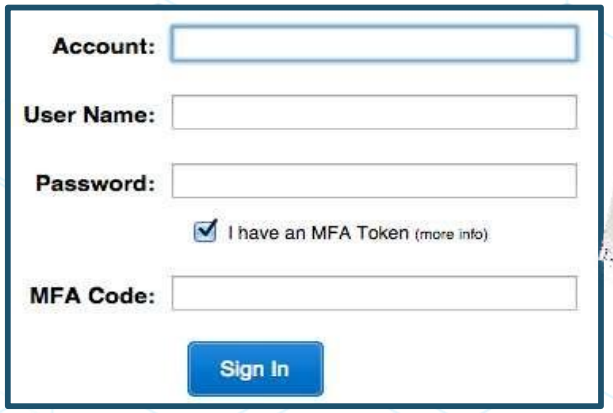
- Acceso a servicios específicos.
- Acceso a consola y/o APIs.

Autenticación de identidad de AWS

AUTENTICACIÓN: ¿CÓMO SABEMOS QUE ERES QUIEN DICES SER?

Consola de administración de AWS

Iniciar sesión con **Nombre de usuario/Contraseña** con opcional **MFA** (recomendado)



Para acceso por tiempo limitado:**una URL firmada Puede** proporcionar acceso temporal a la consola

Acceso API

Acceder a la API usando **Access Key ID + Secret Key**, con MFA opcional

ID DE CLAVE DE ACCESO
Ej.AKIAIOSFODN7EJEMPLO

CLAVE SECRETA
Ej.UTNFEMI/K7MDENG/BPXRficyEjemploClave

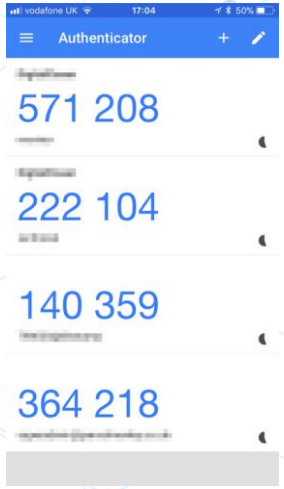
Para acceso por tiempo limitado: Llame al servicio de tokens de seguridad de AWS (STS) para obtener un AccessKeyID + SecretAccessKey + SessionToken temporal

Multi Factor Authentication MFA

MFA aporta seguridad adicional, ya que exige a los usuarios que proporcionen una autenticación exclusiva obtenida de un mecanismo de MFA admitido por AWS, además de sus credenciales de inicio de sesión habituales, para obtener acceso a los sitios web o servicios de AWS.

MFA opciones de dispositivos

Virtual MFA device



Google Authenticator
(phone only)

Authy
(multi-device)

Soporte para múltiples tokens en un solo dispositivo.

Universal 2nd Factor (U2F) Security Key

YubiKey by Yubico (3rd party)

Soporte para múltiples usuarios raíz e IAM usando una única clave de seguridad

MFA opciones de dispositivos

Hardware Key Fob MFA Device

Provided by Gemalto (3rd party)

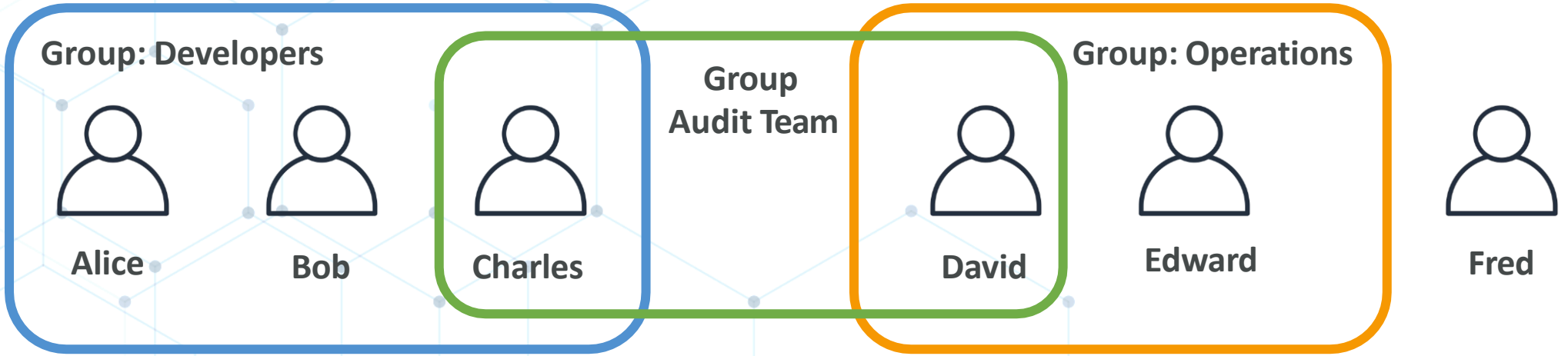
Hardware Key Fob MFA Device for AWS GovCloud (US)

Provided by SurePassID (3rd party)

Laboratorio Configuración de MFA cuenta root

IAM: Usuarios & Grupos

- ✓ IAM = Identity and Access Management, servicio global
- ✓ La cuenta raíz creada de forma predeterminada no debe usarse ni compartirse
- ✓ Los usuarios son personas dentro de su organización y se pueden agrupar.
- ✓ Los grupos solo contienen usuarios, no otros grupos.
- ✓ Los usuarios no tienen que pertenecer a un grupo y pueden pertenecer a varios grupos.



IAM: Permisos

- ✓ A los usuarios o grupos se les pueden asignar documentos JSON llamados políticas
- ✓ Estas políticas definen los permisos de los usuarios
- ✓ En AWS se aplica el **principio de privilegios mínimos**: no dar más permisos que un usuario necesidades

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

IAM Estructura de Política

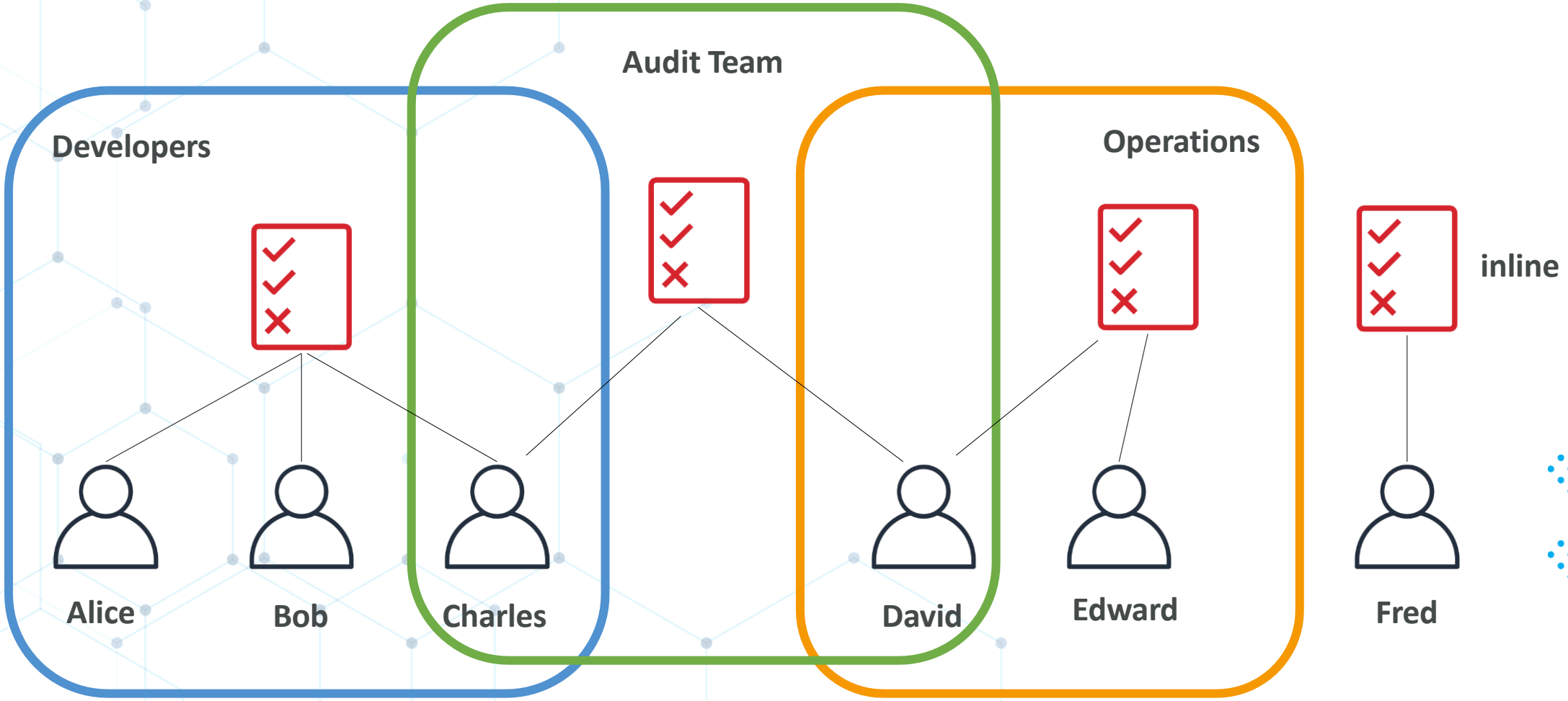
- ✓ Consiste en
  - ✓ **Versión:** versión del idioma de la política, siempre incluya "2012-10-17"
  - ✓ **Id:** un identificador de la política (opcional)
  - ✓ **Statement:** una o más declaraciones individuales (obligatorio)
- ✓ Las declaraciones consisten en
  - ✓ **Sid:** un identificador para la declaración (opcional)
  - ✓ **Effect:** si la declaración permite o niega el acceso (Permitir, Denegar)
  - ✓ **Principal:** cuenta/usuario/rol al que se aplicó esta política
  - ✓ **Action:** lista de acciones que esta política permite o niega
  - ✓ **Resource:** lista de recursos a los que se aplicaron las acciones
  - ✓ **Condition:** condiciones para cuando esta política esté vigente (opcional)

```
{
    "Version": "2012-10-17",
    "Id": "S3-Account-Permissions",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:root"]
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": ["arn:aws:s3:::mybucket/*"]
        }
    ]
}
```

IAM Política de Password

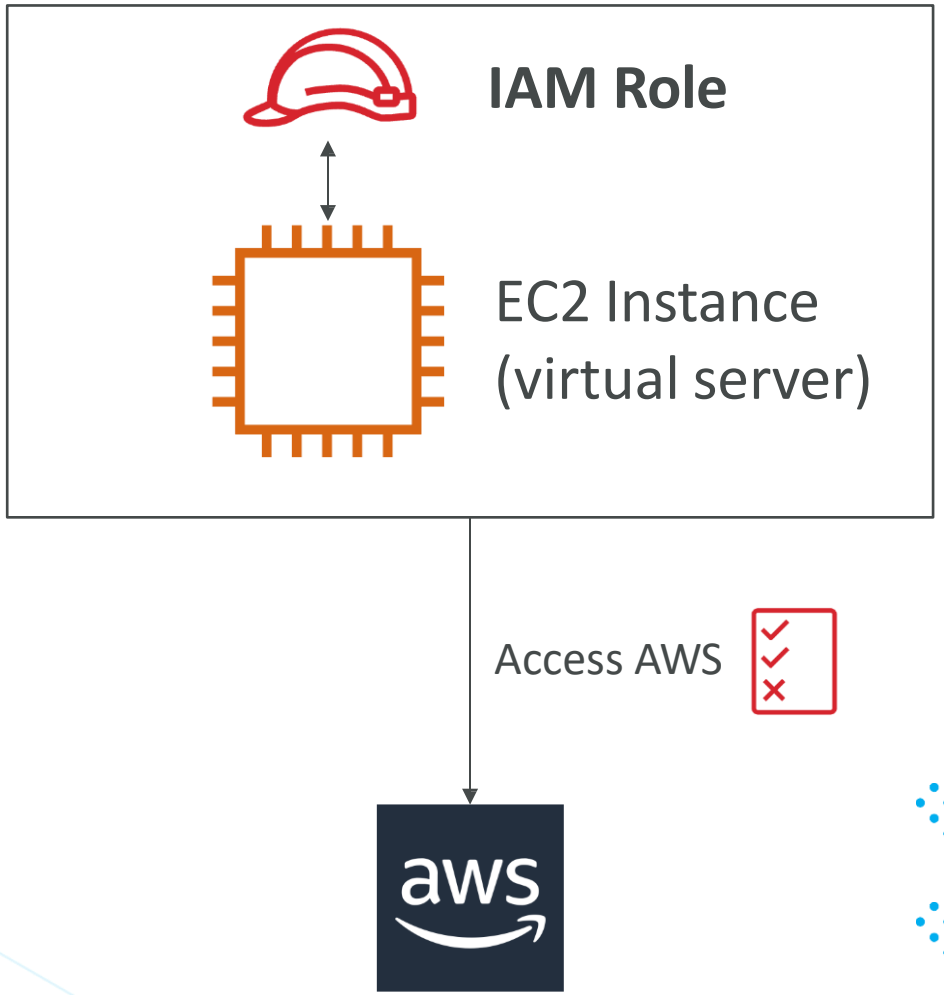
- ✓ Contraseñas seguras = mayor seguridad para su cuenta
- ✓ En AWS, puede configurar una política de contraseña:
  - ✓ Establecer una longitud mínima de contraseña
  - ✓ Requerir tipos de caracteres específicos:
    - ✓ incluyendo letras mayúsculas
    - ✓ letras minúsculas
    - ✓ números
    - ✓ caracteres no alfanuméricos
  - ✓ Permitir que todos los usuarios de IAM cambien sus propias contraseñas
  - ✓ Requerir que los usuarios cambien su contraseña después de un tiempo (caducidad de la contraseña)
  - ✓ Evitar la reutilización de contraseñas

IAM: Herencia de políticas



Roles IAM para servicios

- ✓ Algún servicio de AWS deberá realizar acciones en su nombre
- ✓ Para ello le asignaremos permisos para servicios de AWS con roles de IAM
- ✓ Roles comunes:
  - ✓ Roles de instancia EC2
  - ✓ Roles de la función Lambda
  - ✓ Funciones para CloudFormation



IAM Herramientas de Seguridad

- ✓ **IAM Credentials Report (account-level)**
  - ✓ Un informe que enumera todos los usuarios de su cuenta y el estado de sus distintas credenciales
  - ✓ Para ello le asignaremos permisos para servicios de AWS con roles de IAM
- ✓ **IAM Access Advisor (user-level)**
  - ✓ El asesor de acceso muestra los permisos de servicio otorgados a un usuario y cuándo se accedió a esos servicios por última vez.
  - ✓ Puede utilizar esta información para revisar sus políticas.

Mejores prácticas IAM

- ✓ No utilice la cuenta raíz excepto para la configuración de la cuenta de AWS
- ✓ Un usuario físico = Un usuario de AWS
- ✓ Asignar usuarios a grupos y asignar permisos a grupos
- ✓ Cree una política de contraseñas segura
- ✓ Usar y hacer cumplir el uso de autenticación multifactor (MFA)
- ✓ Cree y utilice roles para otorgar permisos a los servicios de AWS
- ✓ Utilice claves de acceso para acceso programático (CLI/SDK)
- ✓ Audite los permisos de su cuenta utilizando el Informe de credenciales de IAM y el Asesor de acceso de IAM
- ✓ Nunca comparta usuarios de IAM ni claves de acceso

Modelo de Responsabilidad Compartida para IAM

- ✓ Infraestructura (seguridad de red global)
- ✓ Análisis de configuración y vulnerabilidad.
- ✓ Validación de cumplimiento

- ✓ Usuarios, Grupos, Roles, Gestión y seguimiento de políticas
- ✓ Habilite MFA en todas las cuentas
- ✓ Rote todas sus llaves con frecuencia
- ✓ Utilice herramientas de IAM para aplicar los permisos adecuados
- ✓ Analice patrones de acceso y revise permisos

Laboratorio Creación de Cuenta IAM

Planes de Soporte

Precios de los planes de AWS Support

- ✓ Soporte básico: gratuito

Developer	Business	Enterprise On-Ramp	Enterprise
Greater of $29.00 **- or -** 3% of monthly AWS charges	Greater of $100.00 **- or -** 10% of monthly AWS charges for the first $0--$10K 7% of monthly AWS charges from $10K--$80K 5% of monthly AWS charges from $80K--$250K 3% of monthly AWS charges over $250K	Greater of $5,500.00 **- or -** 10% of monthly AWS charges	Greater of $15,000.00 **- or -** 10% of monthly AWS charges for the first $0--$150K 7% of monthly AWS charges from $150K--$500K 5% of monthly AWS charges from $500K--$1M 3% of monthly AWS charges over $1M

Plan AWS Basic

- ✓ Servicio al cliente y comunidades: acceso las 24 horas del día, los 7 días de la semana al servicio al cliente, documentación, documentos técnicos y foros de soporte.
- ✓ AWS Trusted Advisor: acceso a las 7 comprobaciones y directrices principales de Trusted Advisor para aprovisionar sus recursos siguiendo las prácticas recomendadas para aumentar el rendimiento y mejorar la seguridad.
- ✓ AWS Personal Health Dashboard: una vista personalizada del estado de los servicios de AWS y alertas cuando sus recursos se ven afectados.

Plan AWS Developer

- ✓ Todo el Plan de Soporte Básico +
- ✓ Acceso por correo electrónico en horario comercial a los asociados de soporte en la nube
- ✓ Casos ilimitados / 1 contacto primario
- ✓ Gravedad del caso / tiempos de respuesta:
  - ✓ Orientación general: < 24 horas hábiles
  - ✓ Sistema deteriorado: < 12 horas hábiles

Plan AWS Business

- ✓ Diseñado para usarse si tiene cargas de trabajo de producción
- ✓ Trusted Advisor – Conjunto completo de comprobaciones + acceso a la API
- ✓ Acceso por teléfono, correo electrónico y chat las 24 horas del día, los 7 días de la semana a los ingenieros de soporte en la nube
- ✓ Casos ilimitados / contactos ilimitados
- ✓ Acceso a la gestión de eventos de infraestructura por una tarifa adicional.
- ✓ Gravedad del caso / tiempos de respuesta:
  - ✓ Orientación general: < 24 horas hábiles
  - ✓ Sistema deteriorado: < 12 horas hábiles
  - ✓ Sistema de producción deteriorado: < 4 horas
  - ✓ Sistema de producción inactivo: < 1 hora

Plan AWS Enterprise On-Ramp

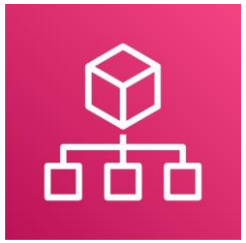
- ✓ Diseñado para usarse si tiene cargas de trabajo críticas para la producción o para el negocio
- ✓ Plan de AWS Business +
- ✓ Acceso a un grupo de gestores técnicos de cuentas (TAM)
- ✓ Equipo de soporte de conserjería (para conocer las mejores prácticas de facturación y cuentas)
- ✓ Gestión de Eventos de Infraestructura, Revisión de Operaciones y Bien Arquitectura
- ✓ Gravedad del caso / tiempos de respuesta:
  - ✓ Sistema de producción deteriorado: < 4 horas
  - ✓ Sistema de producción inactivo: < 1 hora
  - ✓ Sistema crítico para el negocio: < 30 minutos

Plan AWS Enterprise

- ✓ Diseñado para usarse si tiene cargas de trabajo críticas
- ✓ Plan de AWS Business +
- ✓ Acceso a un Gestor Técnico de Cuentas (TAM) **designado**
- ✓ Equipo de soporte de conserjería (para conocer las mejores prácticas de facturación y cuentas)
- ✓ Gestión de Eventos de Infraestructura, Revisión de Operaciones y Bien Arquitectura
- ✓ Gravedad del caso / tiempos de respuesta:
  - ✓ Sistema de producción deteriorado: < 4 horas
  - ✓ Sistema de producción inactivo: < 1 hora
  - ✓ Sistema crítico para el negocio: < **15 minutos**

Estrategias Multi Cuenta

AWS Organizations



- ✓ Servicio global
- ✓ Permite administrar varias cuentas de AWS
- ✓ La cuenta principal es la cuenta maestra
- ✓ Costo-Beneficio:
  - ✓ Facturación consolidada en todas las cuentas: método de pago único
  - ✓ Beneficios de precios del uso agregado (descuento por volumen para EC2, S3...)
  - ✓ Agrupación de instancias EC2 reservadas para un ahorro óptimo
- ✓ La API está disponible para automatizar la creación de cuentas de AWS
- ✓ Restrinja los privilegios de la cuenta mediante políticas de control de servicios (SCP)

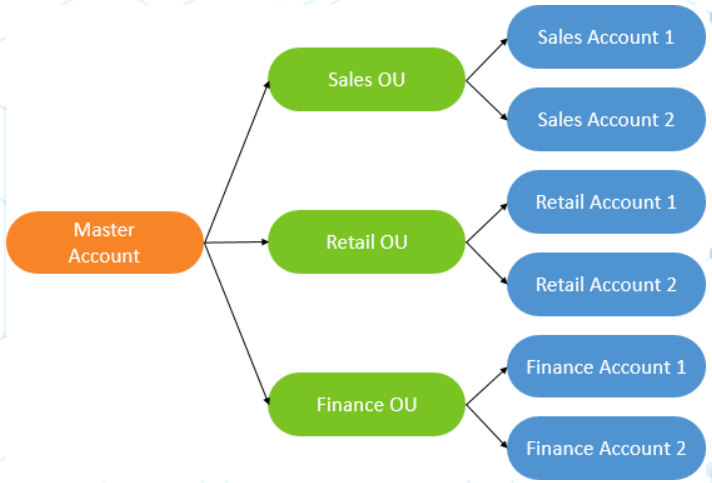
Estrategias Multi Cuenta

- ✓ Cree cuentas por departamento, por centro de costos, por desarrollo / prueba / producción, en función de las restricciones regulatorias (usando SCP), para mejor aislamiento de recursos (por ejemplo: VPC), para tener límites de servicio independientes por cuenta, cuenta aislada para el registro

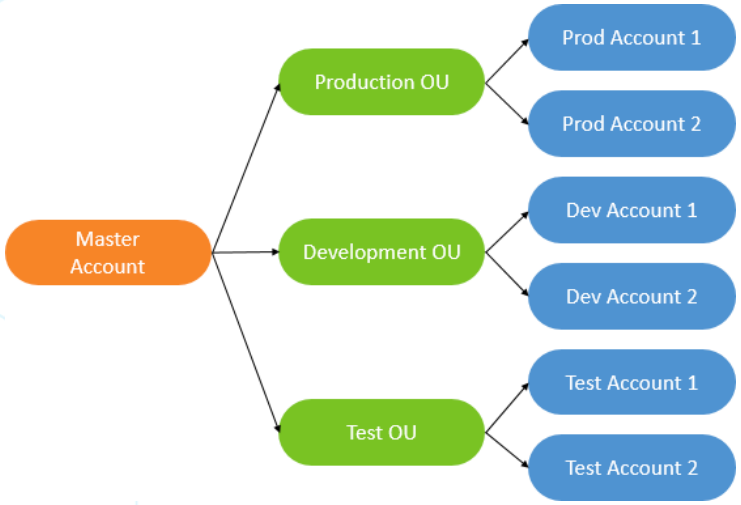
- ✓ Multi Cuenta vs Una Cuenta con Múltiples VPC
- ✓ Usar estándares de etiquetado para fines de facturación
- ✓ Habilite CloudTrail en todas las cuentas, envíe registros a la cuenta central de S3
- ✓ Envío de registros de CloudWatch a la cuenta de registro central
- ✓ Estrategia para crear una cuenta de seguridad

Unidades organizativas (OU) - Ejemplos

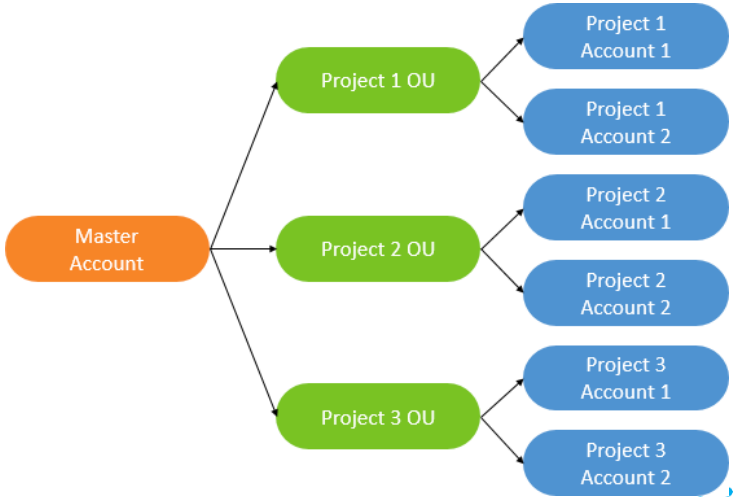
Business Unit



Environmental Lifecycle

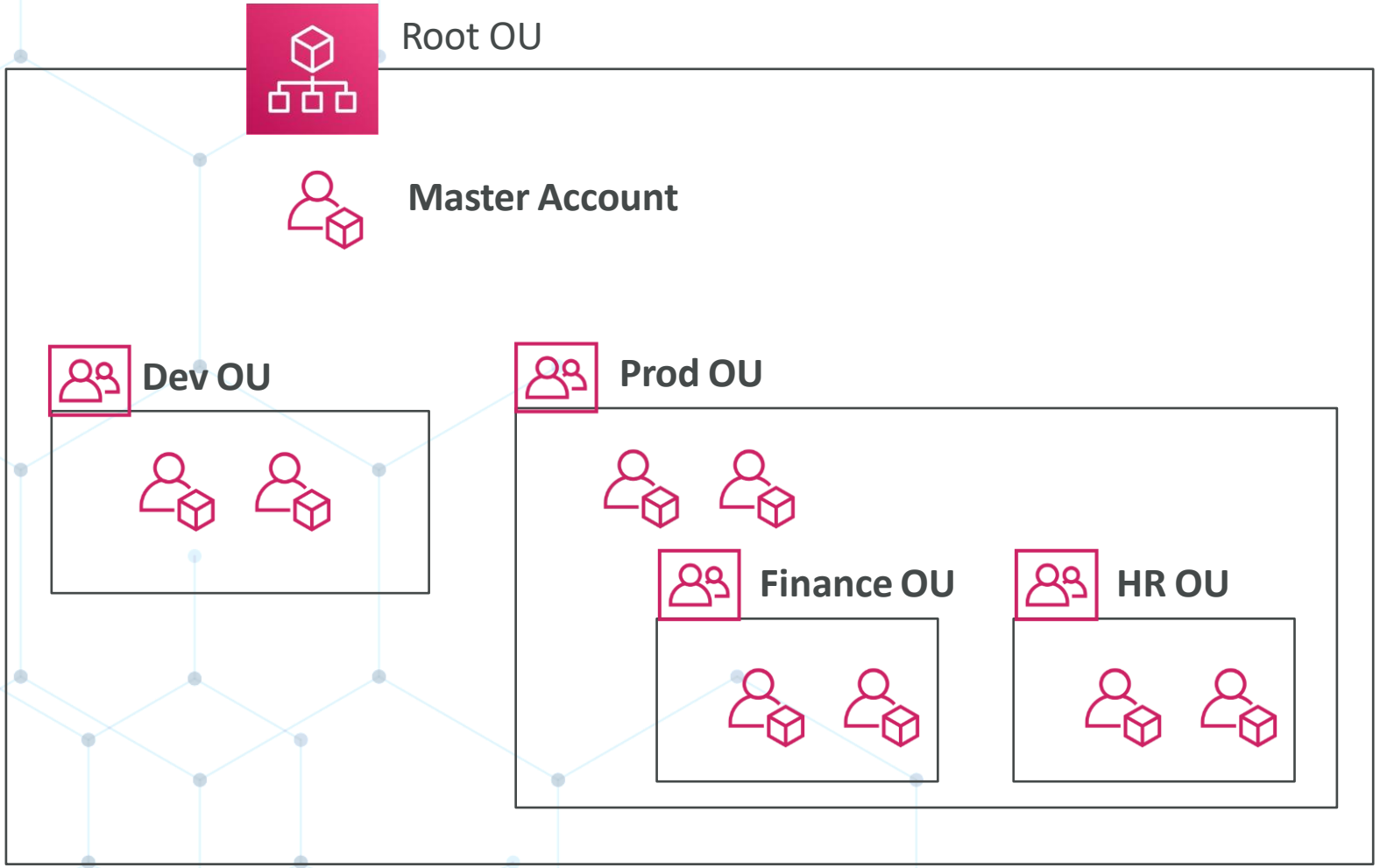


Project-based



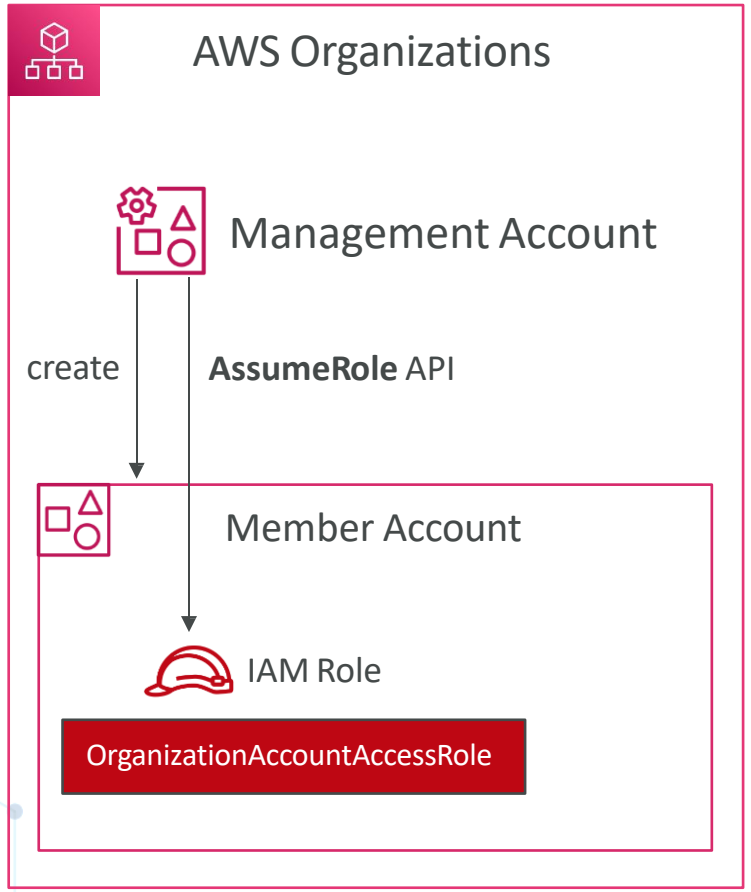
https://aws.amazon.com/answers/account-management/aws-multi-account-billing-strategy/

AWS Organization



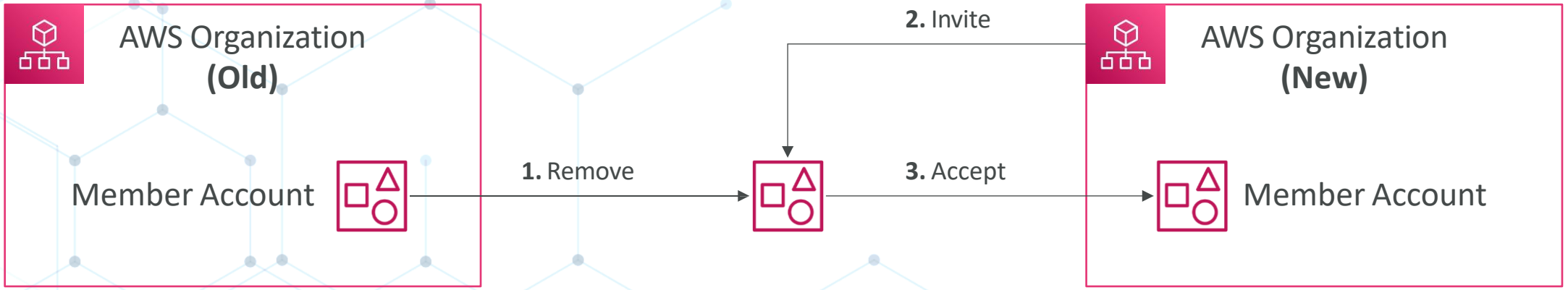
AWS Organizations – OrganizationAccountAccessRole

- ✓ Rol de IAM que concede permisos de administrador completo en la cuenta de miembro a la cuenta de administración
- ✓ Se utiliza para realizar tareas de administración en las cuentas de los miembros (por ejemplo, crear usuarios de IAM)
- ✓ Podría ser asumido por los usuarios de IAM en la cuenta de administración
- ✓ Se agrega automáticamente a todas las cuentas de miembros nuevas creadas con AWS Organizations
- ✓ Debe crearse manualmente si invita a una cuenta de miembro existente



AWS Organization – Moviendo Cuentas

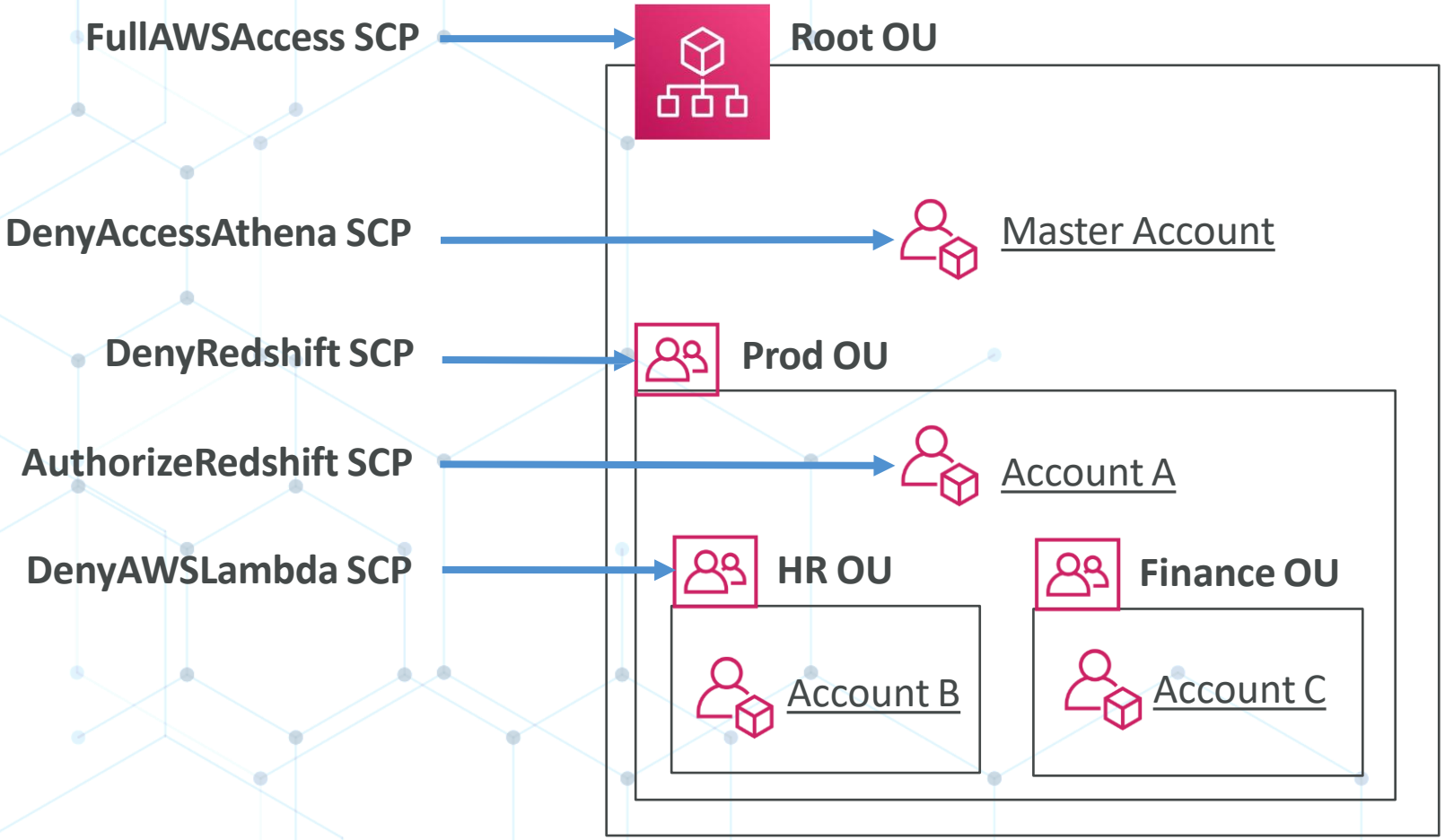
- ✓ Eliminar la cuenta de miembro de la organización de AWS
- ✓ Enviar una invitación a la cuenta miembro desde la organización de AWS
- ✓ Aceptar la invitación a la nueva organización desde la cuenta de miembro



Service Control Policies (SCP)

- ✓ Acciones de IAM en la lista blanca o en la lista negra
- ✓ Se aplica a nivel de unidad organizativa o de cuenta
- ✓ No se aplica a la Cuenta Principal
- ✓ SCP se aplica a todos los usuarios y roles de la cuenta, incluido el usuario root
- ✓ La SCP no afecta a los roles vinculados a servicios
  - ✓ Los roles vinculados a servicios permiten que otros servicios de AWS se integren con AWS Organizations y no pueden ser restringidos por SCP.
- ✓ SCP debe tener un Allow explícito (no permite nada de forma predeterminada)
- ✓ Casos de uso:
  - ✓ Restringir el acceso a ciertos servicios (por ejemplo: no se puede usar EMR)
  - ✓ Aplique el cumplimiento de PCI mediante la deshabilitación explícita de los servicios

Jerarquía SCP



- Master Account
  - Puede hacer cualquier cosa
  - (no se aplica SCP)
- Account A
  - Puede hacer cualquier cosa
  - EXCEPT acceso Redshift (denegación explícita de la unidad organizativa de producción)
- Account B
  - Puede hacer cualquier cosa
  - EXCEPT acceso Redshift (denegación explícita de la unidad organizativa de producción)
  - EXCEPT access Lambda (denegación explícita de la unidad organizativa HR)
- Account C
  - Puede hacer cualquier cosa
  - EXCEPT acceso Redshift (denegación explícita de la unidad organizativa de producción)

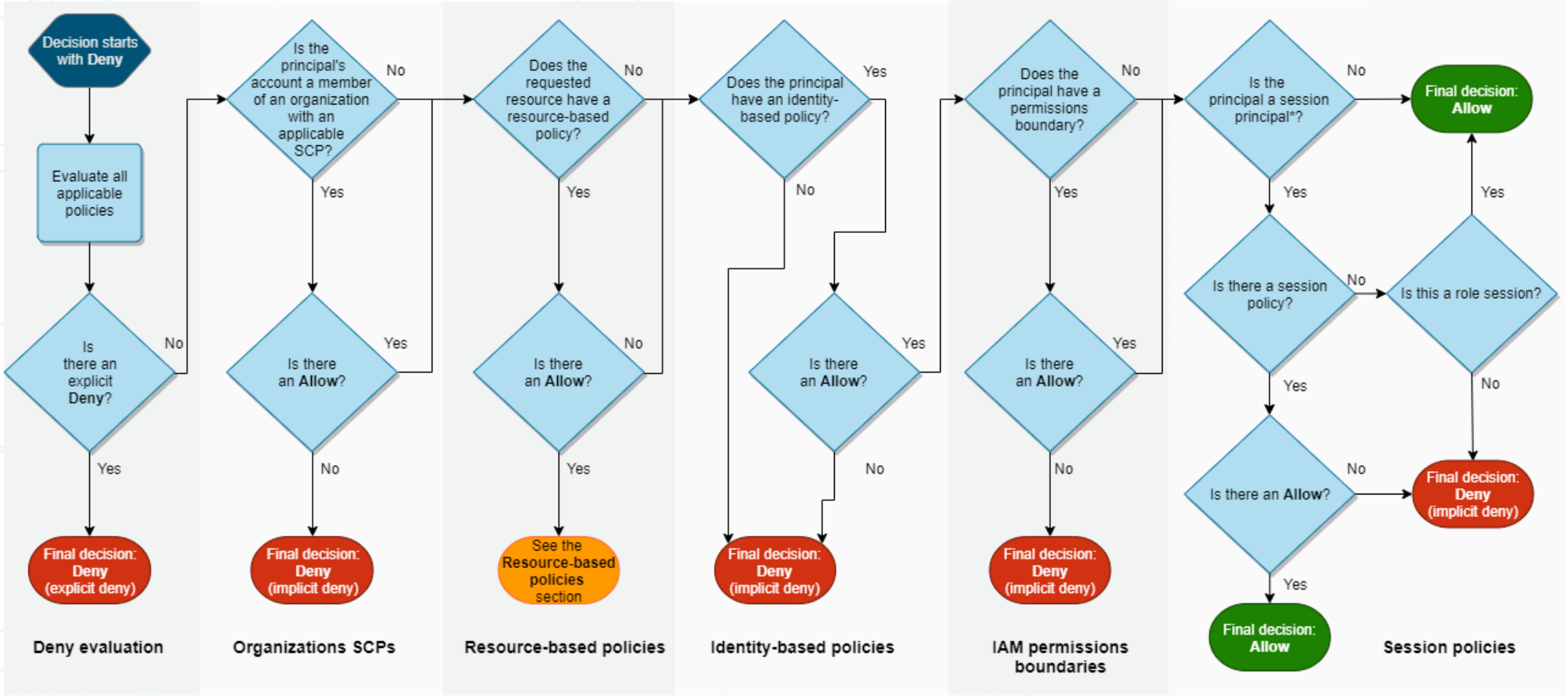
Ejemplos SCP – Estrategias de bloqueo y permisos

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenyDynamoDB",
            "Effect": "Deny",
            "Action": "dynamodb:*",
            "Resource": "*"
        }
    ]
}
```

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

Más ejemplos: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_example-scps.html

Evaluación lógica de Políticas IAM

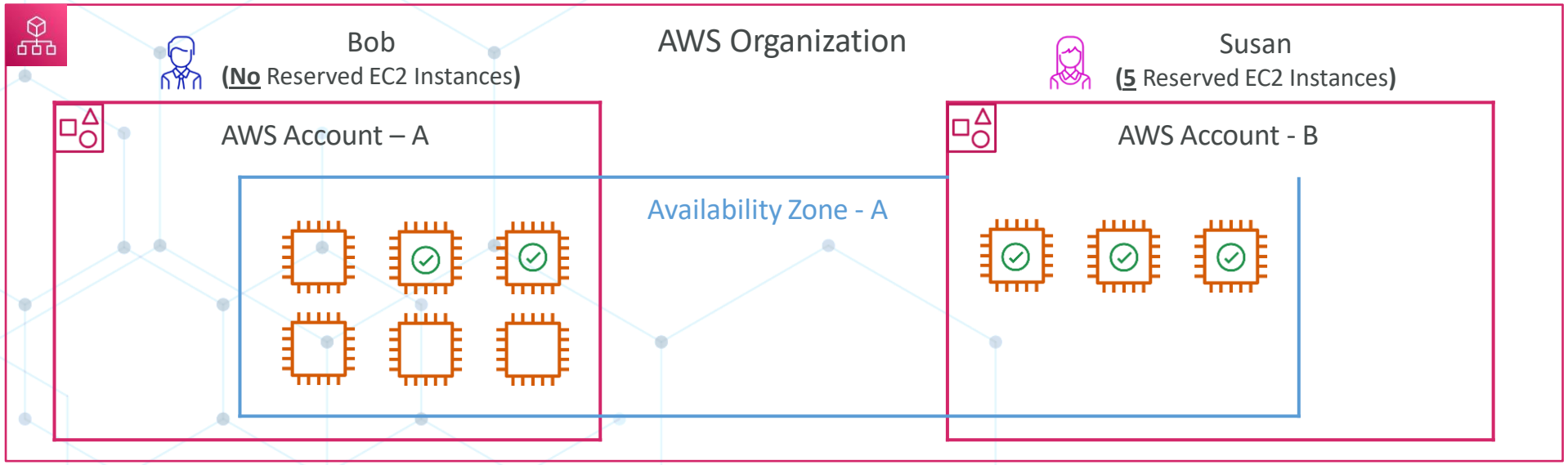


*A session principal is either a role session or an IAM federated user session.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

AWS Organization – Facturación consolidada

- ✓ Cuando está habilitado, le proporciona:
  - ✓ Uso combinado: combine el uso en todas las cuentas de AWS de la organización de AWS para compartir los precios por volumen, las instancias reservadas y los descuentos de Savings Plans
  - ✓ Una factura: obtenga una factura para todas las cuentas de AWS de la organización de AWS
- ✓ La cuenta de administración puede desactivar el uso compartido de descuentos de instancias reservadas para cualquier cuenta de la organización de AWS, incluida ella misma

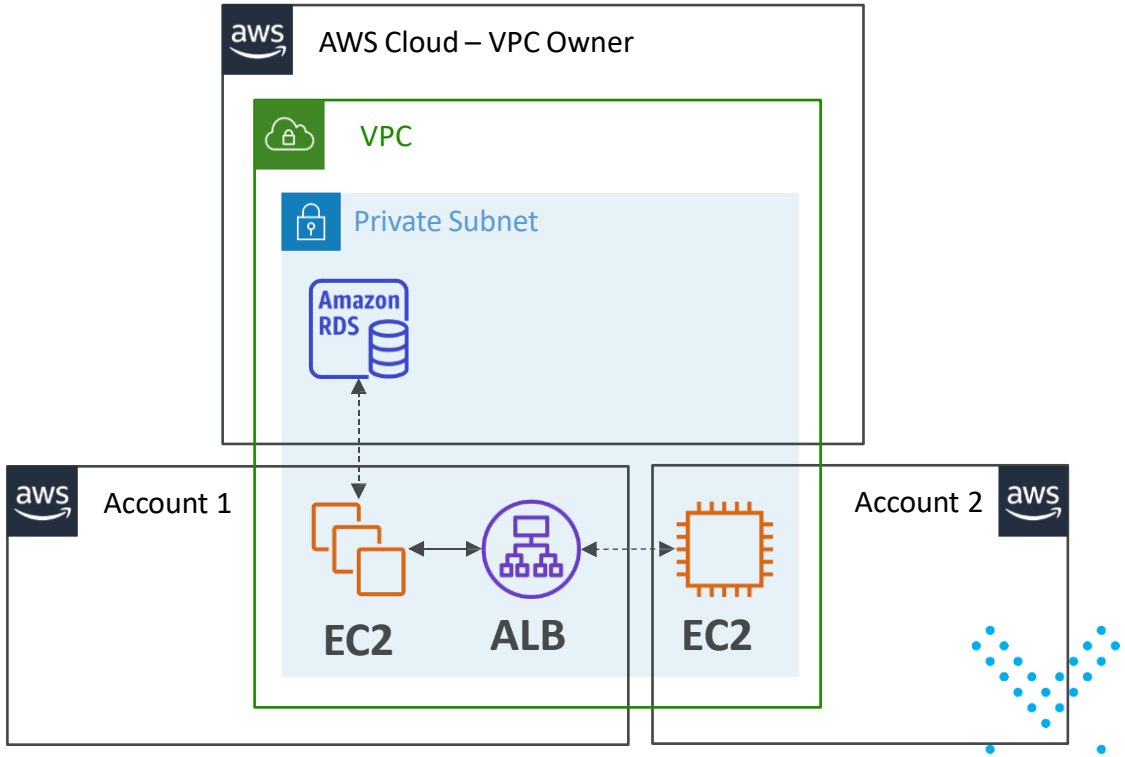


AWS Control Tower

- ✓ Una forma sencilla de configurar y controlar un entorno de AWS multicuenta seguro y compatible basado en las prácticas recomendadas
- ✓ Beneficios:
  - ✓ Automatice la configuración de su entorno en unos pocos clics
  - ✓ Automatice la gestión continua de políticas mediante barreras de protección
  - ✓ Detectar infracciones de políticas y corregirlas
  - ✓ Supervise el cumplimiento a través de un panel interactivo
- ✓ AWS Control Tower se ejecuta sobre AWS Organizations:
  - ✓ Configura automáticamente AWS Organizations para organizar cuentas e implementar SCP (políticas de control de servicios)

AWS Resource Access Manager (AWS RAM)

- ✓ Comparta los recursos de AWS que posee con otras cuentas de AWS
- ✓ Comparte con cualquier cuenta o dentro de tu organización
- ✓ Evite la duplicación de recursos
- ✓ Los recursos admitidos incluyen Aurora, subredes de VPC, Transit Gateway, Route 53, hosts dedicados de EC2, configuraciones de License Manager...



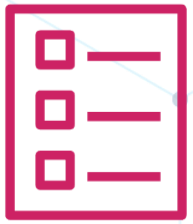
AWS Service Catalog

- ✓ Los usuarios que son nuevos en AWS tienen demasiadas opciones y pueden crear pilas que no cumplan con los requisitos o no estén en línea con el resto de la organización
- ✓ Algunos usuarios solo quieren un portal de autoservicio rápido para iniciar un conjunto de productos autorizados predefinidos por los administradores
- ✓ Incluye: máquinas virtuales, bases de datos, opciones de almacenamiento, etc...

Service Catalog - Diagrama

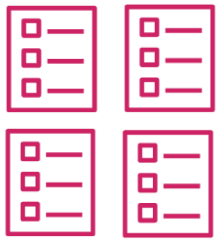
ADMIN TASKS

Product



CloudFormation Templates

Portfolio



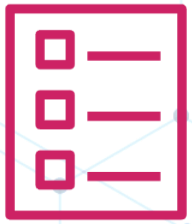
Collection of Products

Control

IAM Permissions to Access Portfolios

USER TASKS

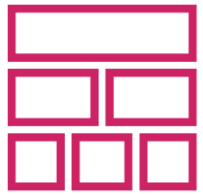
Product List



Authorized by IAM

launch

Provisioned Products



Ready to use
Properly Configured
Properly Tagged

Smart Data
DATA PARA TODOS

Gracias