Actividad: Información general de IAM

Consulta los recursos proporcionados para definir palabras clave y responder a laspreguntas sobre el servicio AWS Identity and Access Management (IAM).

- Identidades de IAM (usuarios, grupos y roles):https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html
- Creación de políticas de IAM:https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html

Palabra	Definición
Usuario raíz	Cuando se crea primero una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de *usuario raíz* de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta.
Usuario	Un usuario de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación.
Rol	Un *rol de IAM* es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona.
Grupo	Un *grupo de IAM* es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios.
Política	Una política es una entidad que, cuando se asocia a una identidad o recurso, define sus permisos.

1. ¿Cuál es la diferencia entre un grupo y un usuario?
   El usuario es una identidad con permisos, la cual puede iniciar sesión dependiendo de los roles y/o permisos que le hayan sido asignados, a diferencia de un grupo, el cual agrupa a 1 o más usuarios, estos no cuentan con contraseña ya que son utilizados para asignar permisos a los usuarios de acuerdo a las políticas que les hayan sido asignadas.

2. ¿Cuándo utilizarías roles de IAM y credenciales de seguridad temporales en lugar de credenciales a largo plazo asociadas a un usuario de IAM?
   La asignación de credenciales temporales o a largo plazo depende de la función y accesos que un usuario necesite, sin embargo, es recomendable utilizar los más posible las credenciales temporales o en su defecto asignar credenciales a largo plazo, pero con cambio de contraseña frecuente.

3. Identifica las prácticas recomendadas de IAM y explica la importancia de cada una de ellas. Usa la página de prácticas recomendadas de seguridad en IAM: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

N.º	Prácticas recomendadas	Importancia
1	Asignar a cada usuario credenciales temporales cuando accedan a AWS. Utilizar AWS IAM Identity Center para asignar acceso de manera centralizada	Para poder acceder a un servicio de AWS de manera certificada.
2	Evitar el uso de usuario root	Al ser un usuario genérico, cualquier persona puede tener acceso a los recursos del sitio web
3	Crear alerta que este monitoreando a los usuarios root	Contar con una señal que indique cuando un intruso quiera acceder al sitio web con privilegios de administrador
4	Autenticación multi-factor	Para escenarios en los que necesite un usuario de IAM o usuario raíz en su cuenta, requiera MFA para seguridad adicional. Con MFA, los usuarios tienen un dispositivo que genera una respuesta a un reto de autenticación.

N.º	Prácticas recomendadas	Importancia
5	Configurar permisos mínimos en cada grupo de usuarios	Para evitar que personas ajenas a la organización accedan a la información se implementa MFA para generar una respuesta a un reto de autenticación.
6	Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración	se recomienda emplear credenciales temporales, en lugar de crear credenciales de larga duración tales como claves de acceso Rotar periódicamente las credenciales de larga duración ayuda a familiarizarse con el proceso.
7	Aplicar permisos de privilegios mínimos	Para segmentar a cada grupo de usuarios las actividades a realizar, de tal forma que no se generen conflictos en labores realizadas por varios usuarios a la vez.
8	Utilizar IAM Access Analyzer para generar políticas de privilegios mínimos basadas en la actividad de acceso	Permite crear politicas para que cada usuario pueda acceder solo a los servicios permitidos. Manteniendo el control de lo que cada usuario puede realizar o que servicios puede utilizar.
9	Revisar y eliminar periódicamente usuarios, roles, permisos, políticas y credenciales no utilizados	AWS, te ofrece la información del ultimo acceso de un usuario, utilización de una política, o permiso, para que así puedas eliminar los usuarios, políticas, permisos, etc., que ya no se estén utilizando.
10	Utilizar condiciones en las políticas de IAM para restringir aún más el acceso	Permite especificar condiciones de cuando una política será aplicada.
11	Verificar el acceso público y entre cuentas a los recursos con IAM Access Analyzer	Nos ayuda a obtener una vista previa y analizar el acceso público y entre cuentas de los tipos de recursos admitidos, antes de hacerla pública.

N.º	Prácticas recomendadas	Importancia
12	Utilizar IAM Access Analyzer para validar las políticas de IAM con objeto de garantizar la seguridad y funcionalidad de los permisos	Nos ayuda a verificar que las politicas creadas cumplen con las prácticas y recomendaciones.
13	Establecer barreras de protección de permisos en varias cuentas	Son un tipo de política de organización que se puede utilizar para administrar los permisos en la organización en el nivel de la organización, unidad organizativa o cuenta de AWS.
14	Utilizar límites de permisos para delegar la administración de permisos de una cuenta	Es una característica para utilizar una política administrada con el fin de establecer los permisos máximos que una política basada en identidad puede conceder a un rol de IAM.
15		
16		
17		