[Publish] - 7. Asegurar que las políticas de IAM permitan solo los privilegios requeridos para cada rol

El hallazgo de seguridad **"Asegurar que las políticas de IAM permitan solo los privilegios requeridos para cada rol"** se centra en el principio de seguridad más importante en la nube: el **principio de mínimo privilegio**. Esta práctica consiste en otorgar a una identidad (como un rol de IAM) únicamente los permisos necesarios para realizar sus tareas legítimas, y nada más.

Los roles con permisos excesivos (sobreaprovisionados) representan un riesgo de seguridad significativo. Si una aplicación o un recurso que asume uno de estos roles se ve comprometido, el atacante obtiene todos los permisos excesivos de ese rol. Esto amplifica el "radio de explosión" de un incidente, permitiendo al atacante moverse lateralmente, acceder a datos sensibles o interrumpir otros servicios.

Análisis de los Roles Reportados

Los siguientes roles de IAM han sido identificados por tener políticas potencialmente sobreaprovisionadas. Basado en sus nombres, muchos parecen haber sido generados automáticamente por servicios de AWS o frameworks de infraestructura como código.

Type	Name	Account Number
IAMRole	AmazonSageMaker-ExecutionRole-20230217T141494	890342916428
IAMRole	AmazonSageMakerServiceCatalogProductsExecutionRole	890342916428
IAMRole	AmazonSageMakerServiceCatalogProductsUseRole	890342916428
IAMRole	cdk-accel-cfn-exec-role-000316901759-us-east-1	000316901759
IAMRole	cdk-accel-cfn-exec-role-000316901759-us-west-2	000316901759
IAMRole	cdk-accel-cfn-exec-role-838155148375-us-east-1	838155148375

IAMRole	cdk-accel-cfn-exec-role-838155148375-us-west-2	838155148375
IAMRole	cdk-accel-deploy-role-000316901759-us-east-1	000316901759
IAMRole	cdk-accel-deploy-role-000316901759-us-west-2	000316901759
IAMRole	cdk-accel-deploy-role-838155148375-us-east-1	838155148375
IAMRole	cdk-accel-deploy-role-838155148375-us-west-2	838155148375
IAMRole	cdk-accel-file-publishing-role-000316901759-us-east-1	000316901759
IAMRole	cdk-accel-file-publishing-role-000316901759-us-west-2	000316901759
IAMRole	cdk-accel-file-publishing-role-838155148375-us-east-1	838155148375
IAMRole	cdk-accel-file-publishing-role-838155148375-us-west-2	838155148375
IAMRole	Dev-BOBJAPPDB-InstanceRole-1CLNU75BH6VNE	398984081329
IAMRole	Dev-CARECCNW-AS-InstanceRole-FST8IARZ4LA1	398984081329
IAMRole	Dev-CARHANADB-InstanceRole-17QAUIOYRCVHO	398984081329
IAMRole	Dev-ECCHANADB-Rhel7AR-InstanceRole-30ZKP8KLCHNQ	398984081329
IAMRole	Dev-ECCNW-AS-Rhel7AR-InstanceRole-	398984081329

	CCOFAU3KSAJ0	
IAMRole	dev-gruposanchezagent2025pocgenia-AmplifyServiceRole	174771279728
IAMRole	dev-gruposanchezagent2025pocgenia-AthenaLambdaRole	174771279728
IAMRole	dev-gruposanchezagent2025pocgenia-Bedrock-kb-Role	174771279728
IAMRole	dev-gruposanchezagent2025pocgenia-BedrockKBLambda-role-xyjhaeaz	174771279728
IAMRole	dev-gruposanchezagent2025pocgenia-ExecutionRole	174771279728
IAMRole	dev-gruposanchezagent2025pocgenia-glue-execution-role	174771279728
IAMRole	Dev-PONWDB-Rhel7AR-InstanceRole-660PMWNLM46E	398984081329
IAMRole	Dev-SLTNWDB-Rhel7AR-InstanceRole-1A96O73IUUZIQ	398984081329
IAMRole	dms-s3	498798756906
IAMRole	DMSS3AccessRole-gs-dlk-dev-s3-artifacts	498798756906
IAMRole	DMSS3AccessRole-gs-dlk-dev-s3-artifacts2	498798756906

IAMRole	DMSS3AccessRole-gs-dlk-dev-s3-landing-zone	498798756906
IAMRole	ebs-snapper-398984081329-LambdaExecutionRole-JZMZ0RJT06KI	398984081329
IAMRole	EC2-CambiarTipoInstancia	002670977573
IAMRole	EC2-Changeinstance-type	398984081329
IAMRole	EC2InstanceStartStop	613703092215
IAMRole	ForecastNotebookRole-Basic	890342916428
IAMRole	gs-dlk-dev-admin-role	498798756906
IAMRole	gs-dlk-dev-data_engineer-role	498798756906
IAMRole	gs-dlk-dev-dms-endpoint-role	498798756906
IAMRole	gs-dlk-dev-glue-notebook-role	498798756906
IAMRole	gs-dlk-dev-glue-role	498798756906
IAMRole	HED-SBX-Role	996126991518
IAMRole	OrganizationAccountAccessRole	005344269008
IAMRole	Prod-BOBJAPPDB-InstanceRole-1GBPUWRM5YQXR	398984081329
IAMRole	Prod-CARHANA-DB-InstanceRole-CWDYMWB04XZ4	398984081329
IAMRole	Prod-CARNW-AS-Rhel7AR-InstanceRole-1AU5MCMVYY2C5	398984081329
IAMRole	Prod-ECCHANADB-LVM-InstanceRole-FU1AFWXS7DJ2	398984081329

IAMRole	Prod-ECCNWAS1-Rhel7AR-InstanceRole-1DJHFC0SFPKZM	398984081329
IAMRole	Prod-ECCNWAS2-Rhel7AR-InstanceRole-1IR3DVGOE9P5R	398984081329
IAMRole	Prod-PONWDB-Rhel7AR-InstanceRole-1OXJZJKTDSJ6I	398984081329
IAMRole	Prod-SAPROUTER-InstanceRole-1SSDRZQGFZA3X	398984081329
IAMRole	Prod-SLTNWDB-Rhel7AR-InstanceRole-1X3BT5N3C26J2	398984081329
IAMRole	Prod-SOLMANABAP-InstanceRole-LRY87TR590Q8	398984081329
IAMRole	Prod-SOLMANJAVA-InstanceRole-3U3JIDVS1ER	398984081329
IAMRole	Qas-ECCHANADB-Rhel7AR-InstanceRole-51UOD97OJ8HD	398984081329
IAMRole	Qas-ECCNW-AS-Rhel7AR-InstanceRole-7W31BAJV39BM	398984081329
IAMRole	RedshiftS3	498798756906
IAMRole	RolForEc2	174771279728
IAMRole	S3_Copiar	002670977573
IAMRole	S3_Leer	996126991518
IAMRole	scn-instance-role-1127533b-1c9c-4b1b-80d9-e822ec686544	002670977573

IAMRole	scn-instance-role-1d7d1245-6053-48bd-bc79-00d6f8d5829f	498798756906
IAMRole	scn-instance-role-46f87414-471d-4383-adfb-bc9438ea85fe	002670977573
IAMRole	sftp-readwrite-policy	498798756906
IAMRole	SSMAgent	002670977573
IAMRole	StackAnalyzer-us-east-1-RSFAWS-StckAnly-Lambda-Role	398984081329

Preguntas para tu Equipo (Acción Requerida)

Para ajustar los permisos de estos roles, es crucial entender su uso real. Por favor, trabaja con los equipos de desarrollo para responder lo siguiente:

1. **Para los Roles de SageMaker:**
   - ¿A qué **buckets de S3 específicos** necesitan acceder los trabajos de SageMaker?
   - ¿Qué acciones necesitan realizar en esos buckets (ej. `GetObject`, `PutObject`, `ListBucket`)? ¿Necesitan acceso de solo lectura o también de escritura?
2. **Para los Roles de CDK:**
   - ¿Qué **recursos de AWS específicos** (ej. Lambdas, tablas de DynamoDB, colas de SQS) crea, modifica o elimina la aplicación CDK durante un despliegue (`cdk deploy`)?
3. **Para Todos los Roles:**
   - ¿Han utilizado **AWS IAM Access Analyzer** para revisar la actividad reciente de estos roles? Esta herramienta puede generar una política basada en los permisos que el rol ha utilizado realmente en un período de tiempo determinado.

Consideraciones de Costo

- **Ajuste de Políticas:** No hay **ningún costo directo** por modificar políticas de IAM o por utilizar herramientas como IAM Access Analyzer para generar políticas de mínimo privilegio.
- **Costo de Inacción:** El verdadero "costo" de no remediar este hallazgo es el **aumento del riesgo de seguridad**. Un rol sobreaprovisionado puede convertir un incidente menor en una

brecha de seguridad mayor, con costos asociados a la respuesta a incidentes, la pérdida de datos y el daño a la reputación.

Cómo Solucionarlo: Proceso para Ajustar Permisos

El objetivo es reemplazar las políticas amplias (como `AmazonS3FullAccess`) por políticas personalizadas y restrictivas.

1. **Generar una Política Base con IAM Access Analyzer:**
   - Navega a la consola de **IAM** y selecciona **Access Analyzer**.
   - En la sección **Generar política**, selecciona el rol que deseas analizar y un rango de fechas (ej. los últimos 90 días).
   - Access Analyzer revisará los registros de CloudTrail y generará una política borrador que contiene solo las acciones y recursos que el rol ha utilizado.
2. **Revisar y Refinar la Política:**
   - Revisa cuidadosamente la política generada. Asegúrate de que los permisos tengan sentido y no incluyan acciones inesperadas.
   - Refina la política manualmente si es necesario, por ejemplo, limitando aún más los recursos a ARNs específicos en lugar de usar comodines (`*`).
3. **Reemplazar la Política en el Rol:**
   - Navega al rol en la consola de **IAM**.
   - En la pestaña **Permisos**, desvincula (detach) la política administrada por AWS que es demasiado permisiva.
   - Crea una nueva política en línea (inline policy) o una política gestionada por el cliente (customer-managed policy) pegando el JSON de la política refinada y vincúlala (attach) al rol.
4. **Probar la Funcionalidad:**
   - Después de aplicar la nueva política restrictiva, es **crucial** probar la funcionalidad asociada al rol. Ejecuta el trabajo de SageMaker o el despliegue de CDK para confirmar que todo sigue funcionando como se espera. Si algo falla, revisa los mensajes de error (generalmente "Access Denied") para identificar el permiso que falta y ajústalo.

Recomendación

Se recomienda que se inicie un proceso para revisar y ajustar los permisos de todos los roles identificados. El principio de mínimo privilegio no es un ejercicio de una sola vez, sino un ciclo continuo. Utiliza herramientas como **IAM Access Analyzer** de forma regular para identificar y eliminar los permisos no utilizados, manteniendo así una postura de seguridad robusta.

Referencias

- Security best practices in IAM - AWS Identity and Access Management