Academia DevOps & Cloud · @jemjaf

IAM EN SIMPLE: USUARIOS, ROLES Y POLÍTICAS

> **IAM** = quién puede hacer qué en la nube. Es aburrido hasta que un error aquí **tumba producción** o deja todo abierto.

LAS TRES PIEZAS

Pieza	Analogía	Cuándo usarla
Usuario	Cuenta con identidad fija	Solo para humanos en consola o llaves de CI (evitar en apps y servidores)
Rol	Credencial **temporal** que asumes o que asume un servicio	EC 2 , Lambda, ECS, CI/CD — **siempre preferible** a llaves de acceso en disco
Política	Lista de permisos en JSON (`Allow` / `Deny` + `Resource`)	Se adjunta al usuario o rol; define exactamente qué APIs puede llamar

TIPOS DE POLÍTICA (AWS)

Tipo	Qué es	Cuándo usarla
Managed AWS	Gestionada por AWS, siempre actualizada	Punto de partida; revisa qué otorga antes de confiar
Managed de cliente	La defines tú, reusable en varios roles	Cuando `ReadOnlyAccess` es demasiado amplia o demasiado estrecha
Inline	Embebida directamente en el usuario/rol	Solo para permisos únicos y no reutilizables; dificulta auditoría
Boundary	Techo máximo de permisos del rol	Delegar creación de roles sin que puedan escalar privilegios

ERRORES COMUNES

Error	Por qué es peligroso	Corrección
`"Action": "*"` + `"Resource": "*"`	Acceso total a la cuenta — blast radius máximo	Política acotada al servicio y recurso concreto
Llaves de acceso en código	Fin en Git o en logs → rotación urgente	Rol con `AssumeRole` ; nunca credenciales hardcodeadas
Usuario root para tareas del día a día	No se puede restringir ni auditar bien	Crear usuario/rol con los permisos mínimos necesarios
Permisos nunca revisados	El entorno crece y los permisos se quedan grandes	`IAM Access Analyzer` + rotación y auditoría periódica

IAM EN LOS TRES GRANDES PROVEEDORES

Concepto	AWS IAM	Azure RBAC	GCP IAM
Identidad de servicio	IAM Role (AssumeRole)	Managed Identity	Service Account
Unidad de permiso	Policy (JSON)	Role Definition	Role (predefined / custom)
Scope de asignación	Resource / Account / Org	Subscription / RG / Resource	Project / Folder / Org

REGLA DE ORO

Mínimo privilegio: solo los permisos necesarios, solo al recurso que los necesita, solo durante el tiempo que los necesita.

FRASE PARA ENTREVISTA

"IAM separa **identidad** (quién eres) de **autorización** (qué puedes hacer). En producción prefiero **roles con políticas acotadas** antes que llaves de acceso de larga duración en servidores — si el servidor se compromete, el blast radius es mínimo."

🌟 COMUNIDAD SKOOL — SIGUIENTE PASO

¿LISTO PARA PRACTICARLO DE VERDAD?

Esta guía es el mapa; la diferencia suele estar en **hacer labs sin quedarte atrapado ante un error** durante tres días. En mi comunidad de Skool aprendes con **cursos** dentro de la plataforma, **sesiones en vivo** y **soporte técnico** cuando tu entorno no levanta o tu despliegue falla.

👥 **Entra en la comunidad — skool.com/jemjaf** ↗️

Qué hay dentro (según la oferta vigente en Skool):

- 📚 **Cursos** grabados para ir a tu ritmo, más **lives** temáticos (cloud y DevOps)
- **Sandboxes temporales en AWS, Azure y GCP**: practica en nube **real** sin el miedo a una factura sorpresa
- 🛠️ **Soporte directo** para destrabar laboratorios, código y dudas puntuales
- 📈 **Career Center** para revisión de CV y LinkedIn con mirada técnica
- 📂 Materiales prácticos y guías que acompañan lo que enseño en clase

👉 **Únete en skool.com/jemjaf** ↗️ — Es formación hands-on y acompañamiento; sin prometer empleos automáticos. El objetivo es que **lleves práctica defendible**.