# MODUL 1

# PENGENALAN KONSEP IAM

# (*IDENTIFY AND ACCESS MANAGEMENT*)

---

## 1.1 Topik Pembahasan

1. Pengertian IAM.
2. Identitas pada IAM (User, Group, Role, Federation).
3. Autentikasi dan Otorisasi.
4. Keamanan dalam IAM.
5. Praktik Terbaik Keamanan IAM.
6. Pentingnya IAM dalam keamanan cloud.

## 1.2 Tujuan Praktikum

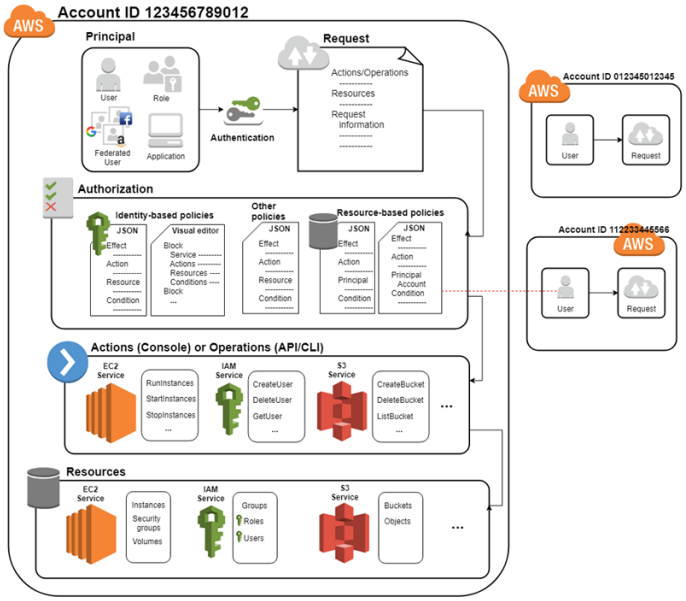
1. Praktikan memahami pengertian dan fungsi IAM di AWS.
2. Praktikan mengetahui jenis-jenis identitas dalam IAM.
3. Praktikan memahami konsep autentikasi dan otorisasi.
4. Praktikan memahami aspek keamanan dalam pengelolaan identitas.
5. Praktikan mengetahui praktik terbaik dalam penerapan IAM di AWS.

## 1.3 Alat dan Bahan

1. Laptop
2. Browser dengan koneksi internet

## 1.4 Dasar Teori

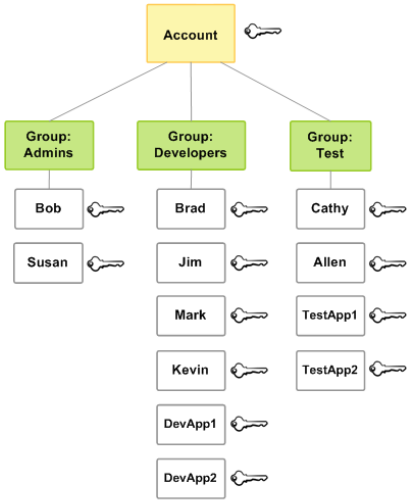
### 1.4.1 Pengertian IAM




Gambar 1 Alur Kerja IAM

*Identify and Access Management* (IAM) merupakan layanan dari AWS yang digunakan untuk mengatur siapa saja yang dapat mengakses sumber daya dan apa yang dapat mereka lakukan. IAM menjadi fondasi keamanan di AWS karena setiap *request* yang masuk akan deverifikasi identitasnya terlebih dahulu sebelum diberi izin. Ketika pertama kali membuat akun AWS, identitas *root user* otomatis tercipta dengan akses penuh ke semua layanan. *Root user* tidak disarankan untuk aktivitas sehari-hari karena terlalu beresiko. Sebagai gantinya, administrator dapat membuat identitas tambahan berupa *user, group, role* sesuai kebutuhan.

### 1.4.2 Identitas IAM



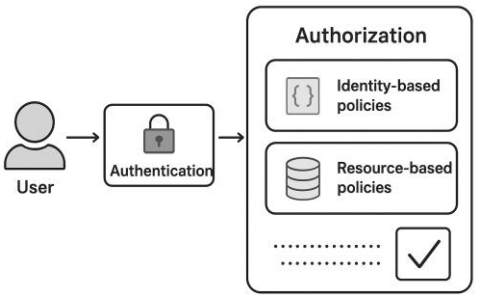

Gambar 2 Struktur IAM user & group

Identitas dalam IAM dibagi menjadi beberapa jenis:

- User : digunakan untuk individu dengan kredensial permanen.
- Group : kumpulan user yang memiliki izin sama.
- Role : identitas sementara yang dapat dipinjam aplikasi atau layanan.
- Federasi Identity : identitas eksternal yang dapat masuk melalui role.

*User* biasanya dipakai untuk individu yang login ke AWS *Console*. *Group* memudahkan manajemen izin secara kolektif. *Role* lebih aman untuk aplikasi karena menggunakan kredensial sementara. Federasi memungkinkan integrasi identitas eksternal tanpa harus membuat *user* IAM permanen untuk tiap orang.

### 1.4.3 Autentikasi dan Otorisasi




Gambar 3 Alur Autentikasi dan Otorisasi IAM

Setiap permintaan ke AWS melewati dua tahap utama:

- Autentikasi : verifikasi identitas (misalnya *password, access key*, MFA).
- Otorisasi : menentukan apakah identitas diizinkan melakukan aksi

tertentu berdasarkan *policy*.

Secara default, semua permintaan ditolak kecuali ada *policy* yang memberikan izin. Jika ada peraturan *explicit deny*, maka permintaan tetap ditolak walaupun ada izin lain.

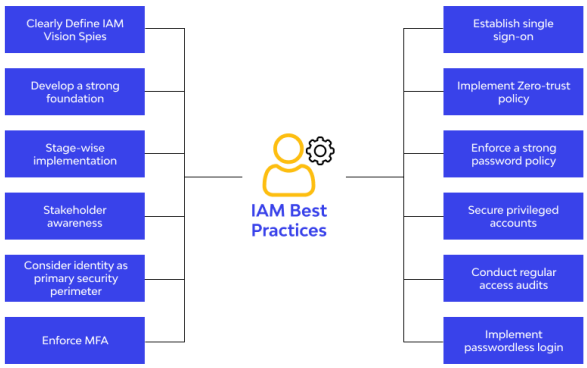
### 1.4.4 Keamanan IAM

Keamanan adalah aspek penting dalam pengelolaan IAM. AWS memberikan beberapa rekomendasi:

- Lindungi *root user* dengan *password* kuat dan MFA, gunakan hanya untuk hal khusus.
- Gunakan MFA pada *user* dengan akses sensitif.
- Utamakan *credentials* sementara melalui role dibanding access key permanen.
- Terapkan kebijakan *password* yang kuat serta lakukan rotasi *credential* secara berkala.
- Audit aktivitas menggunakan AWS *CloudTrail* untuk memastikan keamanan identitas.

Dengan penerapan prinsip keamanan ini, organisasi dapat meminimalisir risiko akses ilegal atau kebocoran data.

### 1.4.5 Praktek Terbaik IAM




Gambar 4 Praktik Terbaik IAM

Beberapa praktik yang disarankan AWS:

- Terapkan prinsip *least privilege* (akses minimum sesuai kebutuhan).
- Gunakan AWS *Managed Policy* untuk kebutuhan umum, lalu buat

*policy* kustom jika spesifik.

- Audit identitas dan *policy* secara rutin, hapus yang tidak digunakan.
- Gunakan IAM *Access Analyzer* untuk memeriksa kemungkinan akses publik.
- Manfaatkan kondisi dalam *policy*, seperti hanya dari IP tertentu atau hanya lewat koneksi SSL.

Dengan praktik terbaik ini, administrator bisa lebih mudah menjaga keamanan dan mengontrol akses di lingkungan AWS.

### 1.4.6 Pentingnya IAM

IAM adalah pondasi keamanan di AWS. Hampir semua layanan, mulai dari EC2, S3, Lambda hingga RDS, menggunakan IAM sebagai pengatur akses. Dengan IAM, organisasi dapat:

- Menetapkan hak akses yang tepat sesuai peran.
- Mengurangi risiko penyalahgunaan akses.
- Menjamin kepatuhan terhadap standar keamanan organisasi.