IAM = WHO CAN ACCESS WHAT?

IAM stands for "Identity and Access Management." IAM is how cloud platform providers, such as AWS and Google Cloud, systematically define users, roles and permissions, and what resources can be created and accessed.

IAM POLICY ANALYZERS

Cloud providers make tools called policy analyzers that can help you 'right-size' your settings. They can validate your existing settings and identify unused roles and permissions, which should be removed, along with no longer needed users.

WHO

Users:

- Humans:
 - Zero-trust
 - Require identity providers, like SAML or LDAP
 - Enforce MFA
 - Avoid long lived passwords
 - Rotate any secrets regularly
- Non-humans (applications and machine workers):
 - Use temporary credentials only
 - single role for single responsibility
 - Leverage certificates for access

Root:

- Don't use for everyday tasks
- Protect credentials and credential recovery path
- Rotate credentials regularly

CAN ACCESS

Roles:

- Sets of users that need similar permissions
- Easier to manage groups than individual permissions

Permissions:

- Always apply principle of least privilege
- EPARC model
 - Effect what should happen if permission is allowed
 - Principle the user that is allowed access
 - Action what will be done if access is allowed
 - Resource the service or data to be accessed
 - Condition "But Only If" statements use often

Take a staged approach:

- Give new and exploratory projects more privileges
- Add more restrictions as you move towards production

The resources and services users can access:

 Authenticate with a certificate authority which will automatically generate and manage certificates

Think about your data perimeter:

 'trusted identities' can access 'trusted resources' from 'expected locations'

