What is ABAC for AWS?

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes.

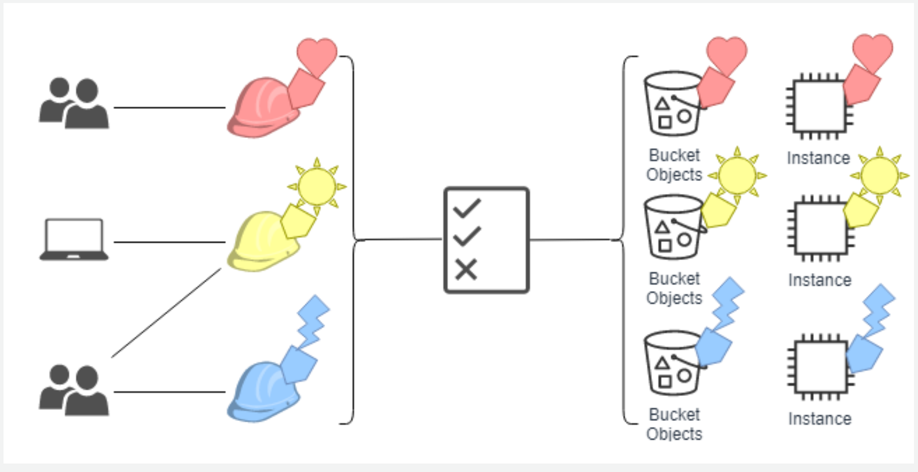
In AWS, these attributes are called *tags*

Tags can be attached to IAM principals (users or roles) and to AWS resources.

You can create a single ABAC policy or small set of policies for your IAM principals. These ABAC policies can be designed to allow operations when the principal's tag matches the resource tag.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

For example:
You can create three roles with the `access-project` tag key.
Set the tag value of the first role to `Heart`, the second to `Sun`, and the third to `Lightning`.
You can then use a single policy that allows access when the role and the resource are tagged with the same value for `access-project`


Bucket Objects
Instance
Bucket Objects
Instance
Bucket Objects
Instance