AWS Certified Cloud Practitioner
Training Bootcamp

Identity Access Management (IAM) Basics 101

Identity Access Management (IAM) Basics 101

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources

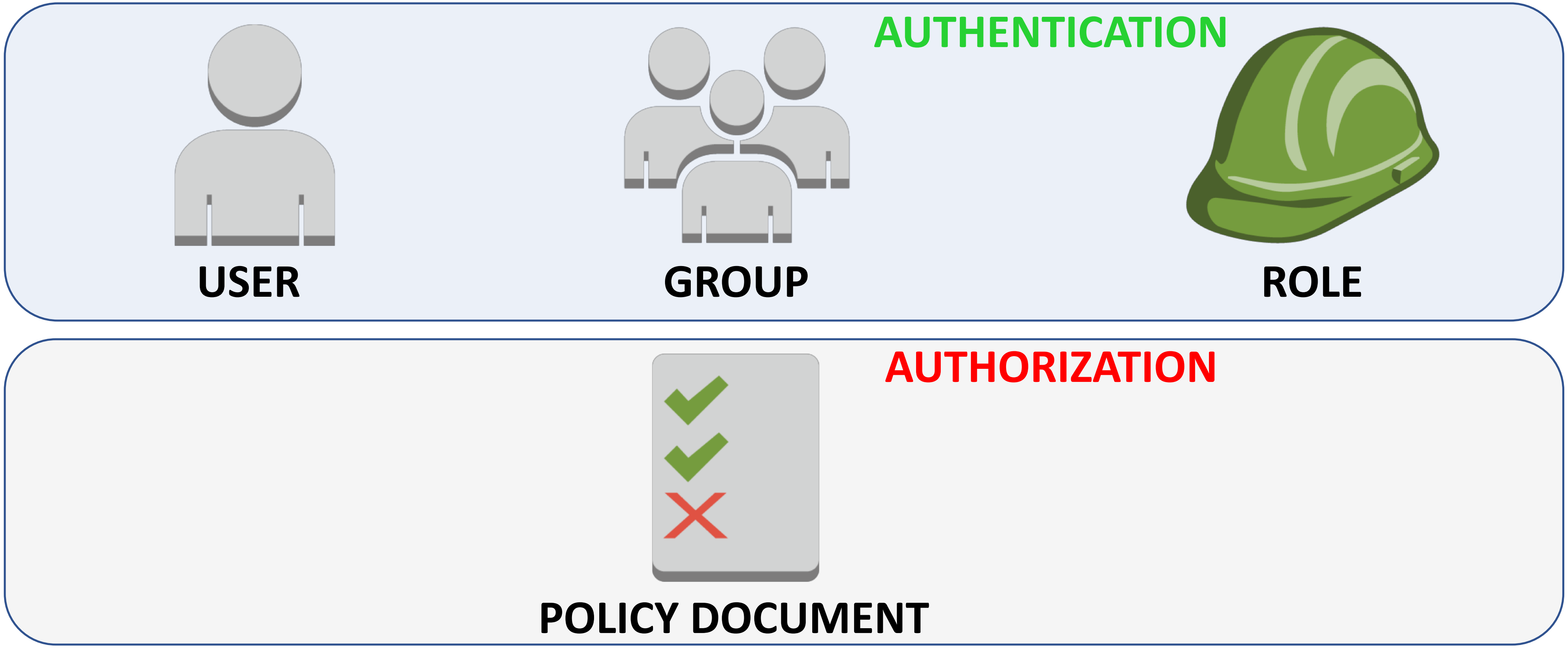
- You use IAM to control *who* is authenticated (signed in) and authorized (has permissions) to use *what* resources

- The key in understanding IAM is represented by these two concepts: authentication and authorization

- Let’s dig more on the subject …

Identity Access Management (IAM) Basics 101

- In order to understand IAM, we need to define and understand the following concepts



AUTHENTICATION

USER

GROUP

ROLE

AUTHORIZATION

POLICY DOCUMENT

IAM Key Concepts

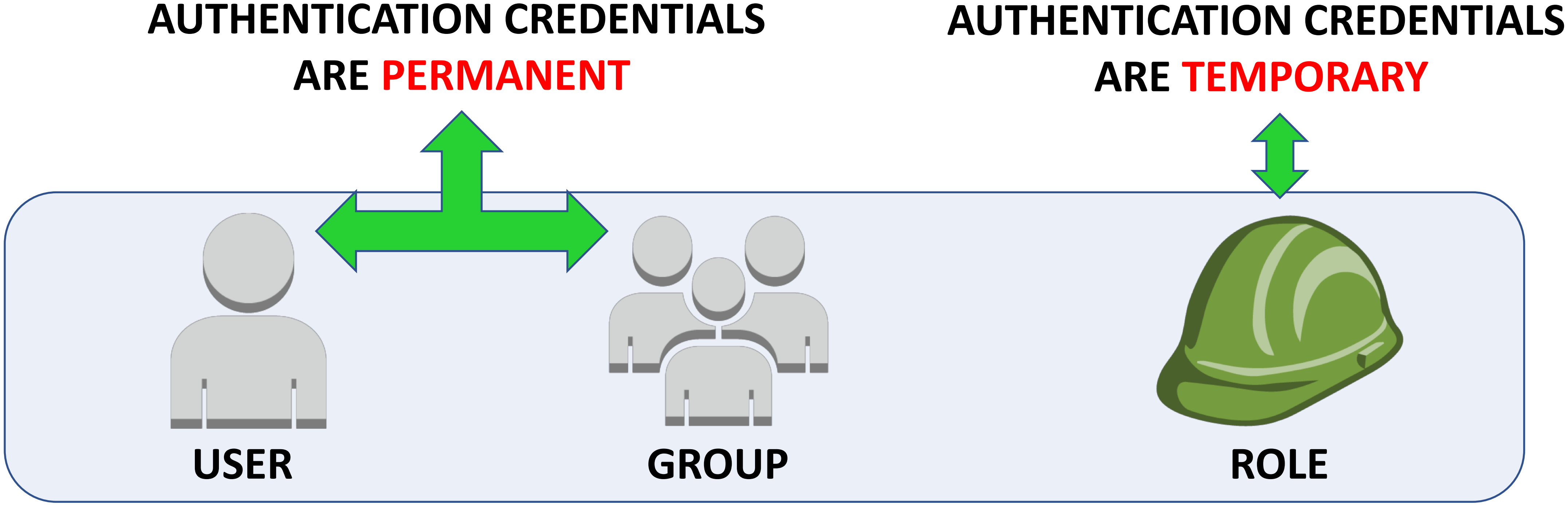
- A USER is a permanent named operator; it can be a human or it can be a machine, or another AWS service

- A GROUP is a collection of users and usually contains multiple users; a user can belong to multiple groups

- A ROLE is an operator too, another authentication method just like a user; a role can be as well a human or another AWS service

- What's the difference ???

Permanent vs Temporary Authentication


AUTHENTICATION CREDENTIALS ARE PERMANENT
AUTHENTICATION CREDENTIALS ARE TEMPORARY
USER
GROUP
ROLE

IAM Key Concepts – Policy Documents

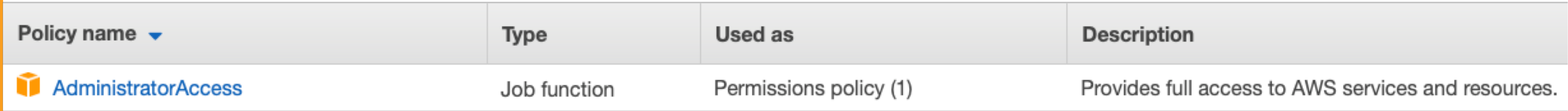
- Once a user/role is authenticated by AWS, it will be given permissions (authorized) based on policy document(s) that are attached to it
- Policy documents (JSON format) can be attached to a user, group or role; if policy is attached to group, once a user joins the group, it will inherit the attached policies
- JSON - JavaScript Object Notation
- How does a policy actually look like ?

AWS IAM Policy Example

AUTHORIZATION

POLICY DOCUMENT

```
{
  "Version": "2012-10-17",          Document Version
  "Statement": [
    {
      "Effect": "Allow",            Permit
      "Action": "*",                Anything
      "Resource": "*"               On Any AWS Resource
    }
  ]
}
```



Policy name	Type	Used as	Description
AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and resources.

IAM – The Complete Picture

- A principal (or operator), human or AWS service, makes a request for an action on an AWS resource (API call)
- First, the user is authenticated, based on username/password pair or access key ID / secret access key (programmatic access – CLI, API, SDK)
- The user's action will be permitted (authorized) based on attached policies
- Every API call will be recorded in AWS by CloudTrail

AWS Certified Cloud Practitioner Training Bootcamp

Thank you