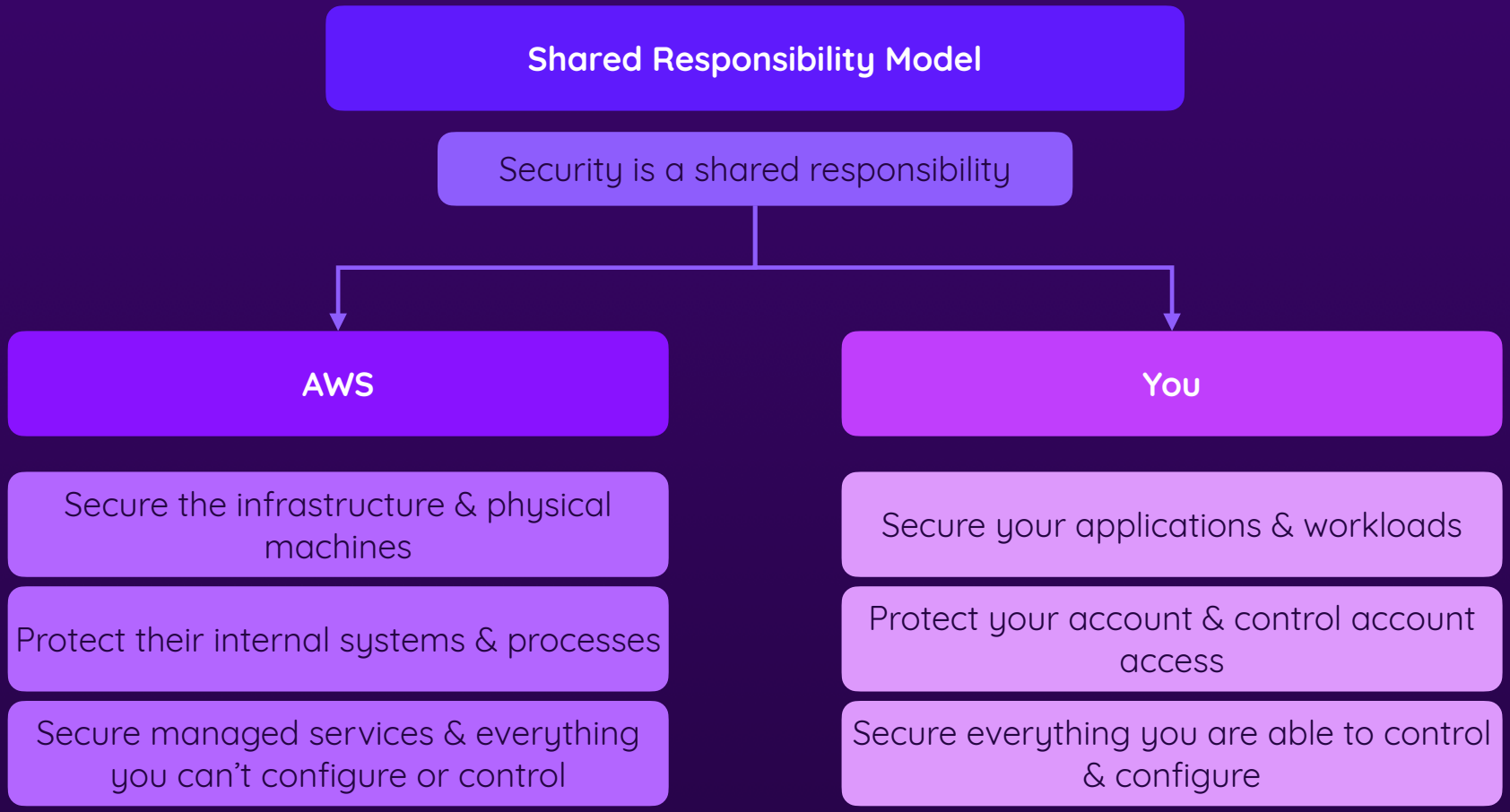
ACADEMIND

Getting Started with AWS Security

Accounts, Authentication & Service Protection

- The AWS Security Model
- Managing Accounts & Authentication
- Understanding Permissions & Access Control

AWS Security Model



Protecting Your Account

Secure Credentials

- Choose a strong password
- Change it frequently
- Don’t share your credentials!

Multi-Factor Authentication

- Enable MFA
- Use a digital or physical solution

Utilize IAM Users

- Create IAM users for accessing your account
- Every person (e.g. colleague) should use a separate user

What Is IAM?

Identity & Access Management

Identities		Access Management
The **entity** for which access rights / permissions are controlled	+	The permissions that are granted (or not granted) to an entity
Who is allowed (or not allowed) to do something?		**What** is an entity allowed to do (with a given service)?
Users, User Groups & Roles		**Permissions**, managed via **Policies**

Users, User Groups & Roles

Users

Typically assigned to humans

Every person that should be able to access the AWS account gets a user

User Groups

Group users to share permissions

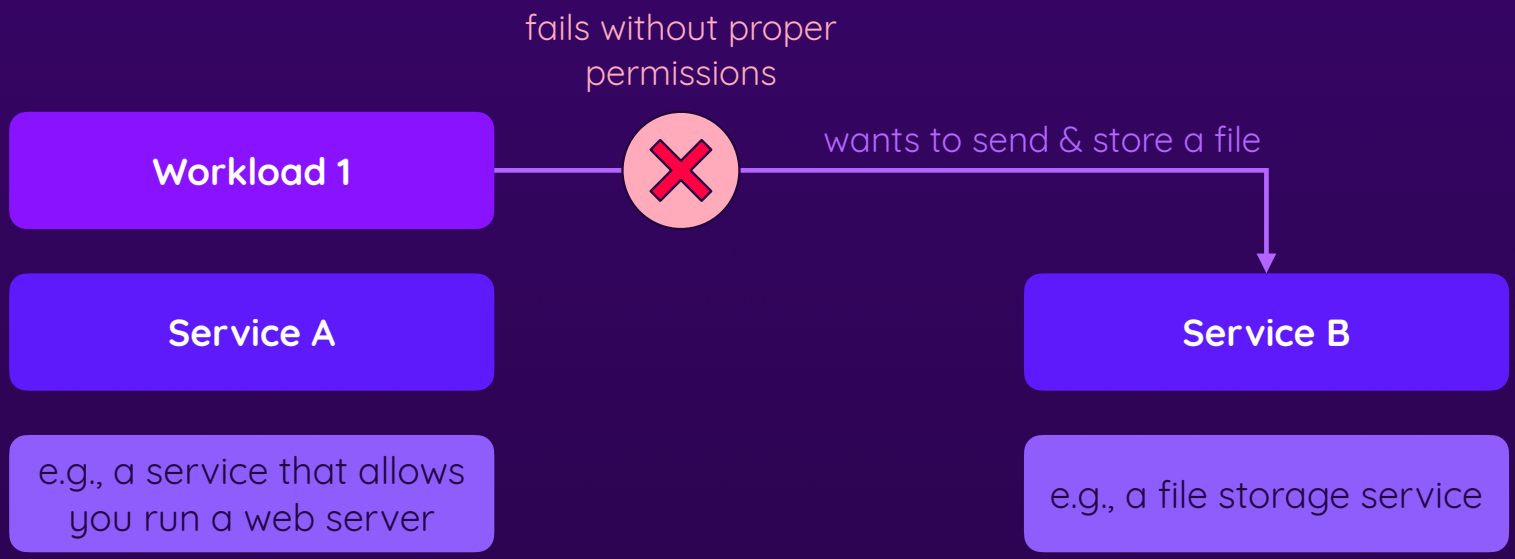
Avoid unnecessary permission copying or tedious per-user access management

Roles

Typically used by services

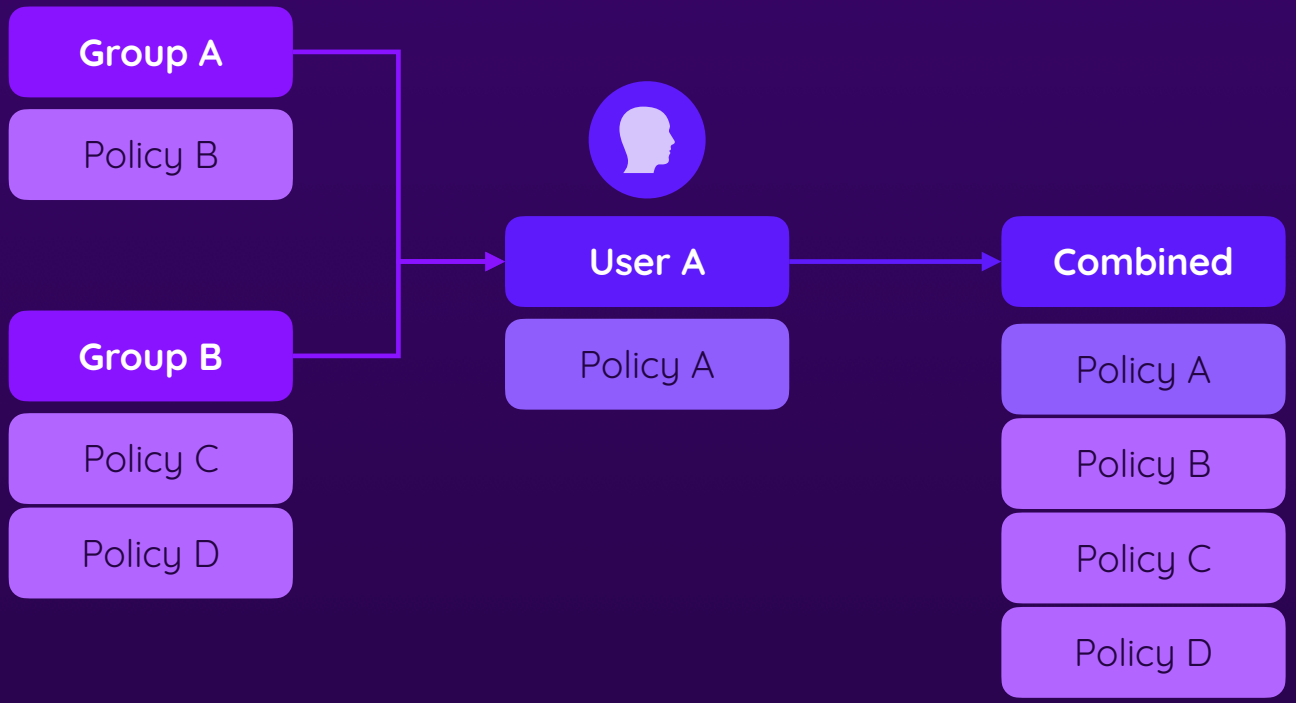
Allows services to perform AWS tasks (e.g., start or use another service)

Understanding Roles

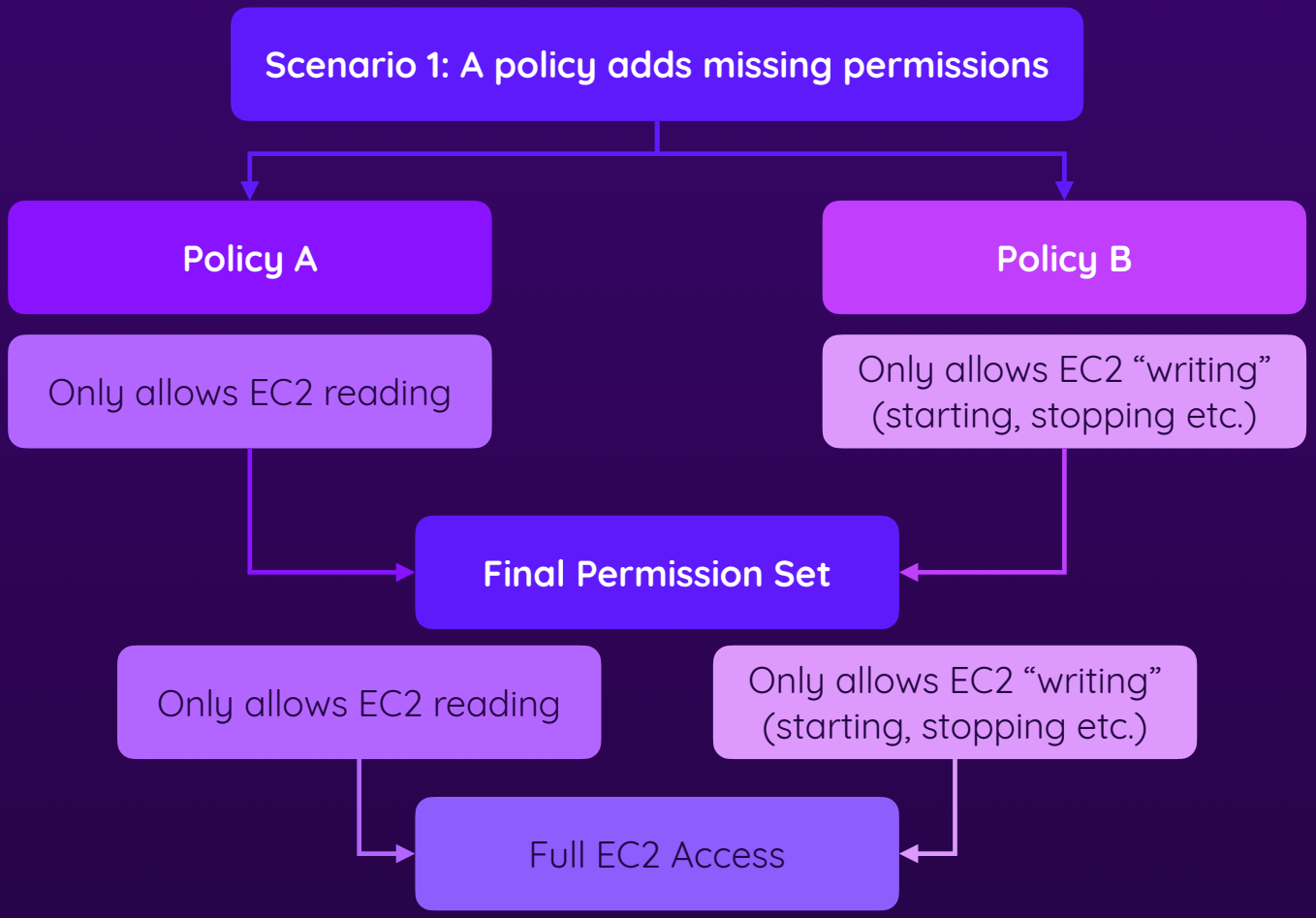


Understanding Roles

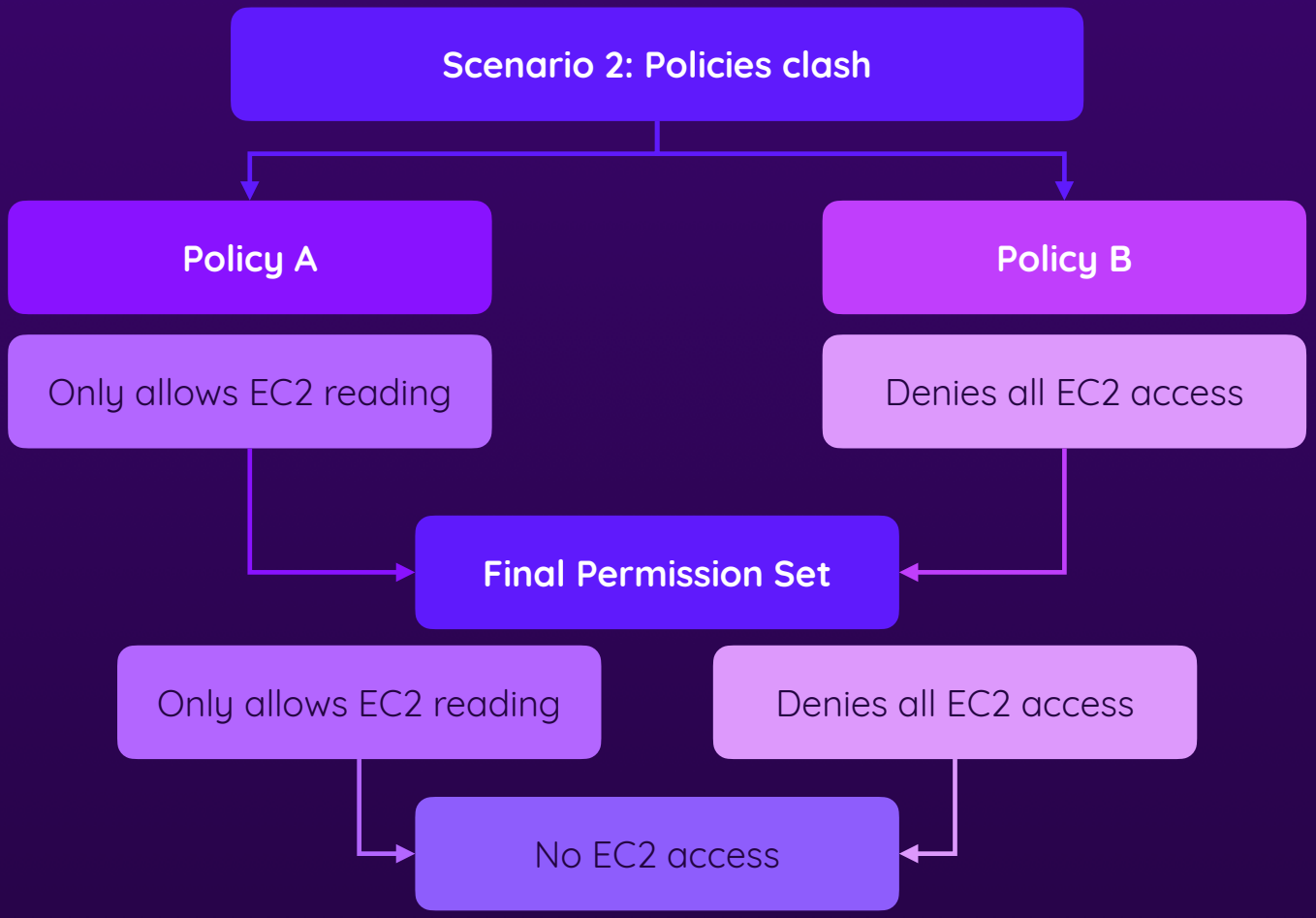
Policies Are Combined



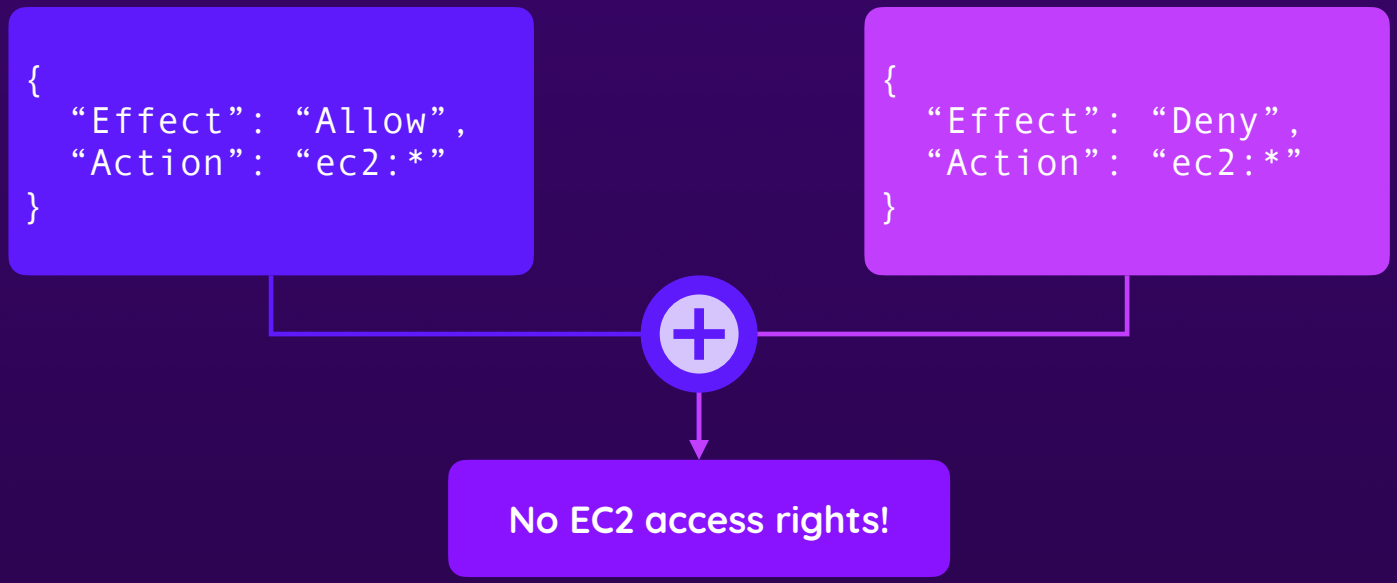
What Happens If Permissions Clash?



What Happens If Permissions Clash?



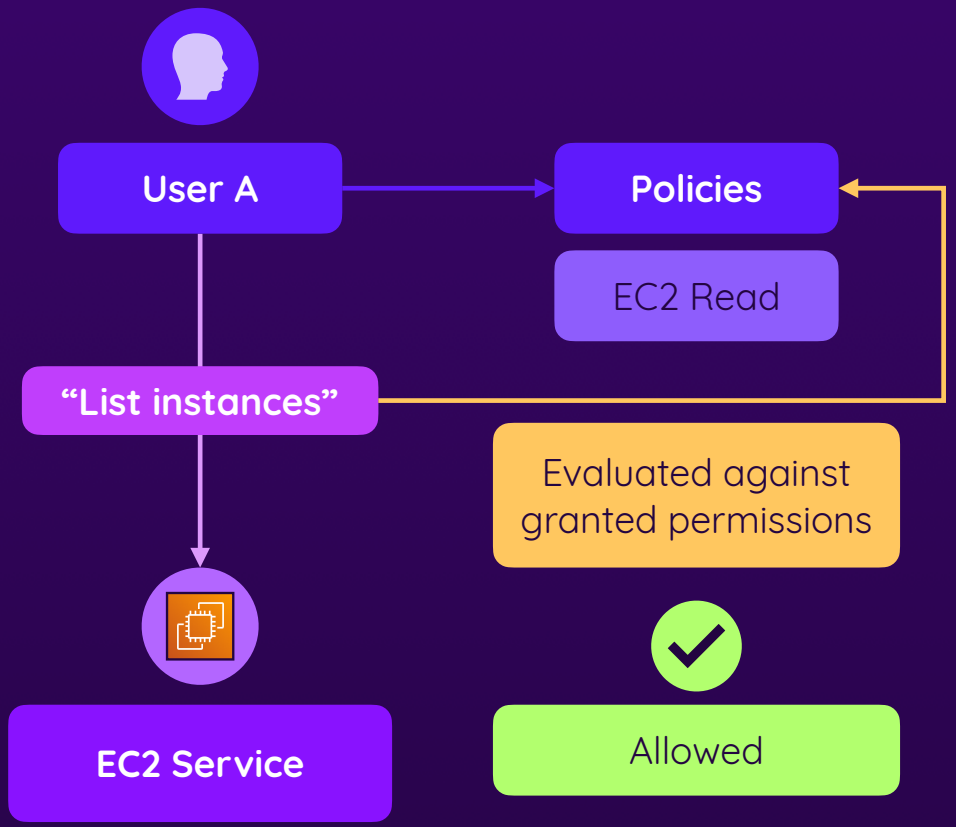
Explicit DENY Statements Always Win!



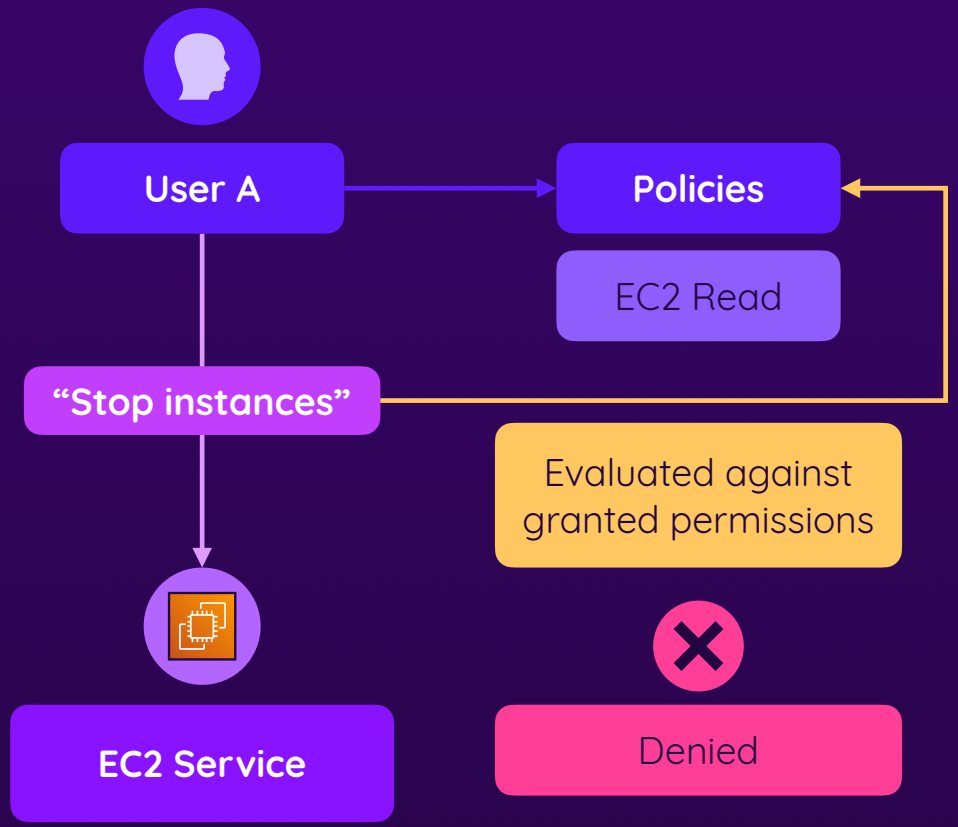
Core IAM Policy & Permission Rules

1. By default, no permissions are granted to any identity (user, user group, role)
2. Multiple policies can be combined to extend the set of permissions
3. Explicit DENYs overwrite explicit ALLOWs

When Are Permissions Evaluated?



When Are Permissions Evaluated?



Summary

Shared Responsibility Model

- Every party secures the things it controls
- AWS secures the infrastructure & managed services
- You secure your applications, workloads & service configs

Account Protection

- Use secure passwords & MFA
- Use IAM users instead of root access
- Don’t share credentials

IAM Key Concepts

- IAM identities (users, user groups, roles) define the WHO
- Policies & permissions define the WHAT
- Policies contain permissions and are attached to identities
- No permissions by default, DENY overwrites ALLOW