Identity and Access Management (IAM)

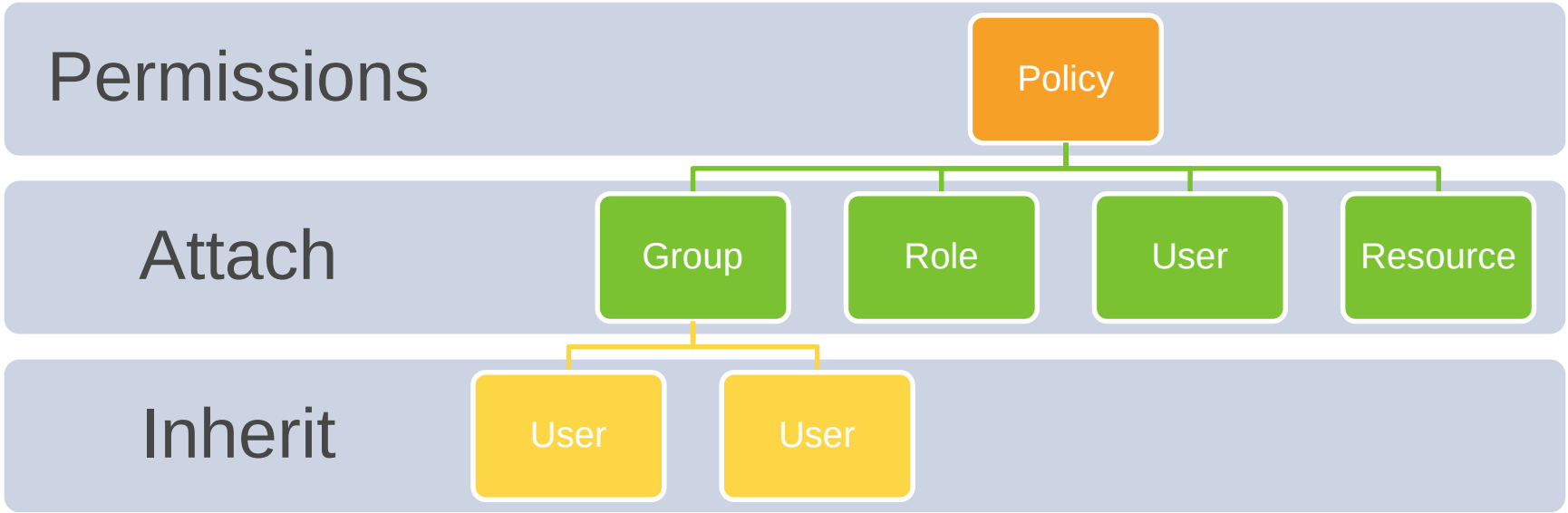
Content Prepared By: Chandra Lingam, Cotton Cola Designs LLC

amazon web services

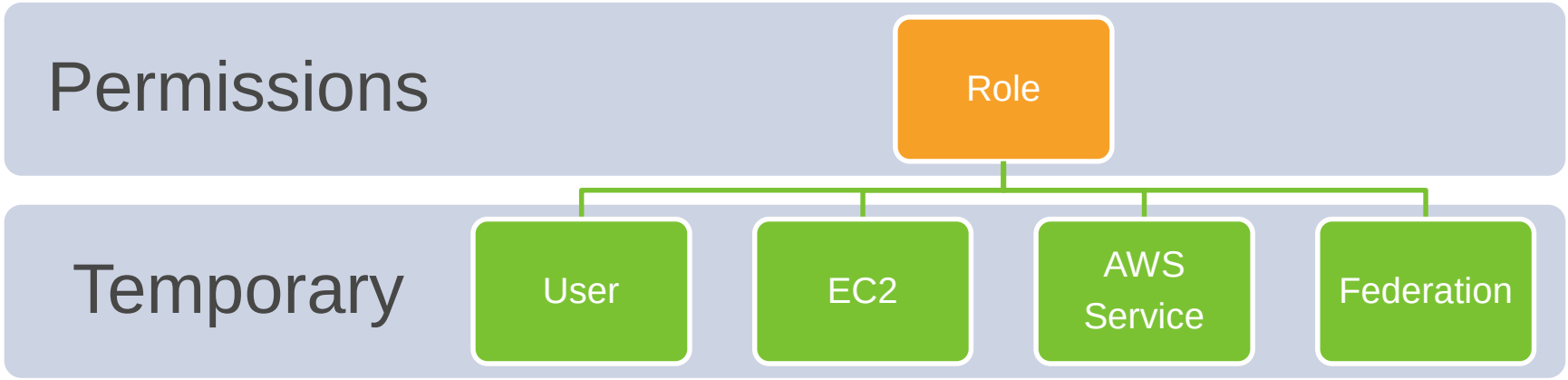
Identity and Access Management (IAM)

- Manage Users
- Granular permissions to administer and access resources
- Grant Permission to EC2 instances to access resources
- Federation - Grant temporary access to your resources for users in corporate network or internet identity providers
- Audit Trail using CloudTrail
- No additional charge

Concepts

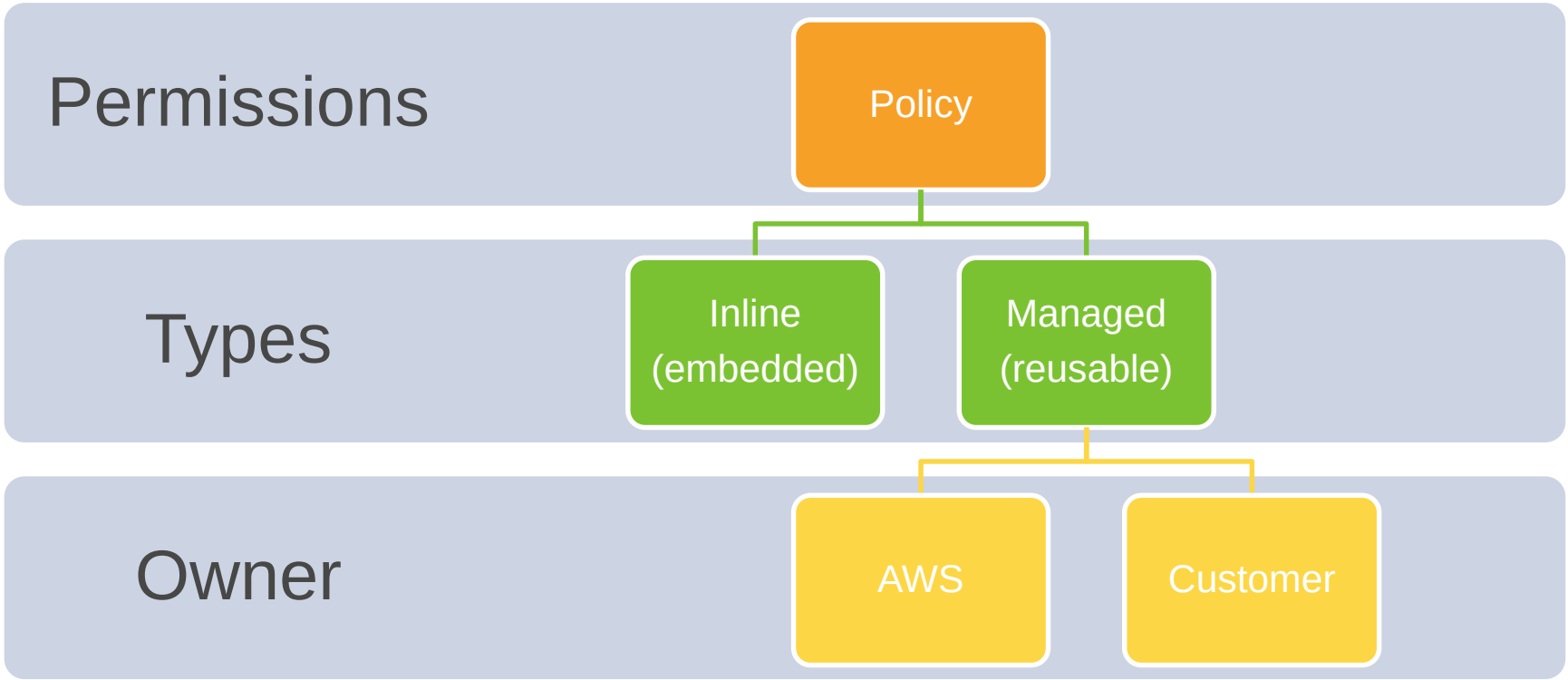


Role



Role has two parts: 1. Who can assume the role and 2. What permissions does a role have

Policy



Users

Root Account

- Account Created when you sign up for AWS
- Credential consists of Email Address, Password
- Unrestricted Access to all resources in your AWS account including billing
- Not recommended for every day use – instead create IAM Users

Users

IAM Users

- Users that correspond to actual employees in your organization
- Part of your AWS account
- Management Console Access – User ID and Password
- Programmatic and CLI Access - Access Key credentials
- Do not share user credentials
- Some users can be applications – To access AWS resources from corporate network using Access Key credentials

Users

Federated Users

- Root Account and IAM Users are part of AWS Account
- Federated Users are users managed outside of AWS who can gain access to AWS resources
- Your Users have identities in Corporate Directory
    - Security Access Markup Language (SAML) 2.0 Compliant Corporate Directory - can provide Single Sign On
    - Non SAML 2.0 need an identity broker application
    - Microsoft Active Directory can establish trust using AWS Directory Service

Users

Federated Users

- Your Users have Internet Identities (Amazon, Facebook, Google, any OpenID Compatible provider)
    - Use Amazon Cognito service for identity federation
- Federated Users get temporary security credentials and are associated with specific IAM Role
    - IAM Roles defines permissions for AWS resources

Identity Federation

Flow: Cognito Identity Federation

Users outside of IAM

Some Services maintain their own mechanism for securing access

- EC2 Instances
  - Linux – Key Pairs for login access to instances
  - Windows – User Name and Password
- Relational Database Service
  - Database specific User Name and Password

Amazon Resource Name (ARN)

- Unique identifier for a resource in AWS
- Used for identifying users, other resources that belong to an AWS account
- Permissions are specified using ARN
- Examples
- More Examples

Policy Document

- Policy document list permissions
- JSON format
- Contains:
  - Effect: Allow/Deny
  - Principal: Who is allowed access
  - Resource: Which AWS resource does this permission apply to?
  - Action: What actions are allowed or denied on that resource
  - Condition: Additional conditions for fine grained control

Demo

CLI Reference

Demo - Admin Group Review

Demo 1: S3 – Bucket Level Policy

Demo 2: S3 – Identity Level Policy

- Inline Policy
- Add Another User with inline policy
- Allow Bucket Location Access for Users
- Inline policy requires manual changes
- Managed Policy – reusable and version tracking
- Group Level Policy

Demo

Demo 3: S3 – Policy Variables for home directory

Demo 4: S3 - Limit IP Access Restrictions

Demo 5: S3 – VPC Access Restrictions

Demo 6: EC2 instance roles (covered as part of EC2 lecture)

Demo 7: Cross Account Access with Role

IAM Evaluation Logic

Flow: IAM Policy Evaluation

Flow: Condition Evaluation

IAM Best Practices

Video: SEC 302 IAM Best Practices to Live By

IAM Policy Overview

Video: SEC 305 How to become an IAM Policy Ninja in 60 minutes or less