aws training and certification

AWS Identity and Access Management (IAM)

Module 5

0

Module 5

aws training and certification

The architectural need

Your organization is big enough now that team members are specializing into roles. You need the protection and access control afforded by need-to-have authorization

Module Overview

- IAM Users, Groups, and Roles
- Federated Identity Management
- Amazon Cognito
- AWS Organizations

1

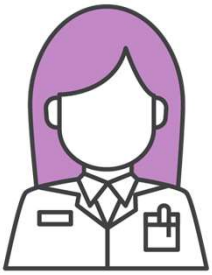
aws training and certification

Account Users and IAM

2

The AWS Account Root User

aws training and certification



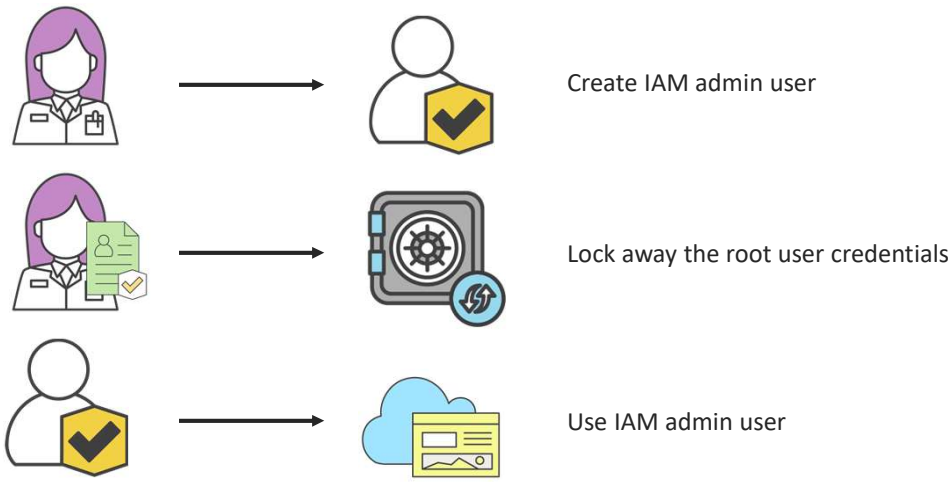
This account has **full** access to **all** AWS services and resources.

- Billing information
- Personal data
- Your entire architecture and its components

The AWS account root user has *extreme* power and cannot be limited

3

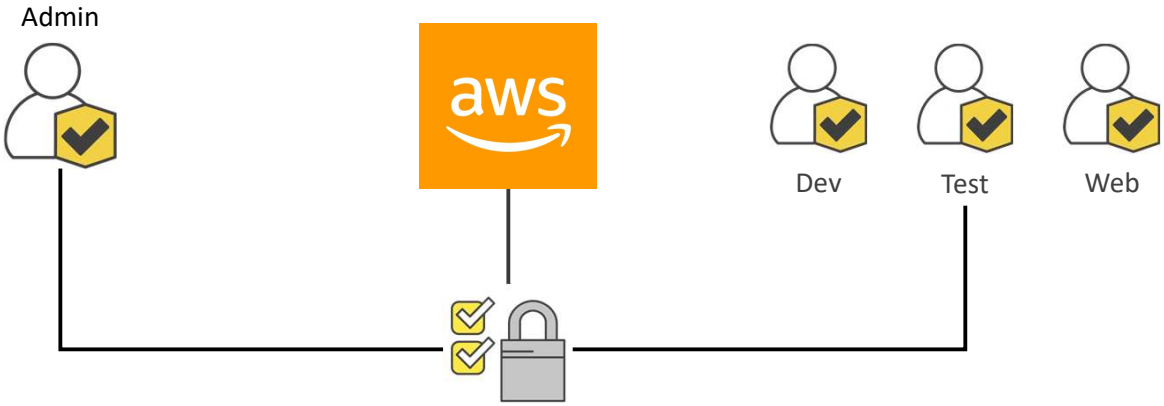
A Safer Way to Administer



4

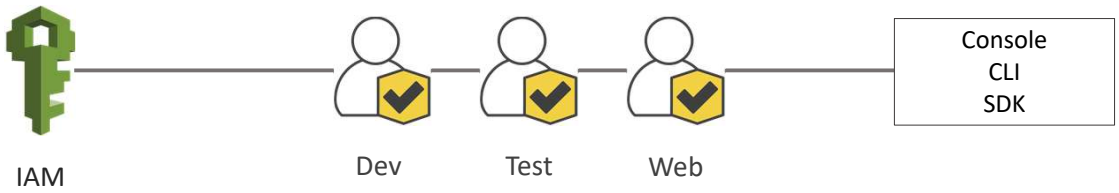
Everybody Wants to Rule the World

Problem: You need to be able to restrict access granularly



5

AWS Identity and Access Management



- Integrates with other AWS services
- Federated identity management
- Secure access for applications
- Granular permissions

6

IAM Principals

IAM user | Federated user | IAM role | Identity provider (IdP)

7

IAM Users

IAM User

IAM users are not separate AWS accounts; they are users within your account.

Each user has their own credentials.

IAM users are authorized to perform specific AWS actions based on their permissions.

8

The Birth of an IAM User

IAM User

There are no default permissions.

Access to the AWS Management Console or CLI must be explicitly granted.

9

Granting Permission

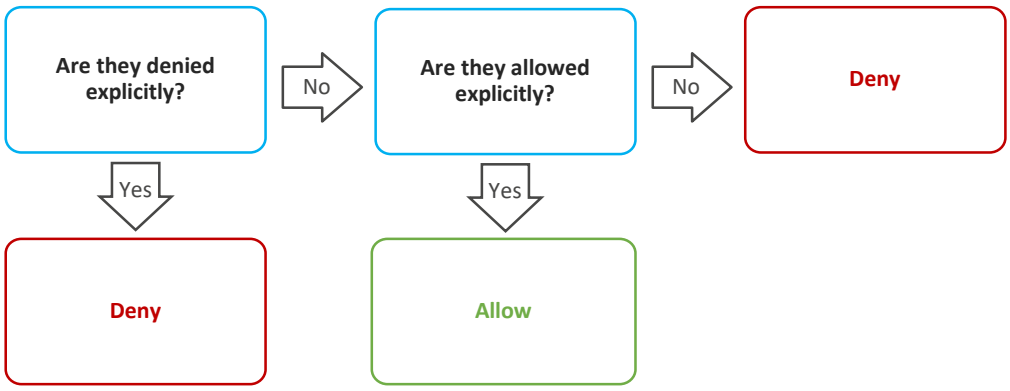
Policy

- A formal declaration of one or more permissions
- Evaluated at the time of request
- IAM policies ONLY control access to AWS services
- IAM has no visibility above the hypervisor

10

IAM Permissions

How IAM determines permissions:



11

Granting Permission

Policy

- **Resource-Based** – Attached to an AWS resource
- **Identity-Based** – Attached to an IAM principal

12

Identity-Based Policy

Identity-based policy

Attached to:

- User
- Group
- Role

Control:

- Actions performed
- Which resources
- What conditions are required

Types of Policies:

- AWS-managed
- Customer-managed
- Inline

13

Resource-Based Policies

Resource-based policy

Attached to:

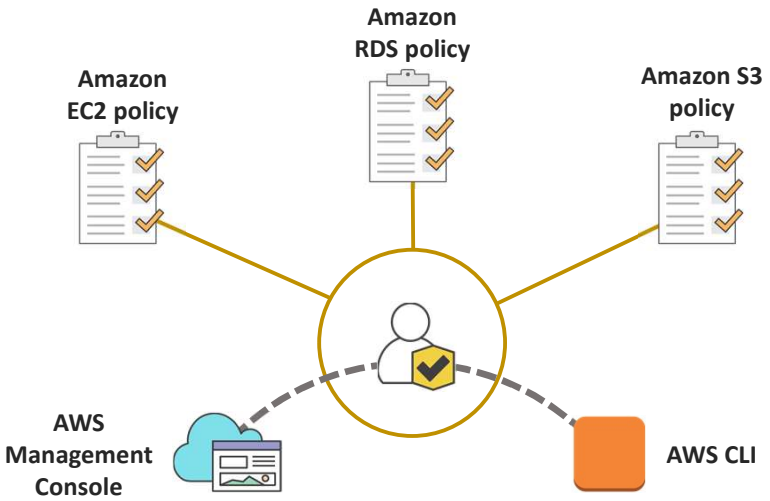
- AWS resources such as Amazon S3, Amazon Glacier, and AWS KMS

Control:

- Actions allowed by specific principal
- What conditions are required
- Are always inline policies
- No AWS-managed resource-based policies

14

Identities with Attached Permissions



15

Applying Permissions

IAM policy

JSON

```
{
 "Version": "2012-10-17",
 "Statement": {
 "Effect": "Allow",
 "Action": "s3:ListBucket",
 "Resource": "arn:aws:s3:::example_bucket"
 }
}
```

16

IAM Policy Example

```
{
 "Version": "2012-10-17",
 "Statement":[{
 "Effect":"Allow",
 "Action":["dynamodb:*","s3:*"],
 "Resource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
 "arn:aws:s3:::bucket-name",
 "arn:aws:s3:::bucket-name/*"]
 },
 {
 "Effect":"Deny",
 "Action":["dynamodb:*","s3:*"],
 "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
 "arn:aws:s3:::bucket-name",
 "arn:aws:s3:::bucket-name/*"]
 }
 ]
}
```

Gives users access to a specific DynamoDB table and…

…a specific Amazon S3 bucket and its contents

An **explicit deny** statement ensures that principals cannot use any AWS actions or resources other than the specified table and bucket

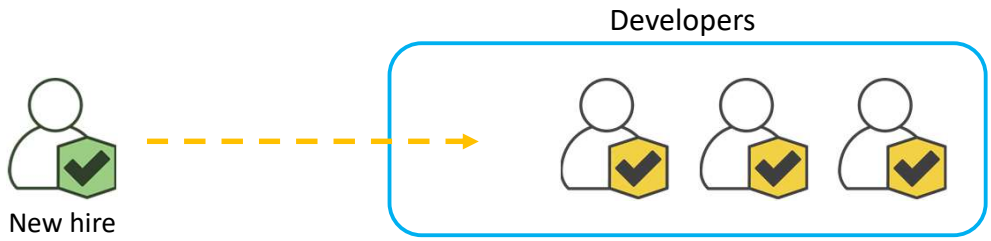
An **explicit deny** statement **takes precedence** over an allow statement

17

Organizing My Users

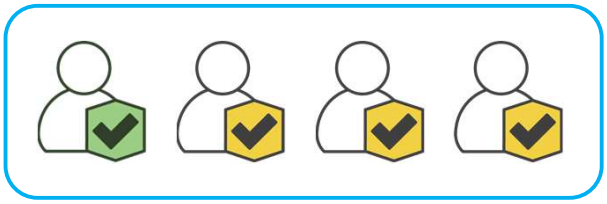
18

IAM User Group



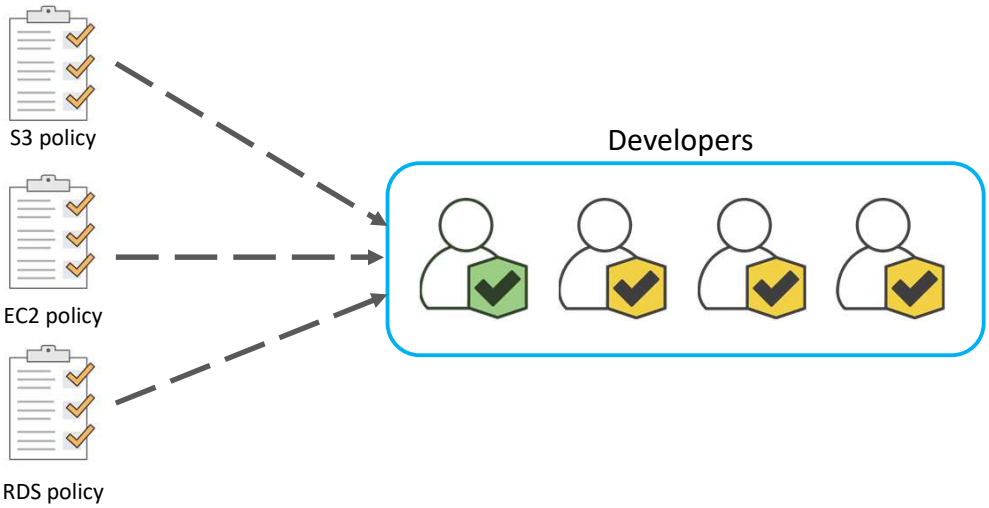
19

IAM User Group



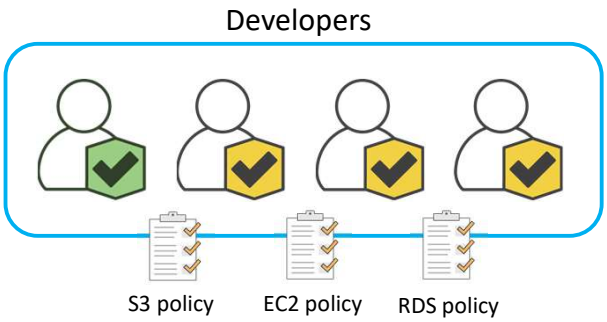
20

IAM User Group



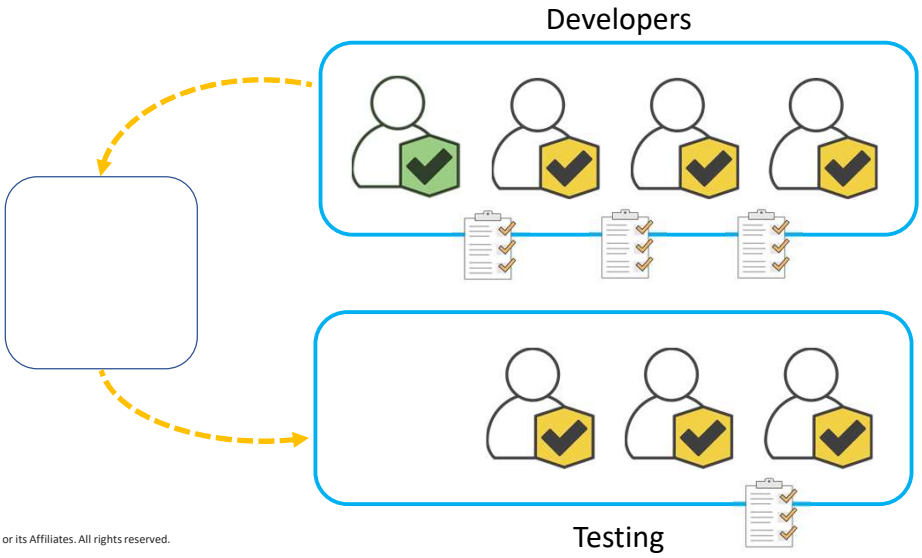
21

IAM User Group



22

IAM User Group



23

aws training and certification

Federating Users

24

IAM Roles

aws training and certification

A role lets you define a set of permissions to access the resources that a user or service needs.

- The permissions are not attached to an IAM user or group.
- The permissions are attached to a role and the role is **assumed** by the user or the service.

25

IAM Roles

Use cases:

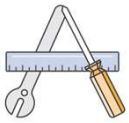
- Provide AWS resources with access to AWS services
- Provide access to externally authenticated users
- Provide access to third parties
- Switch roles to access resources in:
  - Your AWS account
  - Any other AWS account (cross-account access)

26

Assume a Role

AWS Management Console

AWS Command Line Interface (AWS CLI)



AssumeRole API call

AWS Security Token Service (AWS STS)

27

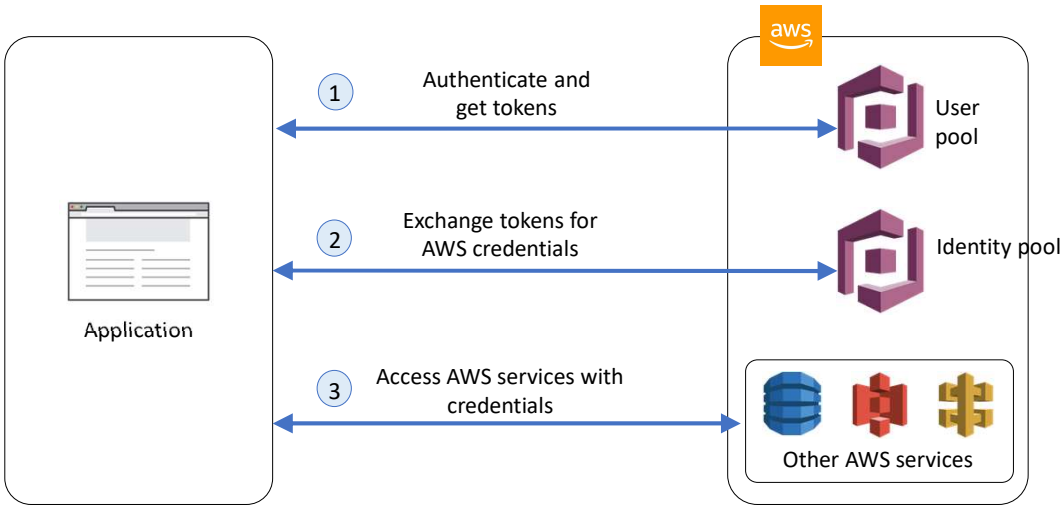
Amazon Cognito

Fully managed service that provides authentication, authorization, and user management for web and mobile apps

- User pools
- Identity pools

28

Amazon Cognito Example



29

Multiple Accounts

30

AWS "In the Wild"

How many AWS accounts does your organization need?

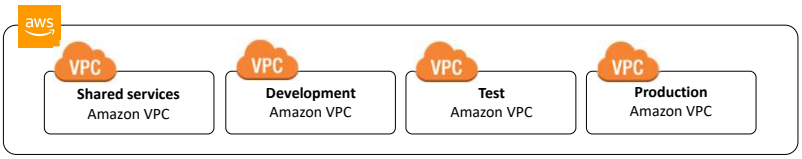
Dev

Test

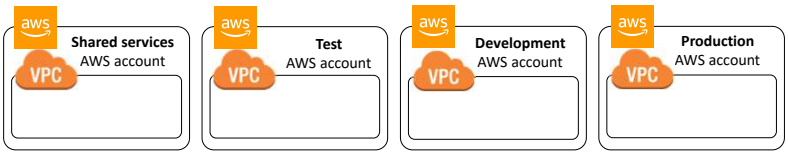
Production

31

AWS Recommendations



One account – multiple VPCs



Multiple accounts – One VPC per account

32

Multiple AWS Accounts

Can be leveraged for isolation:

- Separate business units, dev/test/production environments

Can be leveraged for security:

- Separate accounts for regulated workloads, different geographical locations, governing other accounts

Cross-account access is not enabled by default

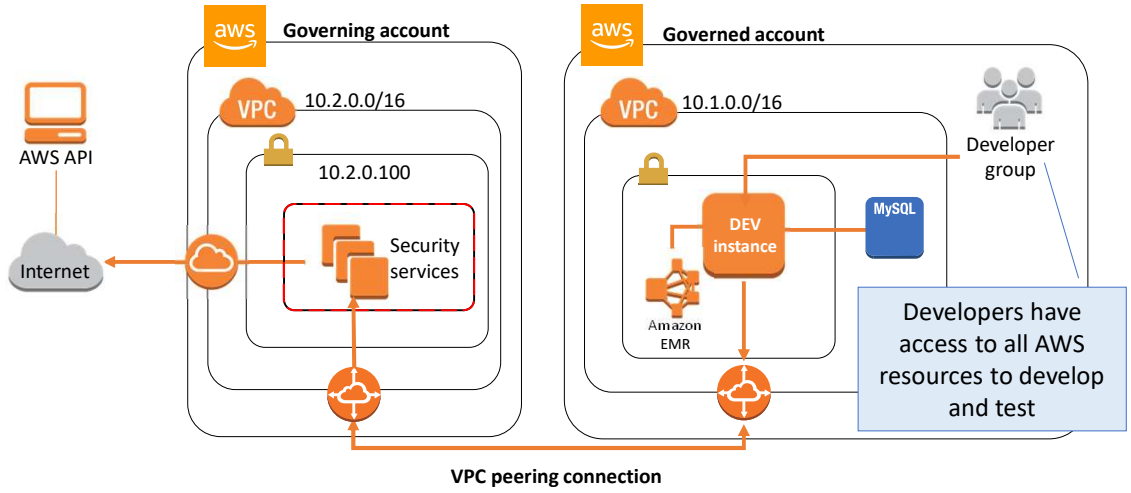
33

Strategies for Using Multiple AWS Accounts

Centralized security management	Single AWS account
Separation of production, development, and testing environments	Three AWS accounts
Multiple autonomous departments	Multiple AWS accounts
Centralized security management with multiple autonomous independent projects	Multiple AWS accounts

34

Using Multiple Accounts for Governance



35

How Do I Manage All These Accounts?

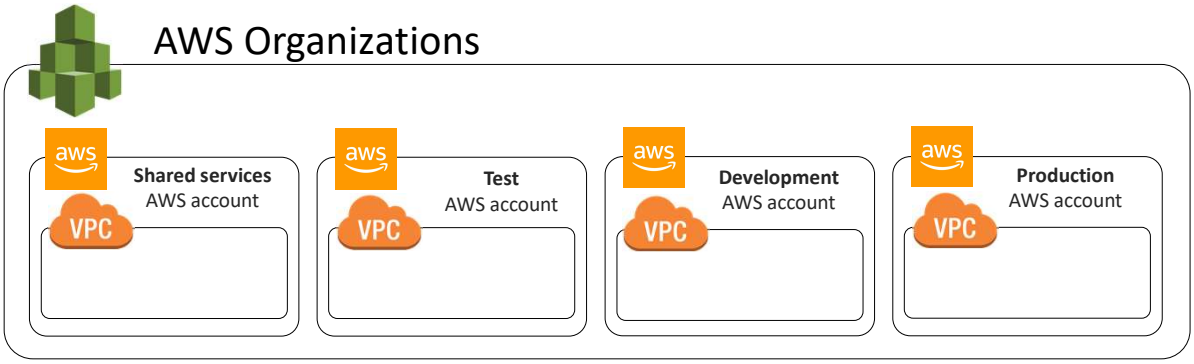
AWS Organizations

Centralized account management

- Group-based account management
- Policy-based access to AWS services
- Automated account creation and management
- Consolidated billing
- API-based

36

AWS Recommendations



37

AWS Organizations: Illustrated

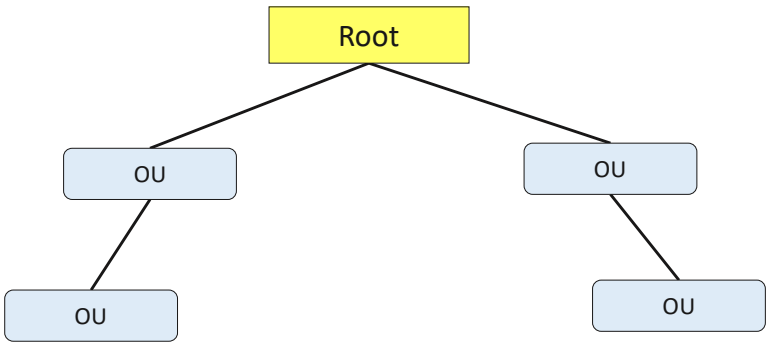
AWS Organization

Root

38

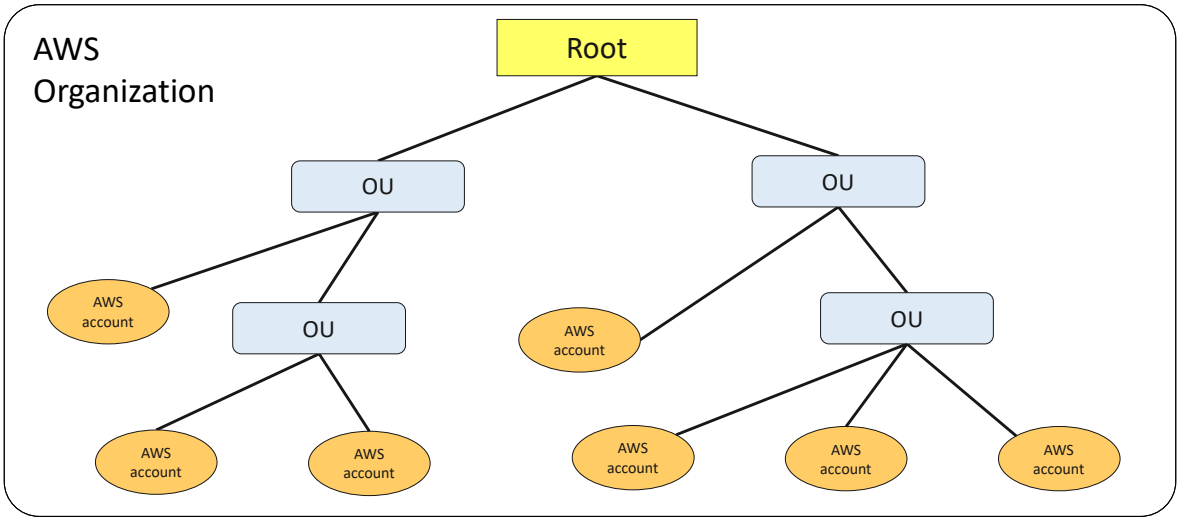
AWS Organizations: Illustrated

AWS Organization



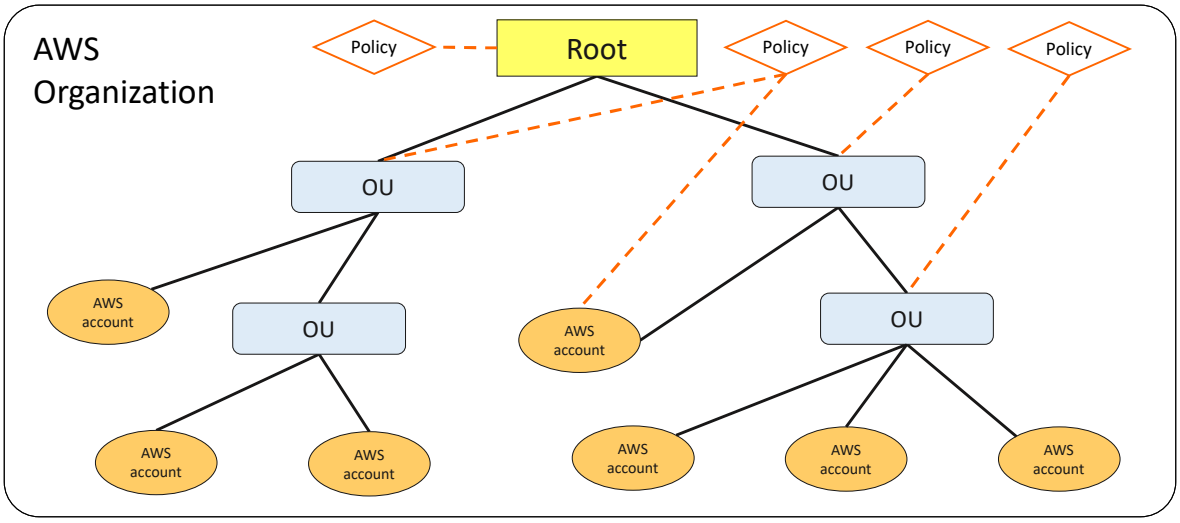
39

AWS Organizations: Illustrated



40

AWS Organizations: Illustrated



41

aws training and certification

Review

42

Review

aws training and certification

If you need to grant temporary permissions to a resource, what would you use?

43

Review

If you need to grant temporary permissions to a resource, what would you use?

IAM role

44

Review

One of your users can't access an S3 bucket. What should you check to identify the cause of the problem?

45

Review

aws training and certification

One of your users can't access an S3 bucket. What should you check to identify the cause of the problem?

The policies attached to the user and to the bucket

46

Review

aws training and certification

1. You have created a mobile application that makes calls to DynamoDB to fetch data.
2. The application is using the DynamoDB SDK and the AWS account root user access/secret access key to connect to DynamoDB from the mobile app.
3. With respect to the best practice for security in this scenario, how should this be fixed?

47

Review

aws training and certification

First: **Stop** using the AWS account root user in production!

Then, if possible, have the app use an IAM role with web identity federation.

48

aws training and certification

Thank You

49