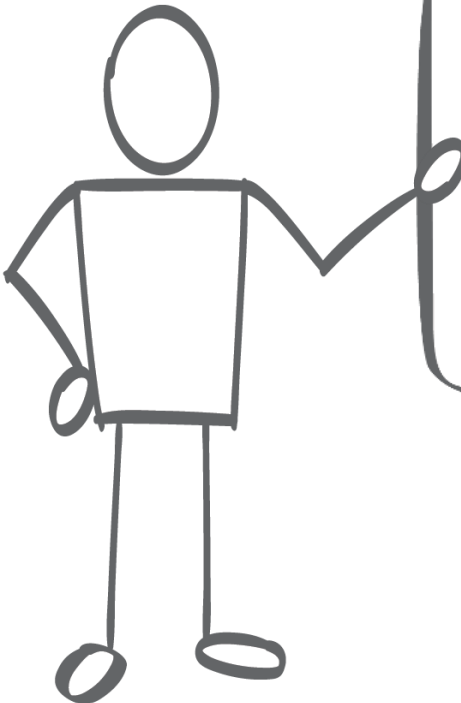




# AWSome Day

ONLINE CONFERENCE



# **Module 3**

## **Security, Identity, and Access Management**

# Shared Responsibility – AWS

**Customer**

**Customer Data**

**Platform, Applications, Identity and Access Management**

**Operating System, Network and Firewall Configuration**

**Client-side Data Encryption  
and Data Integrity  
Authentication**

**Server-side Encryption  
(File System and/or Data)**

**Network Traffic Protection  
(Encryption/Integrity/Identity)**

**AWS**

**Foundation Services**

**Compute**

**Storage**

**Database**

**Network**

**AWS Global  
Infrastructure**

**Availability Zones**

**Regions**

**Edge  
Locations**

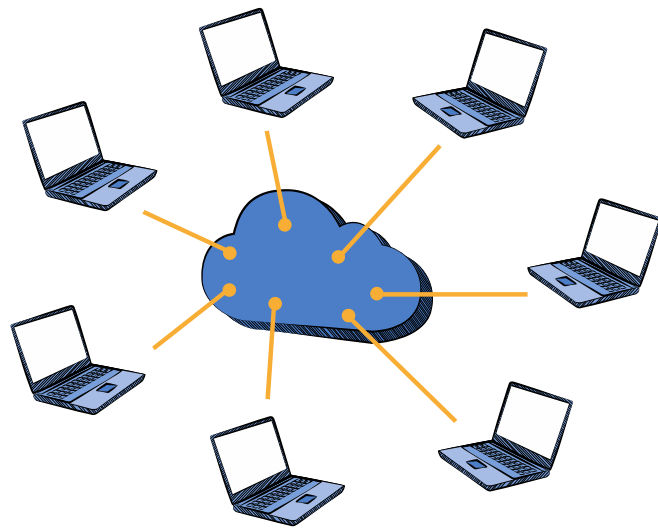
# Physical Security

- 📦 24/7 trained security staff
- 📦 AWS data centers in nondescript and undisclosed facilities
- 📦 Two-factor authentication for authorized staff
- 📦 Authorization for data center access



# Hardware, Software, and Network

- 📦 Automated change-control process
- 📦 Bastion servers that record all access attempts
- 📦 Firewall and other boundary devices
- 📦 AWS monitoring tools



# Certifications and Accreditations



ISO 9001, ISO 27001, ISO 27017, ISO 27018, IRAP (Australia), MLPS Level 3 (China), MTCS Tier 3 Certification (Singapore) and more ...

# SSL Endpoints

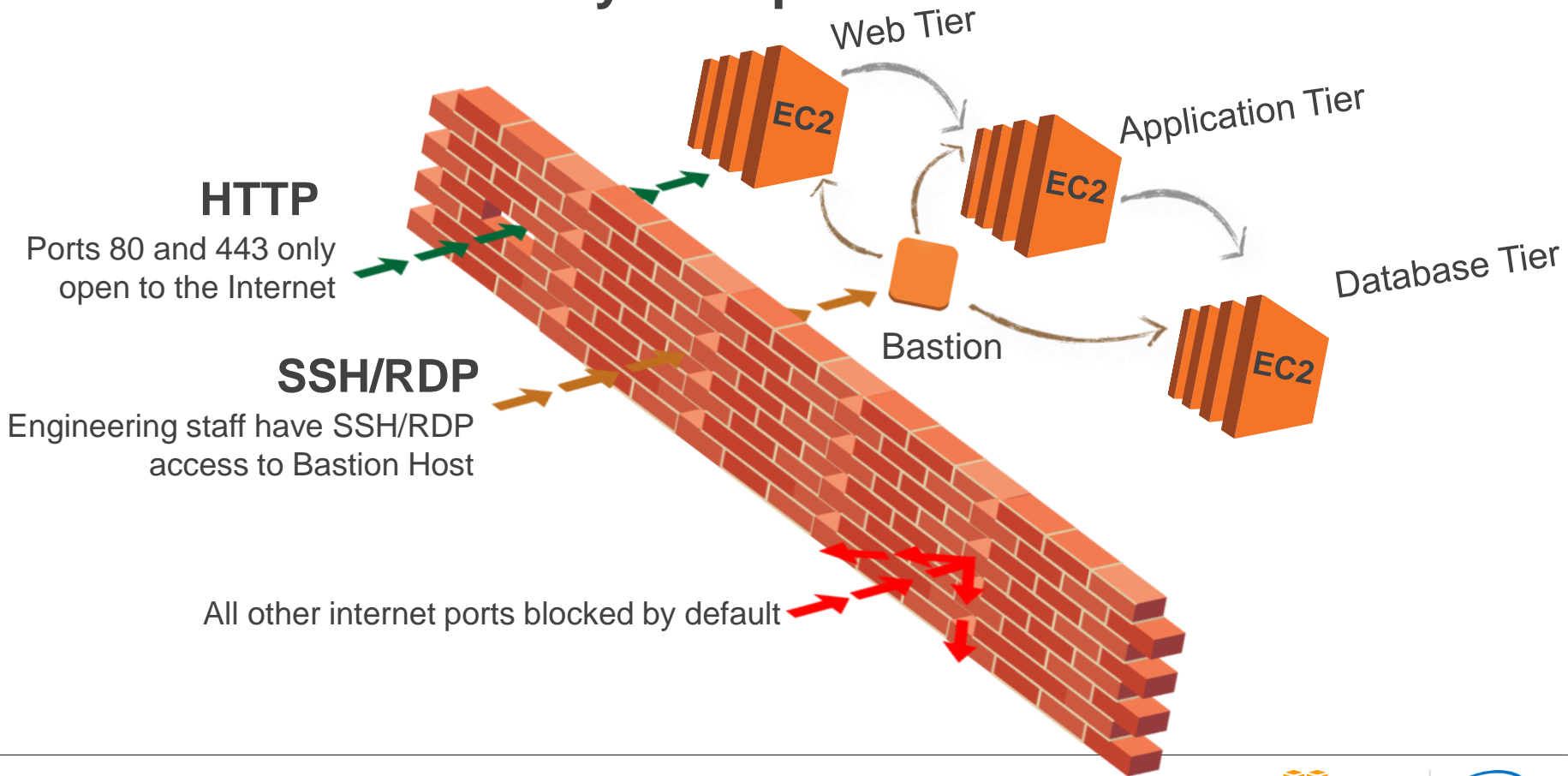
SSL Endpoints	Security Groups	VPC
<b>Secure Transmission</b>  Establish secure communication sessions (HTTPS) using SSL/TLS.	<b>Instance Firewalls</b>  Configure firewall rules for instances using Security Groups.	<b>Network Control</b>  In your Virtual Private Cloud, create low-level networking constraints for resource access. Public and private subnets, NAT and VPN support.

# Security Groups

SSL Endpoints	Security Groups	VPC
<b>Secure Transmission</b>  Establish secure communication sessions (HTTPS) using SSL/TLS.	<b>Instance Firewalls</b>  Configure firewall rules for instances using Security Groups.	<b>Network Control</b>  In your Virtual Private Cloud, create low-level networking constraints for resource access. Public and private subnets, NAT and VPN support.



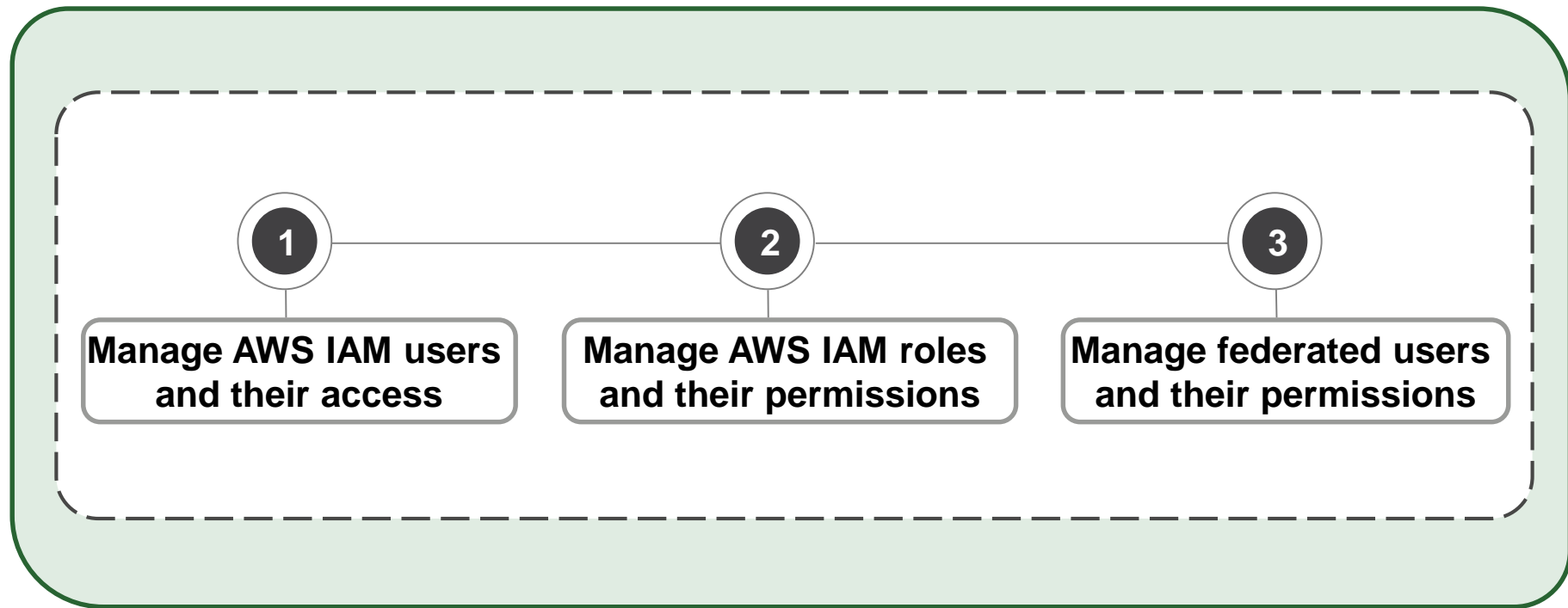
# AWS Multi-Tier Security Groups



# Amazon Virtual Private Cloud (VPC)

SSL Endpoints	Security Groups	VPC
<b>Secure Transmission</b>  Establish secure communication sessions (HTTPS) using SSL/TLS.	<b>Instance Firewalls</b>  Configure firewall rules for instances using Security Groups.	<b>Network Control</b>  In your Virtual Private Cloud, create low-level networking constraints for resource access. Public and private subnets, NAT and VPN support.

# AWS Identity and Access Management (IAM)



# AWS IAM Authentication



## Authentication

### AWS Management Console

➤ User Name and Password



IAM User

Account:

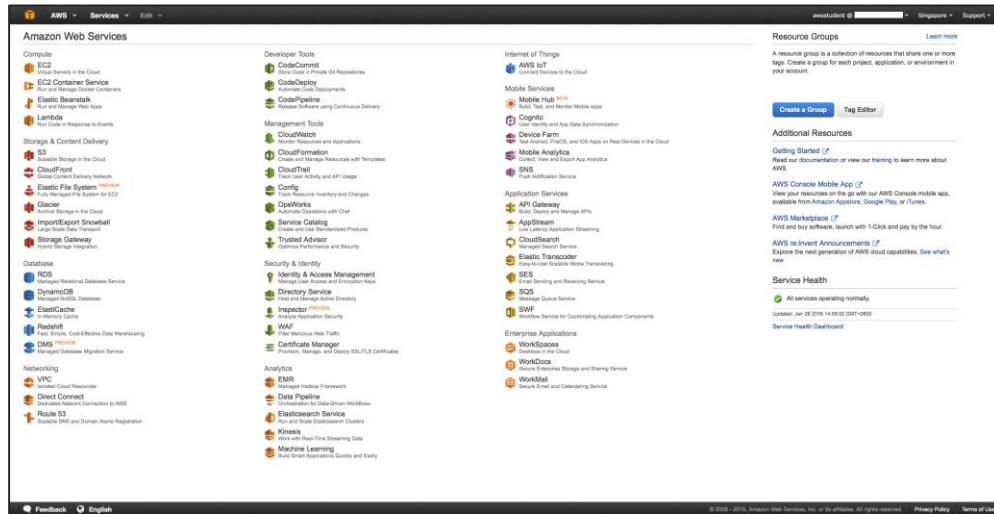


User Name:

Password:

MFA users, enter your code on the next screen.

Sign In



# AWS IAM Authentication



## Authentication

### AWS CLI or SDK API

- Access Key and Secret Key



IAM User

**Access Key ID:** AKIAIOSFODNN7EXAMPLE  
**Secret Access Key:** wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

#### AWS CLI

```
~$ aws configure
AWS Access Key ID [*****O22A]:
AWS Secret Access Key [*****4m8i]:
Default region name [ap-southeast-1]:
Default output format [json]:
```

#### AWS SDK & API



Java

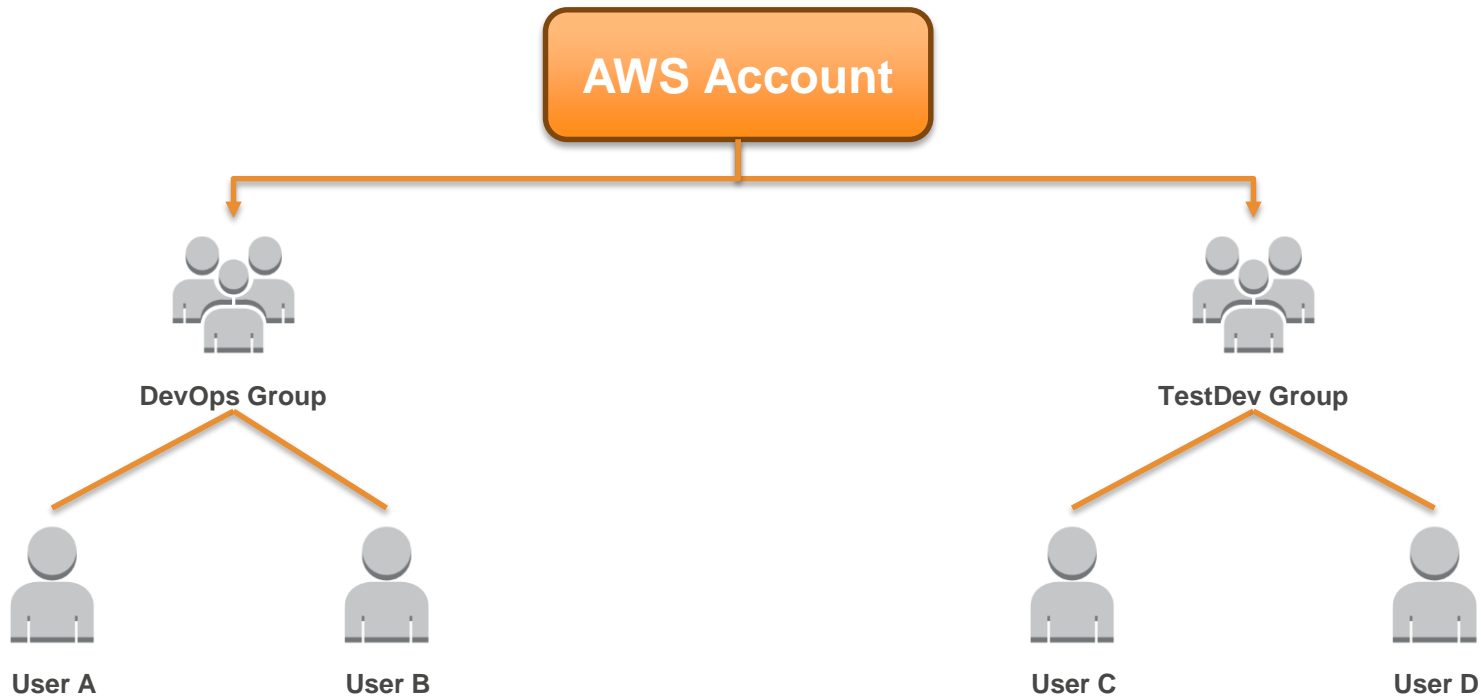


Python



.NET

# AWS IAM User Management - Groups



# AWS IAM Authorization



## Authorization

### Policies:

- Are JSON documents to describe permissions.
- Are assigned to Users, Groups or Roles.



IAM User



IAM Group

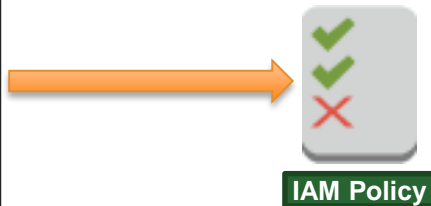


IAM Roles

# AWS IAM Policy Elements

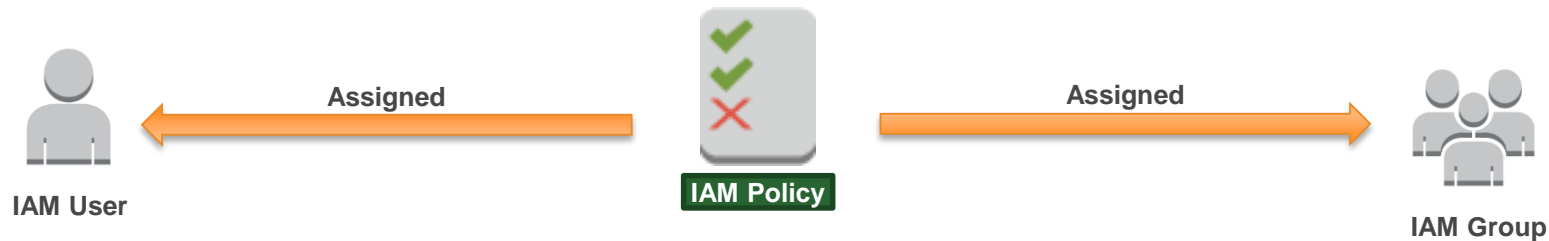


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1453690971587",
      "Action": [
        "ec2:Describe*",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "54.64.34.65/32"
        }
      }
    },
    {
      "Sid": "Stmt1453690998327",
      "Action": [
        "s3:GetObject*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::example_bucket\*"
    }
  ]
}
```

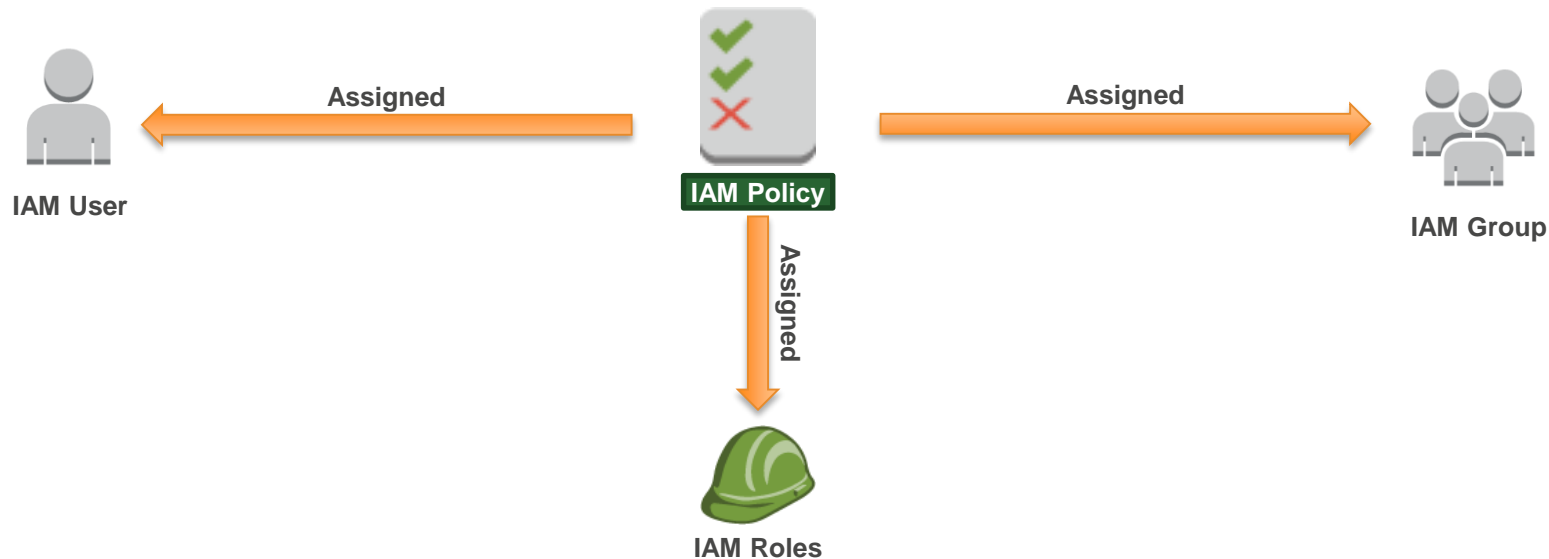




# AWS IAM Policy Assignment



# AWS IAM Policy Assignment



# AWS IAM Roles

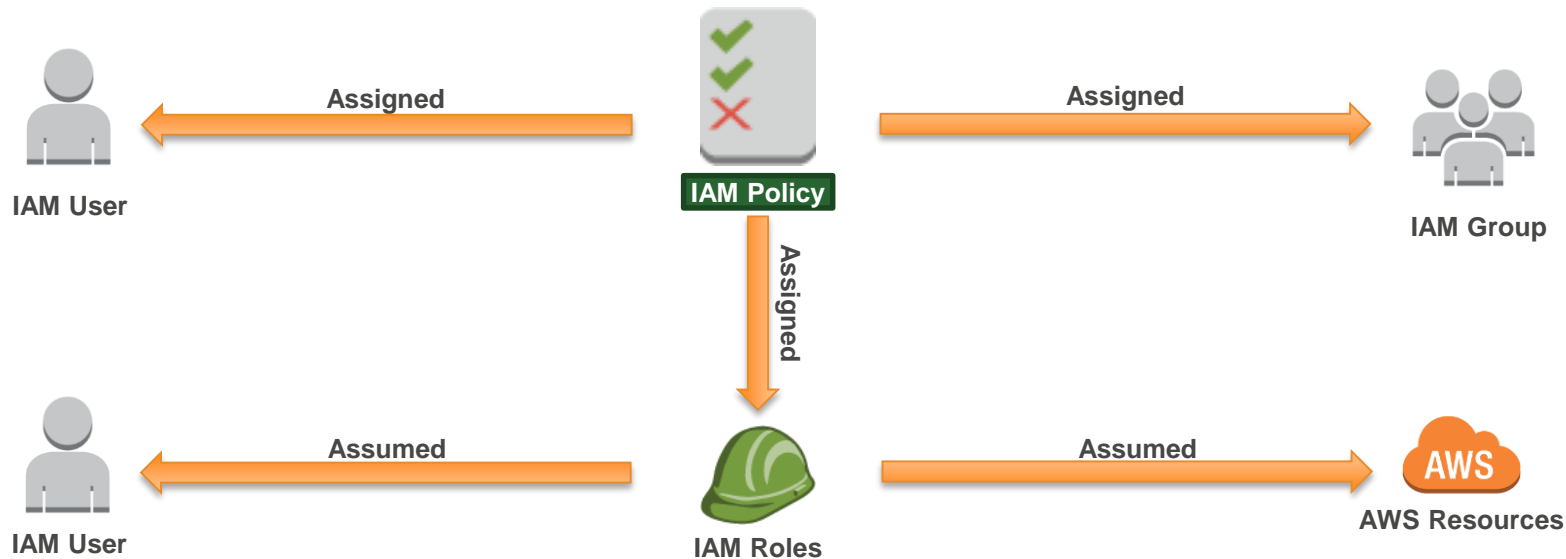


- ❏ An IAM role uses a policy.
- ❏ An IAM role has no associated credentials.
- ❏ IAM users, applications, and services may assume IAM roles.



**IAM Roles**

# AWS IAM Policy Assignment



# Application Access to AWS Resources



- ❏ Python application hosted on an Amazon EC2 Instance needs to interact with Amazon S3.
- ❏ AWS credentials are required:
  - ~~Option 1: Store AWS Credentials on the Amazon EC2 instance.~~
  - Option 2: Securely distribute AWS credentials to AWS Services and Applications.



**IAM Roles**

# AWS IAM Roles - Instance Profiles



Amazon EC2



1

Create Instance

AWS Services Edit

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-5f (172.31.0.0/16) (default) Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP Use subnet setting (Enable)

Domain join directory None Create new directory

IAM role **None** Create new IAM role

- None
- aws-elasticbeanstalk-ec2-role
- EMR\_EC2\_DefaultRole
- PythonEC2AccessS3**

Shutdown behavior

Enable termination protection

Monitoring ☐ Enable CloudWatch detailed monitoring Additional charges apply.

Tenancy Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

Advanced Details

Select IAM Role

2



App &



3

EC2 MetaData Service

<http://169.254.169.254/latest/meta-data/iam/security-credentials/rolename>

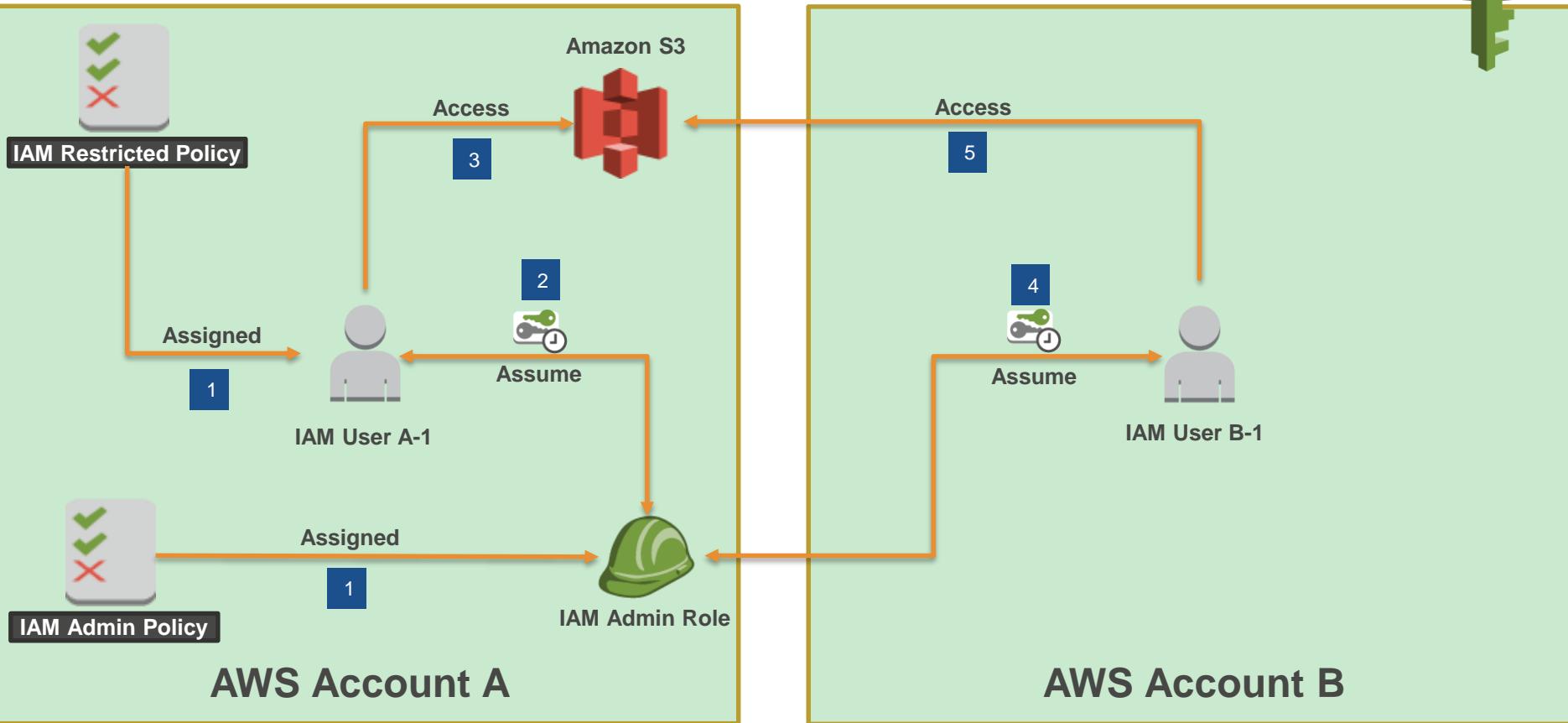
Amazon S3



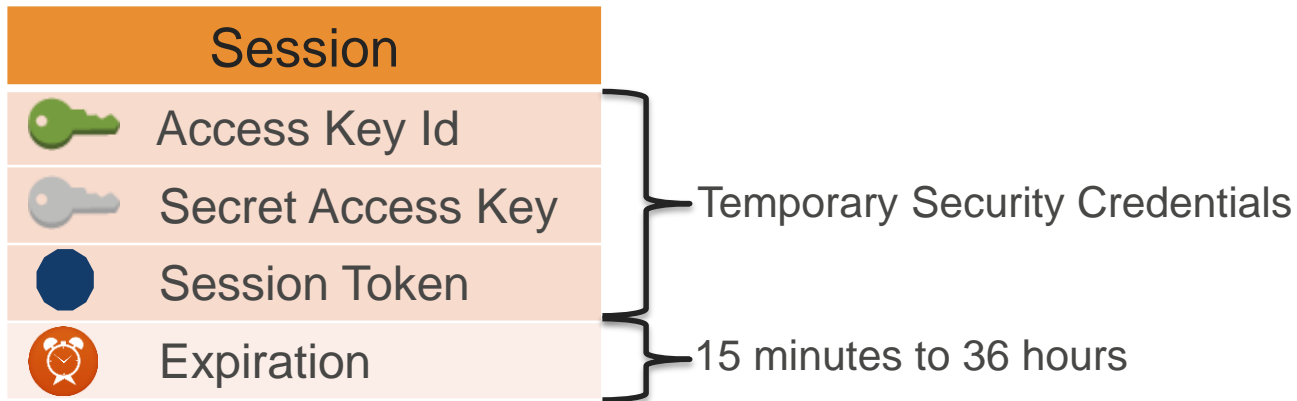
Application interacts with S3

4



# AWS IAM Roles – Assume Role





# Temporary Security Credentials (AWS STS)



## Use Cases

-  Cross account access
-  Federation

-  Mobile Users
-  Key rotation for Amazon EC2-based apps



# Application Authentication



# AWS IAM Authentication and Authorization



## Authentication

### AWS Management Console

- User Name and Password

### AWS CLI or SDK API

- Access Key and Secret Key



IAM User



IAM Group



IAM Roles

## Authorization

### Policies

# AWS IAM Best Practices



- ❏ Delete AWS account (root) access keys.
- ❏ Create individual IAM users.
- ❏ Use groups to assign permissions to IAM users.
- ❏ Grant least privilege.
- ❏ Configure a strong password policy.
- ❏ Enable MFA for privileged users.



# AWS IAM Best Practices (cont.)



- ❏ Use roles for applications that run on Amazon EC2 instances.
- ❏ Delegate by using roles instead of by sharing credentials.
- ❏ Rotate credentials regularly.
- ❏ Remove unnecessary users and credentials.
- ❏ Use policy conditions for extra security.
- ❏ Monitor activity in your AWS account.

# AWS Resource-Based Policies

- Are an alternative to IAM and supported by some services.
- Grant cross-account access to your resources.
- Use a principal to uniquely identify account in the policy.
- Supported AWS services include :
  - Amazon S3 Bucket Policy
  - Amazon SNS Topic Policy
  - Amazon SQS Queue Policy
  - Amazon Glacier Vault Policy
  - AWS OpsWorks Stack Policy
  - AWS Lambda Function Policy

# Instructor Demo

IAM



© 2016 Amazon Web Services, Inc. or its affiliates. All rights reserved.

This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

Errors or corrections? Email us at [aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com).

For all other questions, contact us at:  
<https://aws.amazon.com/contact-us/aws-training/>.

All trademarks are the property of their owners.



# AWSome Day

---

ONLINE CONFERENCE

---