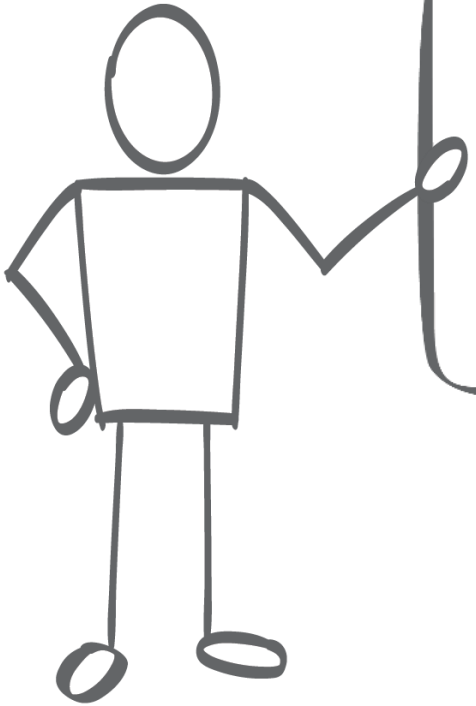
amazon web services | intel

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

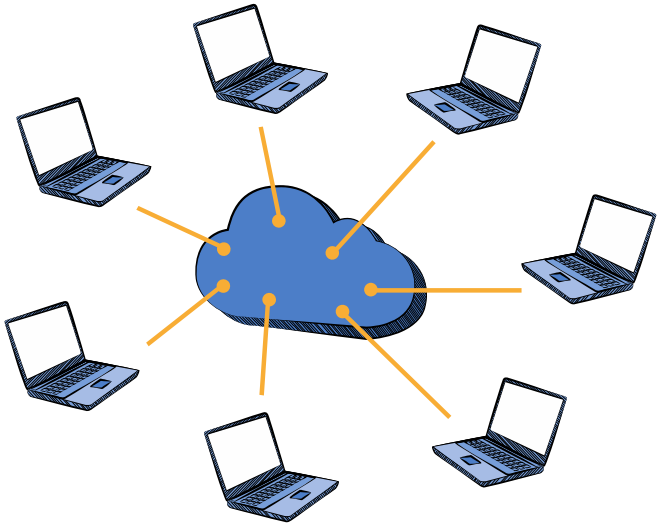
- Foundation Services
  - Compute
  - Storage
  - Database
  - Network
- AWS Global Infrastructure
  - Availability Zones
  - Regions
  - Edge Locations

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 …

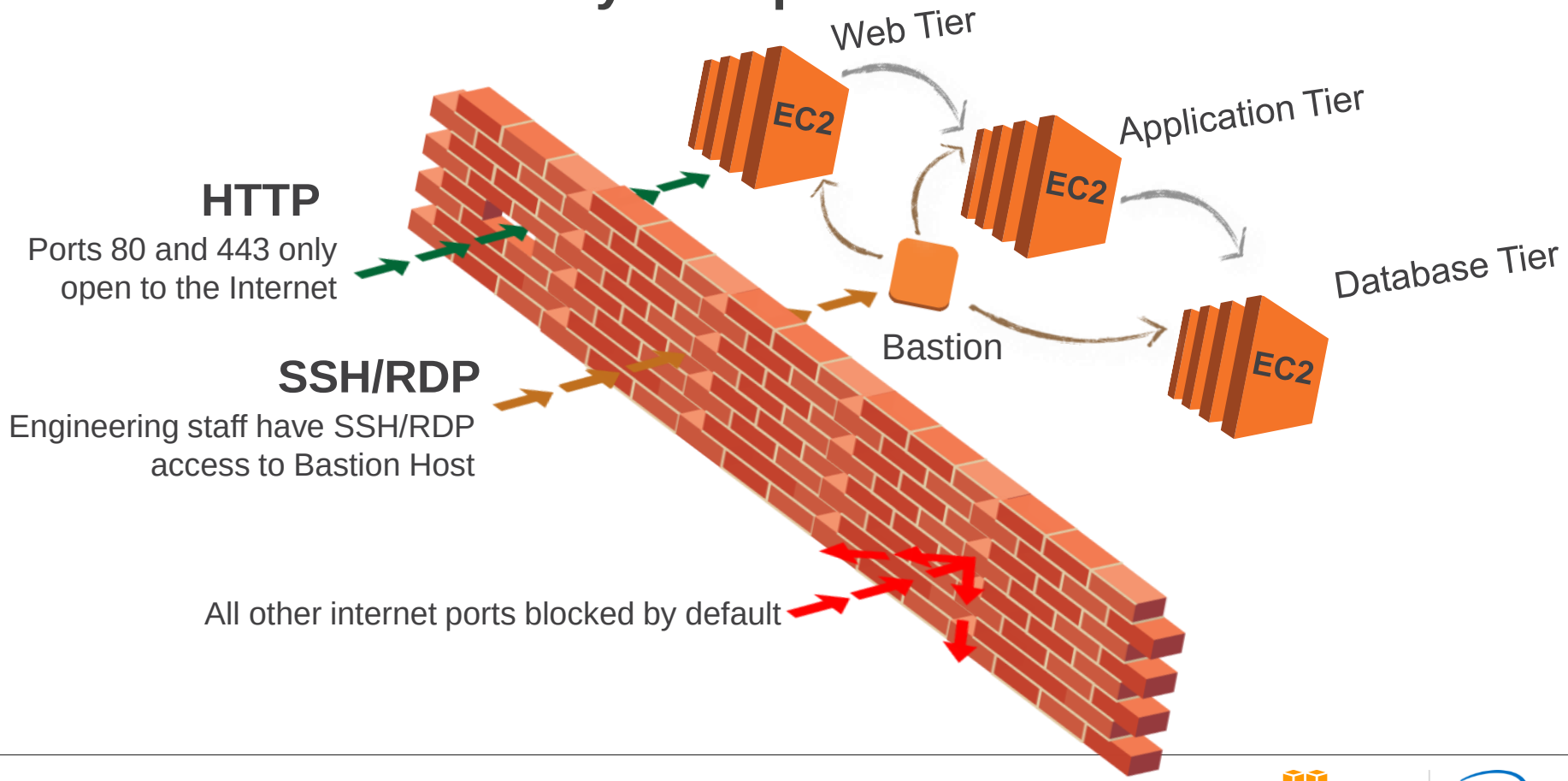
SSL Endpoints

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

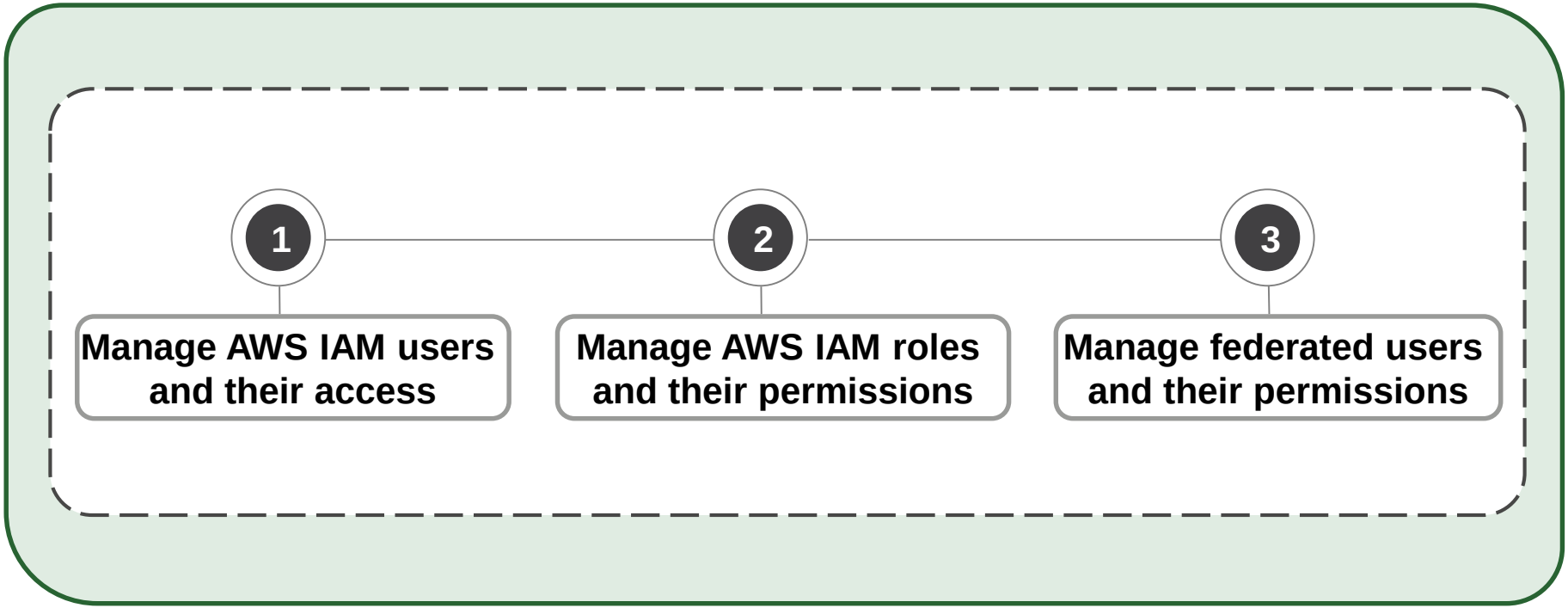
AWS Multi-Tier Security Groups



Amazon Virtual Private Cloud (VPC)

SSL Endpoints	Security Groups	VPC
Secure Transmission Establish secure communication sessions (HTTPS) using SSL/TLS.	**Instance Firewalls** Configure firewall rules for instances using Security Groups.	**Network Control** 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)

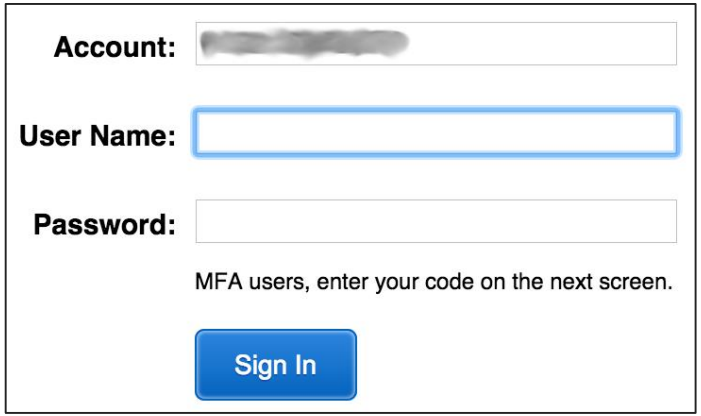


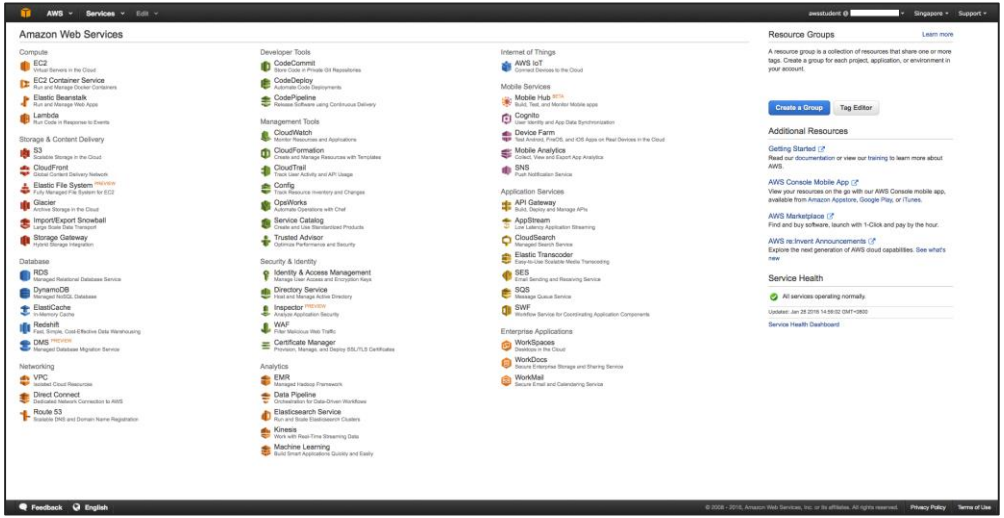
AWS IAM Authentication

Authentication

- **AWS Management Console**
  - User Name and Password

IAM User





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

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

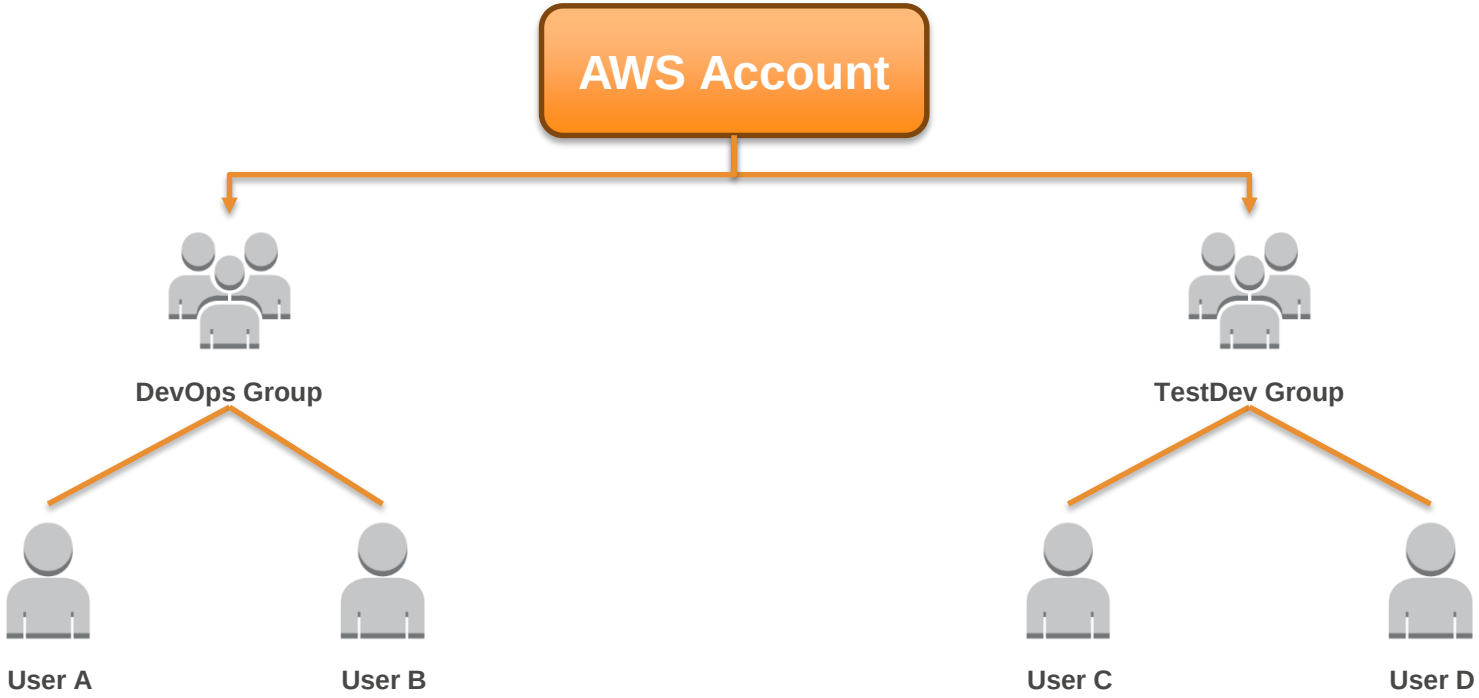
AWS SDK & API

Java

Python

.NET

AWS IAM User Management - Groups



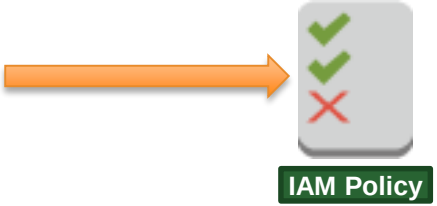
AWS IAM Authorization

Authorization

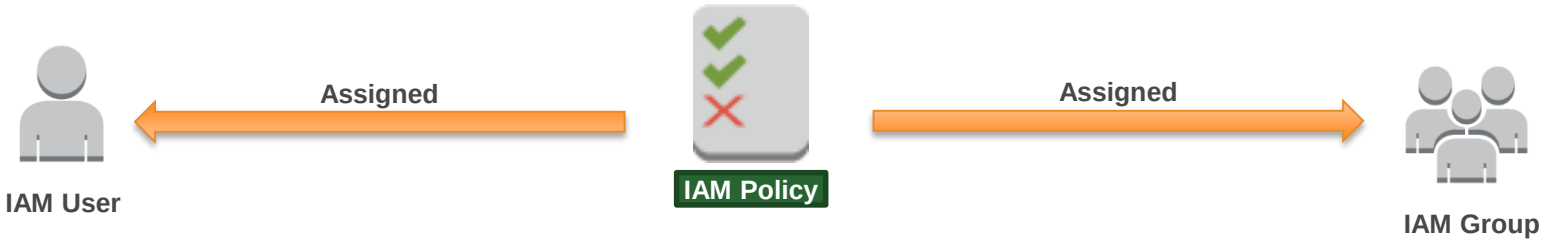
- Policies:
  - Are JSON documents to describe permissions.
  - Are assigned to Users, Groups or Roles.

AWS IAM Policy Elements

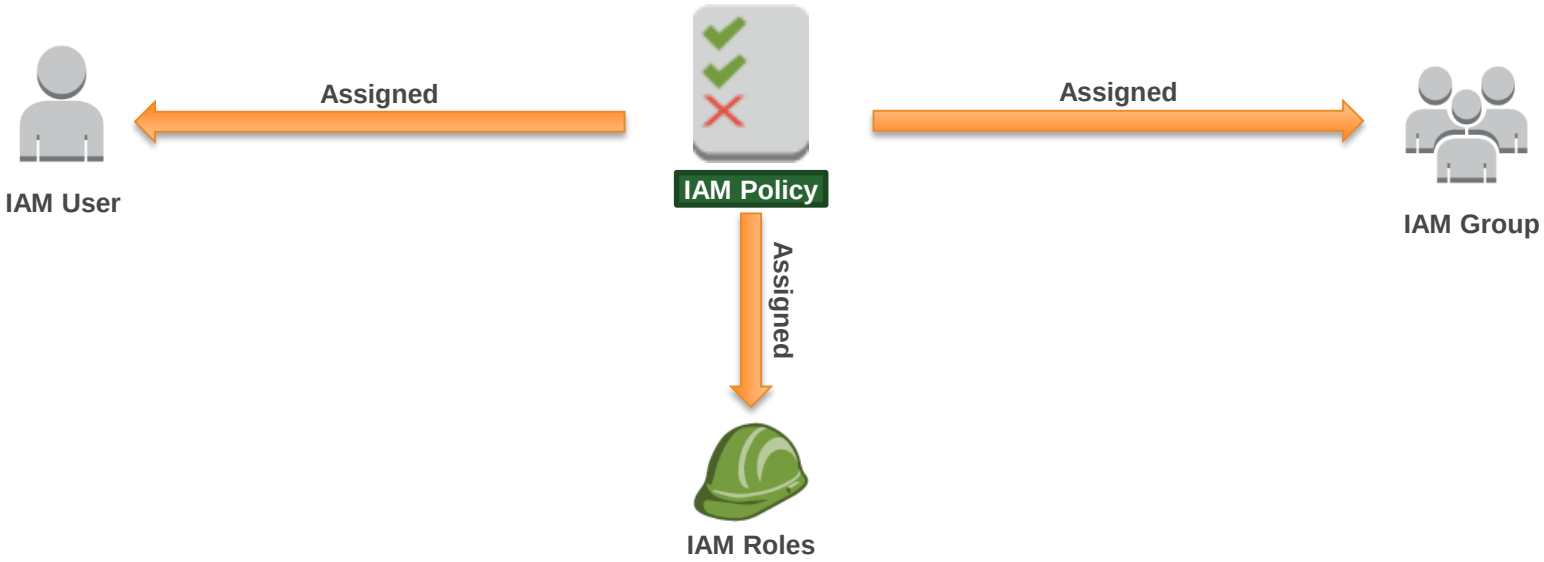
```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "Stmt1453690971587",
         "Action": [
          "ec2:Describe*",
          "ec2:StartInstances",
          "ec2:StopInstances”
          ],
          "Effect": "Allow",
          "Resource": "*",
          "Condition": {
            "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

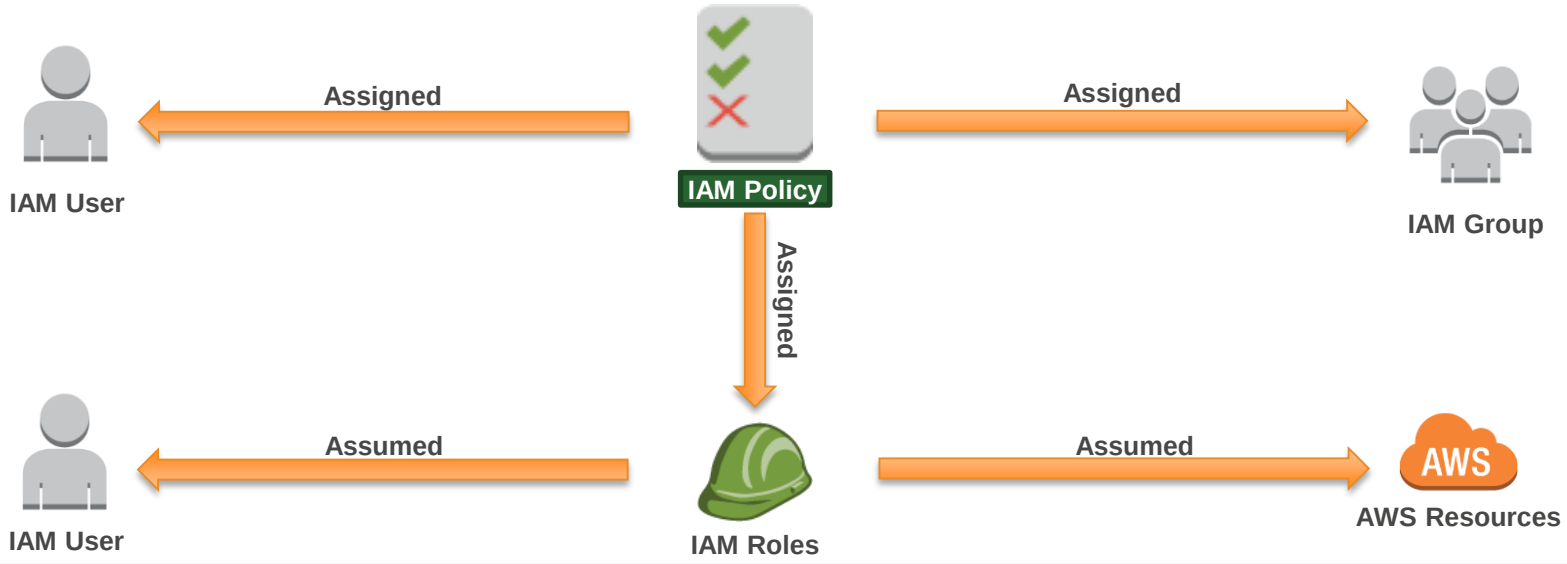


AWS IAM Roles

- 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.

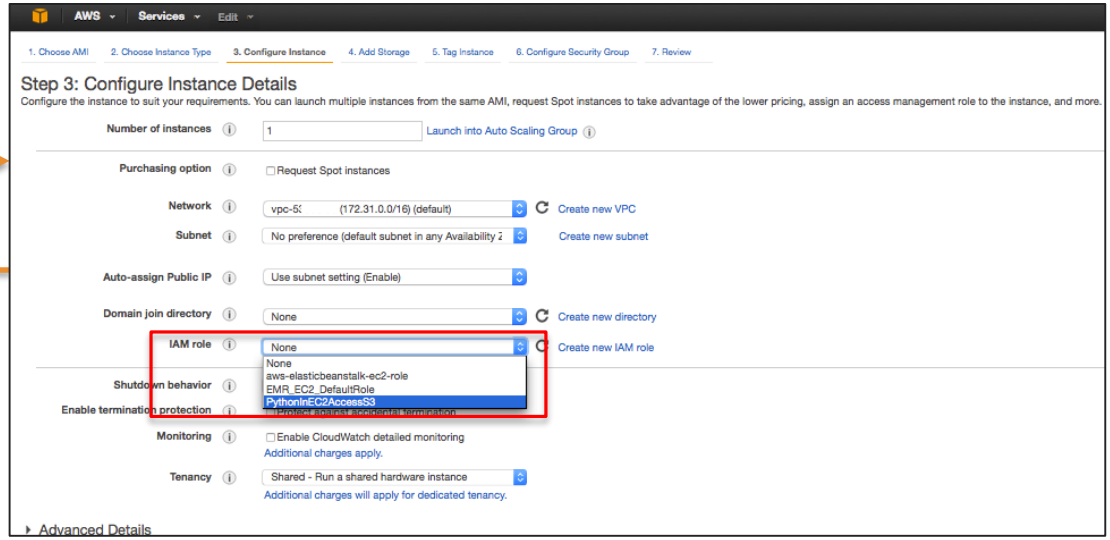
IAM Roles

AWS IAM Roles - Instance Profiles

Amazon EC2

1

Create Instance



Amazon S3

Select IAM Role

2

4

Application interacts with S3

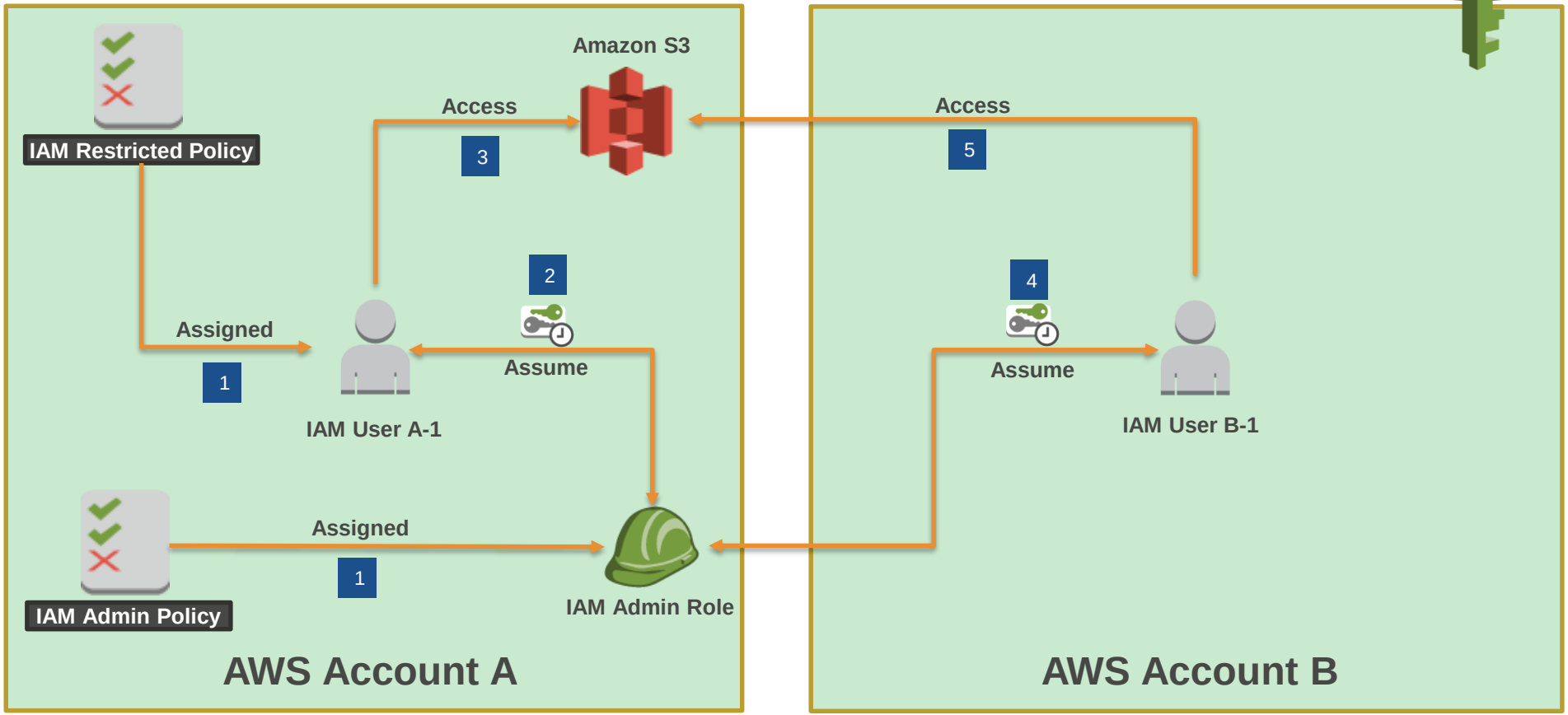
python™ App &

3

EC2 MetaData Service

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

AWS IAM Roles – Assume Role



Temporary Security Credentials (AWS STS)

Session
Access Key Id
Secret Access Key
Session Token
Expiration

Temporary Security Credentials

15 minutes to 36 hours

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
- **Authorization**
  - Policies

IAM User

IAM Group

IAM Roles

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

Errors or corrections? Email us at aws-course-feedback@amazon.com.
For all other questions, contact us at:
https://aws.amazon.com/contact-us/aws-training/.

amazon web services | intel

AWSome Day

ONLINE CONFERENCE