Instructor Notes:

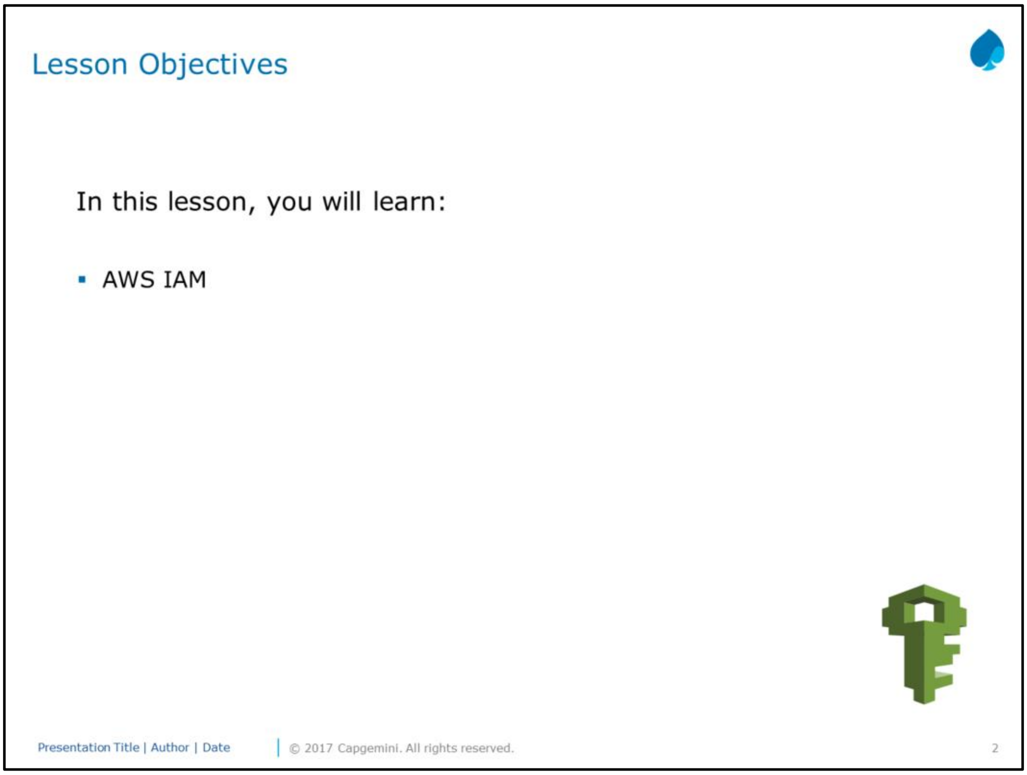
Add instructor notes here.

AWS Administration service

Lesson 08: AWS Administration service

Instructor Notes:

This lesson is to give an Introduction on Java Server Pages



Lesson Objectives

In this lesson, you will learn:

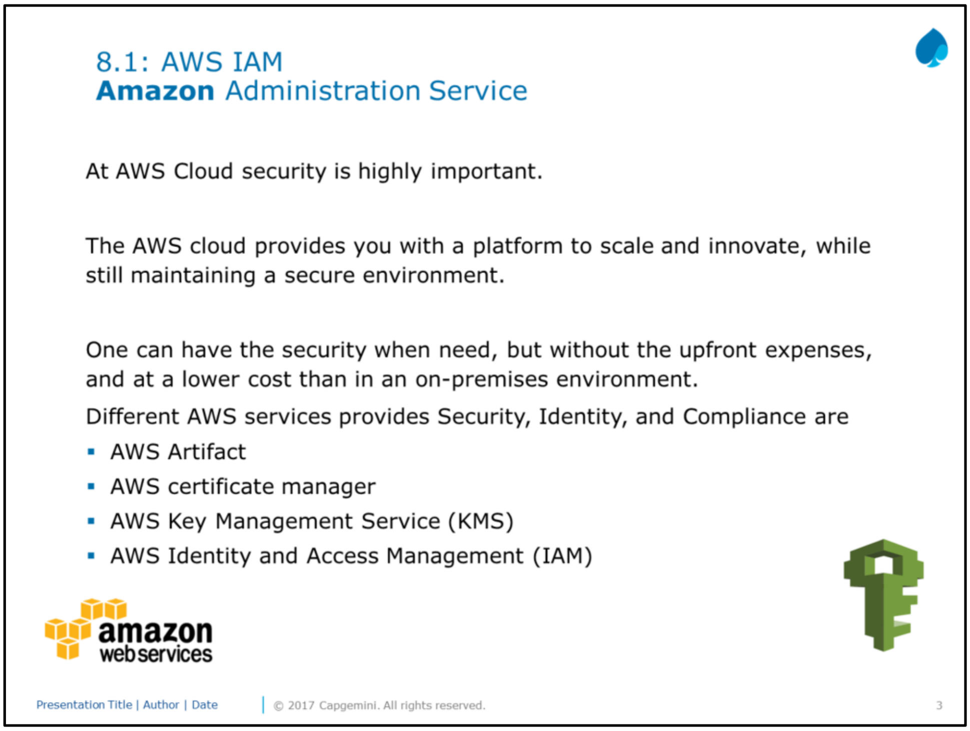
- AWS IAM

Presentation Title | Author | Date

2

AWS IAM

Instructor Notes:



8.1: AWS IAM
Amazon Administration Service

At AWS Cloud security is highly important.

The AWS cloud provides you with a platform to scale and innovate, while still maintaining a secure environment.

One can have the security when need, but without the upfront expenses, and at a lower cost than in an on-premises environment.

Different AWS services provides Security, Identity, and Compliance are

- AWS Artifact
- AWS certificate manager
- AWS Key Management Service (KMS)
- AWS Identity and Access Management (IAM)

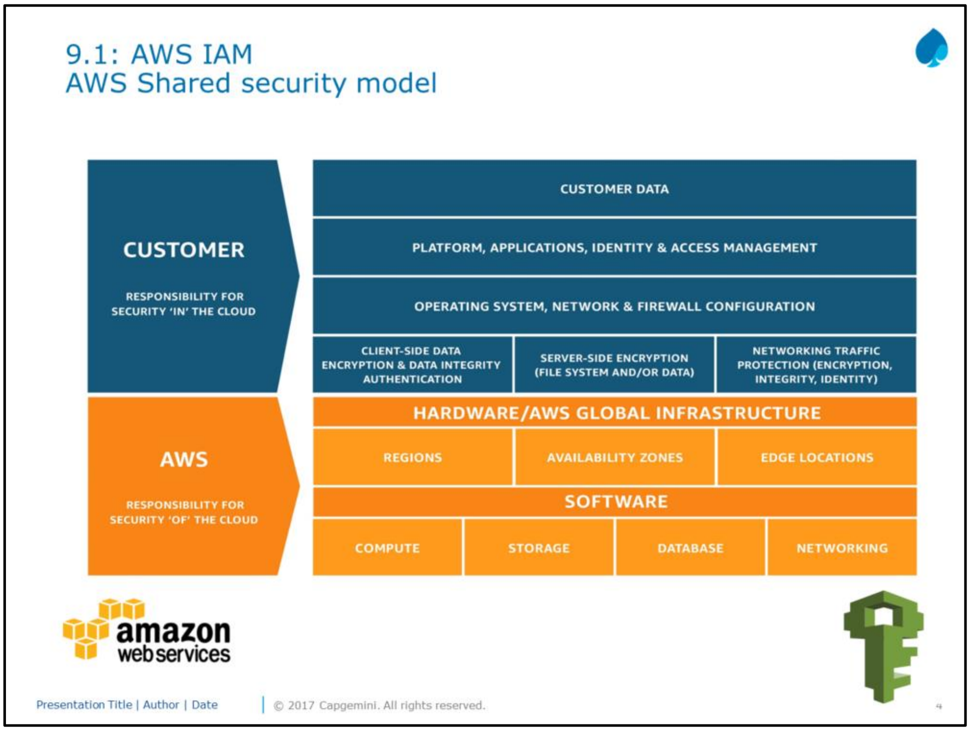
Presentation Title | Author | Date

© 2017 Capgemini. All rights reserved.

3

The AWS Artifact portal provides on-demand access to AWS' security and compliance documents, also known as audit artifacts.
AWS Certificate Manager is a service that lets you easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates.
AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data..

Instructor Notes:



9.1: AWS IAM
AWS Shared security model

CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

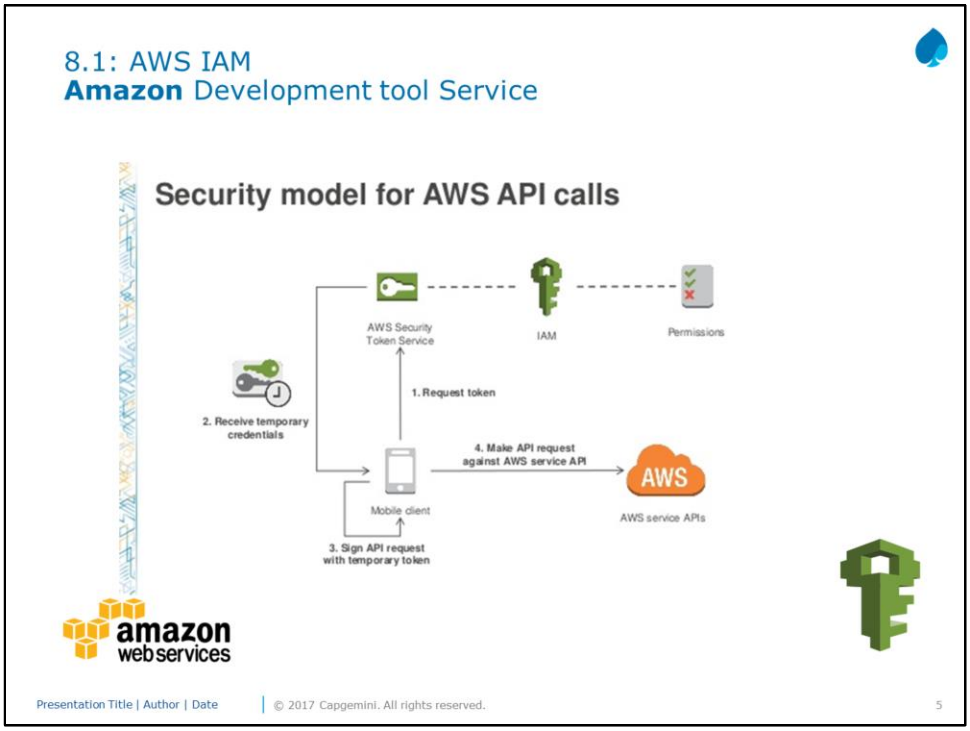
Presentation Title | Author | Date

© 2017 Capgemini. All rights reserved.

4

The AWS Developer Tools is a set of services designed to enable developers and IT operations professionals practicing DevOps to rapidly and safely deliver software. Together, these services help you securely store and version control your application's source code and automatically build, test, and deploy your application to AWS or your on-premises environment. You can use AWS CodePipeline to orchestrate an end-to-end software release workflow using these services and third-party tools or integrate each service independently with your existing tools.

Instructor Notes:



8.1: AWS IAM
Amazon Development tool Service

Security model for AWS API calls

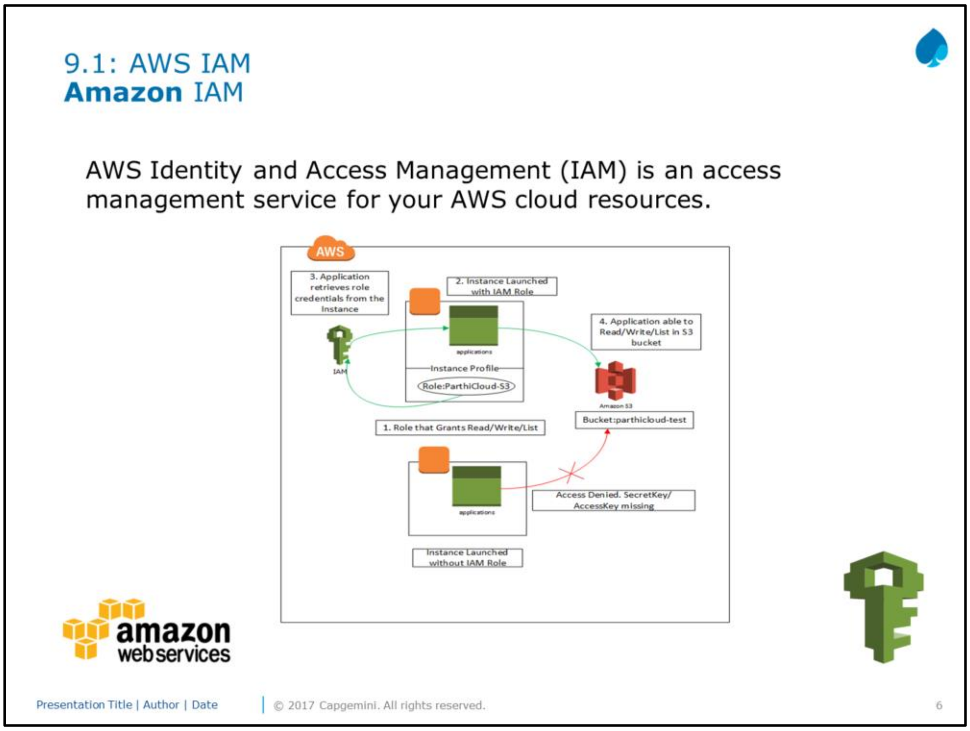
AWS Security Token Service
IAM
Permissions
2. Receive temporary credentials
1. Request token
4. Make API request against AWS service API
AWS
Mobile client
AWS service APIs
3. Sign API request with temporary token
amazon web services

Presentation Title | Author | Date

© 2017 Capgemini. All rights reserved.

5

Instructor Notes:



9.1: AWS IAM
Amazon IAM

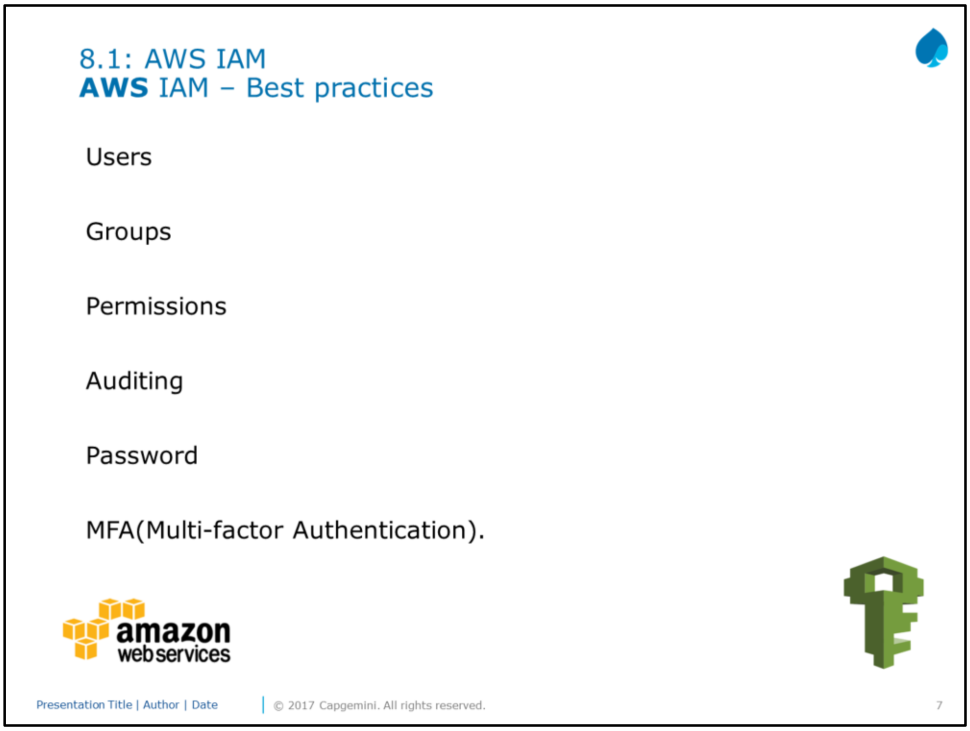
AWS Identity and Access Management (IAM) is an access management service for your AWS cloud resources.

AWS
3. Application retrieves role credentials from the Instance
2. Instance Launched with IAM Role
4. Application able to Read/Write/List in S3 bucket
applications
IAM
Instance Profile
Role:ParthiCloud-S3
Amazon S3
Bucket:parthicloud-test
1. Role that Grants Read/Write/List
applications
Access Denied. SecretKey/ AccessKey missing
Instance Launched without IAM Role
amazon web services

Presentation Title | Author | Date | © 2017 Capgemini. All rights reserved. 6

- AWS Identity and Access Management (IAM) is an access management service for your AWS cloud resources.
- It enables you to securely control access to AWS services and resources for your users.
- One can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.
- IAM is a feature of our AWS account which offered at no additional charge. You will be charged only for use of other AWS services by your users.

Instructor Notes:



8.1: AWS IAM
AWS IAM – Best practices

Users

Groups

Permissions

Auditing

Password

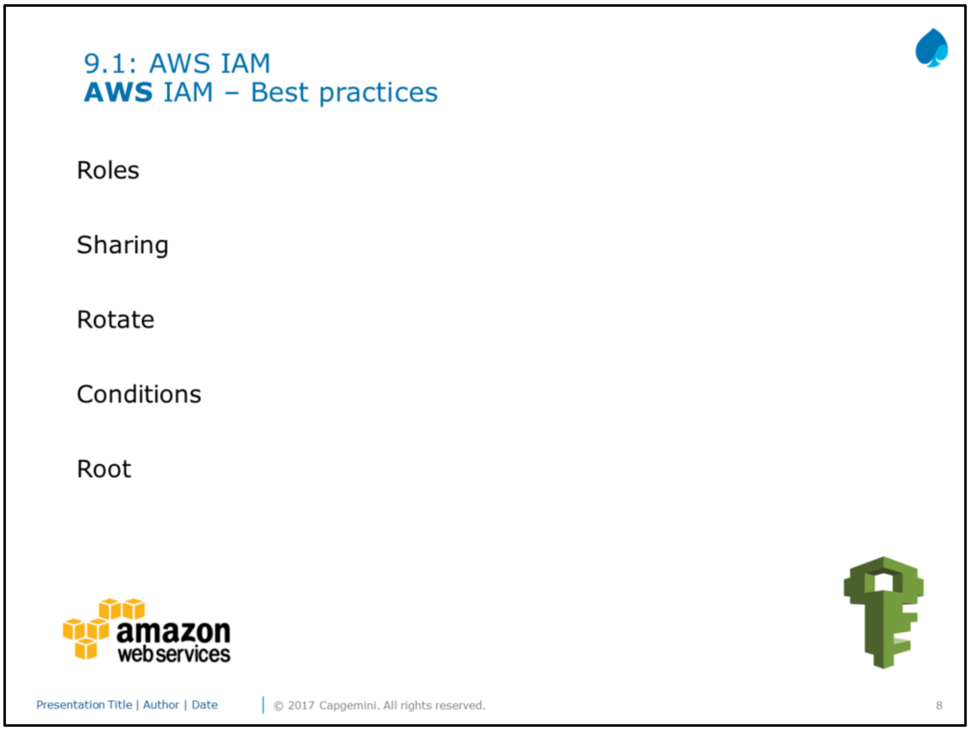
MFA(Multi-factor Authentication).

Presentation Title | Author | Date

7

Users – Create individual users.
Groups – Manage permissions with groups.
Permissions – Grant least privilege.
Auditing – Turn on AWS CloudTrail.
Password – Configure a strong password policy.
MFA – Enable MFA for privileged user

Instructor Notes:



9.1: AWS IAM
AWS IAM – Best practices

Roles

Sharing

Rotate

Conditions

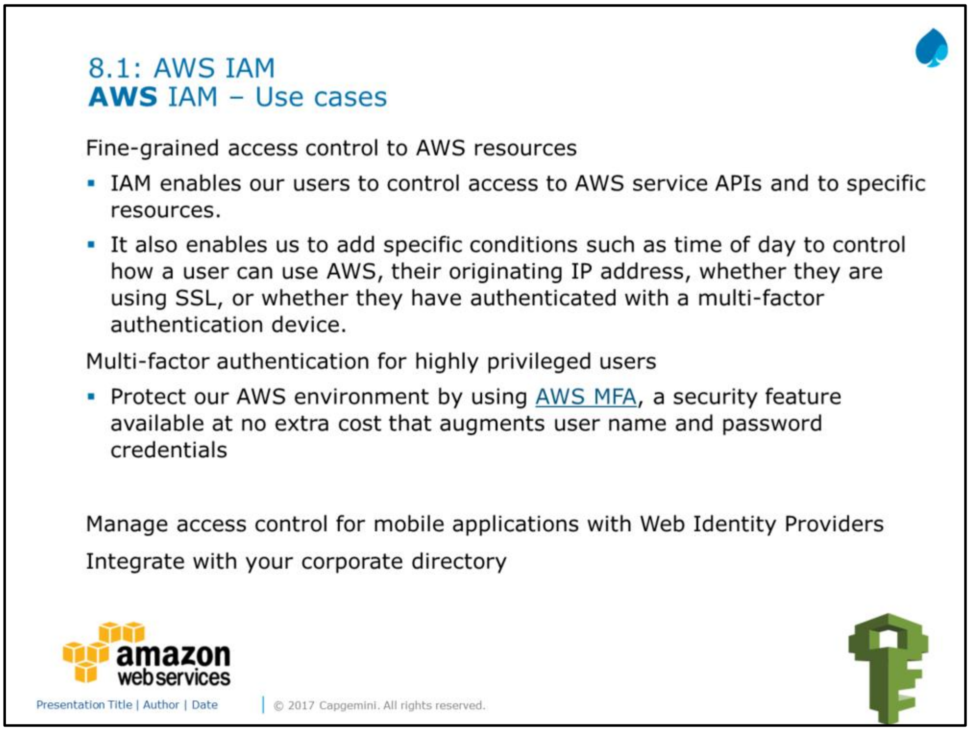
Root

Presentation Title | Author | Date

8

Roles – Use IAM roles for Amazon EC2 instances.
Sharing – Use IAM roles to share access.
Rotate – Rotate security credentials regularly.
Conditions – Restrict privileged access further with conditions.
Root – Reduce or remove use of root.

Instructor Notes:



8.1: AWS IAM
AWS IAM – Use cases

Fine-grained access control to AWS resources

- IAM enables our users to control access to AWS service APIs and to specific resources.
- It also enables us to add specific conditions such as time of day to control how a user can use AWS, their originating IP address, whether they are using SSL, or whether they have authenticated with a multi-factor authentication device.

Multi-factor authentication for highly privileged users

- Protect our AWS environment by using AWS MFA, a security feature available at no extra cost that augments user name and password credentials

Manage access control for mobile applications with Web Identity Providers

Integrate with your corporate directory

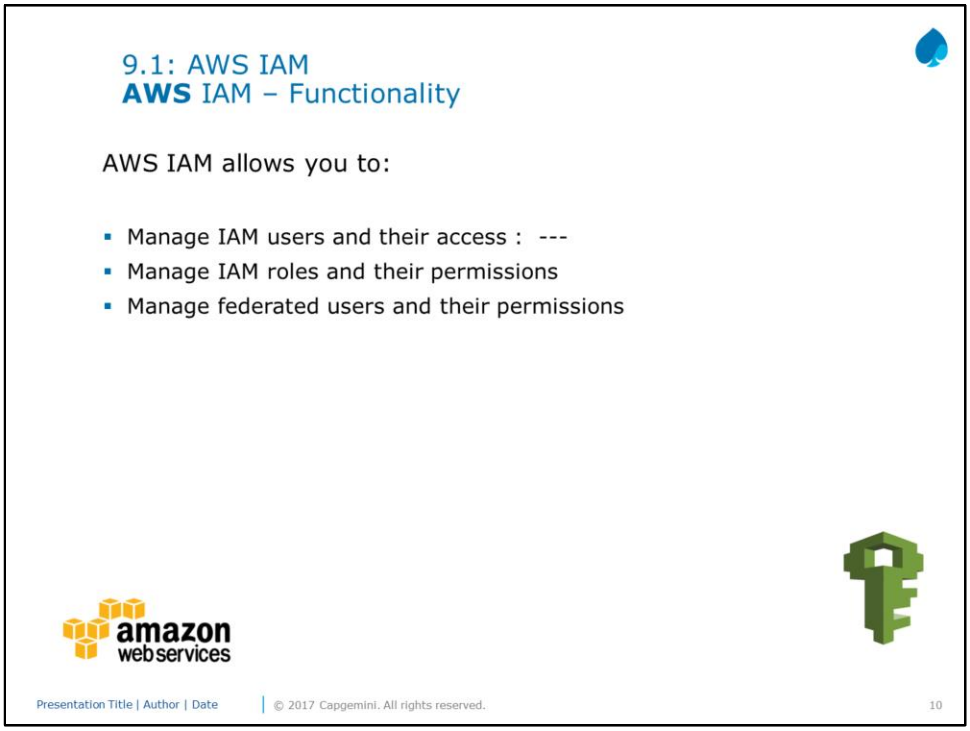
Presentation Title | Author | Date

© 2017 Capgemini. All rights reserved.

You can enable your mobile and browser-based applications to securely access AWS resources by requesting temporary security credentials that grant access only to specific AWS resources for a configurable period of time.

IAM can be used to grant your employees and applications federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation).

Instructor Notes:



9.1: AWS IAM
AWS IAM – Functionality

AWS IAM allows you to:

- Manage IAM users and their access : ---
- Manage IAM roles and their permissions
- Manage federated users and their permissions

amazon
web services

Presentation Title | Author | Date

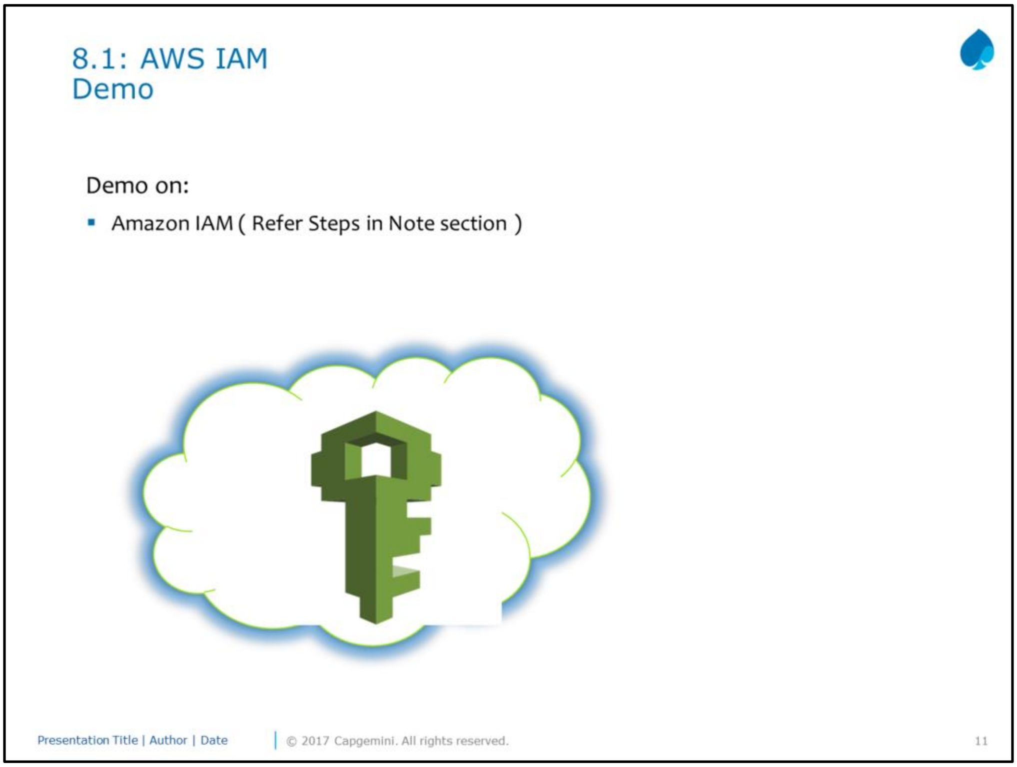
10

You can create users in IAM, assign them individual security credentials (in other words, access keys, passwords, and multi-factor authentication devices), or request temporary security credentials to provide users access to AWS services and resources. You can manage permissions in order to control which operations a user can perform.

You can create roles in IAM and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. You can also define which entity is allowed to assume the role. In addition, you can use service-linked roles to delegate permissions to AWS services that create and manage AWS resources on your behalf.

You can enable identity federation to allow existing identities (users, groups, and roles) in your enterprise to access the AWS Management Console, call AWS APIs, and access resources, without the need to create an IAM user for each identity.

Instructor Notes:



8.1: AWS IAM
Demo

Demo on:

- Amazon IAM (Refer Steps in Note section)

Presentation Title | Author | Date | © 2017 Capgemini. All rights reserved. 11

5.1. Create an EC2 instance.

Follow the Steps to create a user by using IAM service

Step 1: Choose the IAM service in AWS

Step 2 : Click on User link in IAM dashboard and click on AddUser button

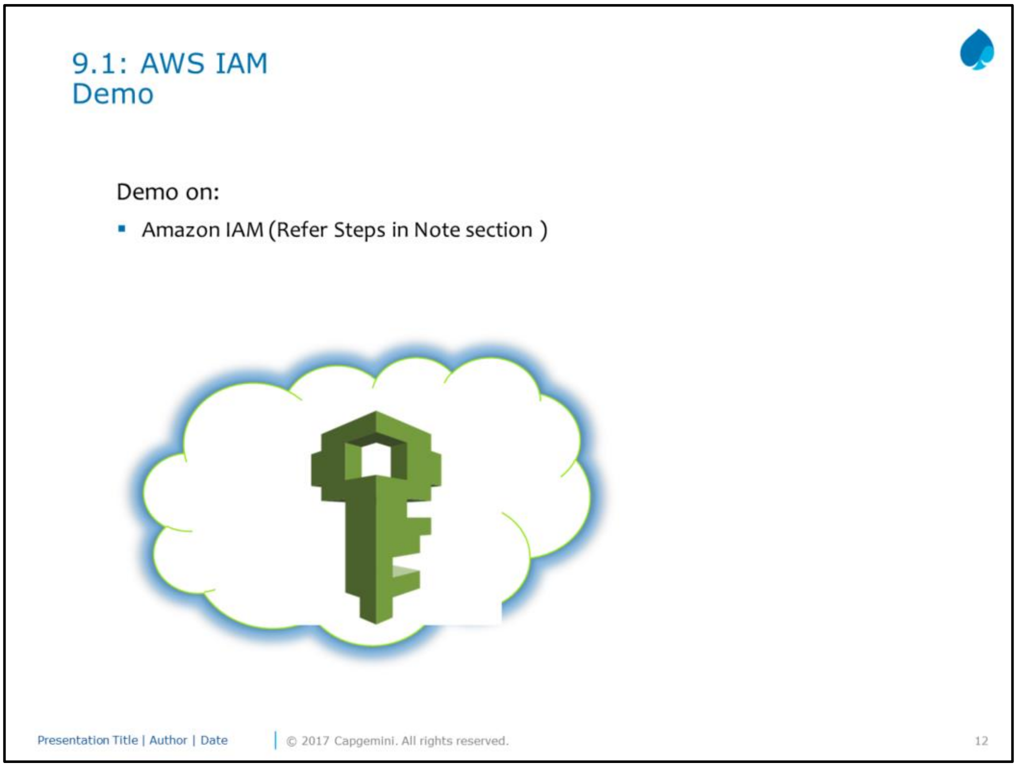
Step 3 : Type a user name and choose both the access type

Step 4 : Select custom password and provide a password .(it must contain at least 12 characters and it must contain a digit)
Step 5 : click on Next permission button.

Step 6 : Click on Attach existing policy button directly
Step 7 : Select AmazonEC2ReadonlyAccess checkbox from existing list and click Next: review button.

Step 8 : click on create user button .
Step 9 : Now download the credential in .csv format and click on close button.
Step 10 : Click on user link and review the policy.

Instructor Notes:



9.1: AWS IAM
Demo

Demo on:

- Amazon IAM (Refer Steps in Note section)

Presentation Title | Author | Date

12

Follow the Steps to create a policy for your Ec2 instance which you have created before.
Step 11 : Click on Policy link in IAM dashboard
Step 12 : Click on createpolicy button
Step 13 : Choose EC2 service.
Step 14 : Click on Select action link and choose List and read checkbox
Step 15 : Select resources and choose specific option

Step 16 : Click on Add ARN link

Step 17 : click on Add button
Step 18 : click on review policy button
Step 19 : click on Add permission link
Step 20 : choose IAM service
Step 21 : select Action and expand Write option
Step 22 : choose checkbox “Update Login Profile”
Step 23 : Now choose specific resources and add ARN

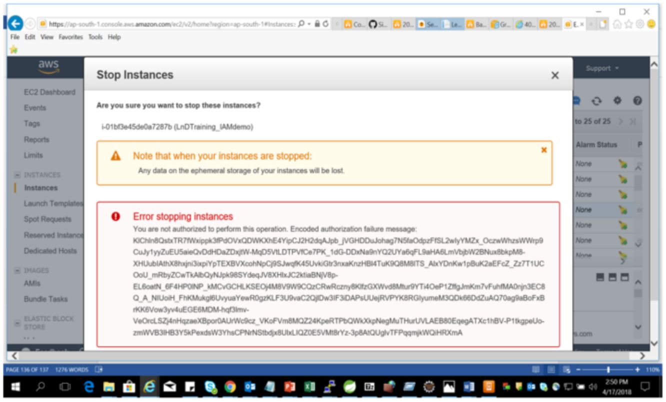
Step 24 : Click on review policy button
Step 25 : click on create policy button
Step 26 : go to user and select the user you created before
Step 27 : detach the previous policy
Step 28 : Add the policy you created before

Instructor Notes:

8.1: AWS IAM Demo

Demo on:

- Amazon IAM (Refer Steps in Note section)



Stop Instances

Are you sure you want to stop these instances?

i-01bf3e45de0a7287b (LnDTraining_IAMdemo)

Note that when your instances are stopped:
Any data on the ephemeral storage of your instances will be lost.

Error stopping instances
You are not authorized to perform this operation. Encoded authorization failure message:

```
KlChln8QstxTR7fWxippk3fPdOVxQDWKXhE4YipCJ2H2dqAJpb_jVGHDDuJohag7N5faOdpzFfSL2wlyYMZx_OczwWhzsWWrp9
CuJy1yyZuEU5aieQvDdHDaZDxjtW-MqD5VtLDTPVfCe7PK_1dG-DDxNa9nYQ2UYa6qFL9aHA6LmVbjbW2BNux8bkpM8-
XHUublAthX8hxjni3ixpiYpTEXBVXcohNpCj9SJwqfK45UvkiGtr3nxaKnzHBI4TuK9Q8M8ITS_AlxYDnKw1pBuK2aEFcZ_Zz7T1UC
OoU_mRbyZCwTkAlbQyNJpk98SYdeqJV8XHlxJC2ktiaBNjV8p-
EL6oatN_6F4HP0INP_kMCvGCHLKSEOj4M8V9W9CQzCRwRczny8KlfzGXWvd8Mtur9YTi4OeP1ZffgJmKm7vFuhfMA0njn3EC8
Q_A_NIUoiH_FhKMukgl6UvyuaYewR0gzKLF3U9vaC2QjlDw3IF3iDAPsUUejRVPYK8RGlyumeM3QDk66DdZuAQ70ag9aBoFxB
rKK6Vow3yv4uEGE6MDM-hqf3lmv-
VeOrcLSZj4nHqzaeXBpor0AUrWc9cz_VKoFVm8MQZ24KpeRTPbQWkXkpNegMuTHurUVLAEB80EqegATXc1hBV-P1tkgpeUo-
zmWVB3IHB3Y5kPexdsW3YhsCPNrNStbdjx8UlxLIQZ0E5VMt8rYz-3p8AtQUglvTFPqqmjkWQiHRXmA
```

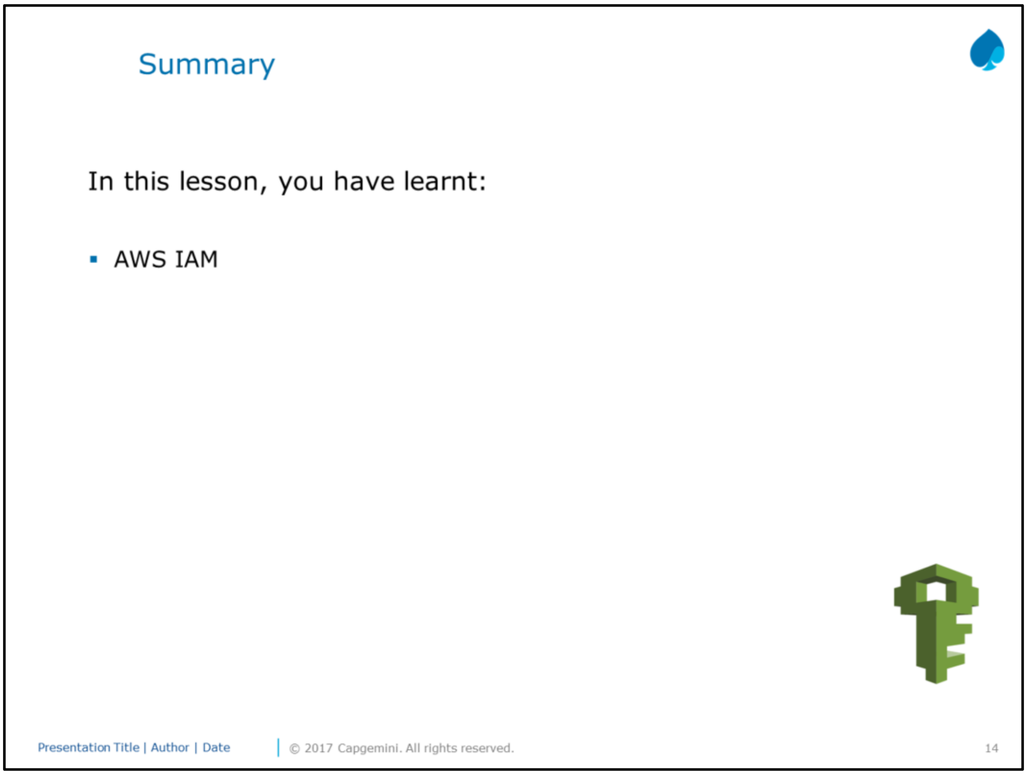
Presentation Title | Author | Date | © 2017 Capgemini. All rights reserved. 13

Step 29: click on Next review button
Step 30 : check the new policy attached to user

Steps to allow the user top signin and see the restrictions

Step 31 : Go to browser and add the user name and password and login
Step 32 : Select EC2 service and see all the instances.
Step 33 : Choose your instance and try to stop it.

Instructor Notes:



Summary

In this lesson, you have learnt:

- AWS IAM

Presentation Title | Author | Date

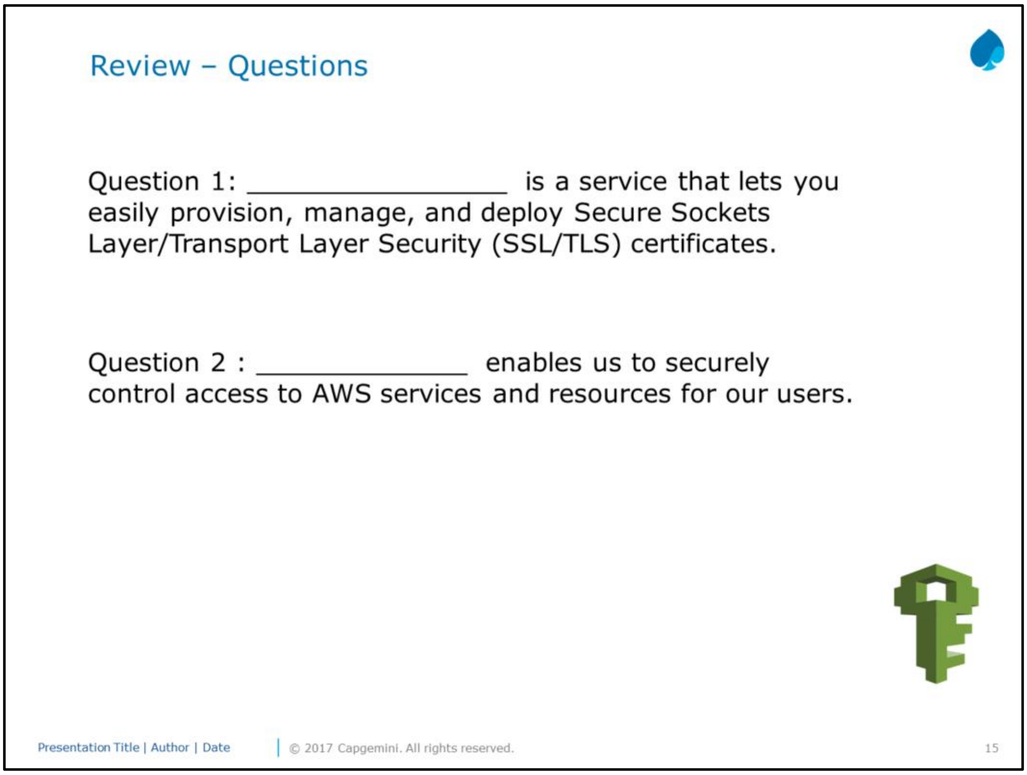
14

Instructor Notes:

Answers for the Review Questions:

Answer 1: AWS Certificate Manager

Answer 2: AWS IAM



Review – Questions

Question 1: ____________________ is a service that lets you easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates.

Question 2 : ________________ enables us to securely control access to AWS services and resources for our users.

Presentation Title | Author | Date

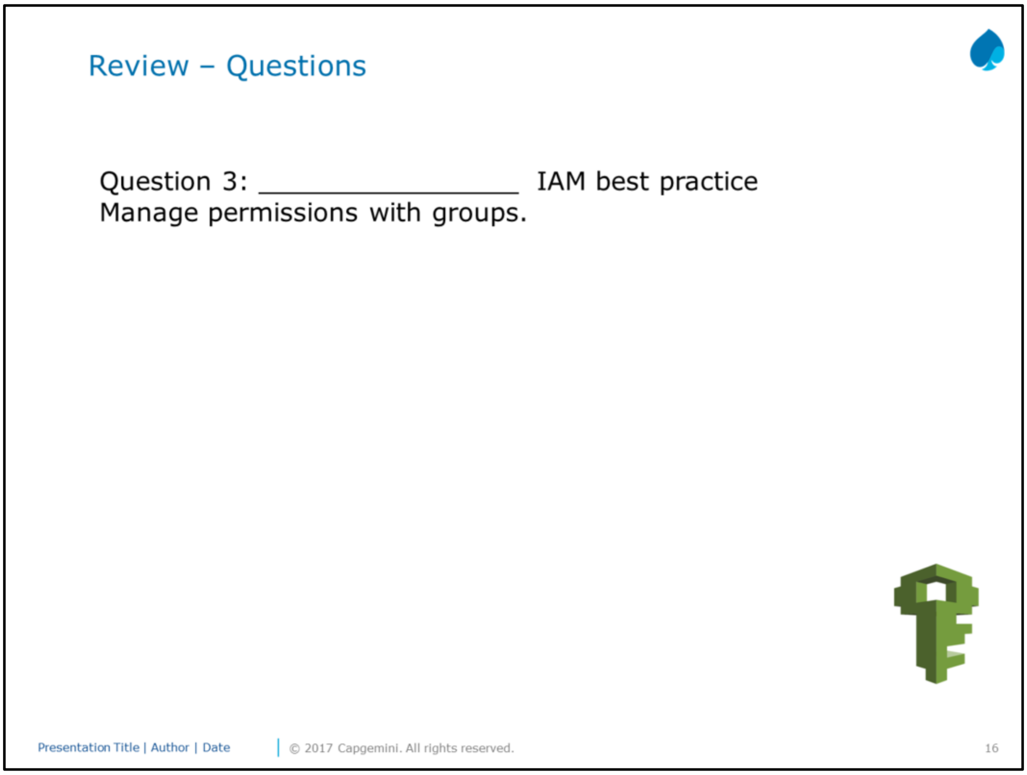
15

Instructor Notes:

Answers for the Review Questions:

Answer 3: IAM Groups

Answer 2: AWS IAM



Review – Questions

Question 3: __________________ IAM best practice
Manage permissions with groups.