TEAM LEAD VERSION (Week-2)

TEAMWORK

CLARUSWAY
WAY TO REINVENT YOURSELF

Meeting Agenda

▶ Icebreaking

▶ Questions

▶ Interview/Certification Questions

▶ Coding Challenge

▶ Video of the week

▶ Retro meeting

▶ Case study / project

Teamwork Schedule

Ice-breaking   10m

- Personal Questions (Stay at home & Corona, Study Environment, Kids etc.)
- Any challenges (Classes, Coding, AWS, studying, etc.)
- Ask how they're studying, give personal advice.
- Remind that practice makes perfect.

Team work   10m

- Ask what exactly each student does for the team, if they know each other, if they care for each other, if they follow and talk with each other etc.

Ask Questions   15m

1. In On-Demand instance model, each virtual machine has an .... price.

A. Yearly
B. Weekly
C. Hourly
D. Monthly

Answer: *C*

2. Encapsulation is the process of taking data from one protocol and translating it into another protocol, so the data can continue across a network.

A. True
B. False

Answer: *A*

3. Which command is used for modifying a user's properties?

A. who am i
B. sudo su
C. usermod
D. groupadd

Answer: *C*

4. The network address of 172.16.0.0/19 provides how many subnets and hosts?

A. 7 subnets, 30 hosts each
B. 8 subnets, 8.190 hosts each
C. 8 subnets, 2.046 hosts each
D. 7 subnets, 2.046 hosts each

Answer: *B*

5. What is the default subnet mask for a Class B address?

A. 255.0.0.0
B. 255.255.0.0
C. 255.255.255.0
D. 255.255.255.255

Answer: *B*

Interview/Certification Questions   20m

1. Which of the following can be used to manage identities in AWS.

A. AWS Config
B. AWS IAM
C. AWS Trusted Advisor
D. AWS CloudFormation

Answer: *B*

AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
For more information on AWS IAM, please refer to the Link

2. You have an application developed in .NET. This applications works with the S3 buckets in a particular region. The application is hosted on an EC2 Instance. Which of the following should ideally be used to ensure that the EC2 Instance has the appropriate access to the S3 buckets?

A. AWS Users
B. AWS Groups
C. AWS IAM Roles
D. AWS IAM Policies

Answer: *C*

The AWS Documentation mentions the following:
You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. For more information on IAM Roles, please refer to the Link

Groups are collections of Users which will not be appropriate for the EC2 Instance so A and B are incorrect.The creation of a new policy cannot ensure appropriate access. They must be attached to a User, Group or Role. Therefore D is incorrect.

3. What happens when one of the resources in a stack cannot be created successfully? (CloudFormation)

Answer:

By default, the "automatic rollback on error" feature is enabled. This will cause all AWS resources that AWS CloudFormation created successfully for a stack up to the point where an error occurred to be deleted. This is useful when, for example, you accidentally exceed your default limit of Elastic IP addresses, or you don't have access to an EC2 AMI you're trying to run. This feature enables you to rely on the fact that stacks are either fully created, or not at all, which simplifies system administration and layered solutions built on top of AWS CloudFormation.

4. A company has a set of EC2 Instances that store critical data on EBS Volumes. There is a fear from IT Supervisors that if data on the EBS Volumes is lost, then it could result in a lot of effort to recover the data from other sources. Which of the following would help alleviate this concern in an economical way?

A. Take regular EBS Snapshots
B. Enable EBS Volume encryption
C. Create a script to copy data to an EC2 Instance Store
D. Mirror data across 2 EBS Volumes

Answer: *A*

Option B is incorrect because it does not help in durability of EBS Volumes.
Option C is incorrect since EC2 Instance stores are not durable.
Option D is incorrect since mirroring data across EBS Volumes is inefficient when you already have an option for EBS Snapshots.
The AWS Documentation mentions the following on AWS EBS Snapshots: You can back up the data on your Amazon EBS Volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data. When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new EBS volume. For more information on AWS EBS Snapshots, please visit the Link

5. A new department has recently joined the organization and the administrator needs to compose access permissions for the group of users. Given that they have varying roles and access needs, what is the best-practice approach when granting access?

A. After gathering information on their access needs, the administrator should allow every user to access the most common resources and privileges on the system.
B. The administrator should grant all users the same permissions and then grant more upon request.
C. The administrator should grant all users the least privilege and add more privileges to only to those who need it.
D. Users should have no access and be granted temporary access on the occasions that they need to execute a task.

Answer: *C*

The best-practice for AWS Identity Access Management (IAM) is to grant the least amount of permissions on the system, enough to only execute the required tasks of the user's role. Additional permissions can be granted per user in accordance to the tasks they wish to perform on the system. Link

Option A. is incorrect because granting users access to the most common resources presents security vulnerabilities, especially from those who have access to resources they do not need.
Option B. is incorrect because granting users the same privileges on the system means other users might get access to resources they do not need to carry out their job functions. This presents a security risk.
Option D. is incorrect because the users are part of the organisation, it will be cumbersome for the administrator to constantly create temporal access passes for internal staff.

Video of the Week   5m

- Introduction to YAML

Retro Meeting on a personal and team level   10m

Ask the questions below:

- What went well?
- What could be improved?
- What will we commit to do better in the next week?

Coding Challenge   5m

- Coding Challenge: Convert Milliseconds into Hours, Minutes, and Seconds

We assume that each group has two sub teams. Each week, one of the sub-teams will present their solution.

Case study/Project   10m

Case study should be explained to the students during the weekly meeting and has to be completed in one sprint (2 weeks) by the students. Students should work in small teams to complete the case study.

- Project-101 : Kittens Carousel Static Website deployed on AWS EC2 using Cloudformation

Closing   5m

-Next week's plan

-QA Session

___