MONASH University

Office Use Only

Semester One 2020
Final Assessment Period

Faculty of Information Technology

EXAM CODES: **FIT5225**

TITLE OF EXAM: **Cloud Computing and Security**

EXAM DURATION: 2 hours 10 minutes or 130 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT: (tick where applicable)

☑ Caulfield □ Clayton □ Parkville □ Peninsula
□ Monash Extension □ Off Campus Learning □ Malaysia □ Sth Africa
□ Other (specify)

During an exam, you must not have in your possession any item/material that has not been authorised for your exam. Any authorised items are listed below.

You must not retain, copy, memorise or note down any exam content for personal use or to share with any other person by any means following your exam.

As a student, and under Monash University's Student Academic Integrity procedure, you must undertake your in-semester tasks, and end-of-semester tasks, including exams, with honesty and integrity. In exams, you must not allow anyone else to do work for you and you must not do any work for others. You must not contact, or attempt to contact, another person in an attempt to gain unfair advantage during your exam session. Assessors may take reasonable steps to check that your work displays the expected standards of academic integrity. e.g. perform similarity checking on your submission. If required, you may be contacted after your exam to discuss any concerns.

Failure to comply with the above instructions, or attempting to cheat or cheating in an exam is a discipline offence under Part 7 of the Monash University (Council) Regulations, or a breach of instructions under Part 3 of the Monash University (Academic Board) Regulations.

AUTHORISED MATERIALS

OPEN BOOK ☑ **YES** □ **NO**

CALCULATORS ☑ **YES** □ **NO**

SPECIFICALLY PERMITTED ITEMS ☑ **YES** □ **NO**
if yes, items permitted are: Internet

Candidates must complete this section if required to write answers within this paper

STUDENT ID: __ __ __ __ __ __ __ __ DESK NUMBER: __ __ __ __ __

Q1	Q2	Q3	Q4	Q5	Q6
/8	/6	/6	/9	/12	/9

Q1. [8 marks]

In your first assignment, you built a web-based system that allows end-users to send an image to a *RESTful* API and receive a list of objects detected in their uploaded image. The web service was hosted in *docker* containers and *Kubernetes* was used as the container orchestration system. For each of the following distributed system challenges, give a practical example from the first assignment that illustrates that challenge (Please do not write more than 5 lines).

NOTE: Discuss Assignment 1 technologies, methods that helped to solve this issues

a) Heterogeneity

Different programming languages
Different OS
Different hardware

b) Openness

Well-defined APIs and Interfaces through which you can extend your application in the first assignment.

c) Security

Security groups in Kubernetes
Resource isolation
Dockers, Pods
Availability

d) Scalability

replicas in the deployment
scale based on the demand

e) Failure Handling

Replicas

Automatic load balancer for replica sets

f) Concurrency

Pods
Simultaneous access to application

g) Transparency

Access transparency
Location transparency
Concurrency transparency
Replication transparency
Failure transparency
Mobility transparency
Performance transparency
Scaling transparency

h) Quality of Service

QoS metrics (depends on system/ application type)

For Assignment 1:
Response time
Availability through Kubernetes service

Q2. [6 marks]

In the lectures, we discussed several technologies that have matured and significantly contributed to make cloud computing viable. Later we introduced Amazon Web Services (AWS) as a public cloud service provider. Discuss representation of each of these technologies in AWS. You should discuss how these technologies have been used or contributed to services offered by AWS, you can consider an exemplary service, e.g. EC2 (Not more than 5 lines).

a) Utility & Grid Computing

Pay as you go, on demand, resource sharing, geographically distributed resources, remote access, etc. Relevant examples: EC2 Pay-as-you-go, S3 Resource sharing, etc

b) Web Services

Web services enabled communication between network resources, services, and entities. It allowed interoperable communications. Discussion around REST APIs, relevant examples including API Gateway, Amazon Web service, etc.

c) Virtualization

Virtualization allowed rapid provisioning of customized resources, increase resource utilization, cost beneficial, etc. relevant examples VM, VPC, etc.

d) Autonomic Computing

Self-managed, self-configurable, self-healing computing paradigm. E.g (Cloud9, Ansible).

Q3. [6 marks]

A software system needs to be improved, and after analysis, we realize that 20% of the entire system could be parallelized.

a) What is the overall performance improvement (speed-up) that can be gained? Briefly explain your answer.

Speed up = 1/(1-0.2) = 1.25

b) If the maximum number of processors that we can provide is 20, what is the overall performance improvement? Briefly explain your answer.

Speedup = 1/((1-P) + (P/N))
= 1/((1-0.2) + (0.2/20))
= 1/(0.8
+ 0.01)
= 1.2345679012
= 1.23

c) If there is significant in-memory shared data that needs to be accessed by different parts of the software and you have a single multi-core machine to run this software, would you choose threads to implement this program or multiple processes? Briefly Justify your answer.

Threads as processes are not suitable as they have separate memory space. Thread share the memory that suits for the problem asked.

d) Explain why parallelization cannot be applied to a Fibonacci function?

Calculation is depended on the previous one and parallelization is not possible.

Q4. [9 marks]

Briefly answer the following questions:

a) [2 Marks] Compare *Paravirtualization* with *full virtualization*. Discuss at least two main pros and cons of each method?

Full VT
Pros:
1-No modified OS
2-Lower performance
Cons:
2. No Modified OS

Para:
1. Higher performance
Cons:
1. Modified OS

b) [5 Marks] You are supposed to give advice to a CEO of a company regarding the right choice between using *VMs* and *Containers* for their enterprise software. For each scenario select the best choice and justify your suggestion.

I. They need to run the maximum number of particular application(s) (e.g., multiple web servers) on a minimum number of servers.

Container
They provide isolation method, fast booting and migration speeds, etc.
Easy to replicate containers and scale with same docker image

II. Their software needs to run multiple applications on multiple servers (e.g., DB and Web Server).

VM
Application needs large independent resources
Higher performances (DB and Webserver)

III. They want to reuse lots of legacy applications that developed earlier.

VM –
As legacy applications usually require full OS and rigid to port onto docker images

IV. Security is very important.

VM
VM provides higher level of isolation compared to containers. They have their own IP, port and preassigned core and memories

V. They need a secure microservices architecture.

Container.
Microservices are lightweight (requiring small amount resources) and fast bootup for which containers are best fit.

c) [2 Marks] What does "Kubernetes uses a Pod as the smallest deployable unit (unit of scaling)" mean? Provide a use case scenario that shows using multiple containers in the same pod is a good practice. Explain why running two *Nginx* servers in a single pod does not make sense?

The statement means that pod is the unit that can be scaled through, for example, Deployment. Kubernetes is not designed to scale containers

Multiple containers should reside in same pod only if they share the same lifecycle. One of the reasons is simpler communication between containers through the network space and shared volumes.

There is a helper process that pulls the files from the remote repo and updates the storage volume. The main container which is a web server serves those static files from the same storage to the outside world

Nginx servers two web servers do not have the same lifecycle. One of the reasons is port conflict and they do not want to share anything.

Q5. [12 marks]

Tollink, a toll road operator company, has decided to shift its on-premise toll management application to Amazon Web Services (AWS). You are hired as a Cloud solution architect/consultant to help them design their migration solution. For each of the following, offer the AWS service(s) that would suit their needs.

a) Their roadside equipment captures the images of vehicles and send them to the system. The first thing Tollink needs to do is to store images for future references. They will keep images for at least 30 days and rarely access those images after the process. After 30 days, images can be archived. The image data is not reproducible if lost. Which AWS service do you suggest to store images if high availability in the first 30 days is the main concern. If the company would like to save costs on storage what do you suggest? Briefly justify your answer.

NOTE: Each of example needs justification

S3-IA
S3-Standard
Explaining why S3-IA or is a suitable solution for this situation.

b) Tollink has an automatic number-plate recognition technology that reads the image and identifies the plate number. This will generate meta-data for each image and loss of that meta-data is not as important as images, since we can regenerate it again using the original image. Which AWS service should you use to persist the non-critical, easily reproducible meta-data, in the most cost-effective way? Briefly justify your answer.

RDS
S3

c) Do you suggest lambda or EC2 for hosting the automatic number-plate recognition program? Briefly justify your answer. A cost-effective solution matters.

Either Lambda or EC2 can be considered correct, depending on the justification. A correct answer mentions the fact that Lambda costs per invocation/usage. hence if the application doesn't need to monitor roads 24/7, it will be cheaper to use

d) Tollink needs to store customers data in a relational database. Offer them an AWS relational database (DB) service. For each vehicle passing the roadside equipment they need to send a query to the database to find the matching customer data. The key factor is scalability, i.e., they would like to increase the performance of read traffic to their DB. What DB solution are you suggesting? Briefly justify your answer.

Best answer is Aurora, explaining its performance and read replica features compared to other RDS services.

Common mistake: mentioning no-sql databases instead of RDS instances.

e) At the end of each year, Tollink requires a huge amount of computing capacity to run computational-intensive tasks designed to be fault-tolerant. Which type of EC2 instances in terms of pricing model do you recommend? Why?

Spot instances, giving a brief explanation about why using spot instances if more cost-effective.

Common mistakes: mentioning different types of EC2 instance types (flavours).

f) The cloud-based solution relies on an on-premise backend system and it requires to communicate some updates with the backend system frequently (small messages < 256KB). These updates are critical to the system. The on-premise backend system is not as reliable as the cloud-based component and sometimes becomes unavailable. What solution and AWS service do you suggest to make sure that they do not lose any update? Briefly justify your answer.

SNS, giving a brief explanation about why this service is suitable.

Common mistake: mentioning other irrelevant services, only mentioning the service name without providing any justifications.

g) Tollink is hosting a web server with lots of media content. Its customers are geographically distributed all over the world. The response time of their web site is very important to them. Which AWS service would help them to provide a better response time? Briefly justify your answer.

CloudFront, giving a brief explanation about why this service is suitable

Common mistake: mentioning other irrelevant services, or just mentioning elastic cache, only mentioning the service name without providing any justifications.

h) Tollink provides subscription-based service to notify some of its key clients (e.g., car rental companies). What AWS service do you suggest in this scenario. Briefly explain your answer.

SNS, giving a brief explanation about why this service is suitable

Common mistake: mentioning other irrelevant services, only mentioning the service name without providing any justifications.

Q6. [9 marks]

Suppose Tollink's cloud architecture consists of a VPC (V) with IP address range of 10.0.0.0/16 that has two subnets (A and B) in the *us-east-1a* availability zone. In subnet A, there is an EC2 instance that runs a Nginx server and an RDS instance that is used as the primary database. In subnet B, there is another EC2 instance that has been created from the same Nginx AMI. In each subnet, there is an Internet gateway that allows instances to connect to the internet and receive the latest updates and security patches.

There is one private key that is used to SSH into the EC2 instances and the following security group is attached to both EC2 instances (assume that all outbound traffic is allowed):

Protocol	Source IP	Port Range
TCP	**0.0.0.0/0**	**22**
TCP	**10.0.0.0/16**	**80-443**

Assume that Tollink has approached you as a security consultant to help them secure their infrastructure and make their website highly available and fault tolerant. Your task is to perform a risk analysis and identify **at least 6 security drawbacks** and misconfigurations in their current solution. In your proposal, you are free to make changes to any of the resources mentioned above and to request new resources of the same type. Briefly (1-2 sentences max) explain your proposed solution for resolving each security flaw.

For the given scenario, there are multiple security shortcomings and misconfigurations: a port range has been specified, the source IP is not correct, not using bastion host and only one keypair for all instances is a threat, services are not highly available and fault tolerant due to use of only one AZ, public and private subnets are not defined and configured correctly.

Common mistakes: Mentioning ACL rules, authentication and authorisation schemes, firewall/IDS, and other resources that can potentially increase the application's security (if configured and used properly), but the question doesn't provide any information about those resources.
Another common mistake was giving a general answer, referring to OWASP top 10 security threats, attacks against hypervisor, etc. that again, is not the correct answer here, because no information has been given about them.

END OF EXAMINATION PAPER