

2208814_WongChing

by Ching Wong

Submission date: 07-Dec-2022 11:02PM (UTC+0000)

Submission ID: 191417434

File name: 41382_Ching_Wong_2208814_WongChing_460442_2044557857.docx (19.87K)

Word count: 2111

Character count: 11769

Name: Wong Ching

Student ID: 2208814

Assignment 1

This essay will discuss about cloud computing. It would be divided into 5 parts.

Virtualization, virtual machine, cloud services, availability, and security concerns.

To begin with, virtual machine (VM) is a virtual environment that functions like a physical computer. Operating systems and applications could be operated in that virtual environment. It could be considered as running another virtual computer on an actual computer simultaneously. By using a virtual machine monitor called hypervisor, it can allocate physical resources between the VM and the actual physical devices. It separates hardware resources from the actual physical machine, to allocate storage, memory, and CPU to different VM.

Virtualization is a technology that could allow multiple virtual environments to operate within a single computer.⁸ Which allows running various applications and

operating systems in a single hardware simultaneously. The functionality of different kinds of physical infrastructure can be obtained by using virtualization technology, such as servers, storage, and networking center. All of those can run it on a virtual environment. Which makes cloud computing possible.

Cloud computing is a pay-as-you-go service to deliver different computing resources to users through the internet, such as databases, storage, networking, and server. Instead of building and maintaining a physical infrastructure in order to obtain these resources by users themselves, they can purchase from cloud providers, and access these services on the internet. As data centers are built and maintained by cloud service providers. Virtualization technology enables users to replace physical files, storage, network, and server devices with a virtual version. And users just need to access these resources online through the API provided by the cloud provider.

There are numerous benefits of using the technology of virtualization. First, it is cost-saving. Hardware resources require huge amount expenses to maintain, such as the electricity fees of all the physical devices, the cooling appliances, and the renting fee of the space. The expense would be decreased as the amount of hardware is reduced

by using virtualization technology. Moreover, all the development scales would become elastic.⁸ The scale of resources could change quickly as what the user needed, no matter increases or decrease. For example, if a company would like to increase the storage of the database. Instead of purchasing new storage hardware, the company just requires to configure the setting in a virtualized environment. It is time-saving and all the adjustments of the development become elastic.

Furthermore, it has a fast disaster recovery. For damage in a physical server, it may take a long time to repair the damage, or even be unable to repair it completely. However, it would just take minutes to repair in a virtualized environment. The recovery would be much faster.

For the part of cloud services. There are mainly three types of cloud services. Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). For the first type of cloud services, Infrastructure as a service (IaaS). Infrastructures are managed by cloud providers, such as servers, networking, and storage. Cloud customers can access those resources via virtual machines on the internet. And customers have the right to deploy the application and operating system by themselves. Amazon Web Services and Microsoft Azure is the examples of using IaaS. IaaS is very efficient in terms of cost and time. Customers do not have to

purchase or maintain infrastructure; it is all done by the provider. They can focus on the deployment of the software. Also, the scalability of IaaS is extremely flexible.¹ Usually, IaaS providers would charge customers as a pay-as-you-go model, charging by the number of virtual machines used. Customers can adjust the storage scale easily. However, as the infrastructure is fully owned by the provider, the performance of the infrastructure has a significant impact on the customer's workload. If the infrastructure is down, customers are not able to operate their service normally, they have no control over it.

For the second type of cloud services, platform as a service (PaaS). It includes some features which are the same as IaaS, such as infrastructure management provided by the cloud provider, using a pay-as-you-go basis. However, it contains more features. The most distinct one is PaaS provides application development tools to customers. It could be a business intelligence analytics tool, that allows customers to analyze the products or services by data, and let customers make better business decisions by using these data.⁶ It could also be a coding tool, allowing users to develop a program using the coding tools instead of coding very lines by themselves. Also, some PaaS provide the function of cross-platform development, users can develop an application for multiple platforms faster and easier. These features allow some extra

advantages over IaaS, such as a shorter time of application development. PaaS offers development tools and cross-platform development; the coding time could reduce with the help of these tools. Moreover, it allows the company to save costs by hiring less experienced developers for software development and maintenance. With the help of the development tools, application development and maintenance become easier, and the company could reduce the expense by hiring less skilled developers. Nonetheless, the disadvantage of PaaS is the accessibility of management. Customers do not have the authority to control or access the operating system and the infrastructure.

For the third type of cloud services, software as a service (SaaS). All resources are provided to the end-user as an application through the internet. ⁶It usually charges on a subscription basis. Users can access the cloud service via the internet and no software installation is required. Same with IaaS and PaaS, the IT infrastructure is managed by the cloud provider. However, SaaS users only have the right to control the data in the software. They are not authorized to manage the application or the operating system. Office 365 and Dropbox are an example of SaaS. There are some advantages of using SaaS, it could be cost-effective. As the software is prepared and managed by the cloud provider, users do not have to pay for application

development and maintenance. It is just a payment for flexible subscription.

However, customers have lack control over the software, users have no right to manage the application provided by the provider. They cannot make special customization that could suit their personal use.

As a Small or Medium size Enterprise, I would suggest the company use platform as a service model. Compared to the three main cloud computing service models, PaaS is very friendly for application development as it offers development tools and cross-platform development, which IaaS does not. Due to the development tools, fewer expert developers are required, and the development speed could speed up, which leads to reduce expense. Moreover, as PaaS users could manage the application and data, it allows the company to develop a website to tailor to their needs which SaaS does not. Because of these reasons, I would recommend the company use the platform as a service model.

For the part of availability. Data centers of cloud providers are distributed in different regions. Cloud users can choose the physically location of the data centers of their services or application. ⁵The connection reliability and speed would depend on the regions. The closer to the regions usually have the faster connection. For example, if

cloud users choose the regions of their services at UK South. People in UK who use their service would have less latency than people in Africa. Different regions may charge differently, and there may be different features provided from the provider. For availability zone, it is the grouping of distinct data centers and linked together within a region.³ Data centers are physically separated. Data center failures can be protected as the design of availability zone. For example, assume the availability zone in UK has three data centers. If one of the data centers goes down, there are still two data centers working, data could be replicated to the working data center and keep the operation continuing. However, not all the regions support availability zone. For resource groups, when cloud users purchase services from provider, such as SQL databases, virtual machines, or web application. These purchased services would be named as resources. Resource groups are used to contain resources in a group. Users could decide the allocation of the resources in the resource group. Usually, resource groups are organized by resources with same type, lifecycle, or department. So that users can manage them as a group easier.

Considering with the case of having a medium budget service. First, all the resources would be duplicated in another availability zone. For example, place the resources in availability zone one and duplicate them in zone two. Which if there is a failure in

one data center in that region would not affect the operation. Also, I would choose the locations of the resources in the regions where have the most target customers. Which could provide the best web service experience to the target customers. Moreover, in order to reduce the operation cost, perform automate monitoring to keep track of the usage of resources, turn off the unused resources when they are not used.

For the case of having a very high budget service with no cost limit. Instead of just duplicate the resources in availability zone. I would duplicate resources in other region for region pairs. Region pairs means the region is paired with another region, and the distance between those two at least 300 miles. It is like the concept of availability zone, but it is linked by regions. By using region pairs method, it can ensure that if one region goes down, the paired region would replicate the resources and continue the operation. It can prevent large scale natural disaster like earthquake.

For the part of security concerns. Authentication is a process to check someone's identity. And authorization is a process to confirm their access right. Using the student accommodation system as an example. Students have their access cards,

when a student places the access card to the sensor of the gate, it is the process of authentication. The access card is to prove that the person is a resident of the accommodation. The gate will only open for people who is a resident. However, as a resident, there are some areas that are restricted for entry, such as staff rooms. And authorization is to check if the cardholder has the access right to enter the room.

Moreover, multi-factor authentication is a method that requires at least two verifications in order to acquire access.⁷ For example, when a customer shopping online, after he inputs the credit card information, the credit system would send a one-time confirmation code via mobile phone. The transaction would only be successful if the customer inputs both credit card information and confirmation code correctly. This method could enhance the security of the system, especially to defend against brute force attacks. Even if the credit card information is stolen by others, they still cannot use the credit card as they are not able to get the confirmation code.

Furthermore, least-privilege permission is a concept that only provides the lowest permissions to the user, and these permissions are just enough to complete their required task, not less and not more.² This concept could enhance the security of the system. The scale of vulnerability is reduced. By applying this concept, the number of

privileged administrators would decrease, which leads cyber attackers to have a less attacking surface, and the likelihood of having malicious insiders would drop. For network security group and Bastions, it can filter and organize the virtual network traffic by containing security rules. Those rules could accept or reject traffic through the inbound or outbound network. It is very important for prevent unauthorized access. For example, network security groups could establish security rules to deny the unauthorized user to access the virtual machine through the internet.

Reference list

1. Boisvert, M., Bigelow, S. J., & Chai, W. (2022, November 10). Infrastructure as a Service (IaaS). Cloud Computing. <https://www.techtarget.com/searchcloudcomputing/definition/Infrastructure-as-a-Service-IaaS>
2. CyberArk Software. (2021, September 28). What is Least Privilege? Principle of Least Privilege Definition. CyberArk. <https://www.cyberark.com/what-is/least-privilege/>
3. Kumar, A. (2022, August 4). Azure Availability Zones, Azure Regions, Availability sets, Fault & Update domain. <https://k21academy.com/microsoft-azure/az-303/azure-availability-zones-and-regions/>
4. Network Security Groups. (n.d.). (C) Copyright 2022. <https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/networksecuritygroups.htm>
5. The Big Deal About Cloud Regions | Lucidchart Blog. (2019, January 7). <https://www.lucidchart.com/blog/what-are-cloud-regions>
6. What Is IaaS, PaaS, and SaaS? Examples and Definitions: A Cloud Report. (2020, April 28). Mindsight. <https://gomindsight.com/insights/blog/what-is-iaas-paas-and-saas-examples-and-definitions/>
7. What is Multi-Factor Authentication (MFA)? | OneLogin. (n.d.). <https://www.onelogin.com/learn/what-is-mfa>
8. What is Virtualization? - Cloud Computing Virtualization - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/what-is/virtualization/?nc1=h_ls

FINAL GRADE

62/100

GENERAL COMMENTS

Instructor

Virtualization/VM: 12

Cloud Services: 18

Availability: 18

Security: 14

Feedback:

++++++

I was hoping for more discussion of virtualisation and VM components.

A reasonable discussion of the available services and your arguments for appropriate service for the presented scenario were also quite reasonable. I would have liked to have seen more thought given to expertise but generally this was good.

The discussion of security was a little brief and slightly confusing.

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

