UNIVERSITY OF WALES
Trinity Saint David
London

Title of report

Cloud Computing Architecture

Module Code: ACCA5025

Assignment 1: Essay

RANGEL GEORGIEV STOITSOV

Student ID: 2029065

Lecturer: SUNETH FERNANDO

Date submission:

06/04/2023

Table of Contents

What is “virtualization” and “virtual machine” in the context of cloud computing. 3

Evaluation of moving the on-premises application to the cloud and its benefits. 5

Infrastructure as a service model for our company. 6

Evaluation of moving an e-commerce website and associated web service of this on-premises application to the cloud. 7

Azure Concepts: 8

REFERENCES 10

What is “virtualization” and “virtual machine” in the context of cloud computing.

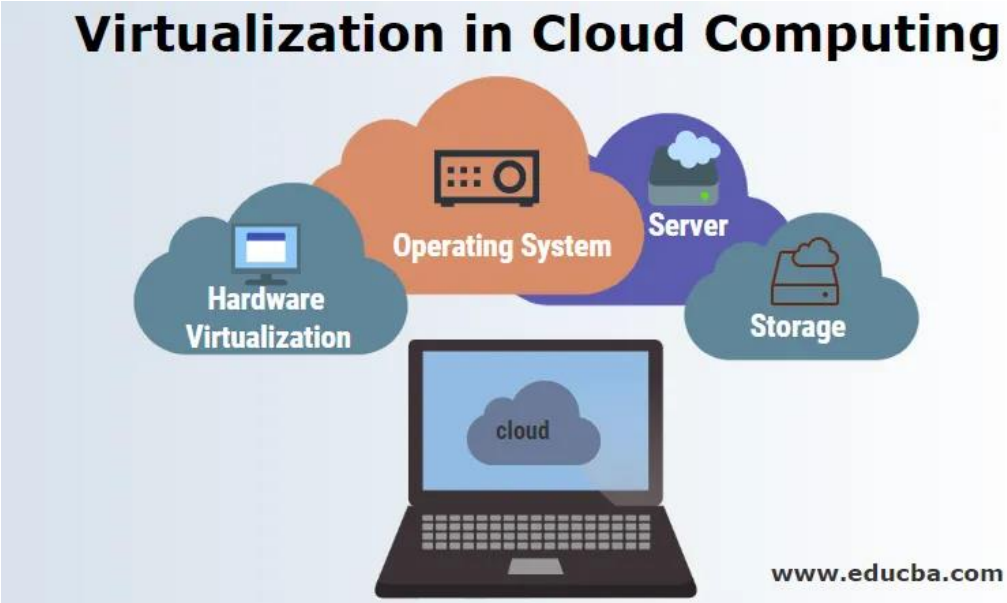

Fig.1

Virtualization in cloud computing is a technology that makes it possible to share the physical instance of one server or resources between multiple users or multiple organizations, in other words, it basically makes a virtual platform of the server's operating system (operating system), storage devices, desktop or network resources. When we talk about cloud virtualization, virtualization is done using resources available in the cloud, which are then shared between users to make cloud virtualization possible. (bg.education-wiki, n.d.)

Virtualization work in cloud computing

There are a few ways to run many programs and numerous users on a single server, and one of these methods is to deploy some software and set virtual machines to migrate from one host to another without ever being allowed to shut down. while they are at work. Live migration is another name for this technique. The alternative strategy uses the load-balancing technique to distribute the load over several hosts to make better use of the resources available to the virtual machine. The method is often referred to as "dynamic resource handling."

When we talk about cloud computing, it's not just about people sharing their data; they're also sharing their infrastructure to create virtualization strategies that may be helpful in practically any company. The standard versions of the cloud computing application are then distributed to consumers. It is effectively possible to make the most recent version accessible to users and the cloud once it has been deployed.

Following are a few ways that enable us to enable cloud virtualization which are:

OS Level Virtualization - In this cloud computing virtualization, multiple instances of an application can run on a single OS.

Hypervisor-based virtualization - In this process, the OS shares the hardware of the host computer and thus allows multiple hosts (operating systems) to run on a single host.

Grid approach - here a given workload is distributed across many physical servers and once the result is calculated, it is delivered back. This type of service is mainly used for scientific purposes.

Types of virtualizations in cloud computing

Some important types of virtualizations in cloud computing are mentioned below:

Hardware virtualization

Operating system virtualization

Server virtualization

Storage virtualization

Hardware virtualization

In hardware virtualization, the hardware system is where the virtual machine management, or VMM, is placed. Hardware virtualization is enabled and VMM is installed as software on the hardware system. Here, the hypervisor's main function is to monitor and manage the hardware resources like memory, CPU, and other.

When hardware virtualization is allowed, a variety of operating systems (OS) may be loaded on it, and various applications can run on those OSs.

Operating system virtualization

In operating system virtualization, the VMM (virtual machine manager) or virtual machine software is installed on the host's operating system (OS) rather than hardware. The main use of operating system virtualization is for testing applications on different operating systems, ie. on a different OS platform.

Server virtualization

When a server is virtualized, the VMM (Virtual Machine Manager) or virtual machine software is placed directly on the server system, allowing it to be divided into a number of servers based on resource utilization utilizing load balancing. The server administrator divides a physical server into several servers to meet the demand for resources.

Storage virtualization

Grouping of physical storage from several servers (which are from various network devices/locations) happens in storage virtualization. After this is finished, it will appear to be a single storage device. The virtual storage system oversees their whole management. Using software programmes is another option

for implementation. The servers are unaware of the location of the data storage in cloud computing virtualization. Storage virtualization is mostly used to offer a backup and recovery method.

Advantages and benefits of virtualization in cloud computing

Security - Firewalls and encryption are used to offer virtualization security. This guarantees the preservation of everything in the virtualized cloud and the ability to stop any illegal access. Additionally, data can be safeguarded against file-related threats like malware, worms, and viruses, as well as cyberattacks.

More cost-effective - As we've seen, virtualization allows us to avoid paying for actual devices like servers and hardware. Also, it is ecologically beneficial because we need fewer servers and use less power. Every organization runs numerous OS because of this (operating system).

Facilitate Agile – By using cloud virtualization, we can create far more adaptable, agile work. Grid computing, which is accomplished through cloud virtualization, can be used to tackle scientific or more difficult technological challenges. Furthermore, it eliminates the requirement for data recovery from broken devices.

Promotes high availability and disaster recovery.

Data transmission is quick and versatile thanks to cloud virtualization, which eliminates the need for users to find storage or hard drives in order to transmit or retrieve data. Using cloud virtualization, it is possible nearly at any moment. Finding, transferring, and retrieving the data becomes quite simple.

Risk of system failure is minimized with cloud virtualization since data saved in the cloud is accessible at all times from a variety of devices, removing this risk. In the conventional scenario, there is a potential that the server might crash while an operation is in progress, which could eventually harm the organization's operational responsibilities. Moreover, clustering is always enabled with cloud virtualization, ensuring that even if one server fails, another is always available. (bg.education-wiki, n.d.)

Evaluation of moving the on-premises application to the cloud and its benefits.

Following the scenario from our assignment task, our company has an e-commerce website and related services, and we want you to evaluate the benefits of moving the on-premises application to the cloud.

There are several kinds of cloud services, such as:

1. The cloud service known as "Infrastructure as a Service" (IaaS) offers users infrastructure in the form of virtual computers, servers, networks, and data storage. Customers can now develop, configure, and administer their cloud infrastructure thanks to this.

2. PaaS, or platform as a service, is a cloud service that offers clients a whole platform for creating, testing, and developing applications. This covers equipment and services for creating software, managing databases, and using other infrastructure services.
3. A cloud-based service called Software as a Service (SaaS) offers ready-to-use software programmes including email, project management, customer relationship management, and more.

The benefits and drawbacks of moving an application to the cloud depend on the specific needs and requirements of the SME. Cost may be a key challenge for SMBs, but moving to the cloud can reduce operating costs for hardware and infrastructure maintenance.

Moving to IaaS can give maximum flexibility and control over the infrastructure, but may require more expertise and support from the SME. PaaS can give great flexibility in application development and management, but can be more restrictive in infrastructure control.

Which server infrastructure components are handled by the cloud service provider and who is in charge of maintaining these components are the distinctions between Infrastructure as a Service (IaaS) and other types of cloud services like Platform as a Service (PaaS) and Software as a Service (SaaS).

When a SME uses IaaS, the cloud service provider supplies the website's infrastructure (hardware, network resources, servers, etc.), but the SME is responsible for administering and maintaining all other facets of the server architecture. This indicates that the SME is totally free to install and administer all apps on the server as well as customise the server infrastructure. For SMEs, however, this independence comes at a high price because they need to have the resources and management skills to operate the infrastructure.

While using PaaS, the cloud service provider offers a platform for creating apps that includes a development tools, database administration, and other services required to run a SME's website. As a result, a SME may concentrate on creating apps without worrying about managing the infrastructure, but they are limited in how they can set up the server architecture. As a result of the greater amount of cloud services it offers compared to IaaS, PaaS may have higher expenses.

Infrastructure as a service model for our company.

We now assume that the company has chosen to move to an infrastructure-as-a-service model. In addition, we assume that we are also working on two large projects with multiple virtual machines which requires high availability. That is, there should be no data loss and services remain available 24/7 with minimal or no loss of service.

Care should be taken while selecting a cloud service provider if the business has decided to switch to an infrastructure-as-a-service (IaaS) model to guarantee high availability and little to no service interruption. The degree of availability is crucial while working on two major projects with several virtual machines, especially when it comes to an e-commerce website that must be accessible always.

An SME can employ several measures to guarantee high availability, including:

Resource allocation across availability zones: By adopting multi-region cloud services from vendors like Amazon Web Services (AWS), Google Cloud Platform, or Microsoft Azure, this is meant to imply that resources are assigned across virtual availability zones. By doing this, it will be guaranteed that even if there is an issue in one availability zone, it won't affect the other zones.

Making use of backups: SMBs may utilize automated data and application backup systems to make sure that, in the event of a problem, they can quickly and with the least amount of data loss.

While picking a cloud service provider, caution should be used if the business has decided to switch to an infrastructure-as-a-service (IaaS) model to guarantee high availability and little to no service interruption. The degree of availability is crucial while working on two big projects with several virtual machines, especially when it comes to an e-commerce website that must be accessible always.

Evaluation of moving an e-commerce website and associated web service of this on-premises application to the cloud.

We are tasked with evaluating the benefits of moving an e-commerce website and associated web service of this on-premises application to the cloud. We present two cases where we have:

1. Very high budget with no spending limit

2. Average budget

We can select the highest class of cloud services when we have a really large budget with no spending limitations. This involves maintaining a high degree of security and data protection, as well as using a cloud with a high level of availability and dependability. Our capacity to easily scale up or down resources in accordance with our demands is made possible by the high level of scalability and flexibility that these clouds normally provide.

The advantages of this strategy are as follows:

Let's weigh the advantages of migrating a web service associated with an e-commerce website and related website to the cloud for both cases. Advantages of migrating a high-budget, limitless e-commerce website and related web service to the cloud:

Scalability: Using the cloud allows you to scale up or down resources to meet business demand. To maintain a positive user experience, the website can now handle an increase in traffic during busy periods.

High Availability: Cloud service providers provide high availability and dependability via redundant servers, data centres, and networks, guaranteeing that the website is accessible to users around-the-clock and without interruption.

Flexibility: Cloud computing services offer a wide range of features and services that may be added or deleted as needed. As a result, the requirements of the e-commerce firm may be met with flexibility and adaptability.

Protection of sensitive client information is made possible by the strong security mechanisms provided by cloud providers, such as firewalls, intrusion detection, and data encryption.

Savings on expenses: Even while a large budget may make prices less of an issue, switching to the cloud may still save money by removing the need to buy and maintain hardware and by cutting down on energy expenditures.

The following are some advantages of migrating an e-commerce website and related web service to the cloud on a typical budget:

Scalability: Shifting to the cloud enables resources to be scaled up or down as needed, enabling the website to manage greater traffic during peak periods and providing a positive user experience without the need for significant hardware expenditures.

High Availability: By using redundant servers, data centres, and networks, cloud providers offer high availability and reliability, guaranteeing that the website is accessible to users around-the-clock and without interruption.

Savings: Switching to the cloud lowers up-front capital expenditures because there is no longer a need to buy and maintain hardware. Moreover, pay-as-you-go models, which let users only pay for what they use, are frequently employed by cloud services.

Flexibility: Cloud services provide a variety of features and services that may be added or deleted as needed. This makes it possible to adapt and customize the system to the requirements of the e-commerce firm.

Security: To secure sensitive client information, cloud providers offer a range of strong security features, including as firewalls, intrusion detection, and data encryption.

There are several advantages to migrating an e-commerce website and related web service to the cloud, including scalability, high availability, flexibility, cost savings, and security. Both a very high budget and an ordinary budget can profit from the transfer, however the amount of investment will define the breadth and scope of the migration.

Azure Concepts:

Locations: There are several places across the world where Azure data centres are situated. These zones are described as having their own power, networking, and cooling systems and being geographically distinct. There are one or more data centres in each region. To minimise latency, adhere to data residency regulations, and increase availability, the proper area must be chosen.

Availability Zones (AZs) are distinct physical areas inside an Azure region made up of one or more data centres outfitted with autonomous power, cooling, and networking. By dispersing them over several zones, AZs may give applications great availability and resilience.

Authentication and permission are two crucial ideas in cyber security.

Verifying a user's or application's identity is the process of authentication. To demonstrate the user's identity, credentials like a username and password must be presented. Users must submit two or more authentication factors when using the multi-factor authentication (MFA) security procedure to confirm their identity. This might be something the user owns, such as a smart card or token, something the user knows, like a password, or something the user is, such biometric information like a fingerprint.

The process of gaining access to resources or doing certain actions, on the other hand, depends on the identification of the user and the rights that have been granted to them. To reduce the risk of unauthorised access and potential data breaches, least-privilege permissions refer to giving users just the minimal amount of access required to carry out their responsibilities.

We may filter network traffic to and from Azure resources using Network Security Groups (NSGs), which are an Azure resource. Depending on the source and destination IP addresses, port, and protocol, NSGs may have rules that permit or prohibit traffic. Secure remote access gateways called bastions, also called jumpboxes, let authorised users connect to virtual computers and other resources inside a private network.

In conclusion, it's crucial to create network security groups and bastions to safeguard access to resources, as well as authentication and authorization technologies like MFA and least-privilege permissions.

Security considerations

Authorization and authentication are two important concepts in information security. Authentication refers to the process of verifying the identity of a user or system by validating their credentials such as a password, biometric identification, smart card, or token. Authorization, on the other hand, refers to the process of granting or denying access to specific resources or services based on the authenticated user's role or permissions.

A crucial security measure known as multi-factor authentication (MFA) requires the user to provide multiple authentication factors in order to access a system or application. This approach is more secure than using a single factor authentication method since it adds an additional layer of security that makes it difficult for attackers to impersonate the user. Applying the principle of least privilege permissions means granting users only the minimum permissions necessary to perform their job responsibilities. This principle minimizes the risk of malicious actors gaining access to sensitive resources or data.

Network security groups (NSGs) are an essential component of network security. They are used to define and enforce network traffic rules by filtering traffic based on the source and destination IP addresses,

protocols, and ports. NSGs can be used to control network traffic within a virtual network or between virtual networks.

Bastions are secure access points that provide a single-entry point into a network or system. They are often used to govern access to sensitive resources like as servers, databases, or other vital systems. Bastions can be used to enforce least privilege permissions and authenticate users.

REFERENCES

1. bg.education-wiki, n.d.
2. "Cloud Computing: Definition, Characteristics, and Service Models" by Ibraheem, Raed, and Abduallah Alwabel, published in the International Journal of Advanced Computer Science and Applications, Vol. 8, No. 2, 2017. DOI: 10.14569/IJACSA.2017.080230
3. Srinivasan, S., & Rodrigues, J. J. P. C. (2018). Cloud computing: An overview. In Handbook of Research on Big Data and the IoT (pp. 391-412). IGI Global.
4. Choudhury, S. R., & Hazarika, H. (2018). Cloud Computing for Small and Medium-Sized Enterprises: A Systematic Review. Journal of Cloud Computing: Advances, Systems and Applications, 7(1), 1-20. https://doi.org/10.1186/s13677-018-0101-1
5. Microsoft Azure. (2021). Top 10 benefits of cloud computing. Retrieved from https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/#benefits.

6. Azure Documentation: Resource Groups in Azure https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal
7. Microsoft Security: Authentication vs Authorization https://www.microsoft.com/security/blog/2019/10/02/authentication-vs-authorization-whats-the-difference/
8. Azure Documentation: Network Security Groups in Azure https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview
9. Azure Documentation: Azure Bastion https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
10. [1] Rouse, M. (2018). Authentication. TechTarget. Retrieved from https://searchsecurity.techtarget.com/definition/authentication
11. [2] Rouse, M. (2018). Authorization. TechTarget. Retrieved from https://searchsecurity.techtarget.com/definition/authorization
12. [3] Microsoft. (2022). Best practices for multi-factor authentication. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-best-practices