**Control questions – session 8**

1. **What is nested virtualization? Describe specific areas and places it is being used in Cloud.**

Nested virtualization allows the user to run a VM instances inside of other VMs , this helps you to create users own virtualization environments .

in cloud it can be used for moving on premise workloads to the cloud without any need for import and convert VM images. Nested Virtualization can also be used in cases where the user can’t run VMs on their Compute Engine. The user can’t run an on premise workload on their VMs that fails over to Compute Engine VMs. Nested virtualization can be useful here and ports the VMs to Compute Engine. Nested Virtualization can be used for critical workloads like the public cloud.

You can also run tests on the nested VM , like for example run tests on the VM that is harmful to for the physical hardware.

1. **What is the difference between hypervisor type 1 and type 2? What kind of virtualization do you know?**

Hypervisors is a software that allows a computer to run multiple VMs by virtually sharing its resources. Their job is to ensure that the VMs doesn’t interfere with each other and ensures that each VM has access to physical resources.

There are to types of hypervisors type 1 and type 2

**Type 1** (bare – metal): communicates with the underlying resources. Type 1 runs on the hosts hardware to manage the guest OS and control the hardware. They act like lightweight OS and is used for running VMs. Examples of hypervisors 1 are Microsoft Hypervisor V and VMware ESX and Oracle Vm

**Type 2** unlike type 1 runs as an application on an existing OS and installed on the top of the OS. it runs as an application to enable virtualization. Type 2 must use the host OS to access and manage the underlying resources since they carry a performance overhead. Examples of hypervisors are VMware Workstation VMware Player and VirtualBox.

**The main** difference between hypervisor Type 1 and Type 2 is that type 1 acts like a lightweight OS and runs on directly on the hosts hardware for managing guest OSs and controlling the physical hardware. While type 2 is runs as an application on the top of the OS like other computer programs.

**3. Present your understanding of CDN, SDN and NAS. How can one use this technologies to mitigate the Denial of Service attacks?**

CDN (Content Delivery Networks) is a geographically group of servers that is linked together in a network to provide fast delivery of internet content securely as possible. Data centers all over the world stores file copies which allows a user to access internet content from internet supporting devices like the phone or computer faster through a proxy server near your location. This allows users to do things on the internet like online shopping, streaming movies or playing games without worrying about the content to have a slow loading process. **CDN also provides protection on the websites against attacks like DDOS. If your website is the being attack by a DDOS attack, the CDN ensures that the webserver is unavailable, and if the website get more traffic than usual the CDN will send this traffic to other servers to help the site from crashing or from being unavailable.**

SDN (Software Defined Network) technology is when networks programmed or controlled by SDN controllers or by software applications. This makes the networking a lot easier by enabling simpler control systems to make managing network operations and functions better. The SDN made networks more flexible and easier to manage. SDN helps to communicate between the physical hardware and network traffic using APIs and controllers that run on the software. It controls the network using the centralized servers. SDN is dynamic, manageable, and cost effective and it is used in dynamic applications. The SDN separates the data plane from the control plane in the routers and switches in the network. Traditional network is hardware based while SDN is software based, this allows the users to administrate the network using SDN and shape their own traffic, change the network rules, increase network speed and block packets from accessing the network. this is more efficient and flexible traffic control.

**If the DDOS attack is detected on the network the Control plane has a module which collects the traffic through the network, this is sent to the DDOS detection module. This module detects DDOS attacks if the network, if the network is being attacked the mitigation module is informed and takes action against the DDOS from harming the network and blocks the suspicious host. The user can also add dynamic policies in the network to block users or traffic, this helps to mitigate attacks such as DDOS or further traffic.**

**NAS**

NAS (Network Attached Storage) is a server used to for storing files and sharing. NAS is hard drive connected to a network instead of a computer used for data storage and file sharing requests, and NAS provide fast and secure services to private networks. NAS devices include a processor and OS so it runs apps and the provides the content needed for files to be easily shared by authorized people. Example of a NAS device is a file server, if the user is writing the file it’s not saved locally but instead stored in the NAS file server. if a file server of the network doesn’t have enough for storage, one can connect a NAS device to the network to increase the storage space. NAS devices provide faster data accessibility, and it has TBs of storage.

**Users can enable DDOS protection in settings on their devices, this helps them to mitigate DDOS attacks. Another thing that can be done is to update the Device firmware to path the device and fix the vulnerabilities when they are detected. Enable authentication on their databases and enable file system security on their devices is an option too for mitigating attacks**

**This reduced the risk for DDOS attacks. It is also important to use encrypted connection to the NAS and the network**

1. **Describe SPI models used in Cloud. In which of the models, one can make edits in Apache and Ngingx web server? What is the model that does not require from user to adjust anything cybersecurity-wise, except access control and publishing the data?**

**There are three types of SPI models**

**SAAS software as a service :** is a full application that is managed and hosted by its provider ( the provider has the responsible for the application , physical server databases , os , virtualization , Network and storage , data center ) , but the consumer can access the SAAS application with a webbrowser (ex: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot)

The SAAS – is when the consumer gets a finished ready to use application (mostly saas applications are built on IAAS and PAAS platforms.

In SAAS the provider hosts and manages the application , the user or consumer has not so much responsibility. The only thing the user is responsible for is to secure their data on the application and control the access yourself. The users are responsible for securing the login credentials so it doesn’t get stolen in phishing or social engineering attacks.

The provider is almost responsible for securing every perspective of the underlying infrastructure to the application

**Platform as A service :PAAS** is gives and provides developed or application platforms (often built on top of an IAAS platform for reducing the need of system administrator) like databases, apps that supports Python,Java , Js , coding etc) . it also provides file storaging and collaboration applications and application processing apps and apps where the api has full access to SAAS apps) :

The difference here is that the consumer only manages the data and apps

1. and the user can’t manage the resources in the underlying server like with any infrastructure or even manage the network. While the provider has the responsibility of the physical server databases , os , virtualization , Network and storage , data center (Has responsibility for everything in cloud.**What are the main essential characteristics of the cloud computing?**

The main essentials of cloud computing in cloud computing is :

Resource pooling (the most fundamendal characterstic) , Consumers provision , broad network , rapid elasticity and Measured service (explain them to show your skills on the exam)

**Resource pooling** is when the provider gathers the resources and collects them into a pool, which can be assign to different consumers

**The Consumers** assignment is to provide resources from pool using on demand self service and manage the resources themselves. They don’t have to talk to the human administrator to take this action.

**Broad Networking Access** means that all resources is available on the network and there’s no need for physical access. The network itself isn’t a part of the service.

**Rapid elasticity** allows the consumer to expand or compress resources for pool to get scalable provision. This allows the consumer to match resource consumption with demand (ex. Add virtual services as demand increases and shutting them down after dropping.

**Measured service** is to ensure that consumers only use the resources they are allocated for and if not , they should be charged for it, the client only pays for what they use.

**2. Name three service models of the cloud and explain their differences, including the level of**

**responsibility fo cybersecurity between cloud user and cloud provider.**

The three service models are : Sofware as a service , Platform as a service , infrastructure as a service

**SAAS software as a service :** is a full application that is managed and hosted by its provider ( the provider has the responsible for the application , physical server databases , os , virtualization , Network and storage , data center ) , but the consumer can access the SAAS application with a webbrowser (ex: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot)

The SAAS – is when the consumer gets a finished ready to use application (mostly saas applications are built on IAAS and PAAS platforms.

In SAAS the provider hosts and manages the application , the user or consumer has not so much responsibility. The only thing the user is responsible for is to secure their data on the application and control the access yourself. The users are responsible for securing the login credentials so it doesn’t get stolen in phishing or social engineering attacks.

The provider is almost responsible for securing every perspective of the underlying infrastructure to the application

**Platform as A service :PAAS** is gives and provides developed or application plattforms platforms (often built on top of an IAAS platform for reducing the need of system administrator) like databases, apps that supports Python,Java , Js , etc coding) . it also provides file storaging and collaboration applications and application processing apps and apps where the api has full access to SAAS apps) :

The difference here is that the consumer only manage the data and apps

and app can’t manage the resources in the undelying server like with any infrastructure or even manage the network. While the provider has the responsibily of the physical server databases , os , virtualization , Network and storage , data center

Ex: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud , IntelliJ

In PAAS unlike the IAAS you have fewer security responsibilities , but instead you are responsible for control the access to the service and configure it. The provider is responsible for the application and the OS and it is also responsible for the security on the server like for example it ensures the users subscription and login creds is secure. The user is responsible for securing the data or any content on the platform.

**IAAS (Infrastructure As A Service)**

IAAS is when the consumer gets the opportunity to access a resource pool of fundamental computing infrastructure like compute, network or storage. In IAAS services like virtual machine, the consumer has more security responsibilities like patching the os system of your vm and securing their data. The provider is responsible for things like the storage and the services , disk , network

Responsibilities and accountibility:

****

**3. What the deployment models of the cloud that you know? What kind of deployment model will**

**you recommend for the following cases keeping in mind data privacy and cybersecurity:**

**(i) public air quality monitoring website, (ii) criminal police cases, (iii) county registry of the education projects in regional schools**

There are four types of deployment models: Public cloud, private cloud , community cloud and hybrid cloud.

1. **public air quality monitoring website**

For this case I would personally recommend using a public cloud. The reason why is because this is a public website which means it should be access by people in public. In public cloud the resource on the site is available for usage, such as storage and apps and so on is also available. The security on the website depends on which cloud provider the site use, for example Google and Azure provides different security mechanisms on their clouds. The website can use third part cloud services to secure the data on the website to secure private data (admin data etc) even though its public. Small organizations don’t have the resources for implementing a strong security on their servers. The security level on public cloud is great because every time a server is attacked the security gets better and in public cloud the consumer doesn’t need to patch their server it is done by the provider itself which helps to improve the security on the website

1. **criminal police cases**

in criminal police cases the data should be kept in private. This means that they should use a cloud that fulfill this requirement. The private cloud would be the best option for the police in this case. The reason why is that is in private cloud, the police is able to control their own cloud, like giving them access to resources. They have control of the underlying infrastructure which means that they can manage things on the cloud, and this helps them to keep their data private and access them through the firewall. It can also be hosted by a third part on prem or off prem. In private cloud the organization is responsible like the police for pathing the OS, upgrade etc to secure the cloud from malware attacks or unauthorized access. The private cloud helps the police to gain better control over the server, network, app security and data on the network. The network on the private cloud is limited which helps police to decide who can access their server which is helpful for improving the security on the server and minimize the risk of malware attacks on the server.

**(iii) county registry of the education projects in regional schools**

This is a special case, because we’re dealing with data that can be both private and public. It depends on the government, they can decide whether this registry should be publicly access or privately or both. If so, I would recommend using hybrid cloud. A hybrid cloud consists of a private and a public cloud (combination of two cloud environments). With this type of deployment model, the organization can decide if the data should be access in public or have private access. Like the when the project is set to begin can be access publicly, but sensitive data about the project like info about the study should be managed in the private cloud and can be only access by the organization users. This helps the government to easily handle their data and helps them to secure the sensitive data from being stolen or modified in transit. The security level in hybrid clouds is also great because of the private and the public cloud. The resources and data can be shared between the clouds, like if someone tries to attack their webserver, the data can be secured by transferring the data from public cloud to private (the data is encrypted).

**A public cloud is made to be available publicly or to industries , it’s operated by organizations who sell cloud servicesublic cloud to reduce the cost**

**Some of the computing can be done on the private cloud and the rest in p**

Public cloud:

Private cloud

Community cloud

Hybrid cloud

**gjør dette på søndag**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**4. Name main differences between virtual machines and containers.**

**A virtual machine (Vm)** is a collection of physical hardware that turns one servere into many servers. The machine uses the hypervisors which allows the computer to run multiple VMs. The disadvantages of VMs is that they include a full copy of the os which require the computer to have a lot of storage or space to run them (they can take up to tens of MBs each and even GBs). The other thing is that they are slow when booting them.

**Containers :** is a unit of software in the app layer that packeges code and its dependencies to help the application to run quickly and reliably from one computer. They can run on the same machine and share the OS kernel with other containers where is running as isolated processes in user space. Unlike the VMs the Containers take less space and take less MBs. The containers handle more apps and require fewer VMs and OS’s..

**The key** difference between Vms and containers is that the Vms vitualize an entire os (this includes the hardware as weel) which require a lot of space and this allows the computer to run multiple vms

While the containers only virtualize the software layers in the Os , this allows the computer to run multiple tasks or containers to run on a single OS , containers require less space than Vm to run.

The containers are similar to Vm unlike the vm which virtualize the entire machine, the container only virtualize above the operating system level which is the software.

Ex: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud , IntelliJ

In PAAS unlike the IAAS you have fewer security responsibilities, but instead you are responsible for control the access to the service and configure it. The provider is responsible for the application and the OS and it is also responsible for the security on the server like for example it ensures the users subscription and login creds is secure. The user is responsible for securing the data or any content on the platform.

**IAAS (Infrastructure As A Service)**

IAAS is when the consumer gets the opportunity to access a resource pool of fundamental computing infrastructure like compute, network or storage. In IAAS services like virtual machine, the consumer has more security responsibilities like patching the os system of your vm and securing their data. The provider is responsible for things like the storage and the services , disk , network

1. **. In which of the models, one can make edits in Apache and Ngingx web server?**

One can make edits in Apache and nginx server using the PAAS model. Both Apache and Nginx acts like web application and that’s why they belong to the PAAS model. In this model the consumer has the permission to for example update , host and edit on the same environment. Which means that a user can modify in the Apache Server and Nginx server in PAAS to ensure the web application or server works as intended.

1. **What is the model that does not require from user to adjust anything cybersecurity-wise, except access control and publishing the data?**

The SAAS model doesn’t require to adjust anything because the provider is responsible for managing and hosting the application and SAAS doesn’t require the user to adjust anything. The user doesn’t have much responsibility here and the only thing they’re responsible for is ensuring the access of the control so no one except the user has access to the application. They’re also responsible for securing the data on the web application whether they have published it or even if its already there.