Cloud

Well, cloud computing is defined as a way of offering on-demand services that extend the traditional capabilities of a computer or a network, out into the Internet.

For cloud computing to gain its intended cost savings and efficiencies, though, it relies heavily on the concept of virtualization.
By using virtualization, numerous logical servers can be placed on a single physical server. This, in turn, can help us reduce the amount of physical space, power, and cooling that's needed inside your data center.
Additionally, by using virtualization, we can achieve higher levels of availability by spinning up additional virtual servers, when necessary.

Most of the same security issues that we have with physical servers also get carried over into the cloud computing environment, too.
Many cloud service providers, though, have taken virtualization a step further with the concept of hyper-converged infrastructure. This allows providers to fully integrate the storage, network, and servers without having to perform hardware changes. Instead, they rely on a software and virtualization technology to perform all of the needed integrations.

Many cloud providers are also offering Virtual Desktop Infrastructure as one of their services. VDI allows a cloud provider to offer a full desktop operating system to an end user from a centralized server.

Now, when we look at these numerous logical servers being stored on a single physical server, we also have to consider that there has to be a way to keep the data confidential and separated from the other logical servers, too.

To do this, we use

1. Secure Enclaves
2. Secure Volumes

Secure Enclaves utilize two distinct areas that the data may be stored and accessed from. Each enclave can be accessed by the proper processor. This is a technique that's used by Microsoft Azure and many other cloud service providers.

Secure volumes, on the other hand, are a method of keeping data at rest, secure from prying eyes. When data on the volume is needed, a secure volume is mounted and it's properly decrypted to allow that access.

Cloud Types

For the Security+ exam, you should know that there are four different cloud types.

1. Public
2. private
3. hybrid
4. community

Public

The most common type of cloud architecture is the public cloud. Under this model, a service provider makes resources available to the end user over the Internet. There are numerous public cloud solutions available today, including those from Google, Microsoft, and Amazon. For example, Google Drive is a public cloud service that's offered both as a free and pay-for-use model.

Private

This service requires that a company create its own cloud environment that only it can utilize as an internal enterprise resource to manage its cloud. With a private cloud, your organization is responsible for the design, implementation and operation of the cloud resources, and the servers that host them. For example, the United States Government runs a private cloud for use by different organizations within the government. But my company and yours can't get access to it, like we could with Google Drive. Generally, a private cloud is chosen when security is more important to the organization than cost.

Hybrid

A hybrid cloud solution combines the benefits of both the public cloud and the private cloud options. Under this architecture, some resources are developed and operated by the organization itself like a private cloud would be, but the organization can also utilize the publicly-available resources or outsource services to another service provider like a public cloud does! Because of this mixture of private and public cloud

resources, strict rules should be applied for what type of data is hosted in each portion of this hybrid cloud.

Community

Under this model, the resources and cost are shared among several different organizations who have a common service need. This is similar to taking several private clouds and connecting them together. Now, the security challenge here is that each organization may have their own security controls. Remember, if you connect your network to another network, you inherit their security risks, as well. This doesn't change just because we've moved to the cloud environment.

Cloud Service Types

The four types you need to be aware of are

1. Software as a Service
2. Infrastructure as a Service
3. Platform as a Service
4. Security as a Service

SaaS

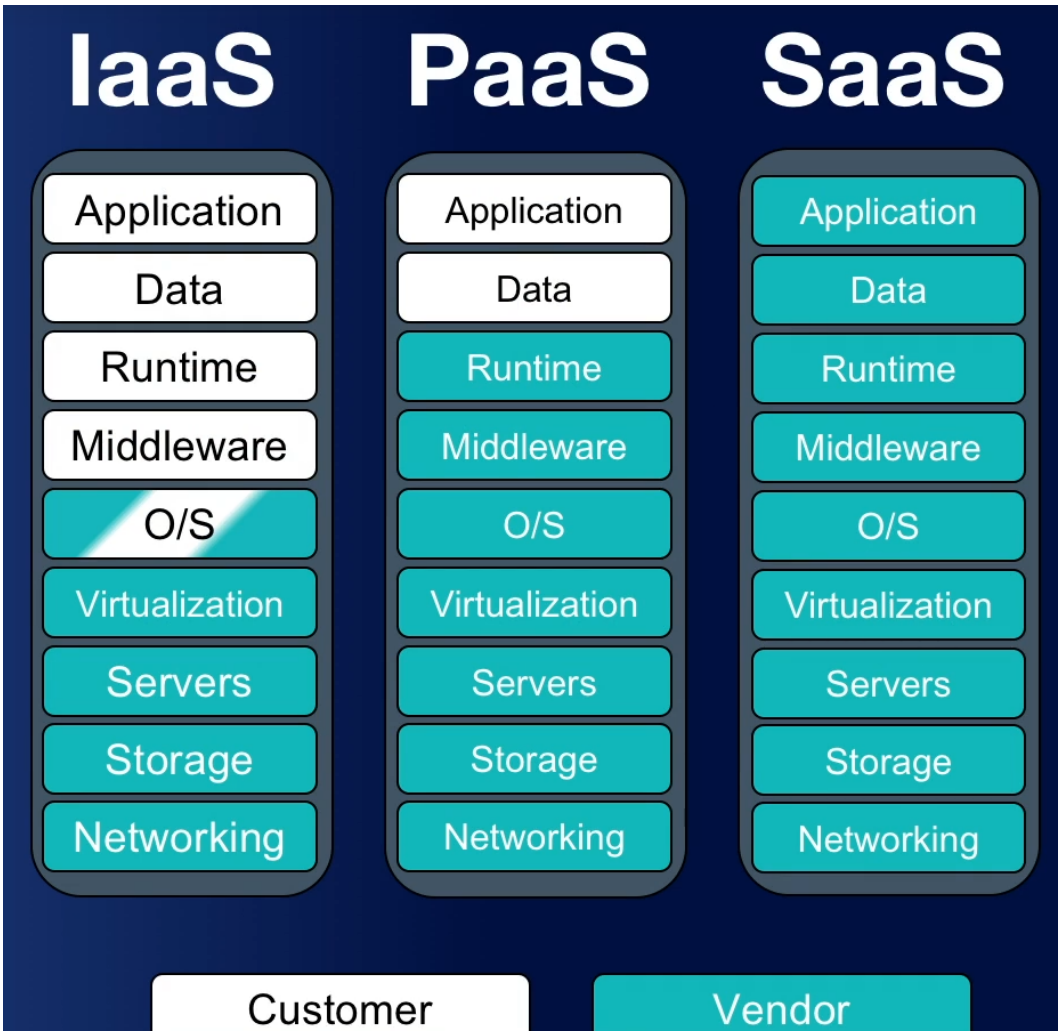
With Software as a Service, you're going to be provided with a complete solution. This includes the hardware, the operating system, the software, the applications, everything that's needed for that service to be delivered. For example, if you use Office 365 for Microsoft, this is considered Software as a Service, and it allows your end users to access their email, their Word documents, their PowerPoint presentations, and all of that directly from within their web browser.

IaaS

In this case, you might only need the service provider to give you the hardware, the operating system, and the backend server software. With Infrastructure as a Service, you get the benefit of this dynamic allocation of additional resources known as elasticity, but you don't have to deal with the headache of long-term commitments and contracts, buying the hardware, and installing the underlying operating systems.

PaaS

The third type of service is called Platform as a Service. Under this model, the third party vendor will provide your organization with all the hardware and software needed for a specific service to operate. For example, if your company is developing a new piece of software, they might have a development platform that's provided by a third-party cloud provider. This might be an example of Platform as a Service.



SECaaS

The fourth one is Security as a Service. This allows smaller organizations that don't have the necessary security skills to essentially outsource them to some larger company. This can provide them with a lower cost than trying to hire a team of cybersecurity professionals to work directly for your organization. It can give your company an immediate security expertise, and you can outsource common tasks

and provide the organization's information technology staff with a simple interface that they can use.

Sandbox

Another security technique that can be provided by cloud services is the use of sandboxing. Sandboxing utilizes separate virtual networks to allow security professionals to test suspicious or malicious files. For example, if your organization is conducting an incident response, your responders could place a piece of malware in a cloud-hosted sandboxed environment to see the effects of the malware as it's run in real time. This will allow them to do a dynamic analysis of it.

Defending Servers

File Servers

First, we have file servers. File servers are used to store, transfer, migrate, synchronize, and archive your files.

Email Server

These servers are a frequent target of attacks because they contain a lot of valuable data from within your organization. In a Windows environment, the most common email server is Microsoft Exchange. Microsoft Exchange and its Unix and Linux counterparts all support the POP3 IMAP and SMTP protocols for receiving and sending email.

Web Server

Next, we have a web server. In the Windows environment, this is usually hosted by Internet Information Services or IIS server. For Linux or Mac, this is usually going to be an Apache web server. Either way, web servers are, by default, open to the Internet to perform their job. So, it's important for us to properly secure them. They should always be placed in your organization's DMZ. They should be properly firewalled, monitored, logged, audited, and patched to ensure their security.

FTP Server

An FTP server is a specialized type of file server that's used to host files for distribution across the web. These servers can be set up to allow anonymous login and receipt of files or they can be secured with a username, password, or other credentials.

Domain Controller

The final type of server we're going to discuss in this lesson is called a domain controller. For a Windows environment, this is known as Active Directory.
In a Linux environment, you're likely going to use an LDAP server, instead. Either way, this server acts as the central repository of all of your user accounts, your computer accounts, and their associated passwords for the network. Because of this, hackers often target the Active Directory server as a method of privilege escalation, or at the very least, lateral movement, by gaining another administrator or user's account credentials and exploiting the server.

Cloud Infrastructure

VPC

Just like you can use your virtual private networks to connect your home users back to your corporate network and give them those protections underneath that corporate umbrella, virtual private clouds can be configured as a private network segment made available to single cloud consumers within a public cloud.
This is a way that we give security. VPC is considered an infrastructure as a service product, so if you're using something like AWS, they have a virtual private cloud service. If you're using Azure, they have their virtual private cloud service.

When we talk about a virtual private cloud, a virtual private cloud is typically going to be used to provision Internet-accessible customer-facing applications or corporate applications that need to be accessed from geographically remote sites. If you're thinking of something that might be a good place inside a DMZ, a virtual private cloud might be a good place to put it, as well.

Cloud vs On-Premise

Well, when you deal with the cloud, you're putting it in somebody else's data center. You're putting it someplace where you're just seeing it as a virtual instance somewhere on the Internet. You don't actually get to go touch that thing. You don't know if it's in Virginia or London or Washington or even care a lot of times because you just care that you have access to it and that's the benefit of having the cloud. It's everywhere you want to be.

Now, when you deal with on-premise, this means it's something in your own data center. You can walk down the hall and you can touch those servers. A lot of the places I've worked over the years, we've run our own data centers. Nowadays, we're starting to use more and more cloud resources, but for the last 20 years, I spent a lot of time in a lot of organizations spending tons and tons of money, millions and millions and millions of dollars, building out data centers and running our own servers.

Cloud access security broker

What is a cloud access security broker, also known as a CASB? Well, this is an enterprise management software designed to mediate access to cloud services by users across all types of devices. Essentially, it's going to be a middle man that helps you with your authentication and ensure that people are using the services they're supposed to use. Now, there are many different vendors who sell this type of product.
They include people like Symantec, which uses the Blue Coat Proxy, which I've personally used in a lot of my organizations.
There's Skyhigh Networks which is made by McAfee, there's Forcepoint, there's Microsoft's Cloud App Security, which is their version.
And Cisco has their version called Cloudlock.

Now, when you talk about a cloud access service broker, I want you to remember they provide visibility into how your clients and other network nodes are using your cloud services. When you start moving everything out to the cloud, you have to think about how my users are using those things? How much time are they spending? Are they using it the right way? Are they taking data and putting it where it shouldn't be? And to do that, we have three different things. We can set it up as either a forward proxy, a reverse proxy, or using API access.

API

When we talk about an API, this is an application programming interface. It's a library of programming utilities that are used to enable software developers to access functions of another application. And this is one of the key things we use when we start talking about piecing things together by using things that are service-oriented in their architecture. Now, when we deal with an API, this is going to allow for the automated administration, management, and monitoring of cloud services, as well as lots of other applications.
Now these APIs are commonly going to use either REST or SOAP, the simple object access protocol as their frameworks. Now, when we talk about APIs, we think about these from the perspective of integration.

FAAS and Serverless

Well, it's a cloud service model that supports serverless software architecture by provisioning runtime containers in which code is executed in a particular programming language. Now, that's a really long way of saying we are going to be able to run things and make applications without actually having our own servers. Now, that sounds pretty cool, right?
Because, now, I don't know about you, but I've been a system administrator for a long time, about 20 years, and the idea of having to run all my own servers and be able to run my own patches and do the updates and do all the testing and do all that stuff, just to be able to run a simple integration program like the one I talked about between Freshdesk and Udemy to able to make tickets go back and forth, sounds like a lot of work.
And so, function as a service eliminates the need for me to do that. Instead, I can write the code in something like Python and then run it in this environment. Now, when we talk about serverless, you notice that keyword in this definition. Serverless is a software architecture that runs functions within virtualized runtime containers in a cloud rather than on dedicated server instances.

An Example

Netflix delivers over 10 billion hours of video to 125 million customers every quarter and they do this using serverless. They do this because they're able to serve that large of an audience by using a wide range of highly complex infrastructure that relies on AWS, specifically its serverless capability known as Lambda. Now, all of this is done using this AWS Lambda, which is a serverless environment. Essentially,

Amazon runs all of these underlying servers and Netflix doesn't have to worry about them at all. All Netflix needs to do is know that when they give them code that's written in Python or some other language, Lambda can run it and they don't care about what that looks like underneath that.

Cloud Threats

1. Insecure APIs
2. Improper key management
3. Improper logging and monitoring
4. Unprotected storage

Insecure APIs

Now, the first thing I want to give you is a word of warning here. When you're using an API, you should always use it over an encrypted channel. That means SSL or TLS using an HTTPS connection. If you don't do that, and you just use HTTP, you are asking for somebody to be able to get there and see what you're doing, be able to steal things like your authorization tokens, and then use that against you. This is a major issue, so you want to make sure you secure your APIs by having end-to-end encryption.

Improper key management

Now, this is a really important thing, because a lot of the things you're going to use your keys for are things like cryptography, authentication, and authorization. And so, these are the areas to help you secure your stuff. And if you're not having proper key management, you're going to have a very insecure API. Whenever you're using an API, you need to make sure you're using secure authentication and authorization, things like SAML and OAuth and OIDC, and you want to use those things to do your authentication and authorization before you access data. Another word of warning I have for you here, do not hardcode or embed your key in the source code.

Improper logging and monitoring

And one of the big problems is insufficient logging and monitoring of cloud services. Now, again, here's a word of warning. If you're dealing with a software as a service, many times, you're not going to have any ability to access log files or monitoring tools. For instance, think about Gmail. That is a software as a service tool. If you use

Gmail, can you go in there and look at your log files? Can you go in there and look at your audit logs? Can you go in there and look at your monitoring tools to see if the service is up and down? No, because that's Google's job, not your job. And so, this is a weak area for us if we start using a lot of software as a service inside of our companies. Now, remember, when you're dealing with logs, your logs have to be copied from these elastic workstations into some place for long term storage. For example, when we have a cloud service and we spin up a new virtual machine and we use it for a while because we have a higher demand, and then that demand is gone, if we're storing those logs on that machine and that machine now is deprovisioned, we just lost all the logs.

Unprotected storage

Now, there are lots of ways you can do storage inside the cloud, but most storage containers are going to be referred to as one of two things. They're either going to be called buckets or blobs. When you call them buckets, this is something that we use inside of AWS. When we talk about blobs, it's usually in Microsoft Azure. Either way, we're talking about cloud storage here. Essentially, when we have a file and we want to save it someplace, we have to put it in a container, and that container, a bucket or a blob, is going to be someplace that we store it. And that can be actually located in lots of different places. For instance, your container could be in the East Coast or the West Coast. It could be in a specific region or any region. But the big thing is you can't nest one container in another. Each container is going to host its own data objects, which are those files that we want to store on that system. Now, once you have that, you have to set up access control. And this is where my word of warning comes in. Access control to storage is administered through your container policies. It's also done through your IAM authorizations, and it's done through object ACLs. By combining these three things, you can get a good level of security.