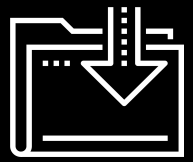
Introduction to Cloud Computing

Cybersecurity

Cloud Security Day 1



Class Objectives

By the end of today's class, you will be able to:

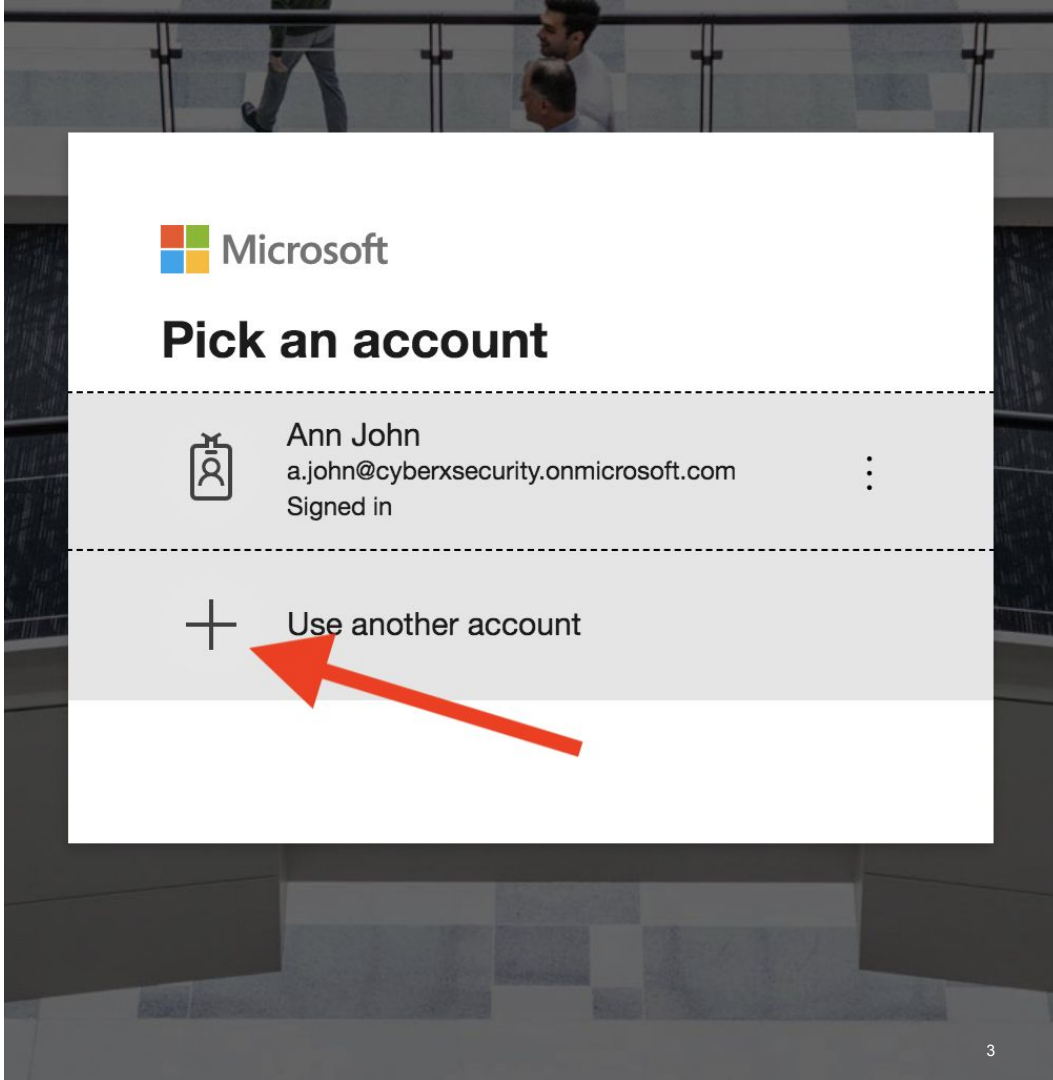
Distinguish between cloud services and identify an appropriate service depending on an organization's needs.

Set up a virtual private cloud network.

Protect the cloud network with a firewall.

Deploy a virtual computer to your a network.

Make sure you are signed in to your personal Azure account, not your cyberxsecurity account.



Introducing Cloud Computing

Today, we'll cover:

Overview of cloud service models and the variety of cloud services available to organizations.

Setting up a virtual cloud network that will run all of your systems during this unit.

Securing a cloud network with a firewall and creating firewall rules.

Virtual computing, creating web VMs in the cloud instance, and a jump box.

Introducing Cloud Computing

On-premises networks

Before the cloud, organizations set up networks on devices they owned and controlled. These setups are called on-premises networks, because they live on machines owned and operated on the company's physical property.

Cloud computing

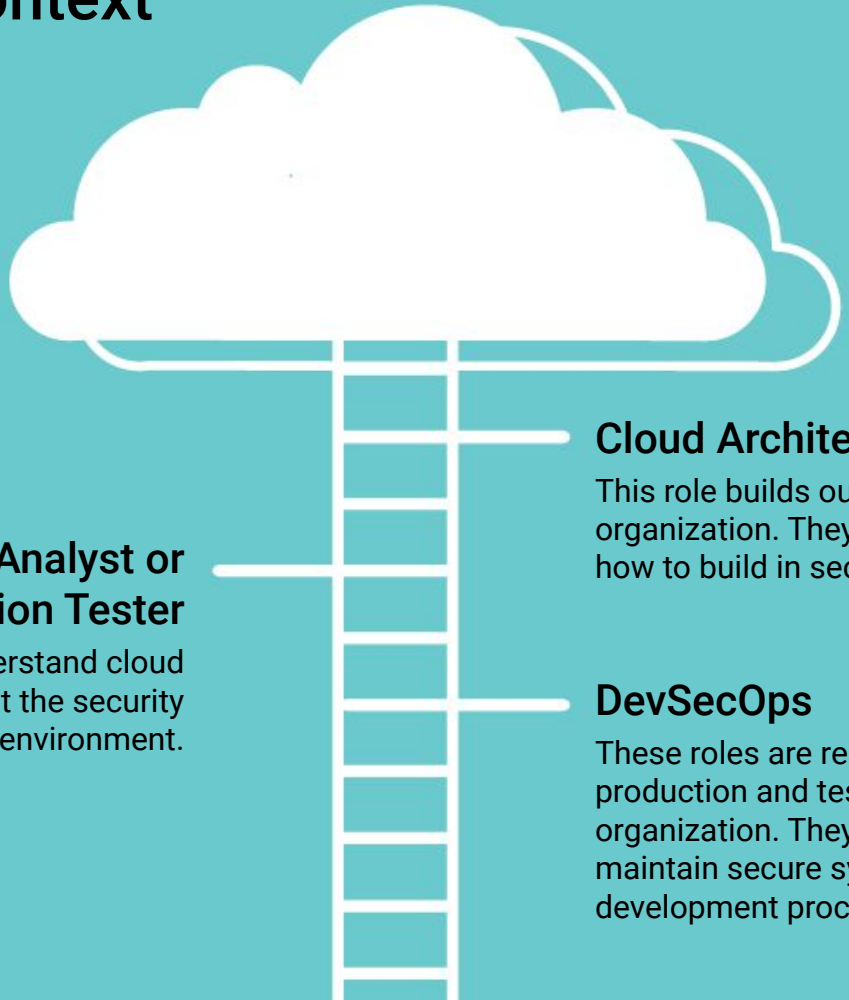
Today, the cloud and cloud services dominate the computing industry. Many organizations want to move operations to a cloud provider but are worried about security.

Complexities of the Cloud

The cloud introduces different security concerns from on-premises setups:

Complex architecture	• Systems must be built to ensure basic security and allow infrastructure personnel to securely monitor, reconfigure, and redeploy machines as needed. • Typically easier to do securely with on-premises machines. • Cloud deployments are remote; extra steps must be taken to ensure they are only exposed to the relevant parties.
Extensive management	• The cloud offers more flexibility than organizations are used to, giving them freedom to create many more machines. • This flexibility makes operations management more complex, requiring additional skills and techniques.
Different threats	• The cloud is exposed to public networks. • Providers handle certain aspects of security, which means security professionals have new and different considerations. • Malicious actors will execute new escalation and lateral movement tactics.
Ensuring availability	• High availability of machines is a large part of security on the cloud. • Ensuring availability and redundancy on the cloud is different than with on-premises environments.

Professional Context



Cloud Architect

This role builds out a cloud environment for an organization. They're expected to understand how to build in security from the ground up.

DevSecOps

These roles are responsible for maintaining production and testing environments for an organization. They're expected to build and maintain secure systems at every step of the development process.

Cloud Security Analyst or Cloud Penetration Tester

These roles must understand cloud architecture in order to test the security settings for a given environment.

Cloud Service Model

Think of the cloud in the same way you would think of an on-site data center or network.

The cloud has all of the same equipment: servers, virtual machines, routers, firewalls, load balancers, etc.

The difference is that, in the cloud, most of these items are virtualized, meaning they are software.

Cloud Service Model

The fact that cloud networks are virtualized and defined by software gives them numerous security benefits:

01 Ground-up security

02 Easy configuration

03 Quick turnaround

04 Personalized provisions from cloud providers

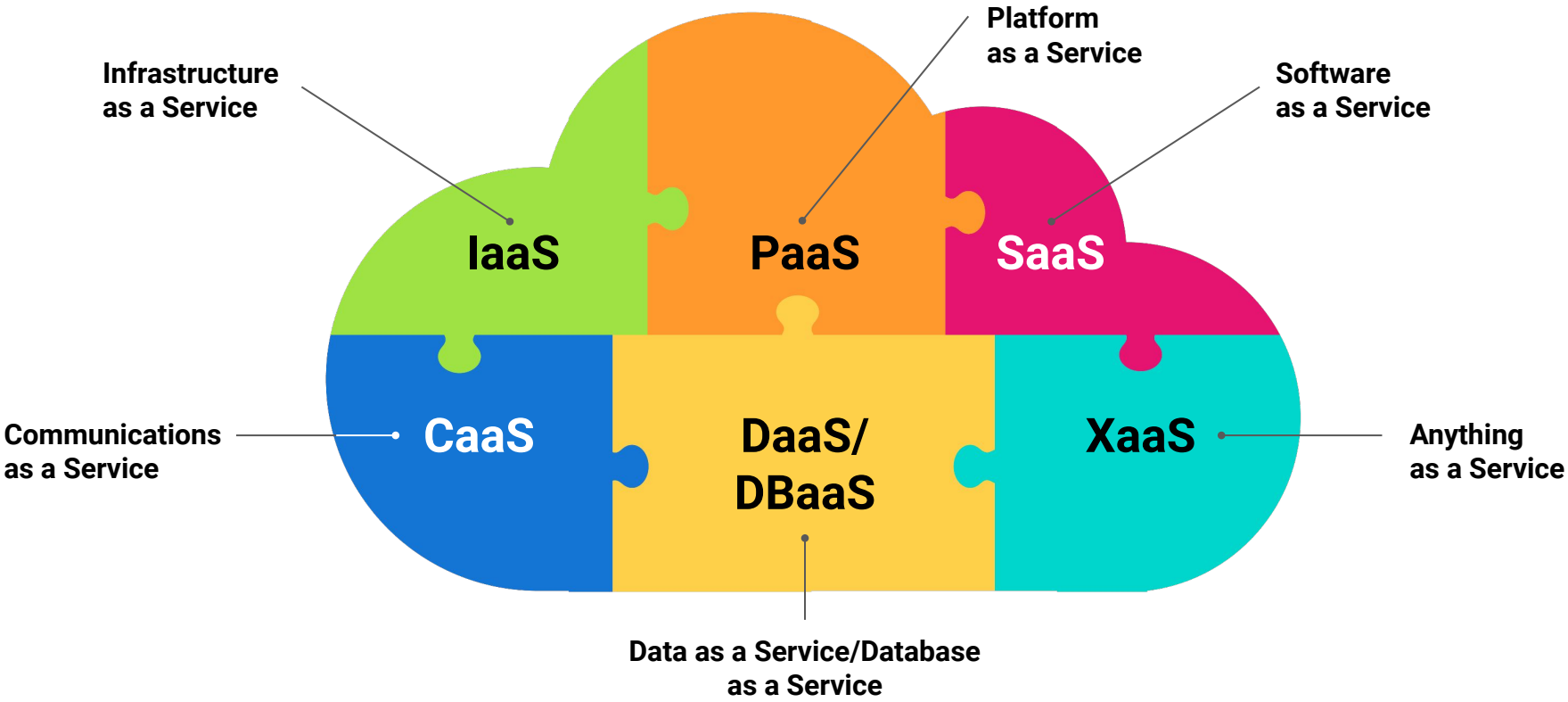
05 High availability and fault tolerance

06 Easy implementation

07 Affordability

Models of Cloud Services

All cloud services add the phrase “as a service” to the name of the service.



IaaS (Infrastructure as a Service)

A service provider offers pay-as-you-go access to storage, networking, servers, and other computing resources in the cloud.

IaaS (Infrastructure as a Service)

Security benefits include:

01 High availability.

02 Assurance that base machines are up-to-date at the time of deployment.

03 Provider-enforced security controls, such as basic access management.

Organizations can focus on implementing functionality and security relevant only to their business concerns, and not worry about the basics of secure deployments.

Google Cloud

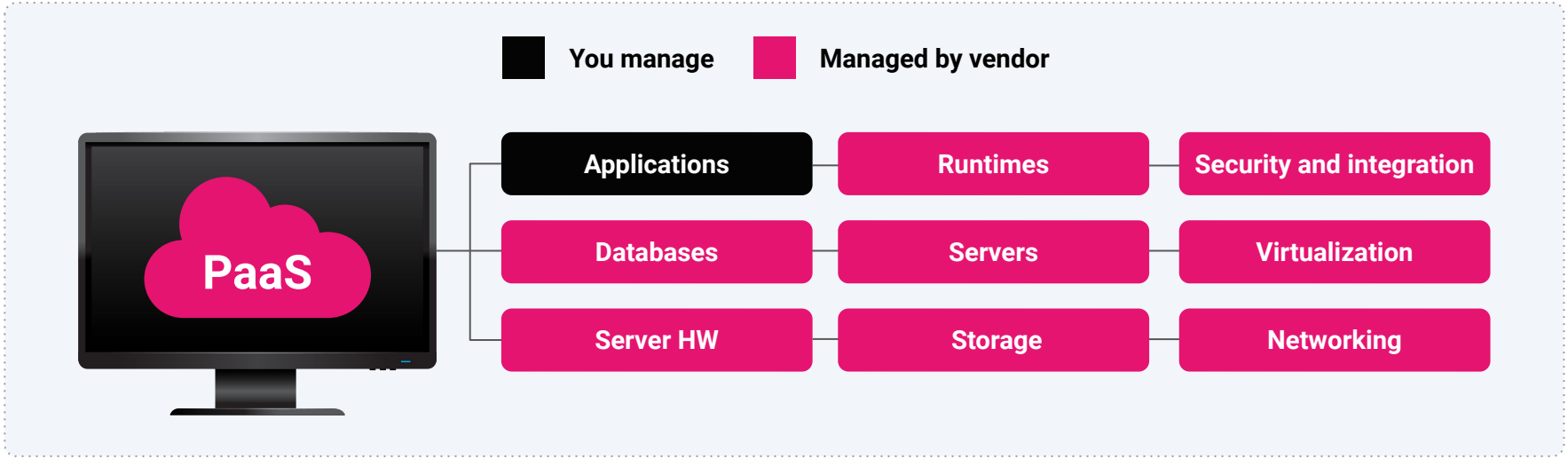
all offer **IaaS**

PaaS (Platform as a Service)

A service provider offers access to a cloud-based environment in which users can build and deliver applications.

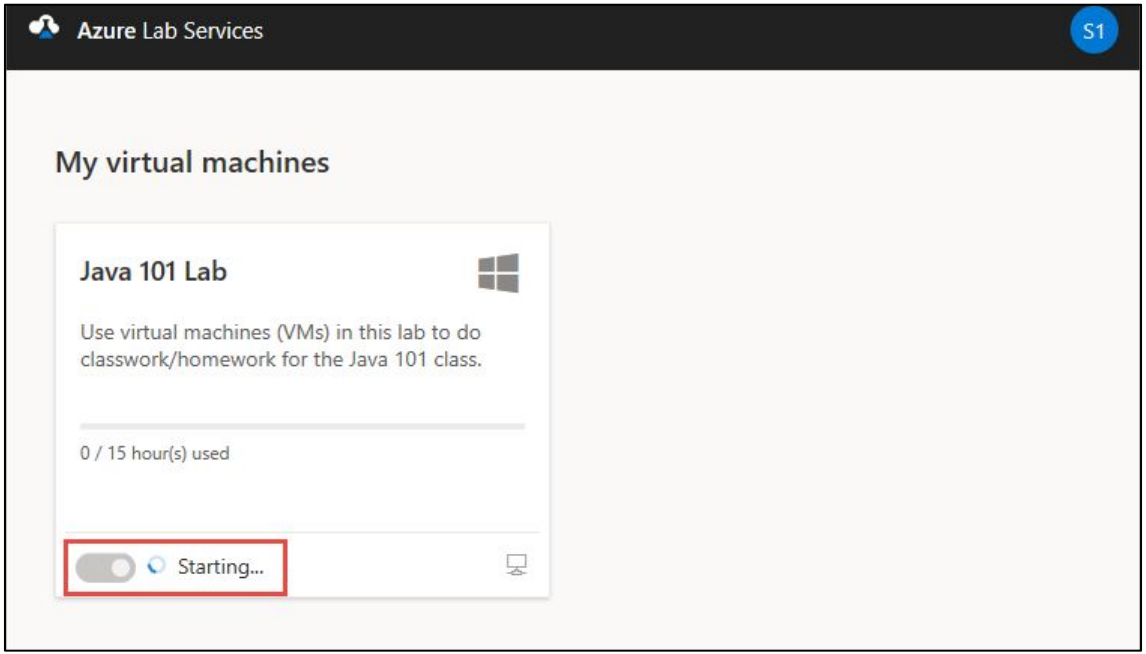
PaaS (Platform as a Service)

The provider supplies the underlying infrastructure.
Organizations can leverage powerful applications that are guaranteed to be secure and available, without having to implement security themselves.



PaaS (Platform as a Service)

Azure Classroom Labs, on top of which this course's lab environments are deployed, is one example. It guarantees availability and provides access only to the ports necessary to connect to the labs.



(Microsoft Azure)

SaaS (Software as a Service)

A service provider delivers software and applications through the internet.

SaaS (Software as a Service)

Users subscribe to the software and access it through the web or vendor APIs.

The software runs in environments that are guaranteed by the provider to be secure.

Engineers do not need to worry about secure deployment.

Cloud software such as the **Microsoft 365 Office Suite** and **Apple's iWork** are examples of SaaS.

DaaS/DBaaS (Data as a Service/ Database as a Service) A service that provides a company's data product to the user on demand, regardless of geographic or organizational distance between provider and consumer.

DaaS/DBaaS
(Data as a Service/Database as a Service)

The main security advantages of DaaS are high availability and fault tolerance.

DaaS ensures data is always available, even if there is a power outage at a single data center, and ensures that data is deployed as close as possible to those consuming it, reducing latency.

DaaS/DBaaS
(Data as a Service/Database as a Service)

An example of a DaaS is a marketing company that keep databases of consumers categorized for many different industries.

CaaS (Communications as a Service)

A service that provides an outsourced communications solution.

Such communications can include Voice over IP (VoIP or internet telephony), instant messaging (IM), and collaboration or video conference applications.

CaaS (Communications as a Service)

CaaS guarantees security by ensuring that communications are not vulnerable to eavesdropping, and provides comprehensive monitoring/record-keeping for auditing purposes.

(Zoom.us)

are all examples of **CaaS**

CSaaS (Cybersecurity as a Service)

A service that offers threat monitoring, detection, response, and mitigation, as delivered by specialized experts.

CSaaS provides end-to-end cybersecurity solutions for businesses, including threat monitoring, attack mitigation, and incident response.

CSaaS (Cybersecurity as a Service)

- Sophos Intercept X, McAfee MVISION Cloud, as well as Azure and AWS services are examples of CSaaS

CCaaS (Cybercrime as a Service)

This refers to the practice where individuals or groups can purchase cybercrime tools and services from underground markets to launch attacks without needing their own expertise or resources

CCaaS Cybercrime as a Service

RaaS - Ransomware as a Service

RaaS involves ransomware operators creating and renting out ransomware tools to affiliates, who then distribute and deploy these tools to attack victims. The profits from ransom payments are shared between the affiliates and the ransomware operators.

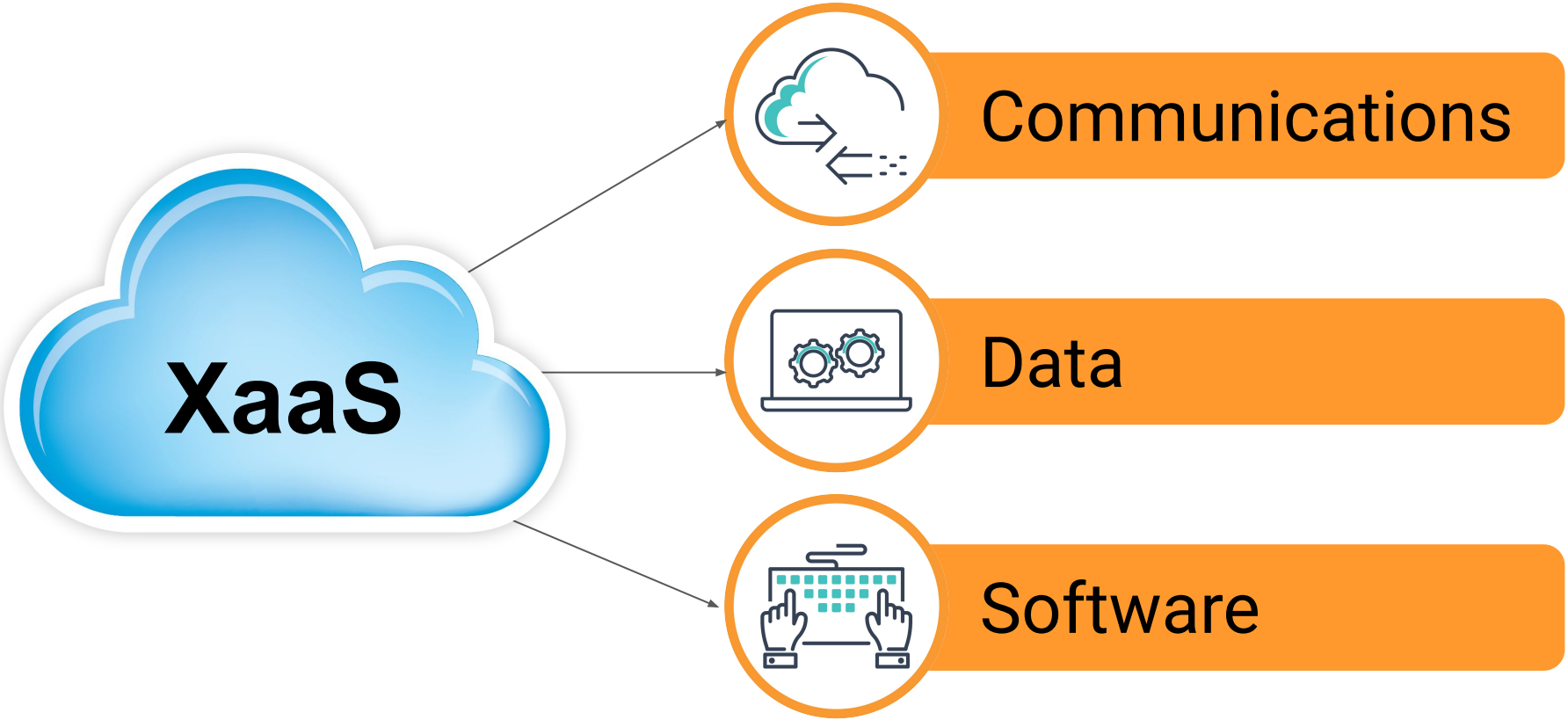
DDoS as a Service

DDoS as a Service DDoS as a Service allows individuals to hire attackers to launch Distributed Denial of Service (DDoS) attacks against targeted websites or online services. The goal is often to overwhelm the targets with a flood of internet traffic, making them inaccessible to users.

XaaS (Anything as a Service)

Services providing all the offerings via cloud computing as opposed to locally, or on-premises.

XaaS (Anything as a Service)



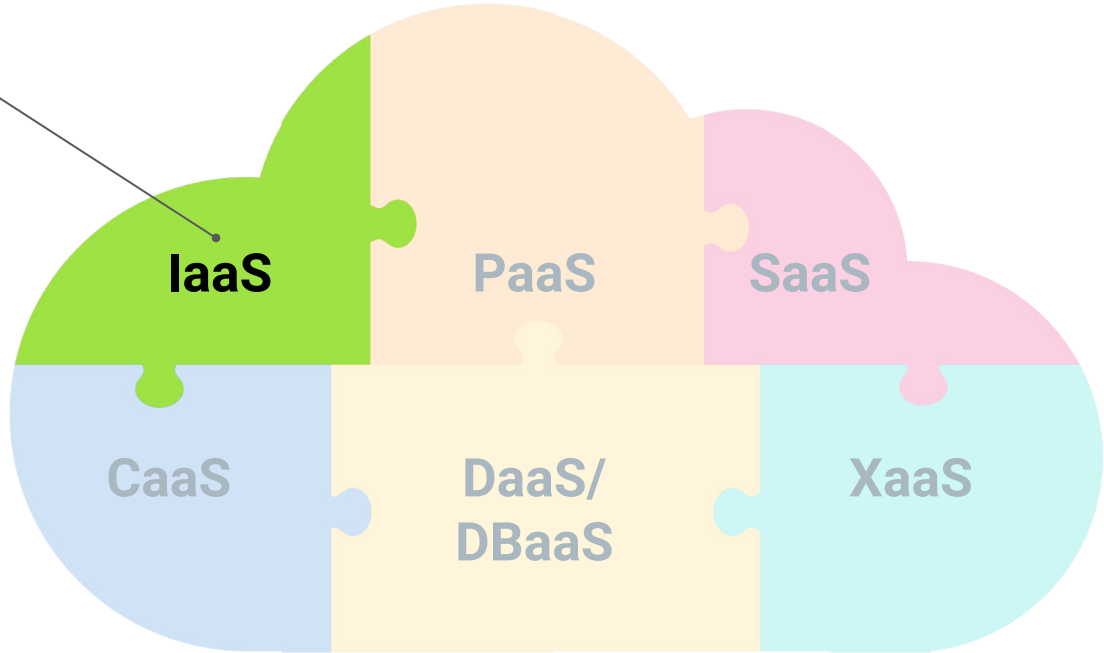
Virtual Networking

Virtual Networking

This week will focus on the **IaaS** offering from **Microsoft's Azure**.

IaaS is the most fundamental cloud service.

All other services are software-based and assume that the infrastructure is already set up.



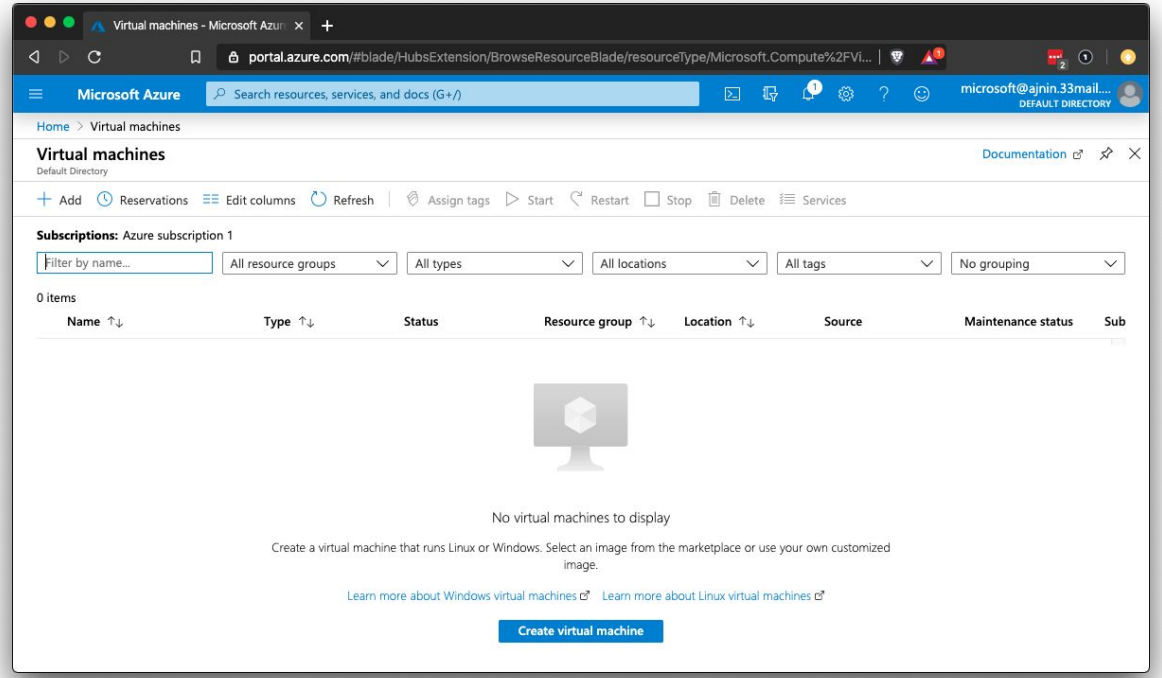
Selecting Available Regions

When selecting the resources for your cloud environment, you will need to select a region indicating where the resource geographically located.

- It is important to keep all resources in the same geographic region, as resources work together more efficiently when they are located physically close to each other.
- Ideally all geographic regions would always be available. However, that is not the case with cloud providers, including Microsoft Azure.
- Therefore, it is important to determine an available region before we create any cloud resources.

Available Region Follow-Along

In this walkthrough, students will follow along on their machines to determine the available region that they will use throughout the activities.



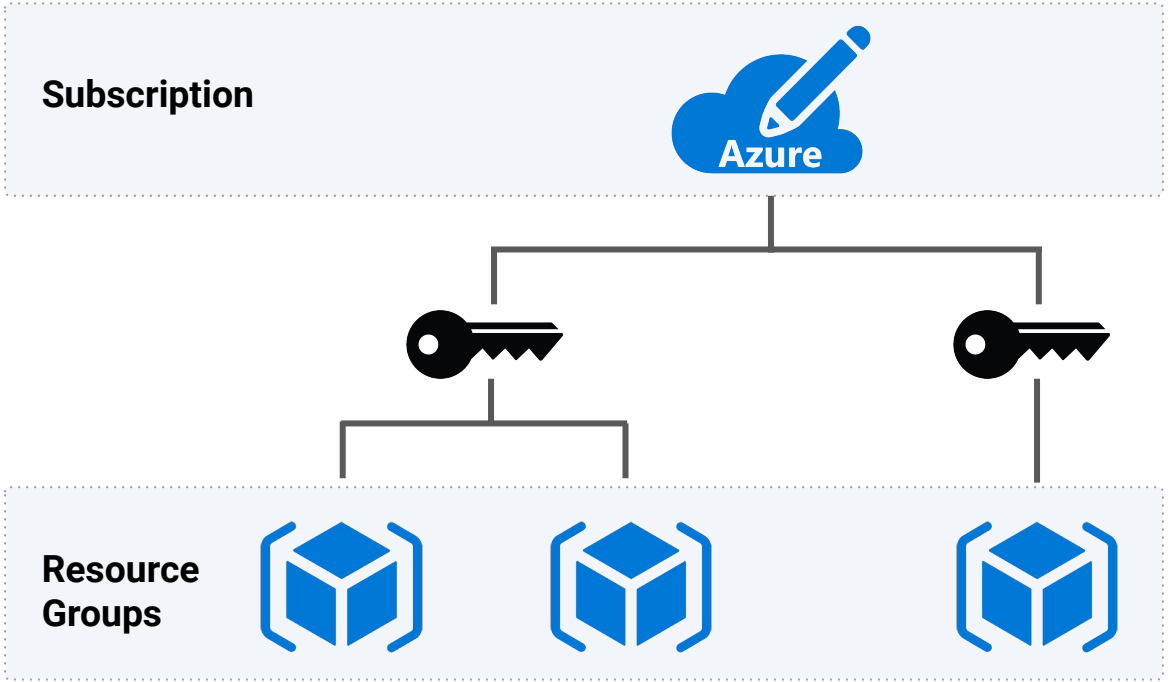
Instructor Demonstration

Availability Region
Follow Along on Your Machines!

Now that we have determined our region, we will begin creating a cloud infrastructure environment that we'll use for the rest of this unit.

Staying Organized: Resource Groups

In Azure, resource groups allow engineers to sort related resources into different groups, each of which can be easily located by name.

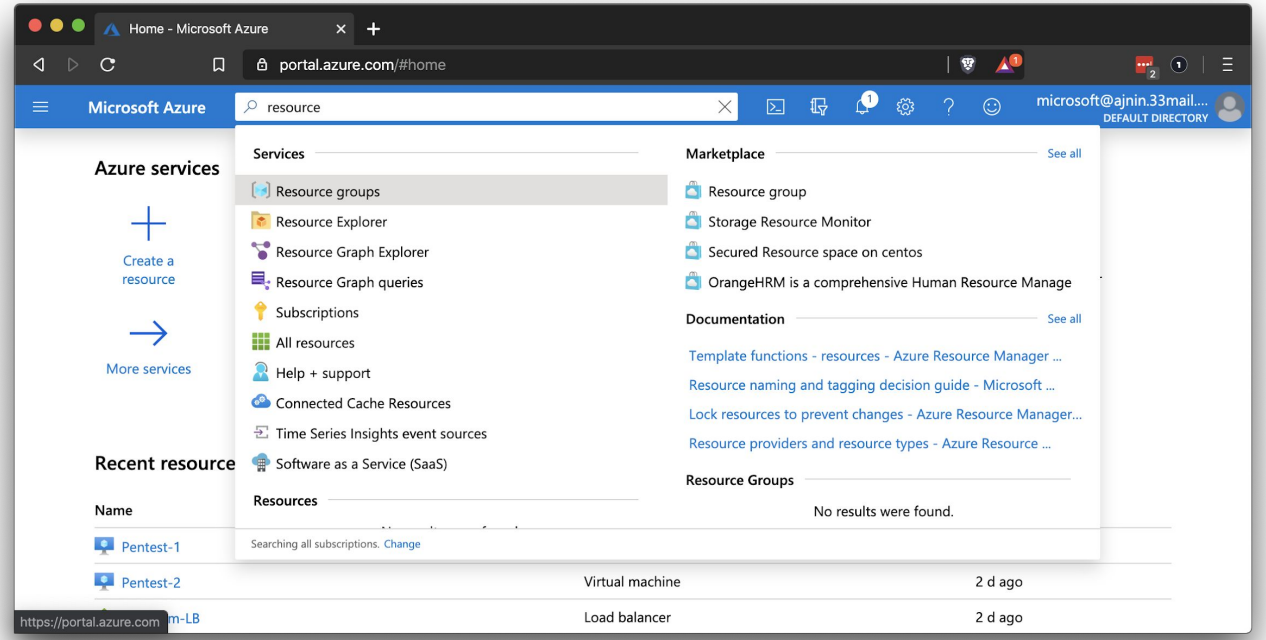


A resource group:

- Is a logical grouping of all resources used for a particular setup or project.
- Will contain the network, firewalls, virtual computers, and other resources needed for setup.

Creating Resource Groups

The first step to creating an environment in Azure is to create a resource group. We can then start adding other items, the first of which will be a virtual network.



Instructor Demonstration

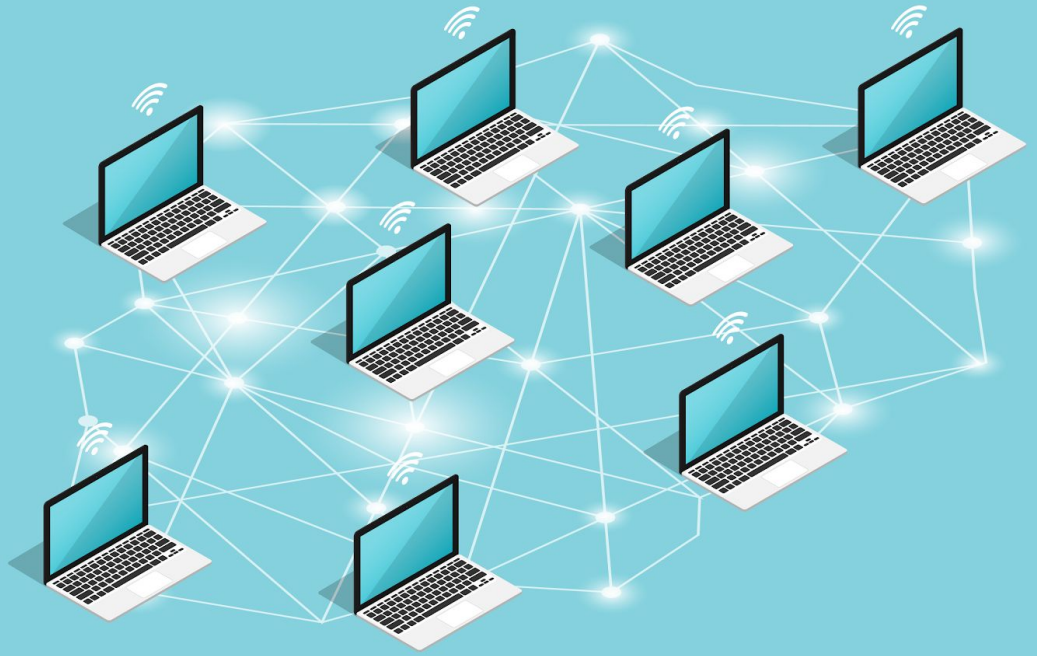
Setting Up Resource Groups

A **virtual network** is just what it sounds like: a collection of virtual machines that can communicate with each other.

Adding Virtual Networks

Unlike physical networks, where connections and discovery depend on physical wiring, virtual networks are much more flexible.

- VMs on a virtual network can live in different data centers but perform as if they are wired, and provide improved availability.
- Virtual networks can be quickly and easily reconfigured by clicking a few buttons in the portal.
- This is dramatically faster and safer than rewiring a physical network to implement improved segmentation. It also results in less human error.



Adding Virtual Networks

In order for virtual networks to behave identically to physical ones, cloud providers use software to emulate everything a physical machine uses to interact with the network, including:

vNICs (virtual network interface cards)	• Similar to physical machines, VMs have software versions of “normal” NICs. • Just like physical machines, VMs can have multiple vNICs.
IP addresses	• VMs have IP addresses, just like physical computers. • IP addresses are considered their own type of resource in Azure, AWS, and other cloud environments.
Subnets	• Like IP addresses, subnets are considered separate resources in the cloud, meaning they can be created independently of other resources. • After creating a virtual network, we can create a new virtual subnet and add it to the existing network. • We can also create a new public IP address resource and associate it with an existing virtual machine.

Let’s review the IP structures that we learned earlier in the course.

Quick Review: IP Address Structures

Private networks will use one of three IP schemes:

```
192.168.x.x
```

```
172.16.x.x
```

```
10.x.x.x
```

We can also use CIDR notation when defining a network space:

```
192.168.1.0/24
```

When creating a network in Azure, we will define a large network as well as a subnet inside that network:

```
10.0.0.0/16
```

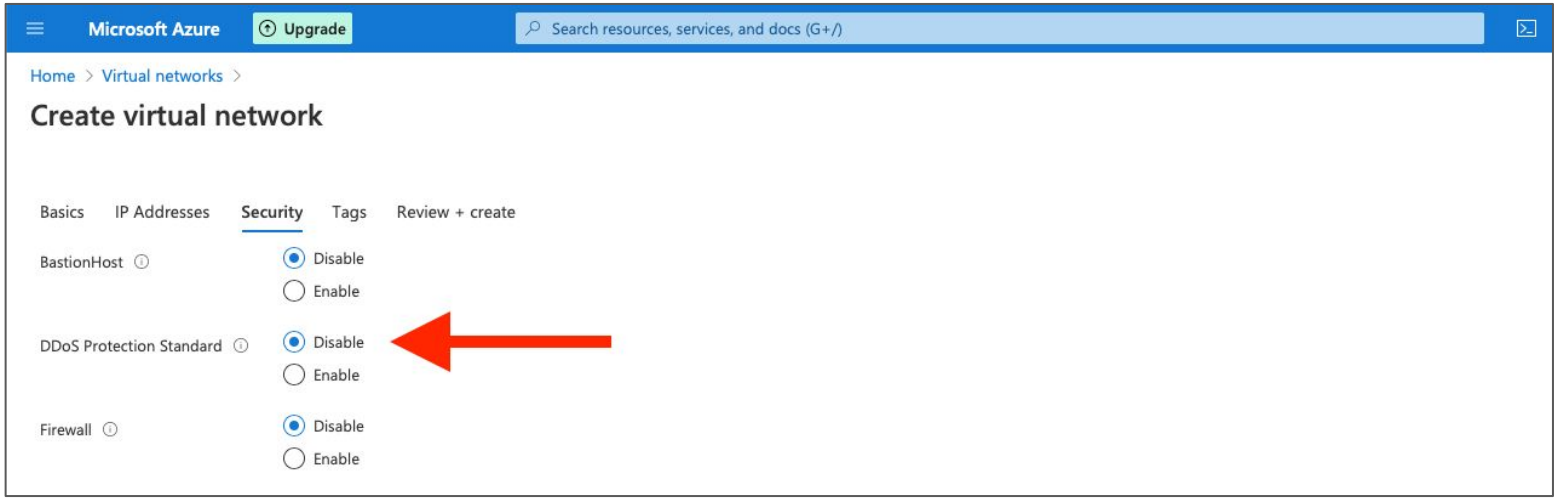
For the large network:

```
10.0.1.0/24
```

For the first subnet.

Creating Resource Groups

As you set up your virtual network, avoid recurring charges by making sure DDoS Protection Standard is **not** enabled.



In a real application, we would enable this in order to configure DDoS protection. When enabled, Azure provides near real-time monitoring for DDoS traffic.

In class, avoid using this feature so that you do not incur additional charges of up to $3,000!

Activity: Virtual Networking

In this activity, you will create a resource group and virtual network for a Red Team training environment.

Important:
For this and all activities, make sure that you are using your personal Azure account.

Suggested Time:

20 Minutes

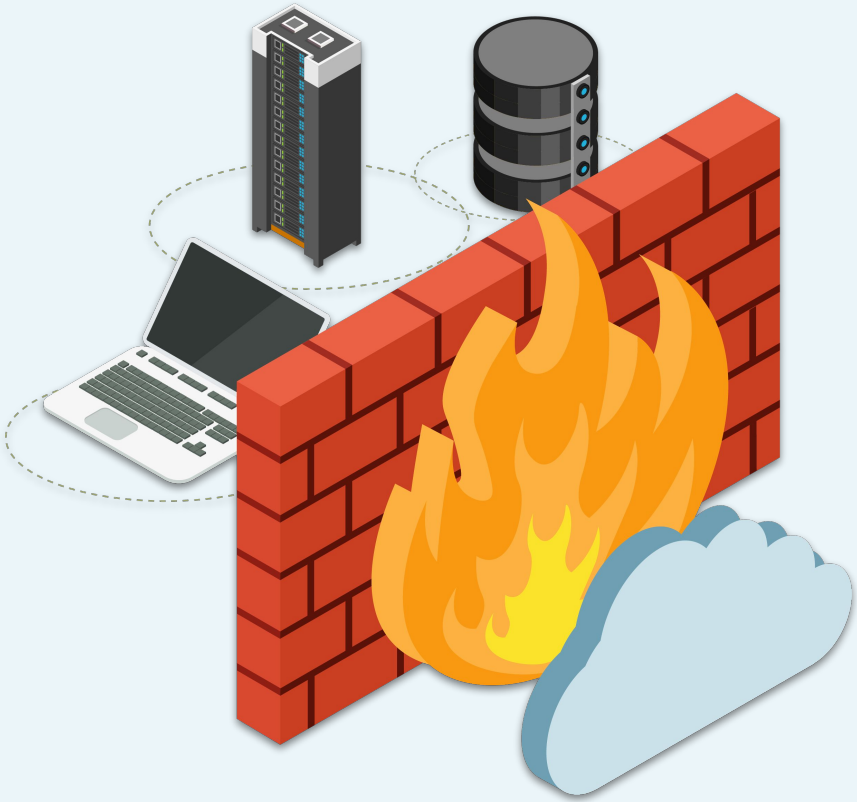
Time's Up! Let's Review.

Questions?


Break

Security Groups

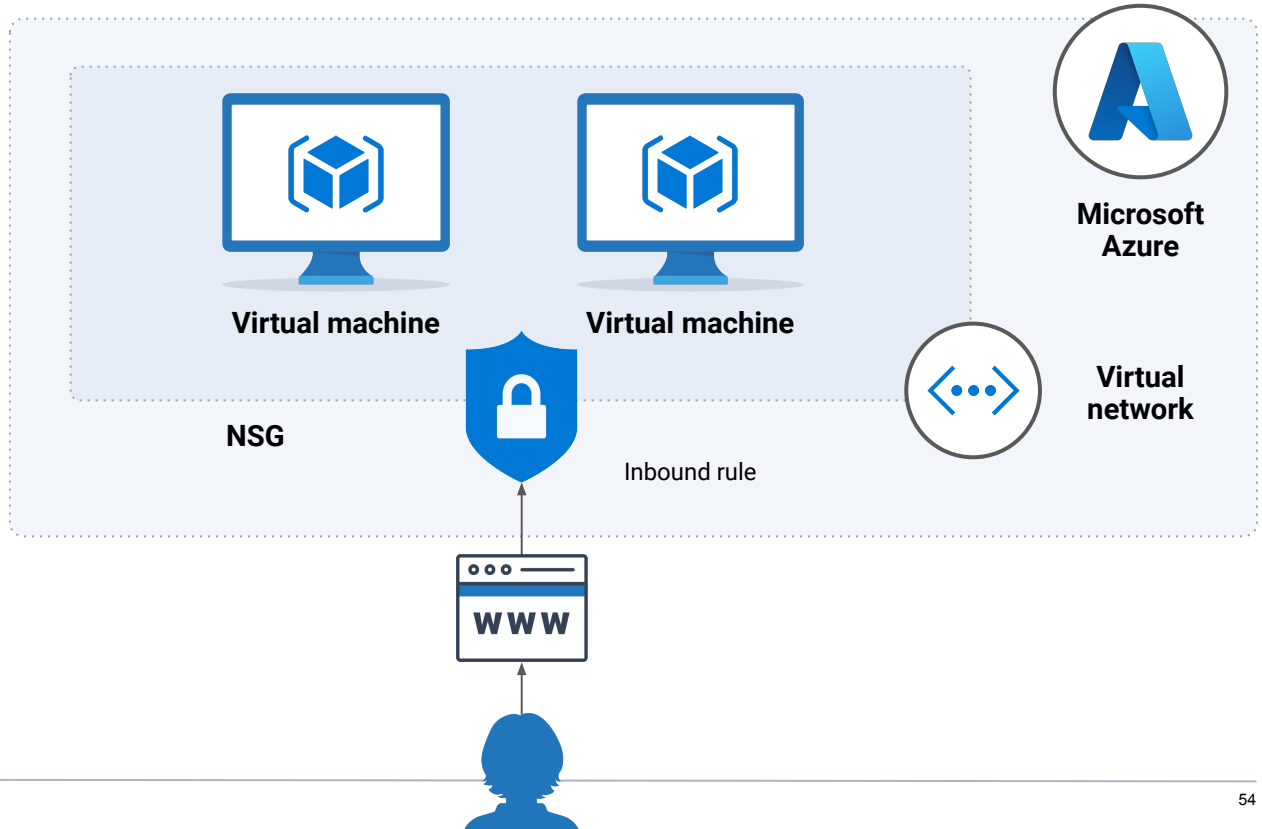
Now that we have a virtual network set up, we will protect it with a **firewall**.



Security Groups

On the Azure platform, our basic firewall is called a **network security group (NSG)**.

We will use a network security group to block and allow traffic to our virtual network and between machines on that network.

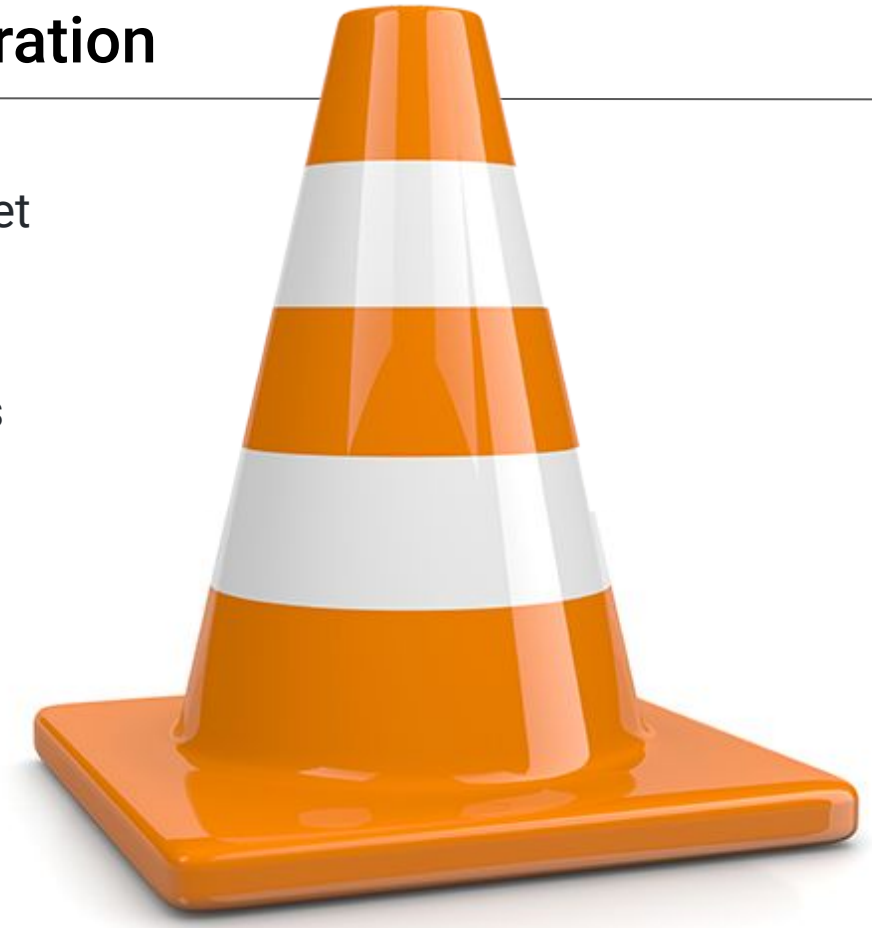


Security Groups Demonstration

Many resources can be created independently of any particular Vnet and then attached to a VNet after creation.

NSGs are a perfect example of this concept.

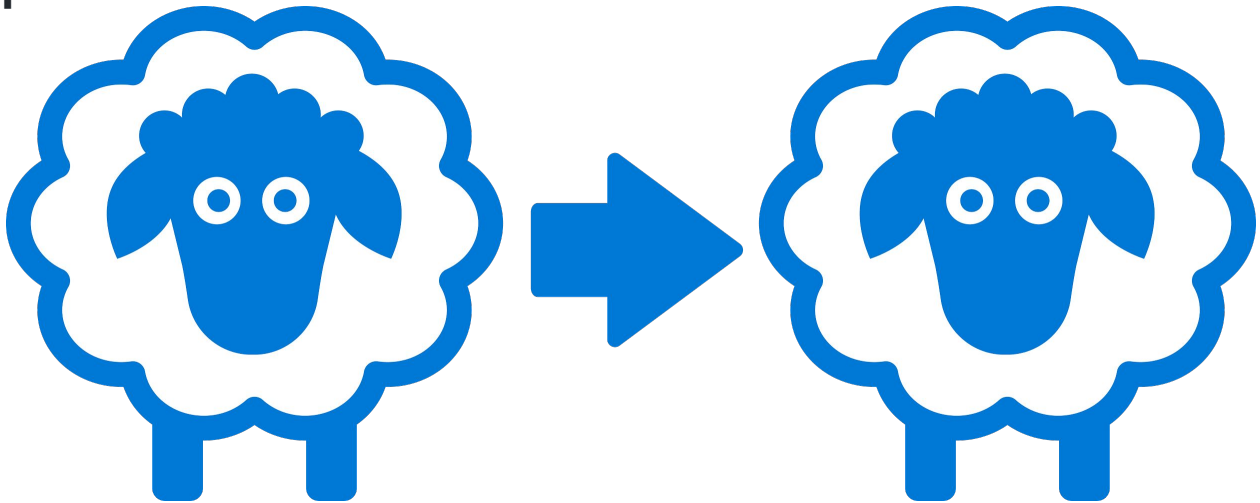
In the next demonstration and activity, we will create an NSG that blocks all traffic to and from the network, and then attach it to the VNet.



Security Groups Demonstration

This model has the advantage of allowing security engineers to create NSGs for different traffic profiles, which they can then replicate and apply to any VNet.

For example:



We can create an NSG called Desktop Connections, which clears RDP and VNC traffic to and from the VNet.

Engineers can then use this NSG as a template, clone it, and apply it to any new or existing VNet that requires this type of access.

Instructor Demonstration

Setting Up Security Groups

Activity: Security Groups

In this activity, you will create an NSG to control access to any resources in the subnet you created in the last activity.

Important:
For this and all activities, make sure that you are using your personal Azure account.

Suggested Time:

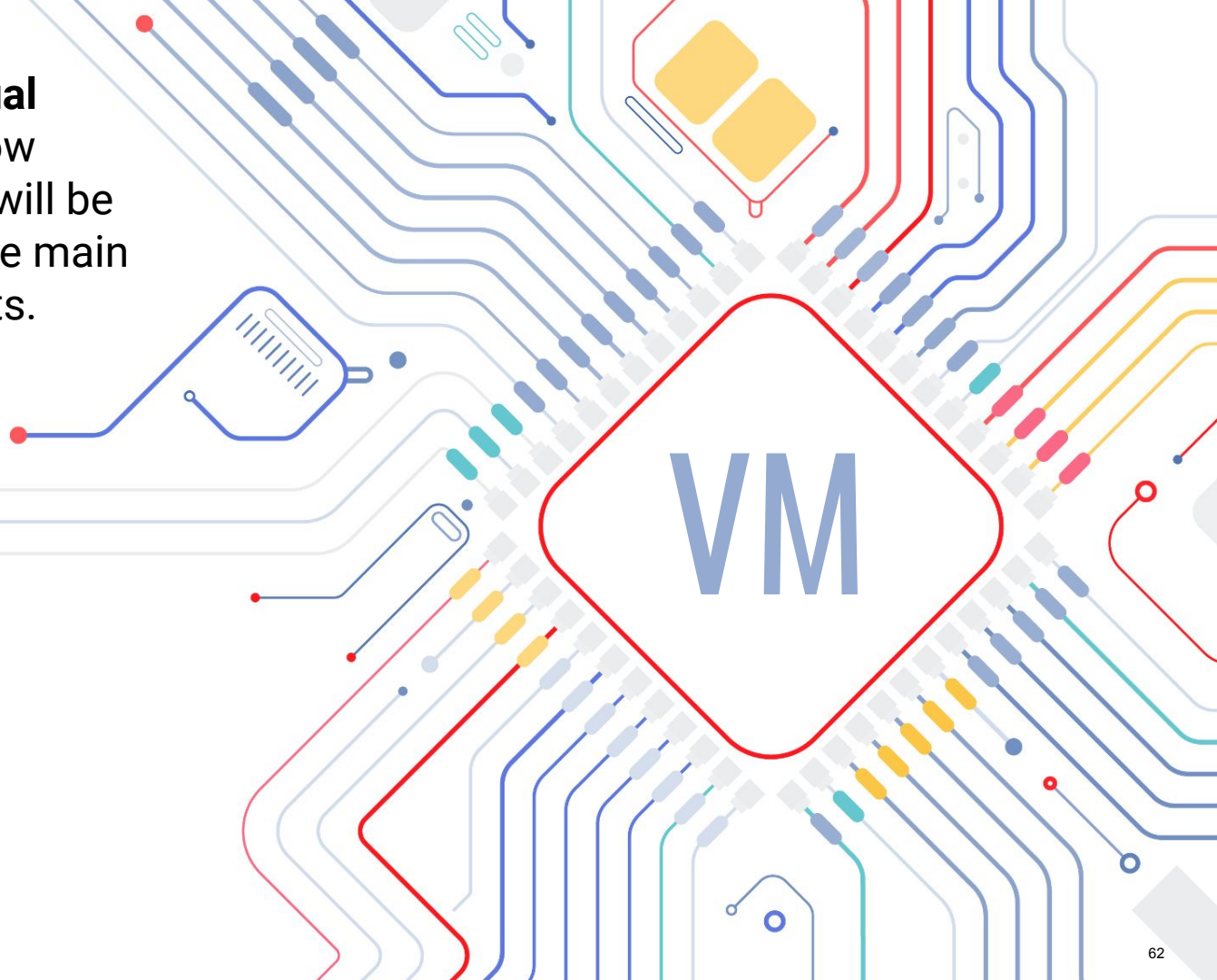
20 Minutes

Time's Up! Let's Review.

Questions?

Virtual Computing

When we set up a **virtual machine**, we decide how powerful the machine will be by choosing each of the main “hardware” components.



Hardware Components

Term	Definition
RAM (random access memory)	The amount of memory dedicated to running computer operations. The computer uses RAM to temporarily store data that it needs to access quickly.
Storage (HDD / SSD)	The part of the computer that stores data permanently. This is data that you do not expect to lose when the computer is turned off.
Disks	Disks attached to a VM fall into two general categories: • **OS disks** contain the operating system, kernel, and everything required for the VM to function. • **Data disks** contain data that the VM doesn't need in order to run, but which users need to do their jobs.
CPU (central processing unit)	CPU is like the brain of the computer. It's the part that actually computes all the 1s and 0s. The CPU takes code and data out of the long term storage, loads it into RAM, and performs the computations specified by an application.

Virtual Computing

A virtual computer has software versions of these components.

When we create a virtual computer, we define the "hardware," such as:

- The amount of RAM
- The storage space
- The CPU

Once this is defined, we can install an operating system and use it as if it's a typical computer.

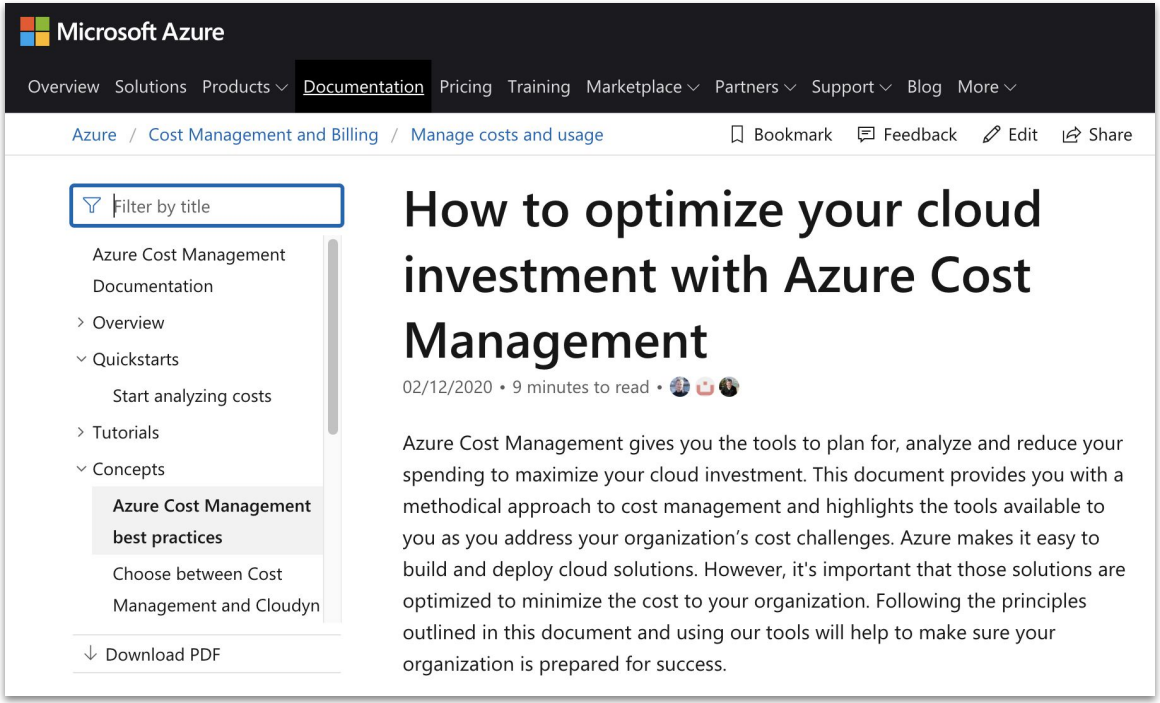
Availability vs. Cost Tradeoff

While it is possible to simply choose the “best” option available, it’s not advisable.

- The cloud provides great flexibility for users, but this flexibility can come at a cost.
- Before working with devices on the cloud, we must **always** set budget limits and cost-control policies.
- Otherwise, we can accidentally exceed our employer’s budget.

Availability vs. Cost Tradeoff

Azure provides cost-control tools as a free service, which you should study prior to managing live cloud deployments.



(Microsoft.com)

Instructor Demonstration

Getting Ready to Create a VM

Activity: Virtual Computing

In this activity, you're tasked with setting up a new Ubuntu VM inside the Red Team resource group to be used as a jump box.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Daily Checklist

By the end of today, you should have completed the following critical tasks:

- Created a total of three VMs—one jump box and two web VMs.
- Configured all three VMs with the same SSH key.
- The SSH key being used does not have a password associated with the key.
- Web VMs are created using the same availability set.
- Web VMs should have 2 GB of RAM.
- Jump-Box VM only needs 1 GB.
- All three VMs should have 1 vCPU.
- All VMs are using the same security group and Vnet.

Don’t forget to stop all VMs in your Azure account!

⚠️ Shut Down Your Machines ⚠️

Don’t forget to stop all VMs in your Azure account!

You will need the remaining hours to complete your work.


The End.