

# Introduction

## Introduction to Cloud Computing

### Public Cloud Computing

These are just services made available to you over the Internet.

#### Compute



#### Azure Virtual Machine

Operating System  
Windows 10/11  
MacOS



#### Laptop

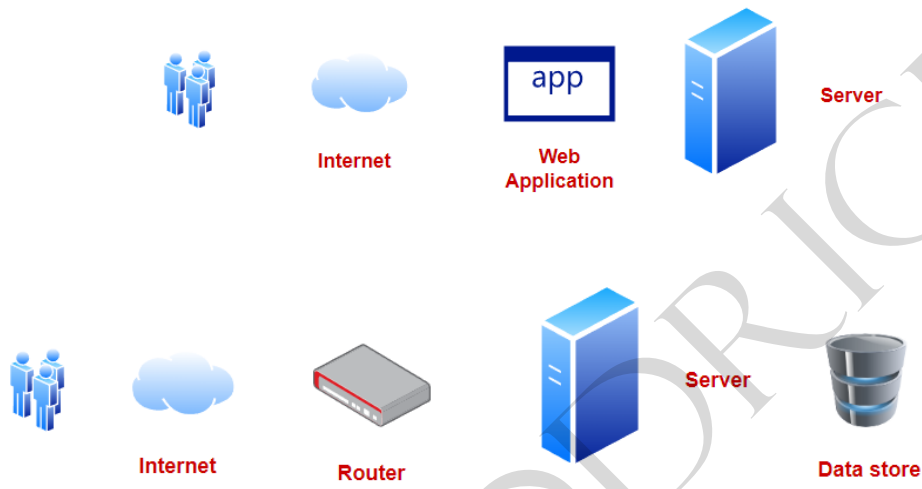
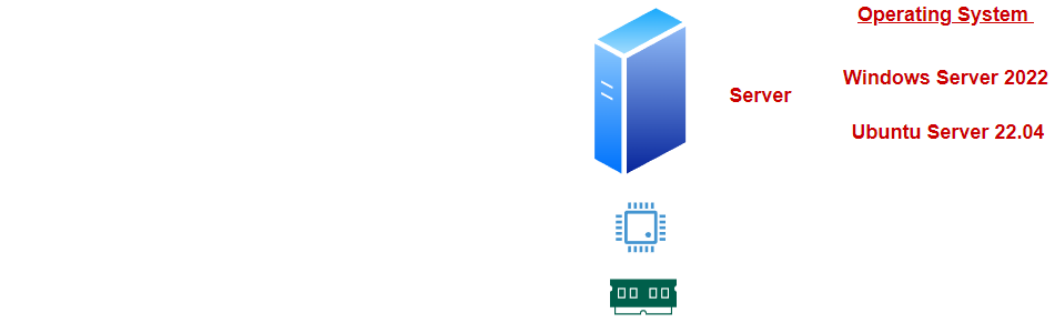
#### Desktop

CPU



RAM





All of the systems are part of a network

What is Microsoft Azure

This is a cloud platform

They make services available to you over the Internet

You can use this service to build, run and manage applications

Some key terms



# Describe Azure architecture and services - Azure compute

## Deploying a virtual machine



### Virtual Machine Service

This service allows you to create a virtual machine on Azure

You don't need to manage physical servers

You can make use of On-demand pricing

You only pay based on how much you use



Buy servers

Costs money

Buy storage

Setup a network

Machines are normally part of a network

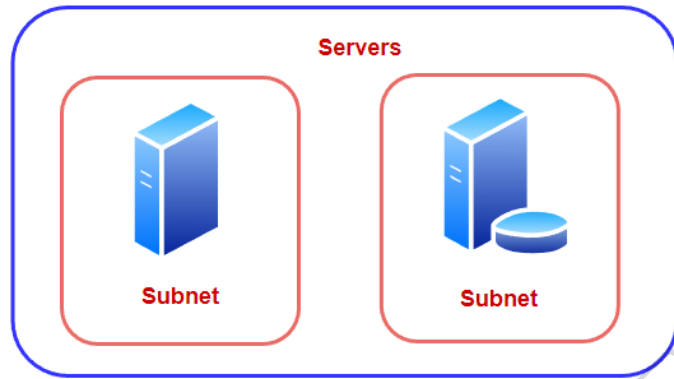


Each of your devices also gets assigned an IP address

This IP address helps to identify the devices on the network.

Wifi Router

All devices are part of the network managed by your Wifi Router

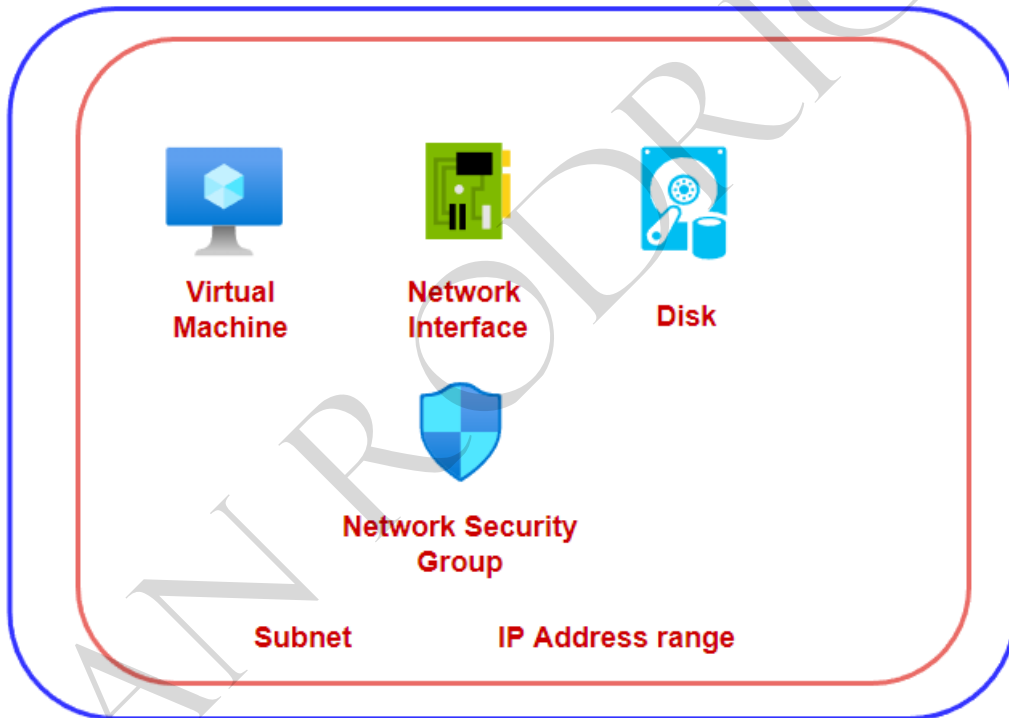


**Network**

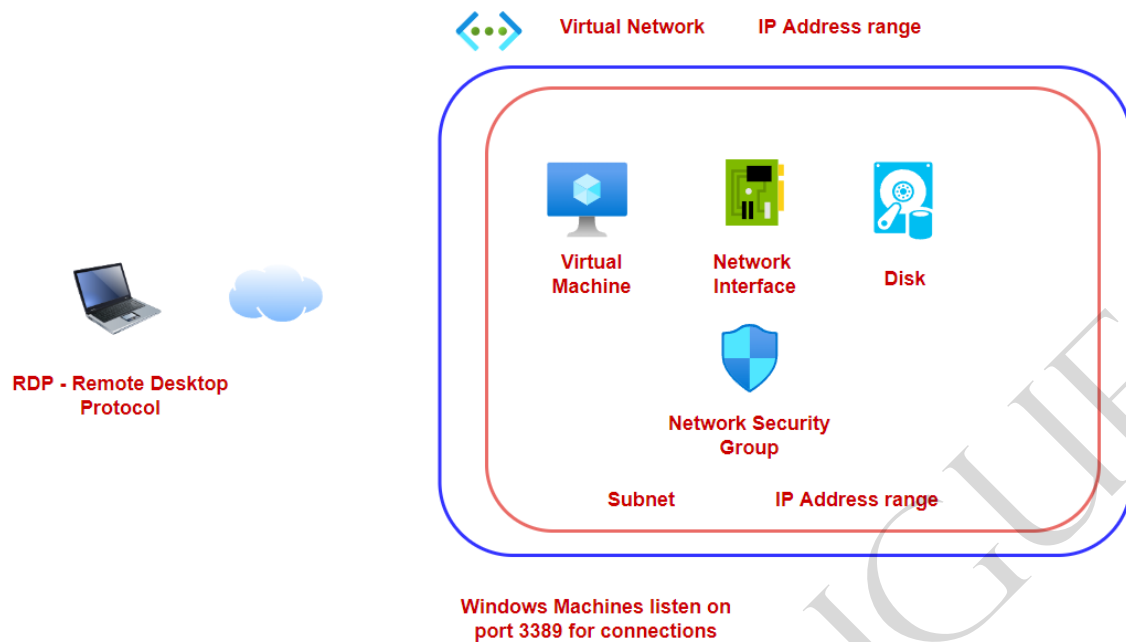


**Virtual Network**

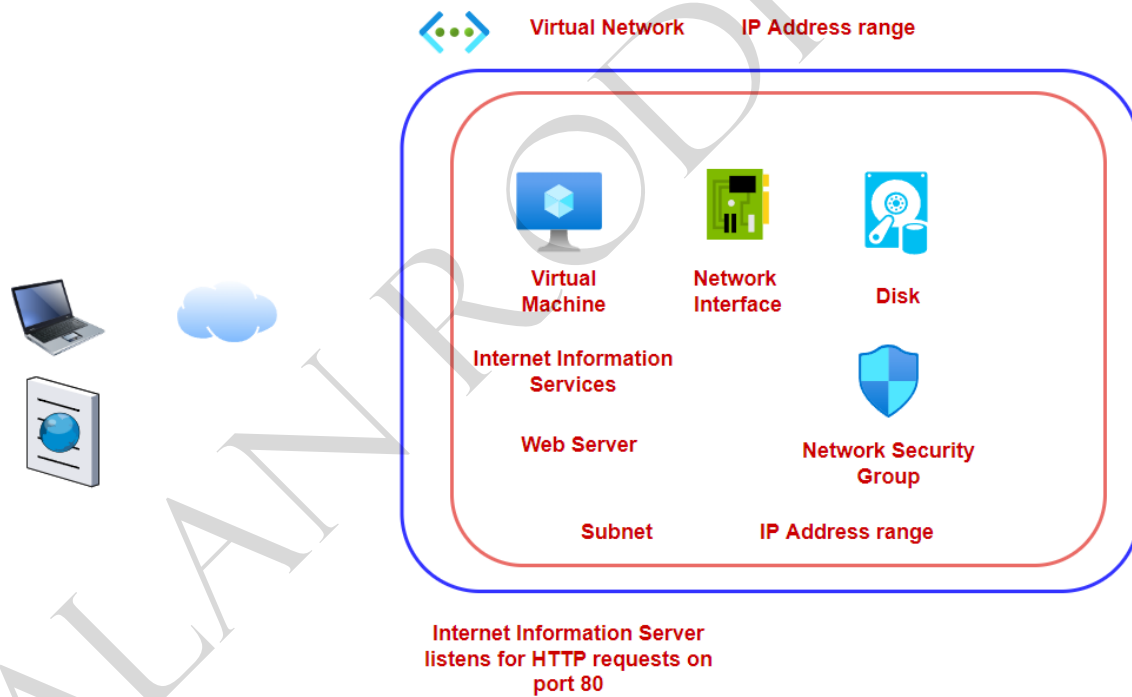
**IP Address range**



## Connecting to an Azure Windows Virtual Machine



## Lab - Installing Internet Information Services

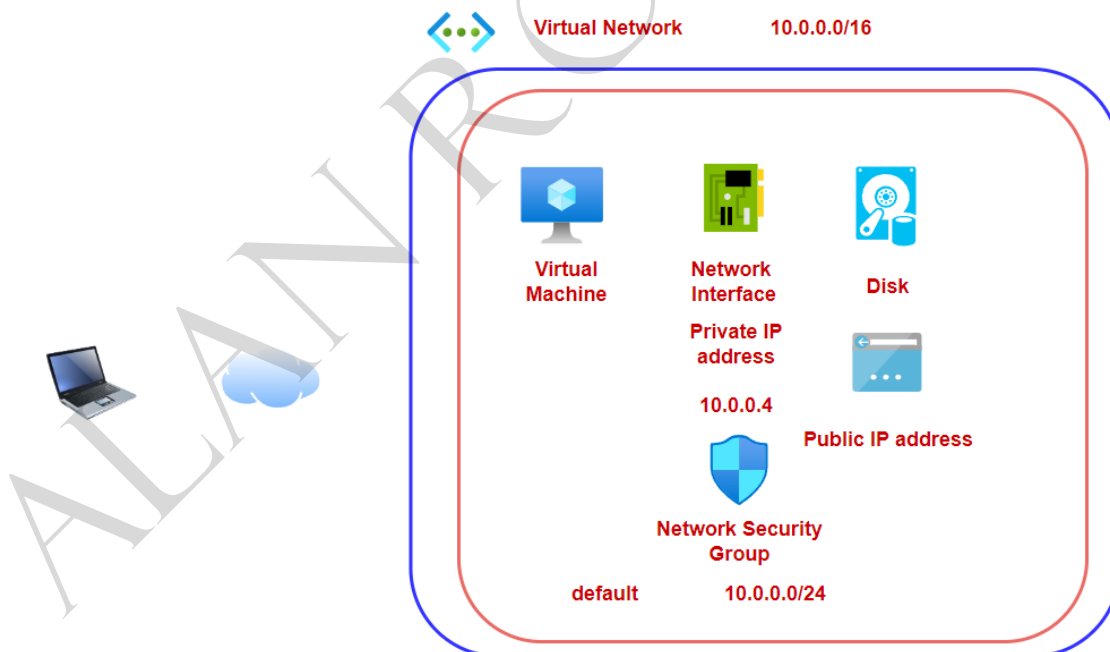


## Virtual Machines - OS and Temporary disk



The Virtual Machine gets assigned an operating system disk  
 This is a managed disk - These are designed for high availability  
 Most VM's also get a temporary disk. This is not a managed disk.  
 The data on the temporary disk could get lost in the case of a maintenance event or when you redeploy the virtual machine.

## Virtual Machine - IP addresses



The Public IP address allow Internet resources to communicate inbound to the Azure resources

Why do we choose a region



Virtual Machine Service

You don't need to manage physical servers



But the servers are still required to host the virtual machines.

It just that Azure is now managing the data centers that host these physical servers.

That is why you need to choose a region to deploy the Azure Virtual Machine

Depending on the region you choose, the Virtual Machine will be hosted on some physical server in that location.

There are some services that are available at the global level.

Which region should you choose

Make sure the service is available in that region.

Costing for that service in that region.

Maybe your company has a restriction that data should only be hosted in that region.

You might want to ensure that resources are closest to the users.



East US



**Availability Sets**

**The availability set is a logical grouping of VM's. It helps to improve the entire availability of your application.**



**Azure Virtual Machine**



**Physical server in a datacenter**

**What happens if there is a fault in the underlying physical server?**

**Or maybe Azure needs to apply an update on the physical server that requires a restart of the server.**

ALAN R. ORIGUES

Availability Sets can be used to manage these issues.

Fault Domain

Update Domain

When you place your virtual machine as part of an Availability set, it gets assigned a fault and update domain.

#### Update domain

Here Azure will apply updates to the physical infrastructure one update domain at a time.

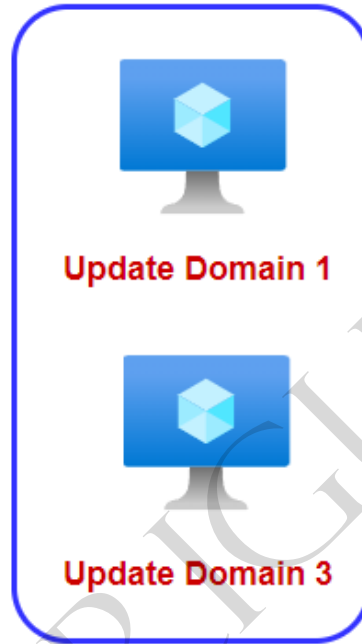
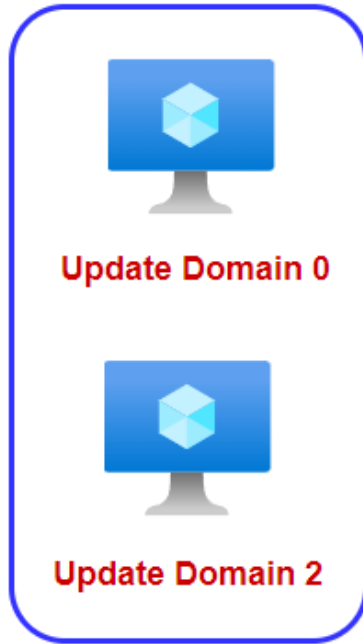
#### Fault domain

Here the virtual machines in the fault domain share a common power source and network switch.

ALAN RODRIGUES

**Fault Domain 0**

**Fault Domain 1**



ALANKODRICKS

### Common questions

**Is there a cost for using Availability sets?**

**No. You just need to pay for the underlying virtual machines.**

**Am I supposed to create multiple virtual machines? Or does the Availability set feature create duplicate copies of the VM?**

**You have to create the multiple VM's. The Availability set is just a feature for managing availability of your machines.**

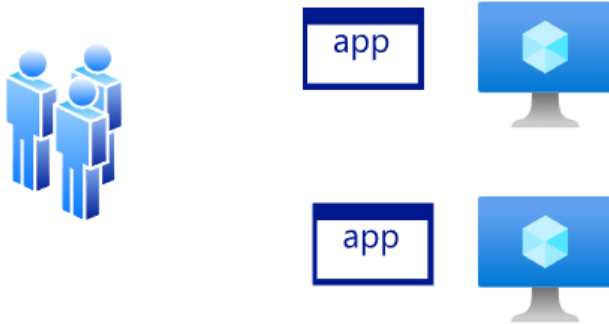
**Does the Availability set replicate data across the VM's.**

**No. You manage all of these aspects. Remember the Availability set is just a feature for managing availability for your machines.**

Availability Zones

### Availability Zones

These are physical locations within an Azure region. These are made up of one or more datacenters. They have independent power, cooling and networking.



### Azure Virtual Machine

In an Availability set, the machines might be located in a single datacenter

What happens if the datacenter goes down?

You can spread the deployment of your machines across datacenters by deploying them to different Availability zones

ALAN RONDIGUES



### Common questions

Is there a cost for using Availability zones?

No. You just need to pay for the underlying virtual machines.

Then why not just make use of Availability zones instead of Availability sets?

This is because there is a charge of data transfer per GB between availability zones.

Does Availability zones replicate VM's or do data transfer?

No. Again this is all managed by you. Availability zones is just another availability feature from Azure.

Azure Dedicated Host



Physical host

Azure Dedicated host

1. Hardware isolation - No other VM's will be placed on the host

2. You can control the maintenance events

## Virtual Machine Scale Set service

### Virtual machine Scale Set



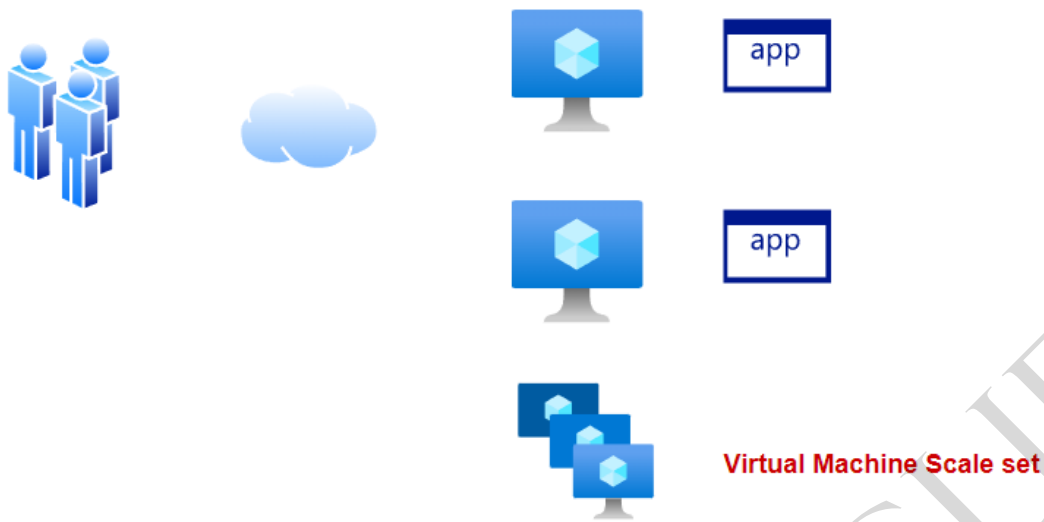
**Load on the application increases**

**The load on the machine starts to increase**

**Application could face performance issues because of the load on the Azure virtual machine**



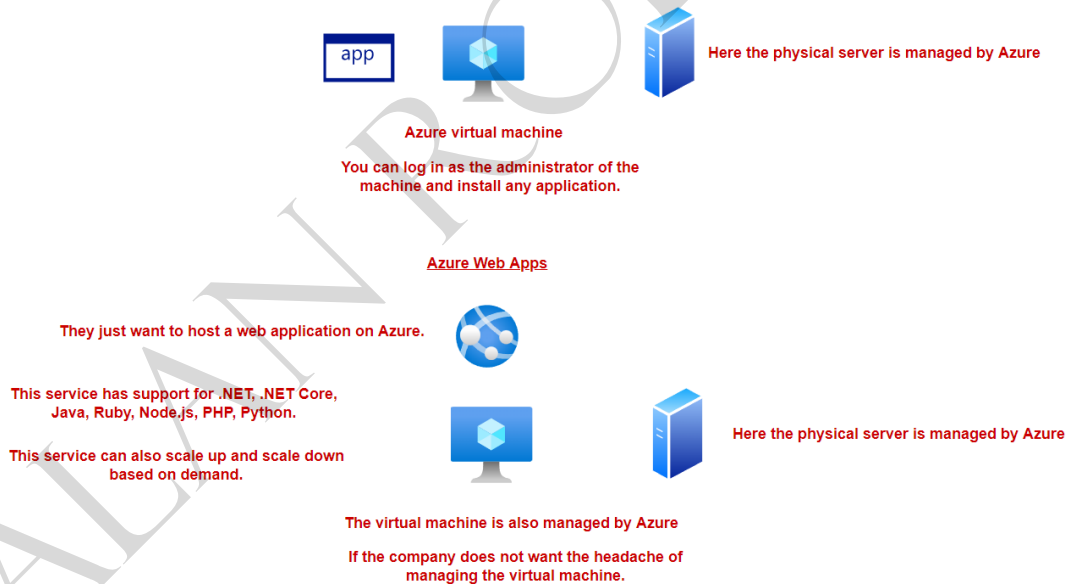
**In today's world of automation, manually adding a machine to your infrastructure setup is not the most ideal approach.**



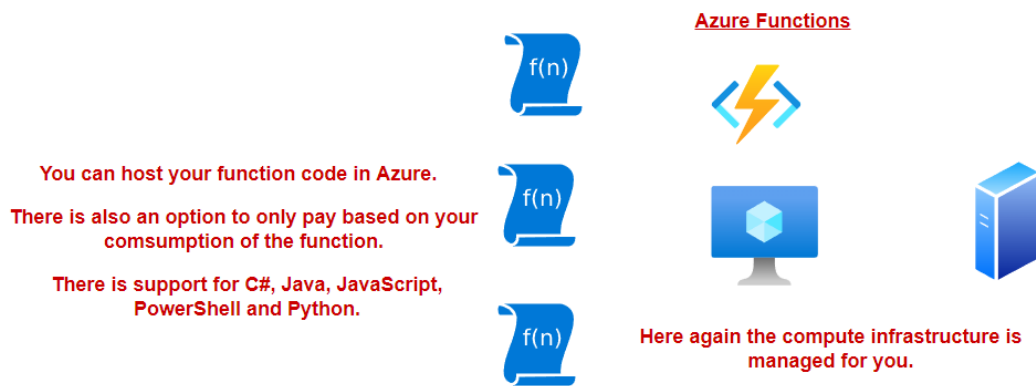
**Virtual Machine Scale set is a group of virtual machines**

**Here the number of virtual machine instances can increase or decrease based on demand.**

### About Azure Web Apps



### About Azure Functions

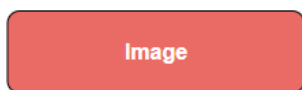
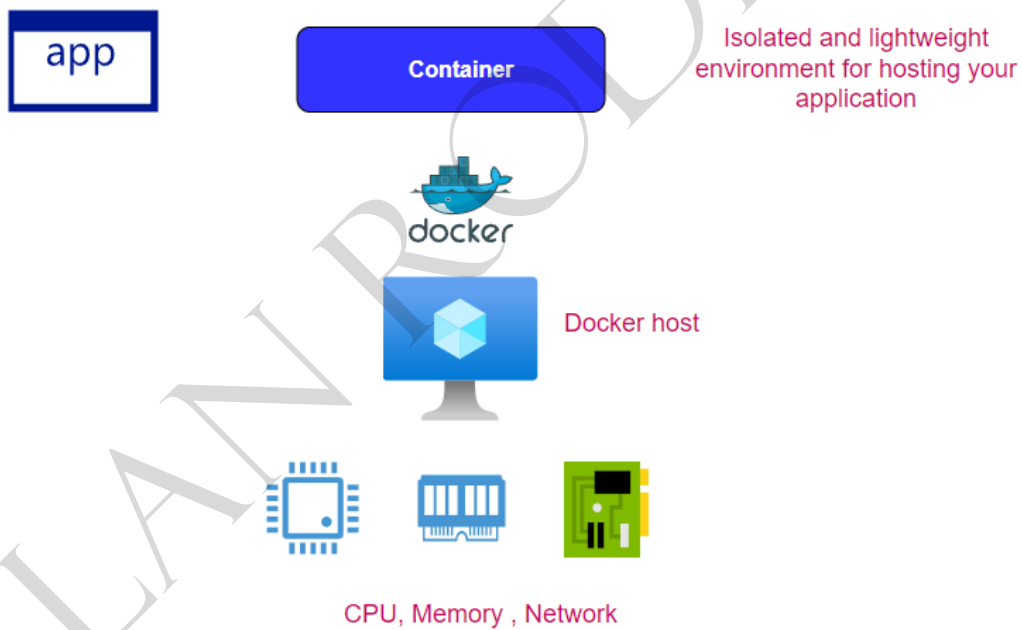


Primer on containers

What is Docker

This is an open platform that is used for developing, shipping and running applications.

Docker has the ability to package and run an application in a loosely isolated environment called a container

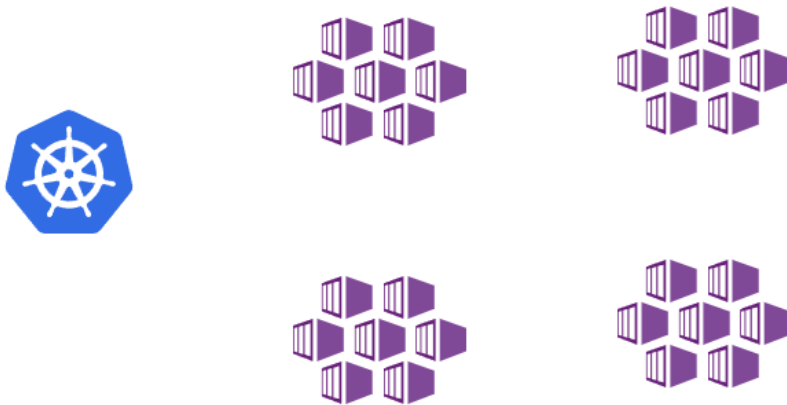


This is a read-only template with instructions that are required to create the Docker container



This is a runnable instance of an image

## Kubernetes



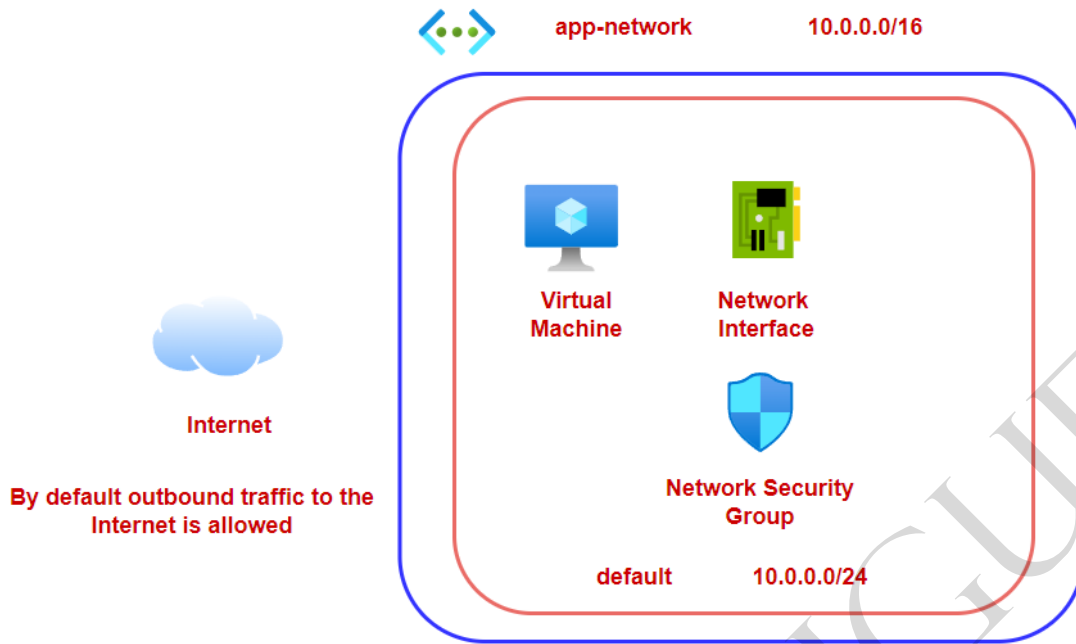
### Managing containers at scale

**Azure Kubernetes - Managed service for Kubernetes on Azure**

**Kubernetes is used to orchestrate your containers for hosting your applications**

Describe Azure architecture and services - Networking

Azure Virtual Network

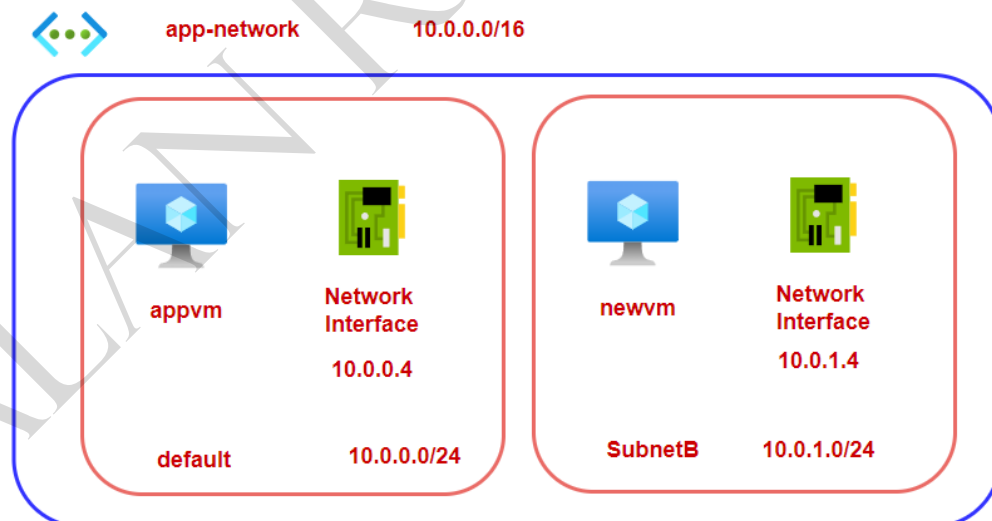


This is the equivalent of an on-premises network

This is an isolated network on Azure

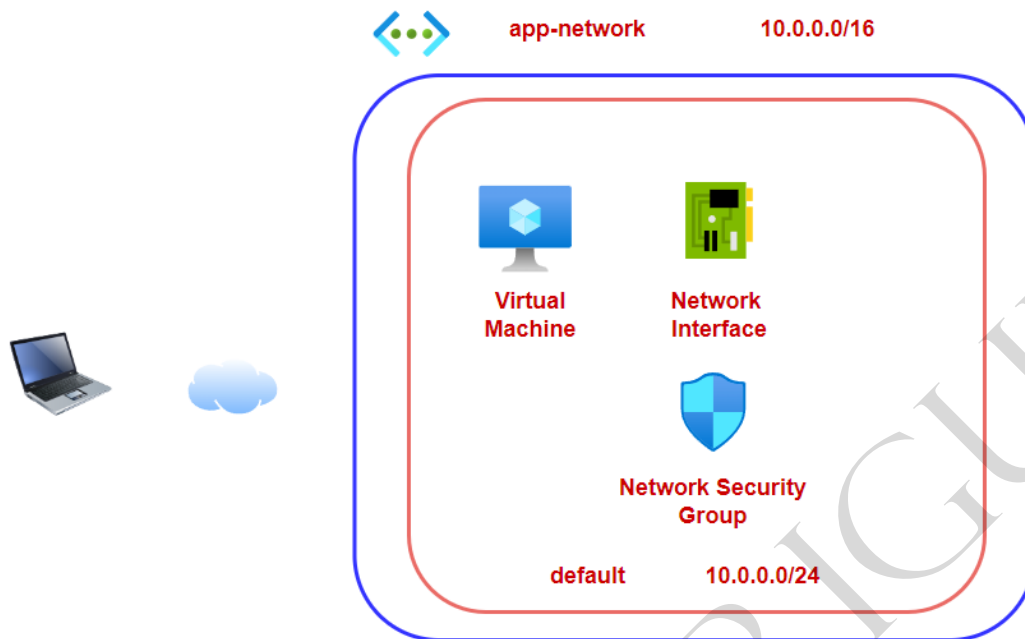
If you want to isolate workloads that run on Azure virtual machines, deploy them in different virtual networks.

### Lab - Communication across virtual machines in a virtual network



By default communication between machines in different subnets is allowed.

## Network Security Groups



**The Network Security Group is used to filter network traffic to and from Azure resources within an Azure virtual network**

**The group contains rules that are used to allow or deny inbound and outbound traffic.**

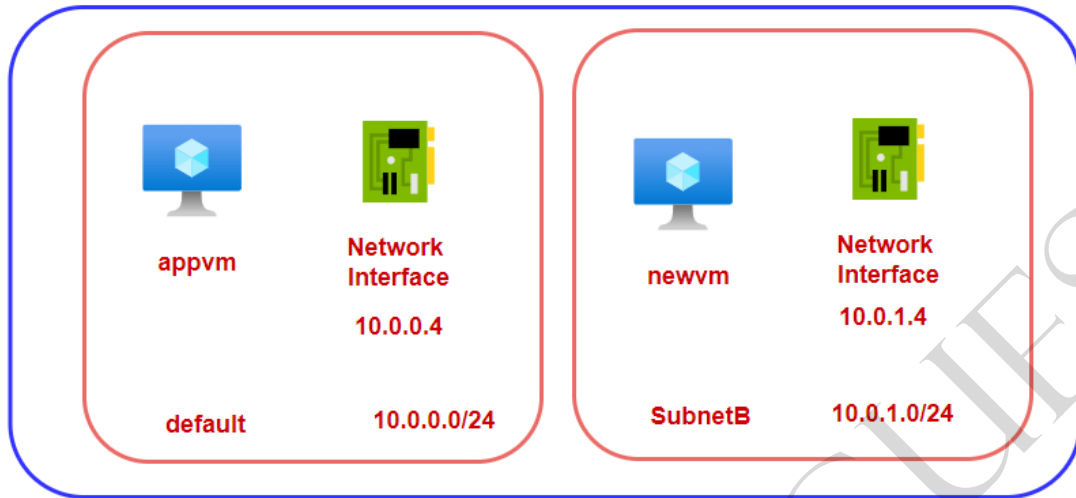
**Network Security Groups can be attached to a subnet or a network interface**

## Application Security Groups



app-network

10.0.0.0/16



Network Security Group

You can define one rule that allows Inbound traffic from 10.0.1.4 to 10.0.0.4

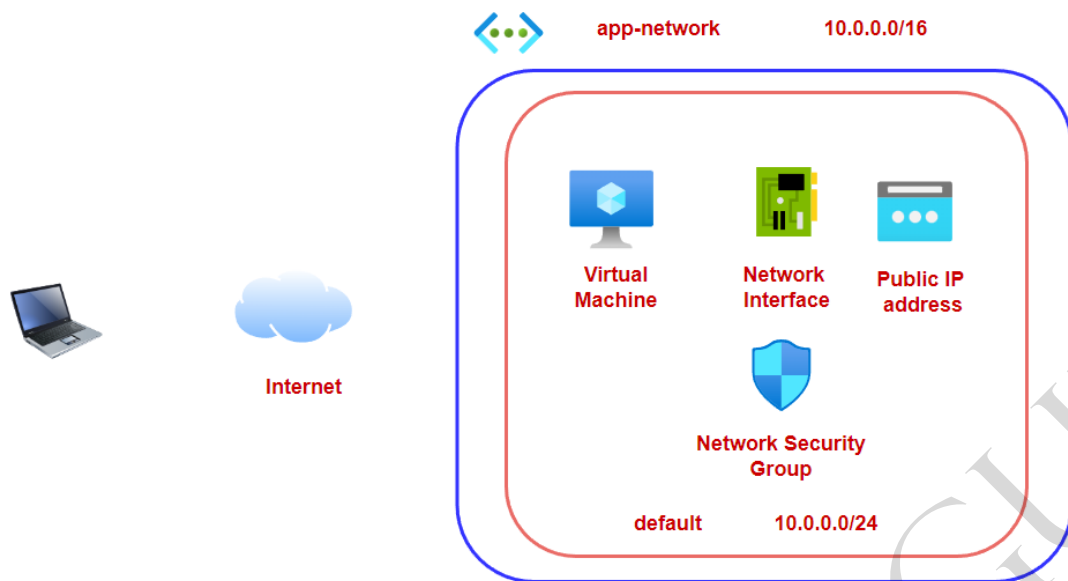
But here there is a dependency on the IP address

Instead you can make newvm part of an Application Security group - Let's say app-asg

**And then define the rule in the Network Security Group to allow traffic from app-asg to 10.0.0.4**

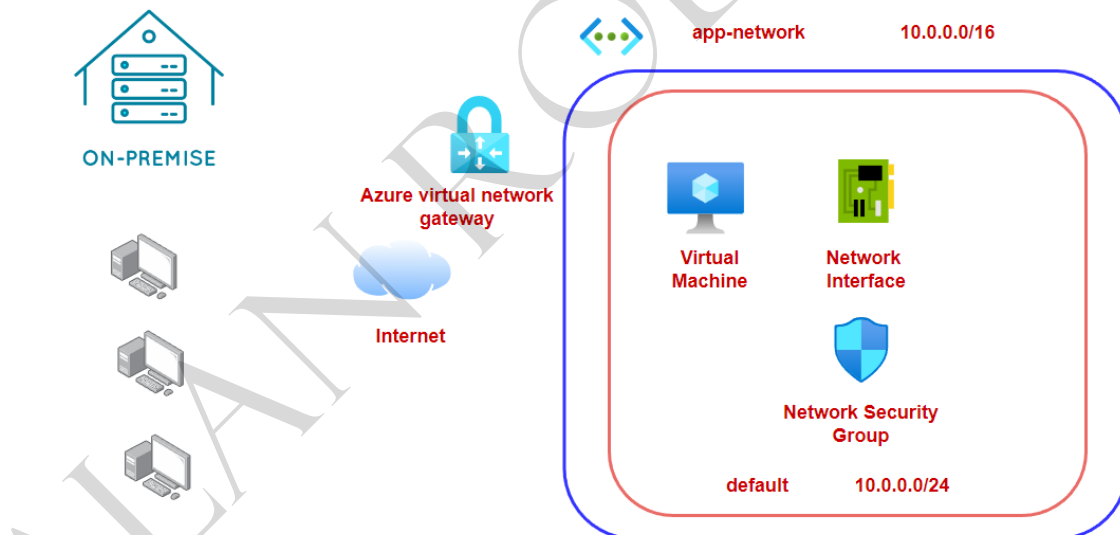
ALAN RICHARDS

## Overview of VPN connections to Azure

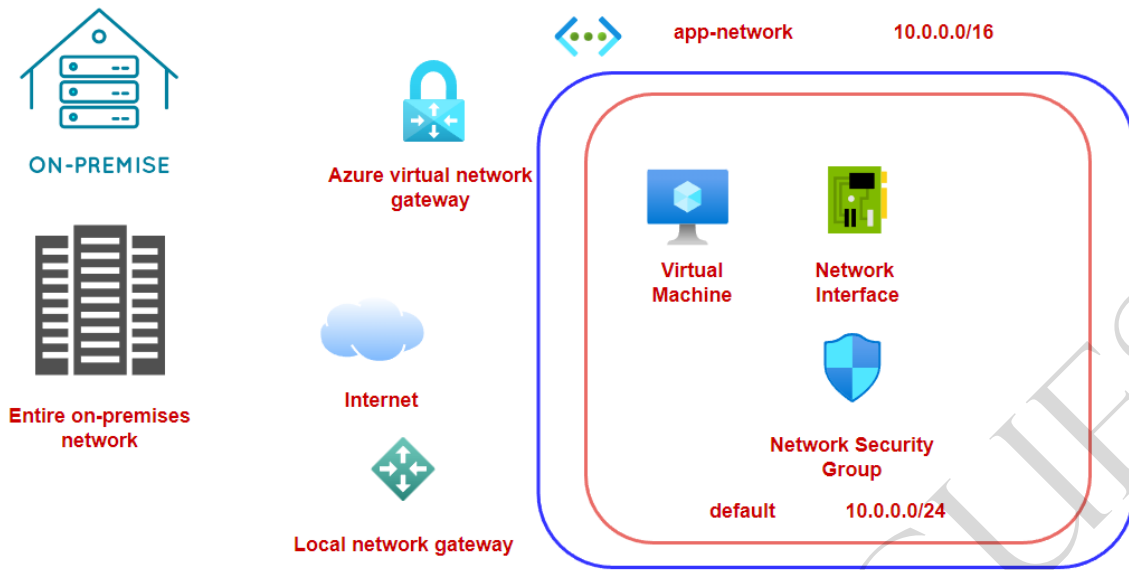


But there could be some Azure virtual machines in the Azure virtual network that don't require a public IP address.

Company could want machines in their on-premises environment to connect using the private IP address of the machine.



You can use a Point-to-Site VPN connection to connect each individual machine to the Azure virtual network



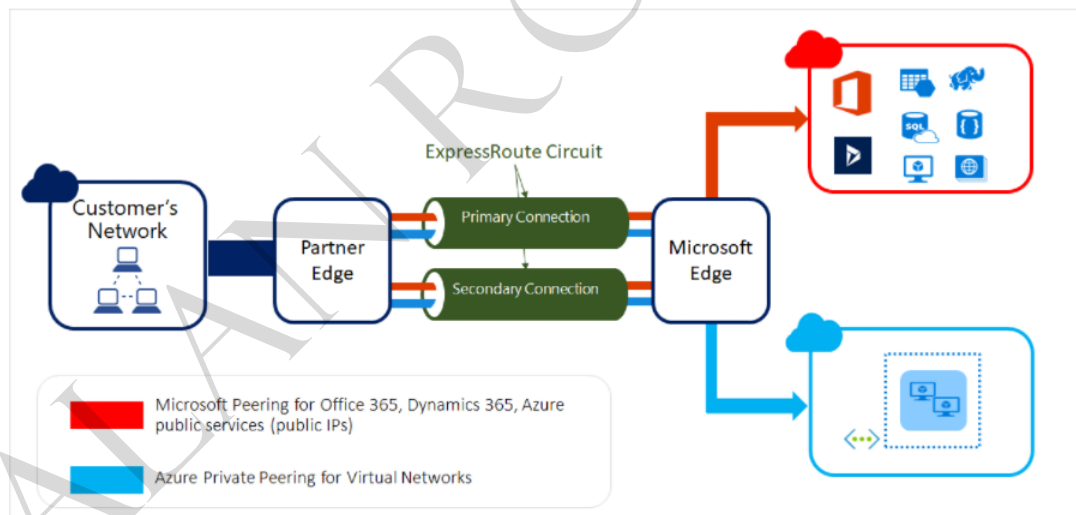
You can use a Site-to-Site VPN connection to connect an entire site to an Azure virtual network

## Overview of Azure ExpressRoute

### Azure ExpressRoute

Allows you to connect your on-premises networks to Microsoft cloud over the private connection

Here the connection is established with the help of a connectivity provider



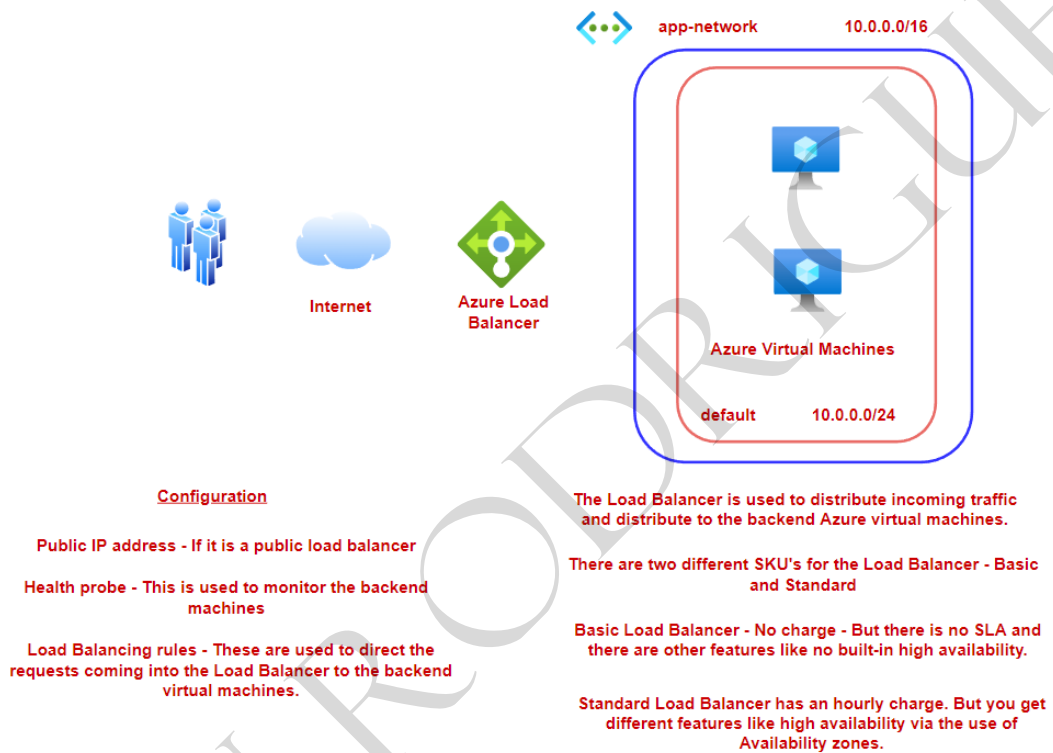
Reference - <https://docs.microsoft.com/en-ca/azure/expressroute/expressroute-introduction>

The ExpressRoute connection does not go over the public Internet

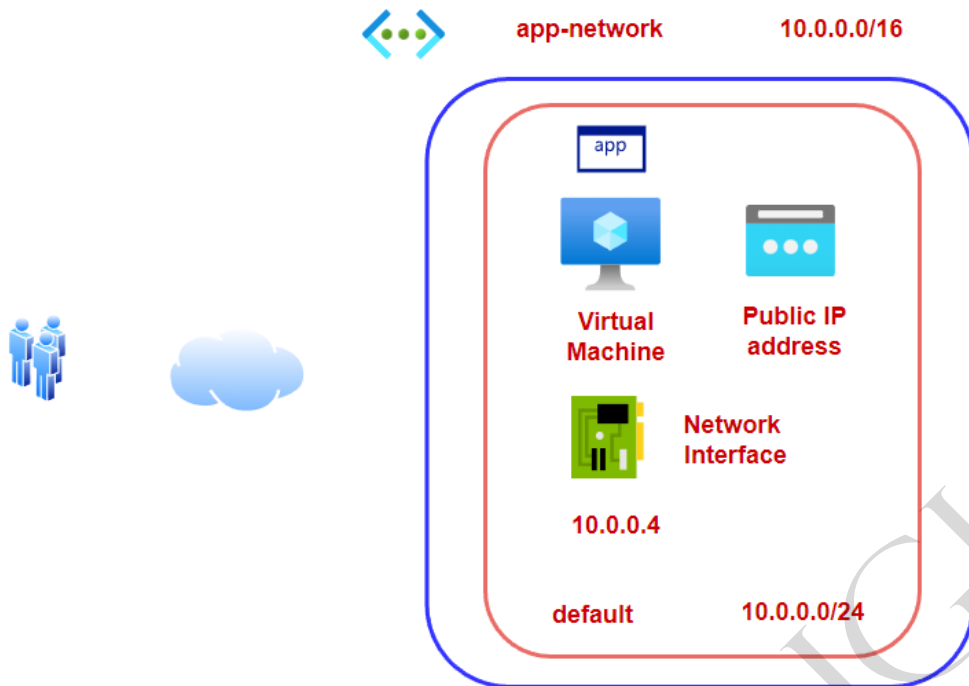
Your connections are more reliable, faster and you get less latency

You get two connections for each ExpressRoute circuit for redundancy

## Azure Load Balancer



## Azure DNS

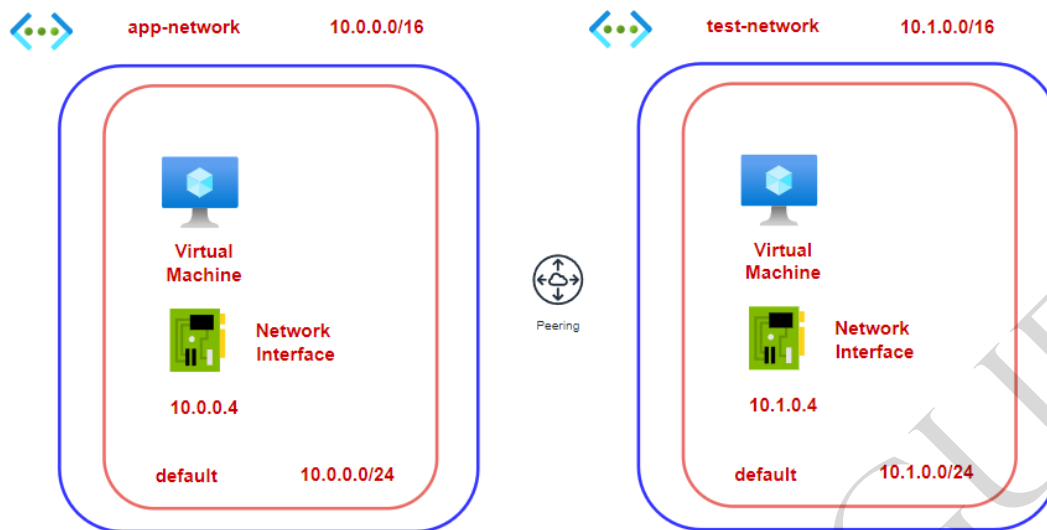


You could access the web application via the Public IP address or the DNS allocated by Azure.

You can route the user traffic to your application via your own domain name.

You can use the Azure DNS service when it comes to name resolution.

## Lab - Azure virtual network peering



An Azure virtual network is an isolated network on the cloud

By default the Azure virtual machines cannot communicate across Azure virtual networks

For this you have to create an Azure virtual network peering connection

Describe Azure architecture and services – Storage

## Azure Storage Accounts



**This is storage on the cloud via the use of different services.**

## Azure Blob storage

**This is an object storage service**

**This is great for storing unstructured data**



**Data Disk**

**Azure virtual machine**



Ideal approach is to store the videos in an Azure storage account

**Azure virtual machine**

**Azure Blob storage can grow automatically based on demand**

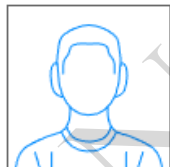
**Its great when you want to use it to store images, video, audio files.**

**Even good for storing backups.**

**Azure File shares**



**File Server**

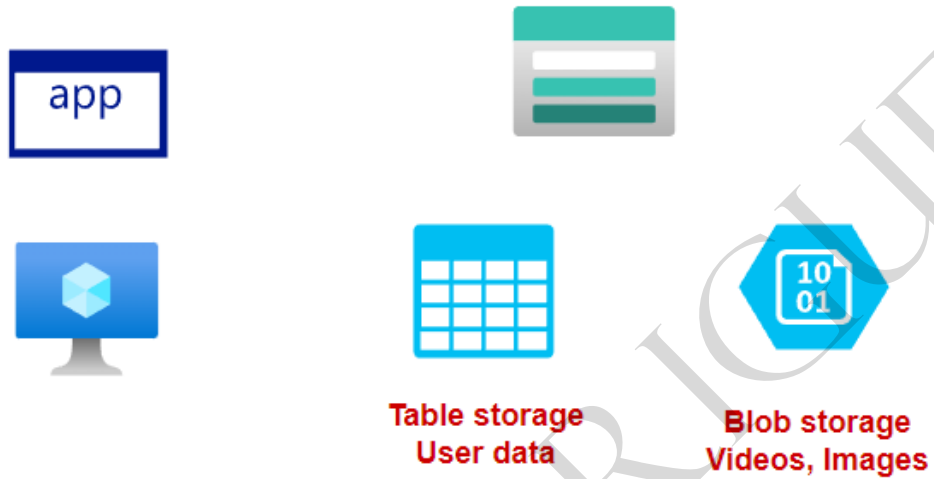


**Azure Storage Account - File shares**

### Azure Table storage

This is great when you want to store non-relational structured data

This is when your data conforms to a schemaless design



### Azure Queue storage

This is a messaging based service



Azure Storage Accounts - Access tiers

## Azure storage access tiers



### Objects

There is a cost for storing objects

There is a cost for accessing objects

Companies might store millions of objects in a storage account

Use case - Initial there could be some objects that are accessed quite frequently. Then after some time, maybe a week or two, those objects are accessed less frequently.

Can a company save on costs when it comes to less frequently accessed objects.



### An object can be set to a particular tier

Hot  
Access  
tier

This is optimized for objects accessed more frequently  
Here you have high storage costs and lower access costs

Here the data needs to be stored for at least 30 days

Cool  
Access  
tier

This is optimized for objects accessed or modified infrequently  
Here you have lower storage costs but higher access costs when compared with the Hot access tier.

This is optimized for objects that are rarely accessed

Here the data needs to be stored for at least 180 days

Archive  
Access  
tier

Here you have lower storage costs but higher access costs when compared with the Cool access tier.

Good for long-term backups.

**You can set the Hot and the Cool access tier at the storage account level.**

**You can set the Hot ,Cool and Archive access tier at the blob level.**

## Azure Storage Accounts - Data Redundancy

**Azure Storage account - Redundancy**

**Multiple copies of your data are stored**

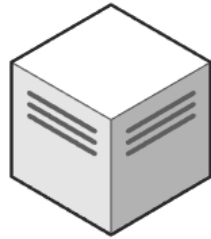
**This helps to protect against planned and unplanned events - transient hardware failures, network or power outages.**



**Storage Device**

Locally-redundant storage

Data Center



Central US



Here three copies of your data are made

It helps to protect against server rack or drive failures



Storage Device

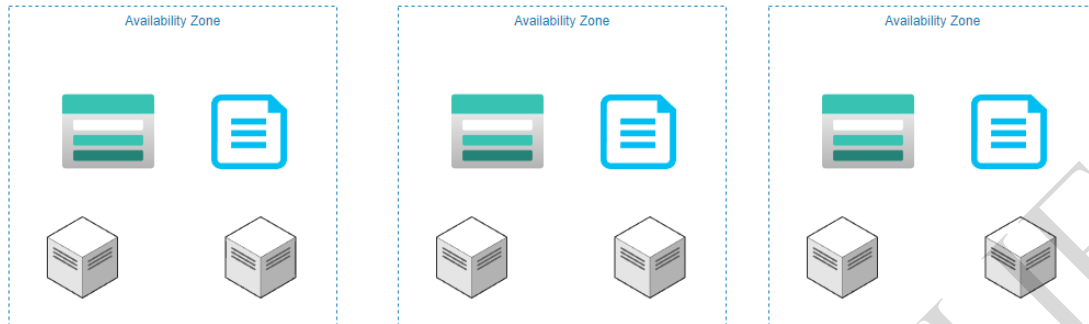
Storage Device

Storage Device

Zone-redundant storage

This helps to protect against data center level failures

Here data is replicated synchronously across three Azure availability zones

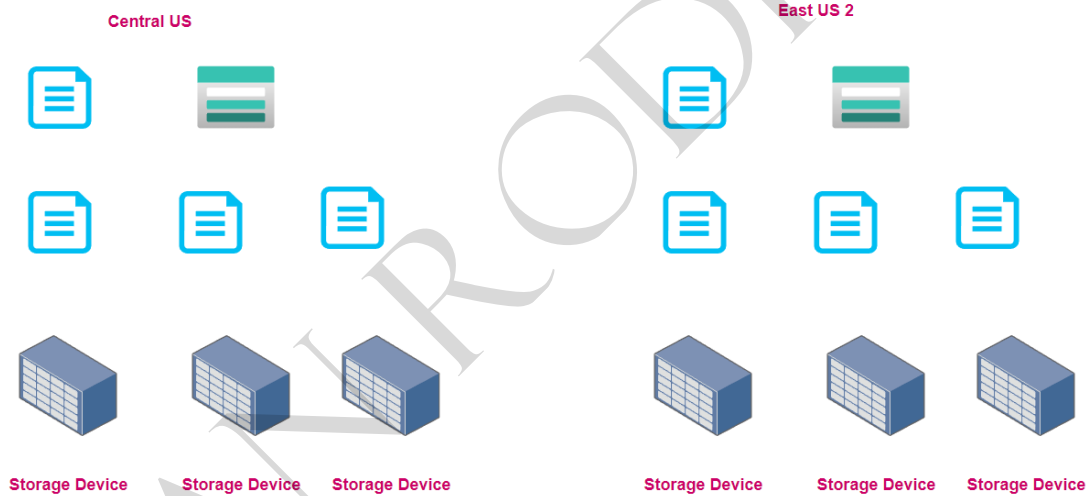


Central US

Each availability zone is a separate physical location with independent power, cooling and networking

Geo-redundant storage

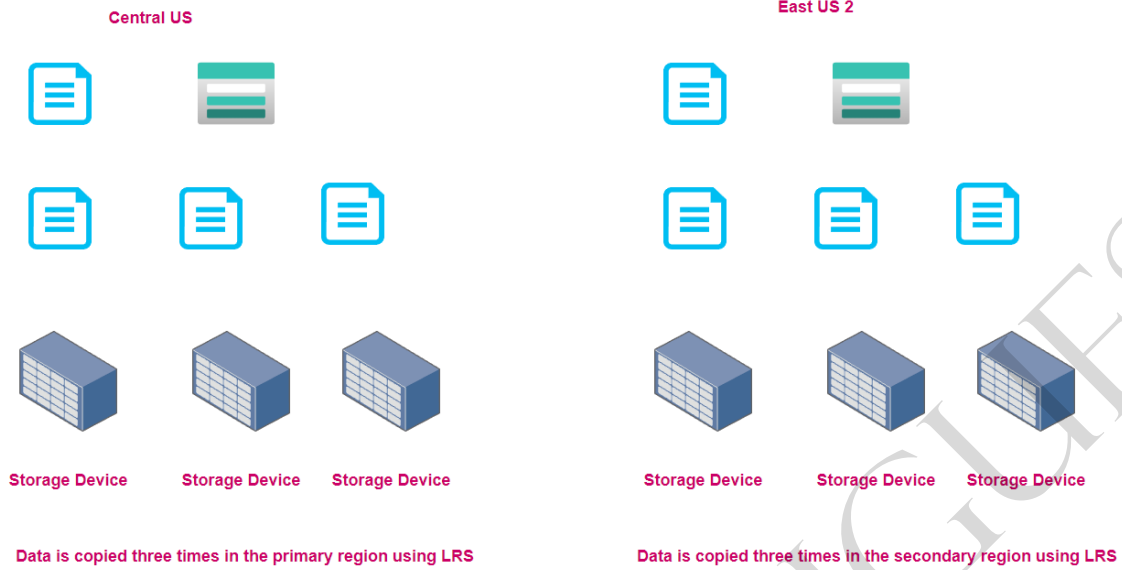
Here data is replicated to another region



Data is copied three times in the primary region using LRS

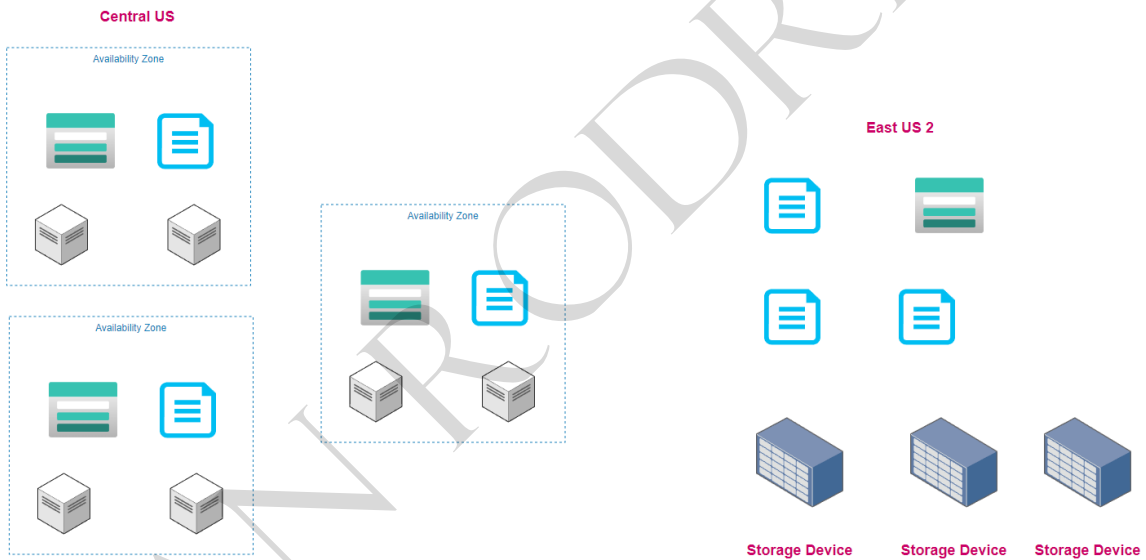
Data is copied three times in the secondary region using LRS

Read-access geo-redundant storage



Geo-zone-redundant storage

Read Access geo-zone-redundant storage



Note - Azure File Sync service

## Azure File Sync

## File shares



## Azure Storage Account - File shares

Windows Server can be used to cache frequently used files.

You can achieve this with the Azure File Sync service

Here one of the steps is to download and install the Azure File Sync agent on the Windows server

ALAN RODRIGUES

## Premium storage accounts



### Premium block blobs

**This is used when you need high performance when it comes to storage and access to data.**

**Here the data in the background is stored on solid-state drives. These are optimized for low latency.**

**Here the file transfer is also much faster.**

**Workloads - Streaming , Machine Learning**

**You have higher storage costs but lower transaction costs**

### **Data redundancy**

#### **Data redundancy**

Performance ⓘ \*

Premium account type ⓘ \*

Redundancy ⓘ \*

**Locally-redundant storage (LRS):**  
Lowest-cost option with basic protection against server rack and drive failures. Recommended for non-critical scenarios.

**Zone-redundant storage (ZRS):**  
Intermediate option with protection against datacenter-level failures. Recommended for high availability scenarios.

Locally-redundant storage (LRS) ▾

**You can't set the access tiers**

**Premium file shares**

Here again you get high performance and low latency

Backed by solid-state drives for storage

Data redundancy

Performance ⓘ \*

Premium account type ⓘ \*

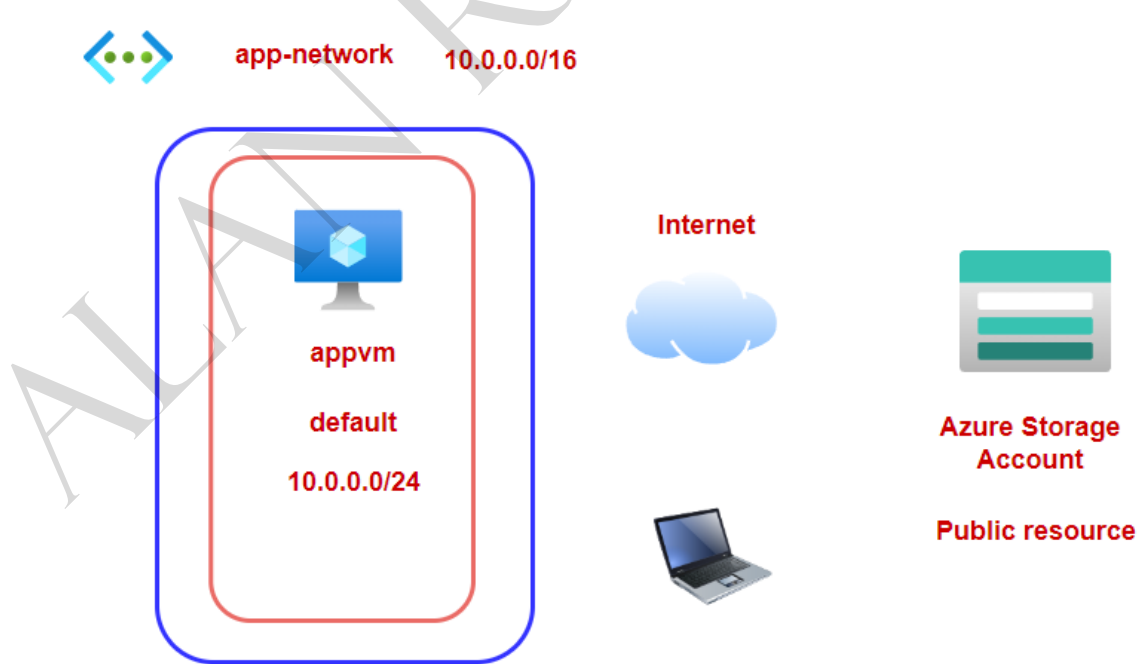
Redundancy ⓘ \*

|  |
|--|
| Locally-redundant storage (LRS):<br>Lowest-cost option with basic protection against server rack and drive failures. Recommended for non-critical scenarios. |
| Zone-redundant storage (ZRS):<br>Intermediate option with protection against datacenter-level failures. Recommended for high availability scenarios.         |
| Locally-redundant storage (LRS) ✓  |

Virtual Network Service Endpoints

**Virtual Network Service Endpoints**

This provides secure and direct connectivity to Azure services over the Azure backbone network



# Describe Azure architecture and services – Databases

## Azure SQL Database service



**Virtual Machine**  
**IaaS**

**Install Microsoft SQL Server**

**Configure the server**

**Configure high availability**

**Configure backups**



**Azure SQL database**  
**PaaS**

**Here the infrastructure is managed for you**

**Backups are managed for you**

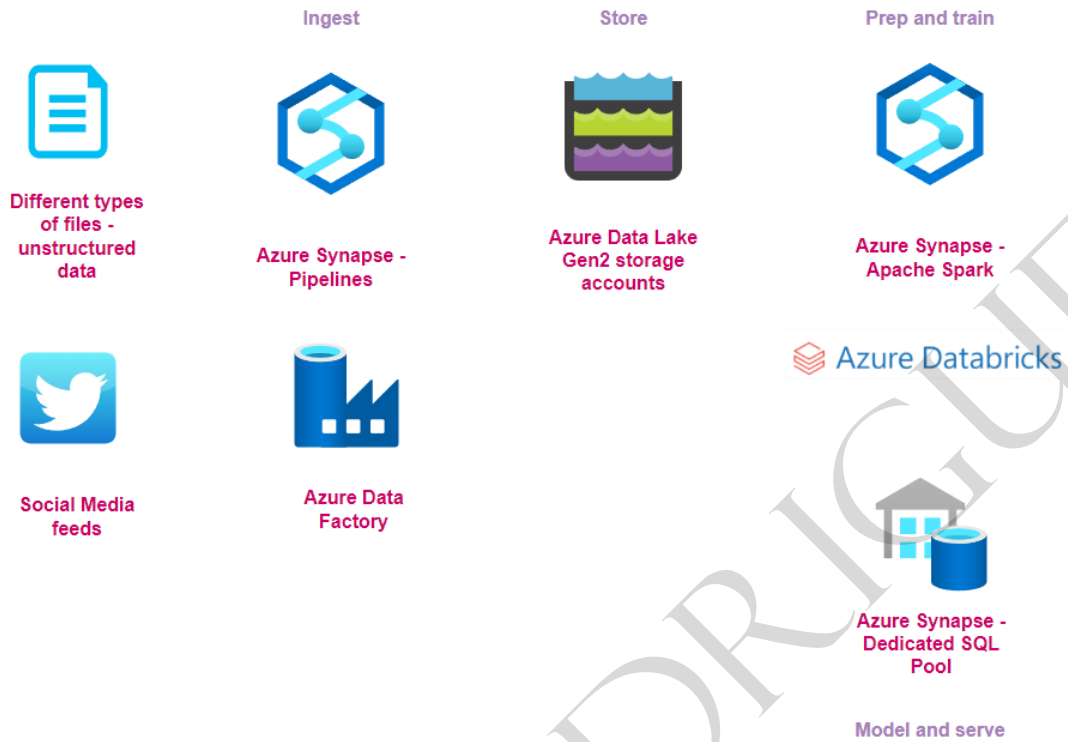
**You get built-in high availability**



**Virtual Machine**

## Enterprise Data warehouse architecture

## Enterprise Data Warehouse Architecture



## About Azure Cosmos DB



### Azure Cosmos DB

Fully Managed NoSQL database

You get single-digit millisecond response times

Scales automatically based on demand

SQL API

MongoDB

Gremlin

Cassandra

Table

**Database  
account**

**Database**

**Container**

**Items**

Azure SQL Database vs Cosmos DB



**Azure SQL Database**



**When you need to have relationships between tables**

**When you want to have constraints like foreign key constraints**



**Azure Cosmos DB**

**NoSQL data store**

**Flexible schemas**

**No need of joins between data structures**

A sample architecture - use case 1

ALAN RODRIGUES



Web Application



Database server



Web Application



Azure SQL Database



Azure Web App



Database server

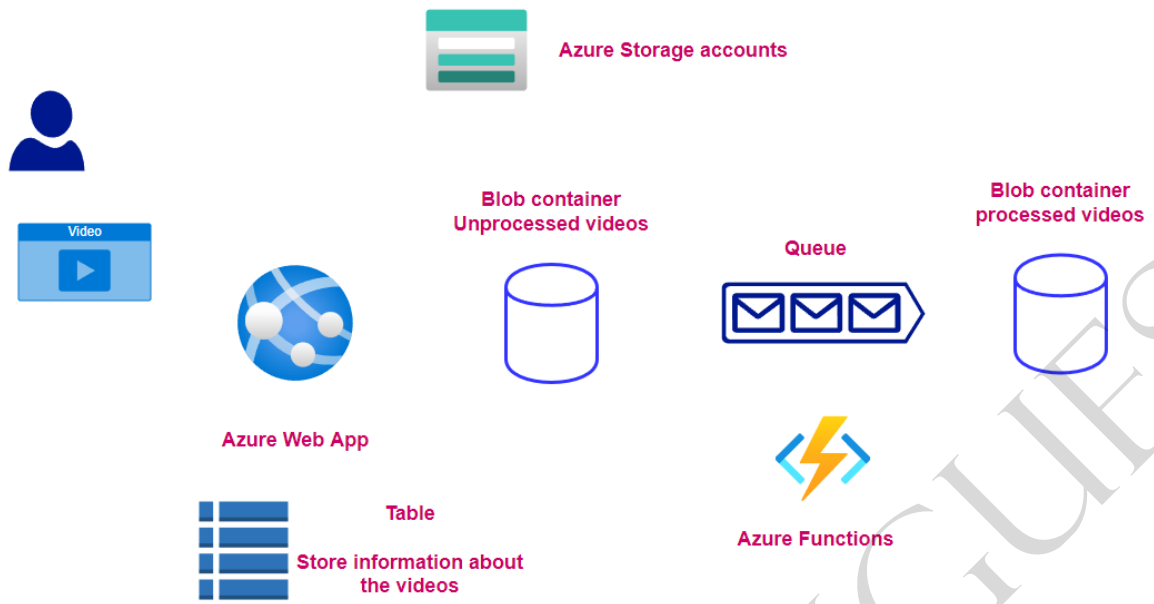


Azure Web App



Azure SQL Database

A sample architecture - use case 2

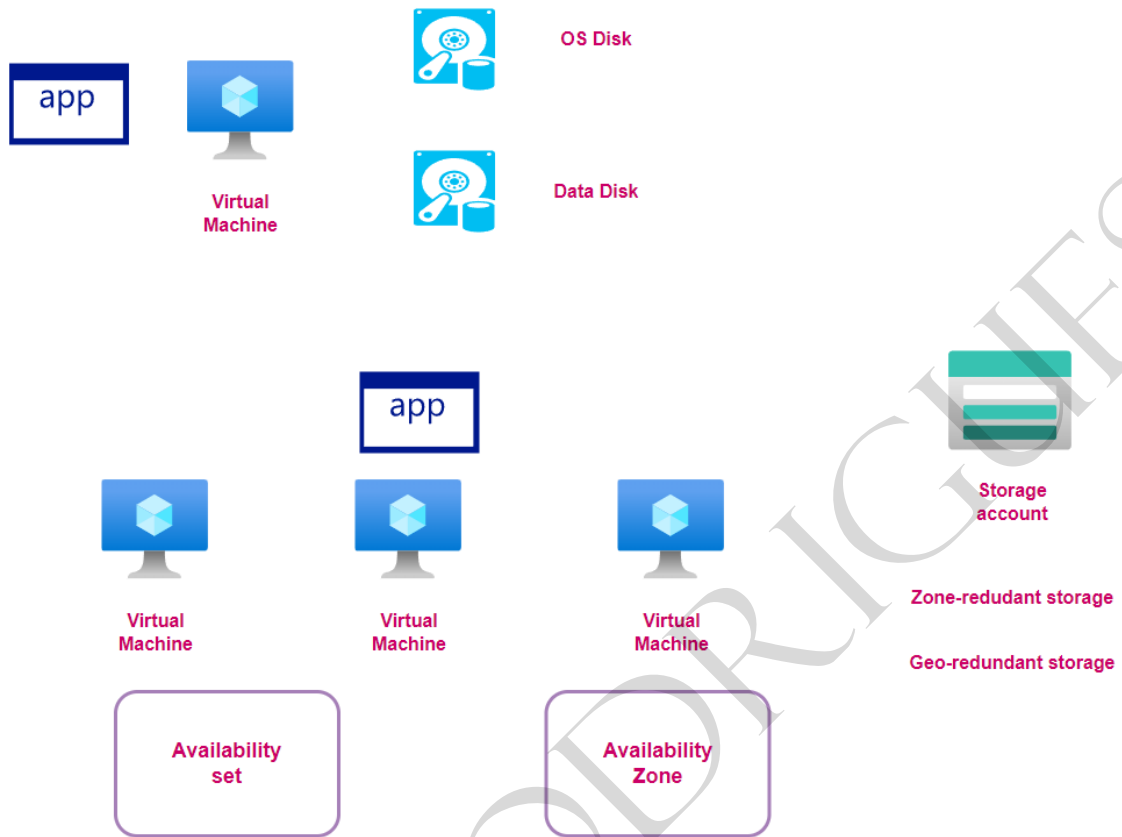


Describe cloud concepts

ALAN RODRIGUES

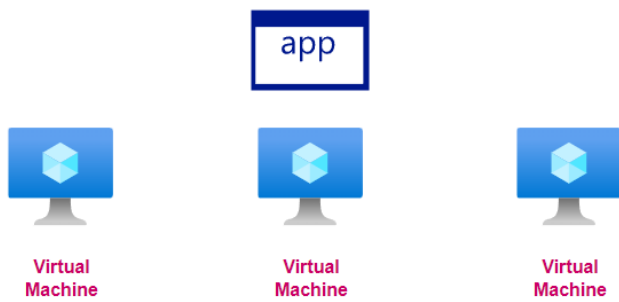
## Benefits of the cloud - High Availability

### High Availability



## Benefits of the cloud – Scalability

### Scalability



You don't need to worry about the underlying storage

It will grow automatically



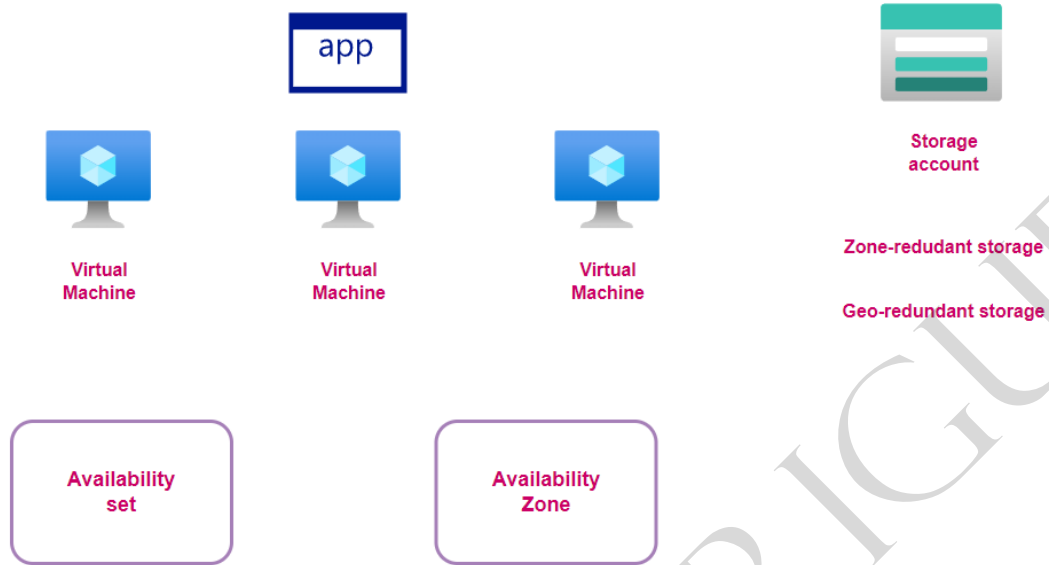
### Benefits of the cloud - Disaster recovery

#### Disaster Recovery



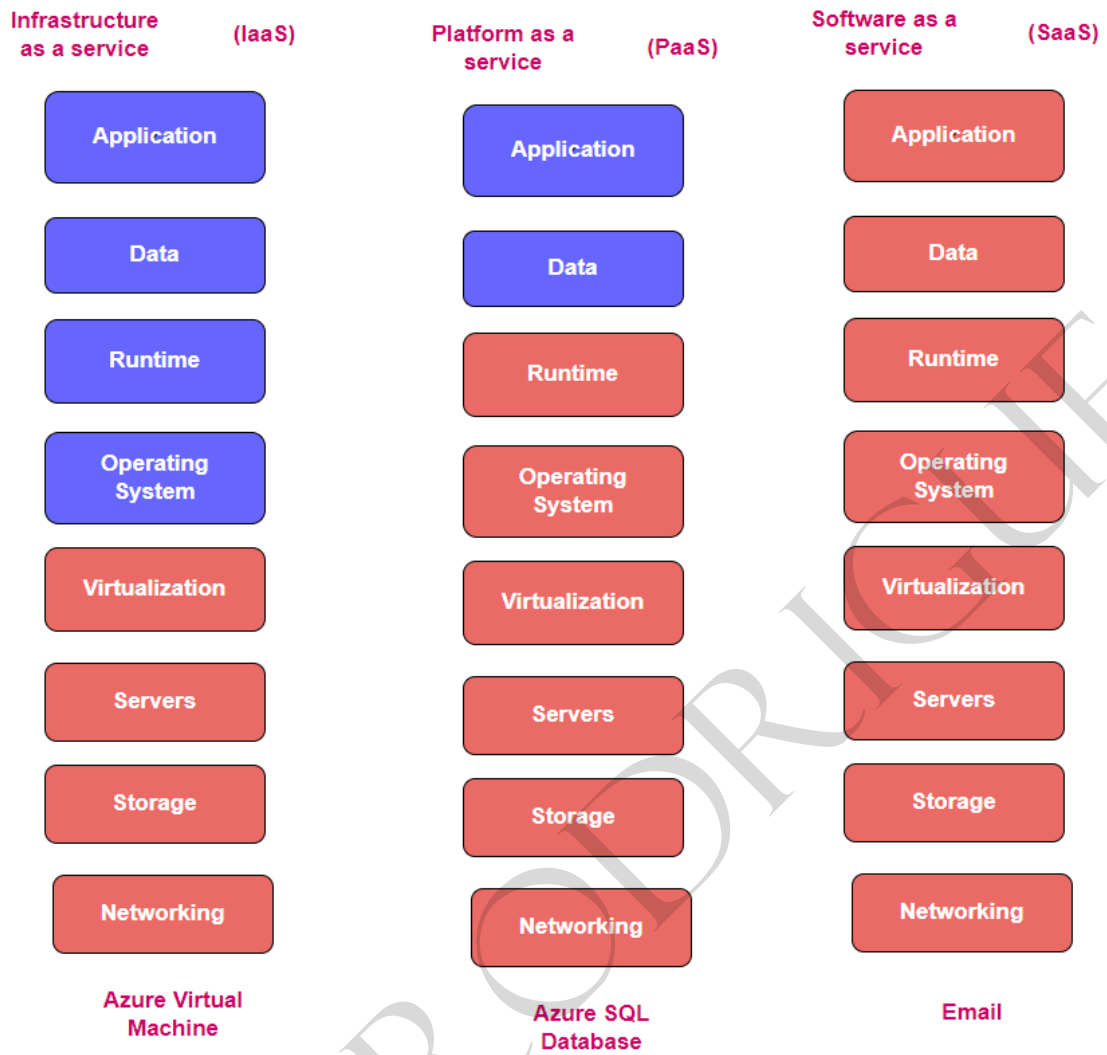
## Benefits of the cloud - Fault tolerance

### Fault tolerance



ALAN RODRIGUES

# Cloud service model



# Cloud model types

## Cloud Model types

**Public Cloud**

**Private Cloud**

**Hybrid Cloud**

**Public Cloud**



**Private Cloud**



**Hybrid Cloud**



# Describe Azure architecture and services - Other services

## Azure Traffic Manager

### Azure Traffic Manager

This is a DNS-based traffic load balancer.

You can distribute traffic to public facing applications across different Azure regions.

You can direct traffic based on different routing methods.



Azure Traffic Manager Profile

Priority Routing Method



North Europe

Azure Web App



UK South

Azure Web App



Azure Traffic Manager Profile

Weighted Routing method



North Europe

Azure Web App



UK South

Azure Web App

# Azure Content Delivery Network

## Azure CDN

### Content Delivery Network

Helps to deliver content to users across the globe by placing content on physical nodes placed across the world



East US



North Europe



Web Application

Central US

ALAN RODRIGUES



**East US**



**CDN Profile**

**Global level**

**Endpoint**



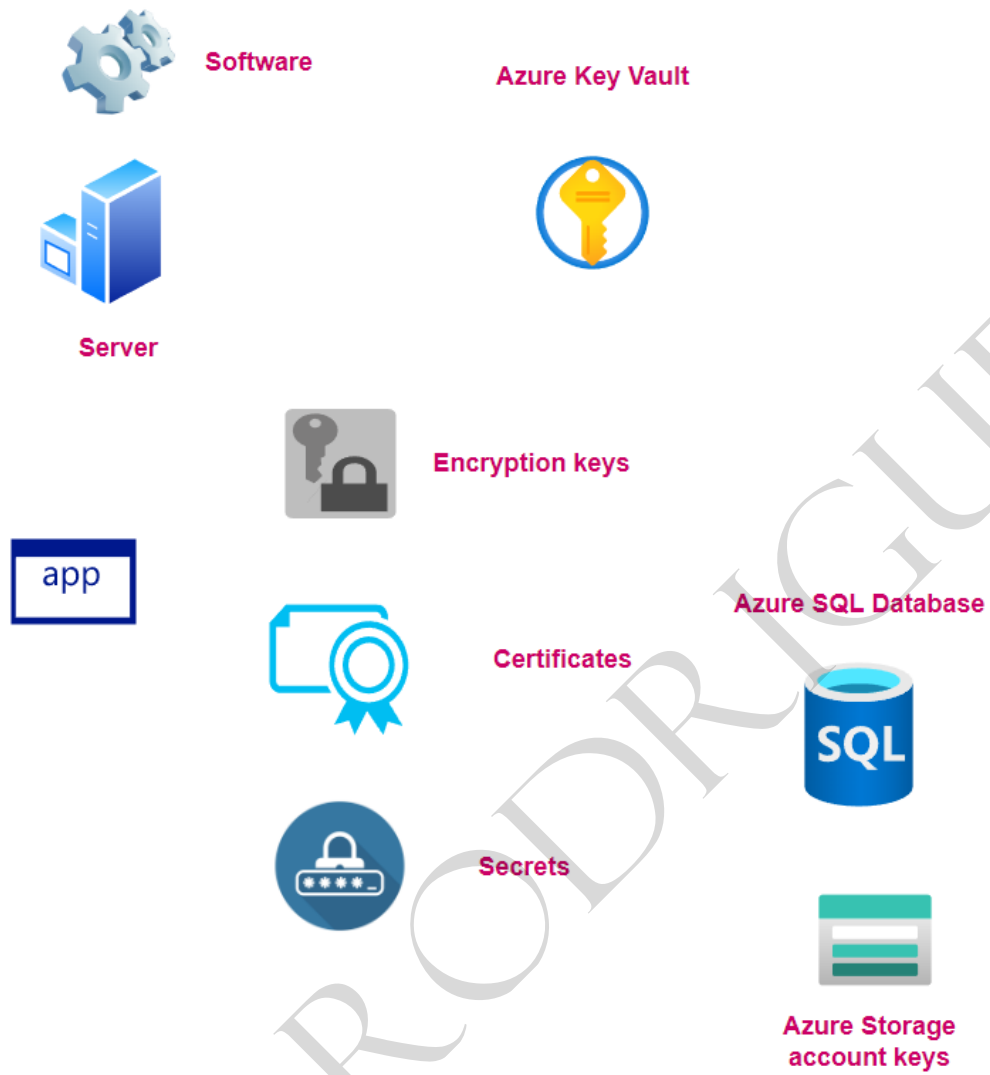
**Web Application**

**Central US**

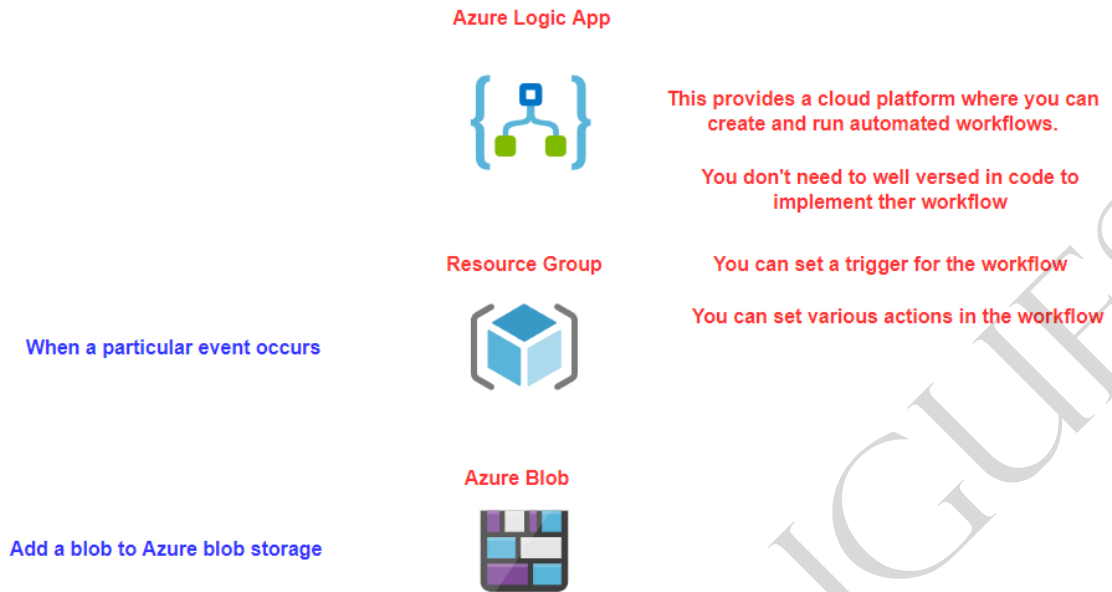
**Source**

1. The user in the **East US** location makes a request to the **CDN endpoint**
2. The **CDN** checks whether the **Point of presence** location closest to the user has the requested file.
3. If not a request is made to the source to get the required file.
4. A server in the **Point of presence** location will then cache the required file.
5. The server will also send the file to the user.
6. Subsequent users from the same location will now be served the file from the server in the point of presence location.

# Lab - Azure Key Vault



## Azure Logic Apps



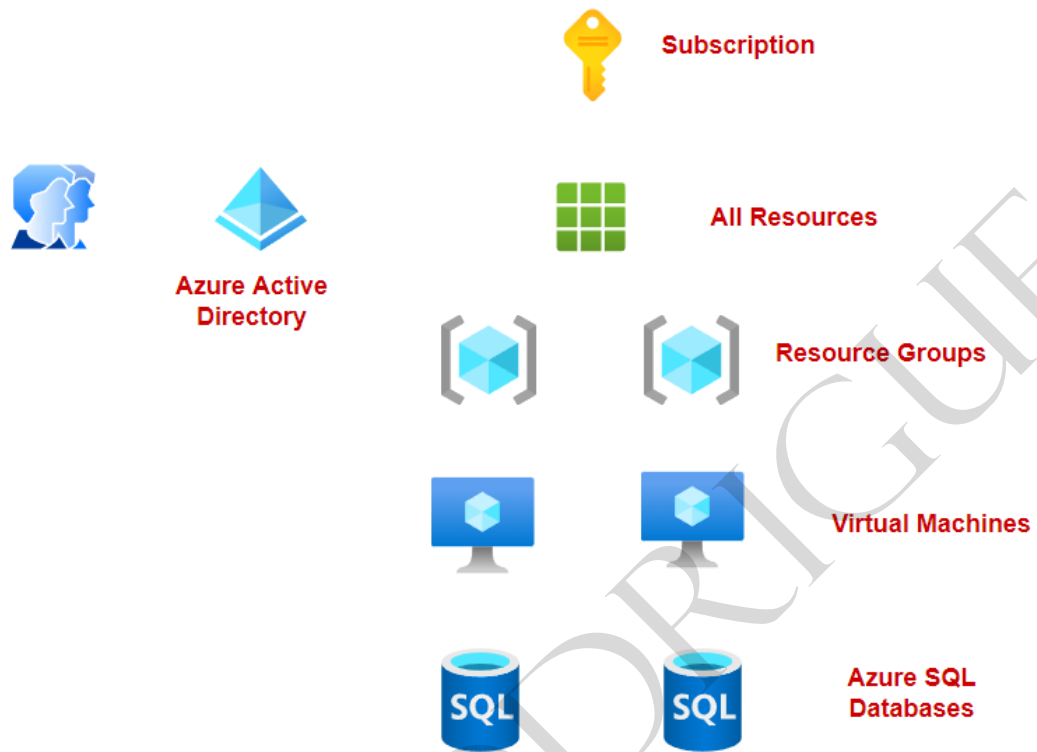
## Describe Azure architecture and services - Identity and Access

### Azure Active Directory

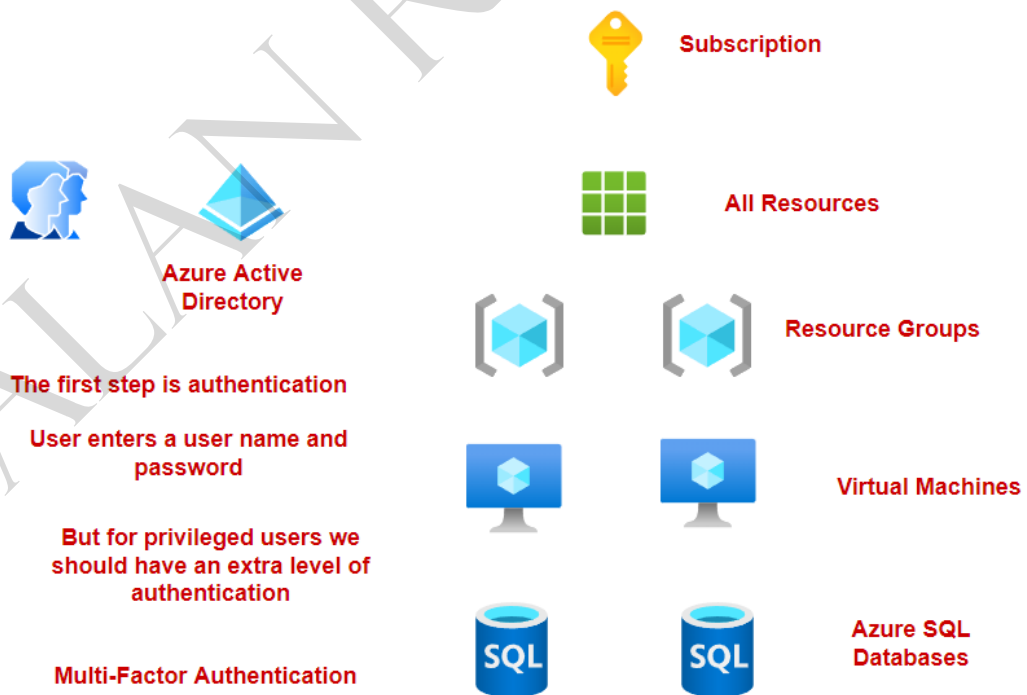


# Role Based Access Control

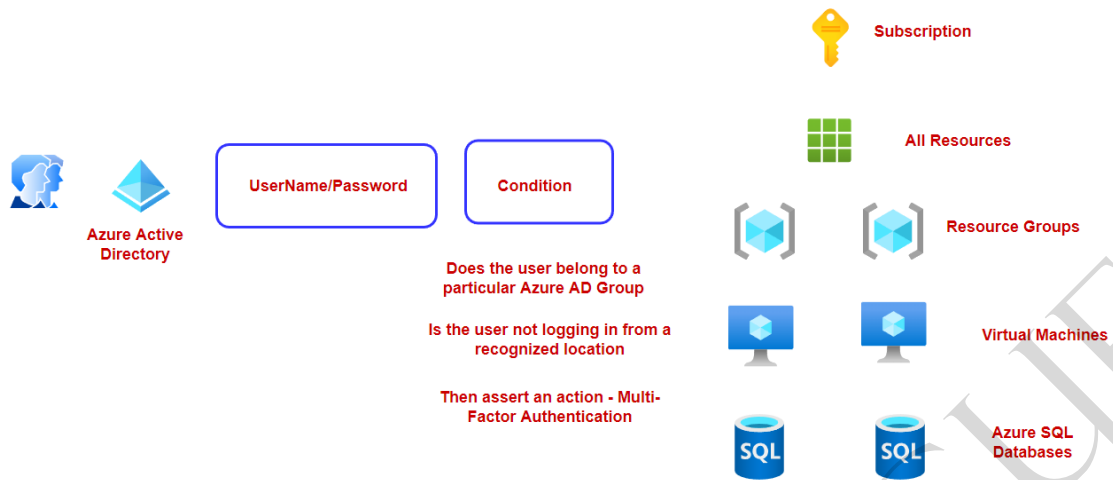
## Role-based access control



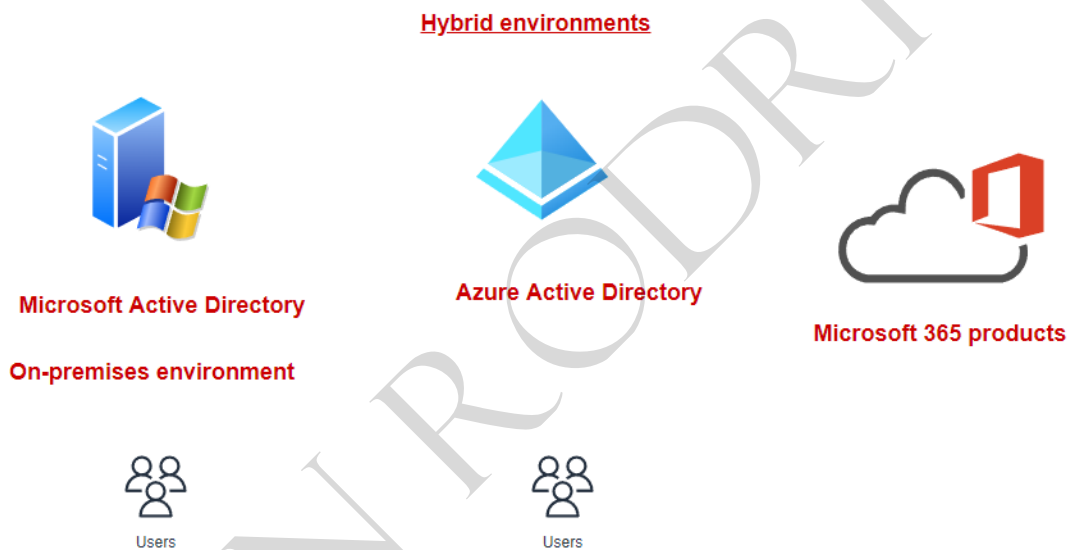
## Lab - Multi-Factor Authentication



## Conditional Access Policies



## Hybrid environments – Identities





Microsoft Active Directory

On-premises environment



Users



Azure AD Connect



Azure Active Directory



Users

**Azure AD Domain Services**

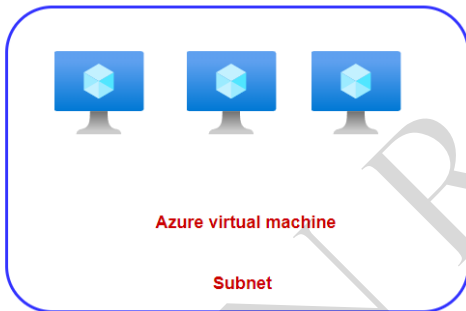
This gives you the option of hosting the full version of Microsoft Active Directory as a managed software on the cloud.

You get the options of domain join, group policy, lightweight directory access protocol and Kerberos/NTLM authentication.

Microsoft Sentinel



Azure virtual network



Log Analytics workspace



Microsoft Sentinel

Security Information and Event Management  
Security Orchestration , automation and response

1. Collect data

2. Detect threats

3. Respond and investigate threats

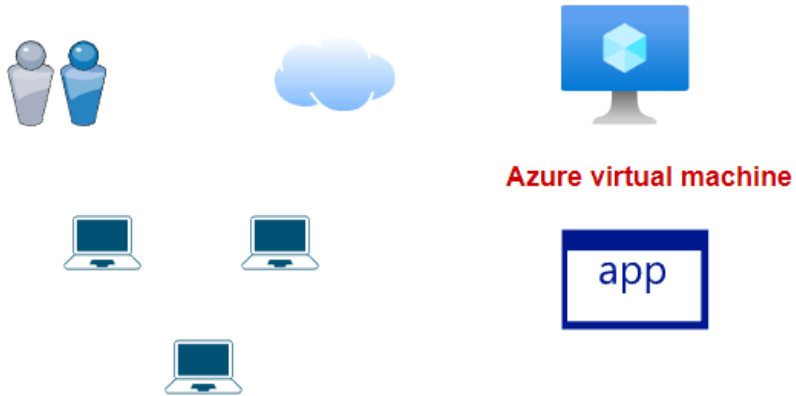


Azure Activity Log



Azure Active Directory sign-ins

## Azure DDoS protection



**DDoS attack**

**Distributed Denial of Service**

**Here the systems are trying to  
flood the target with traffic**

**Azure DDoS protection**

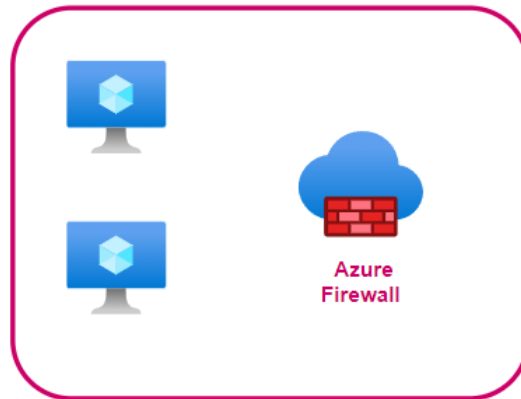
**Service helps to protect resources in an Azure virtual network  
against DDoS attacks**

ALAN RODRIGUES

## Azure Firewall



Virtual  
Network

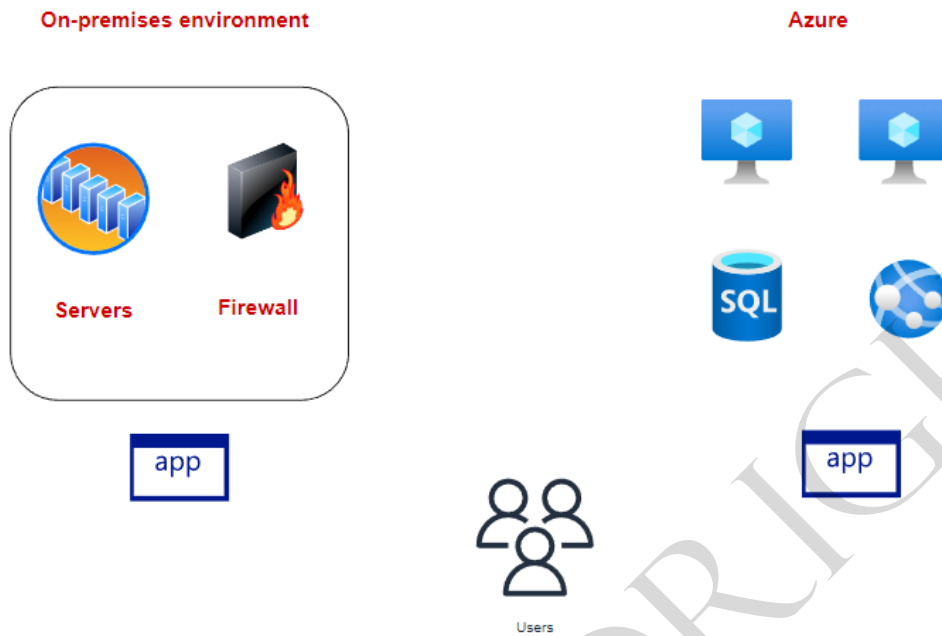


Internet

1. Has built-in high availability
2. Can deploy the Azure Firewall Instance across two or more Availability zones - 99.99% SLA
3. You can filter traffic based on fully-qualified domain names
4. You can also create network filtering rules - Based on source and destination IP address, port and protocol
5. It is stateful in nature, so it understands what packets of data to allow
6. It has built-in Threat Intelligence - Here you can get alerts or deny traffic from/to malicious IP addresses and domains

# Concept of Zero Trust

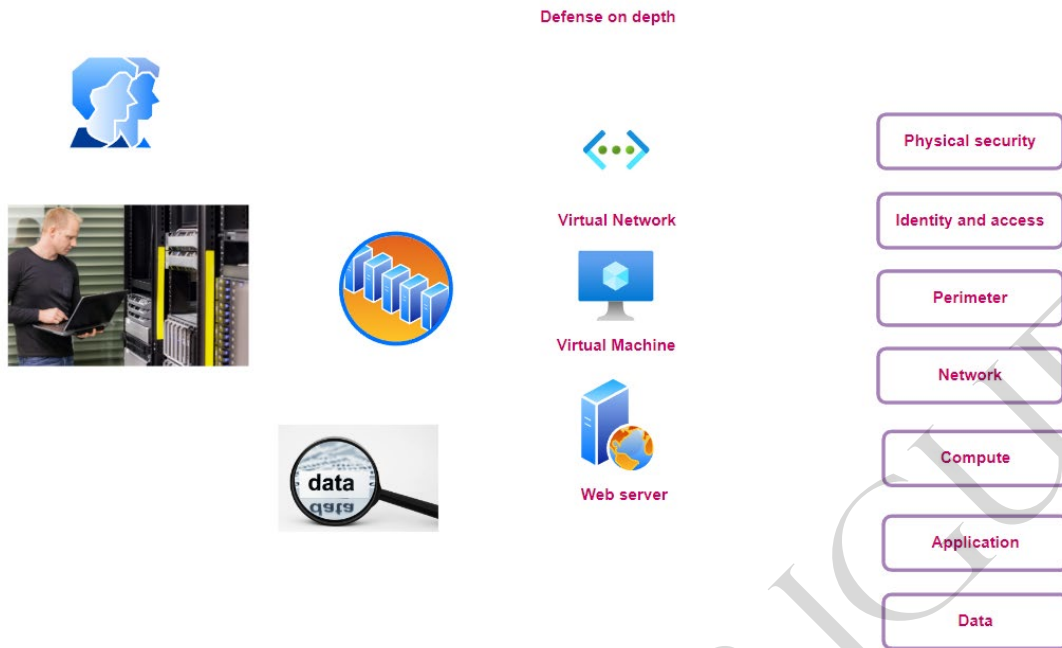
## Zero trust



### Foundation principles

1. Verify explicitly - Ensure to always authenticate and authorize users
2. Use least access privileges wherever possible
3. Assume breach - Understand your surface area when it comes to threats , look at threat intelligence.

## Defense on Depth



Describe Azure management and governance

## Management Groups

Role-based access control

Azure Policies



Tenant Root group



Management Groups



Subscriptions



Resource groups



Resources

## Azure Blueprints



Azure Blueprints

Orchestrate the deployment of artifacts to Azure

ARM Templates



Azure Policies



Resource Groups



Role-based access control



Management Groups



Subscriptions

## Lab - ARM templates



Azure virtual network



Azure virtual machine



Azure virtual machine



Azure SQL database



Azure Web App

You define your infrastructure as code

Create an Azure Resource Manager template

This is a JavaScript Object Notation file that actually contains the definition of the infrastructure

You can store the ARM templates in your source code repository along with your application code

Microsoft has also release a new language called Bicep that has the same capabilities as ARM templates.

Bicep just uses a syntax that is easier to use.

Azure Monitor service

**Azure Monitor**



**Azure virtual machine**



**Azure Monitor**

**CPU Utilization**

**Network utilization**



**Azure Monitor alerts**

**If the CPU utilization goes beyond a particular threshold**

## Lab - Log Analytics

### Azure Monitor



Azure virtual machine



Azure Monitor

CPU Utilization

Network utilization



Azure Monitor alerts

If the CPU utilization goes beyond a particular threshold



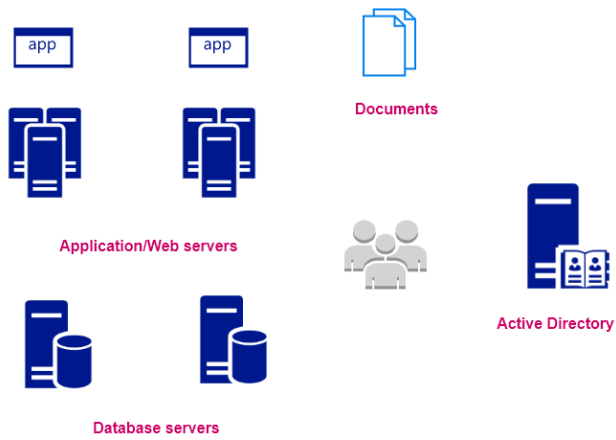
Log Analytics workspace

You can send other performance data and log data to a Log Analytics workspace

Putting everything together

Understanding your requirements

### Understanding your requirements

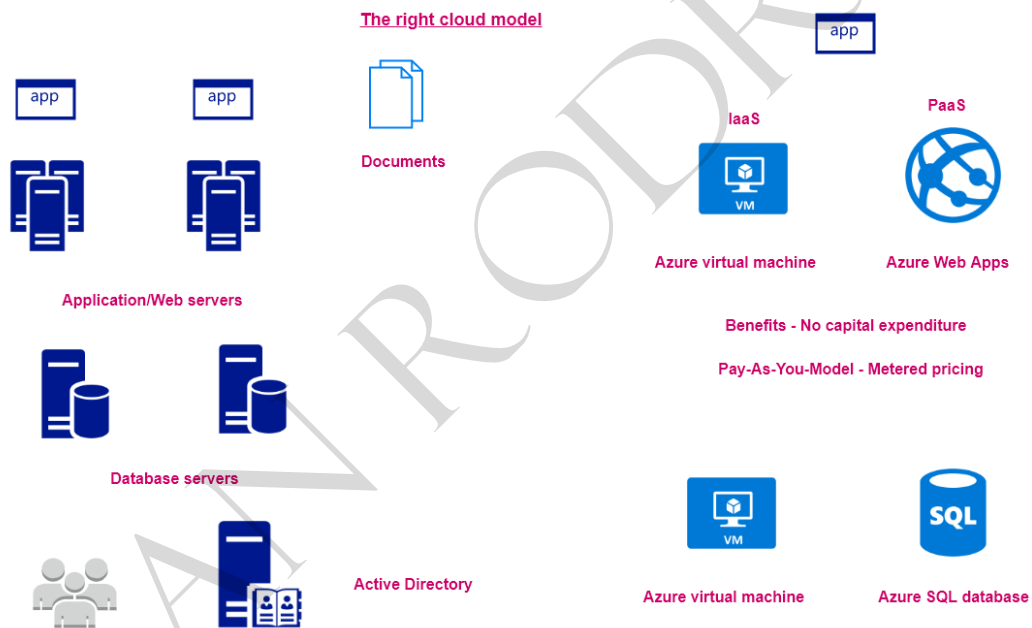


You want to migrate some of the workloads onto Azure

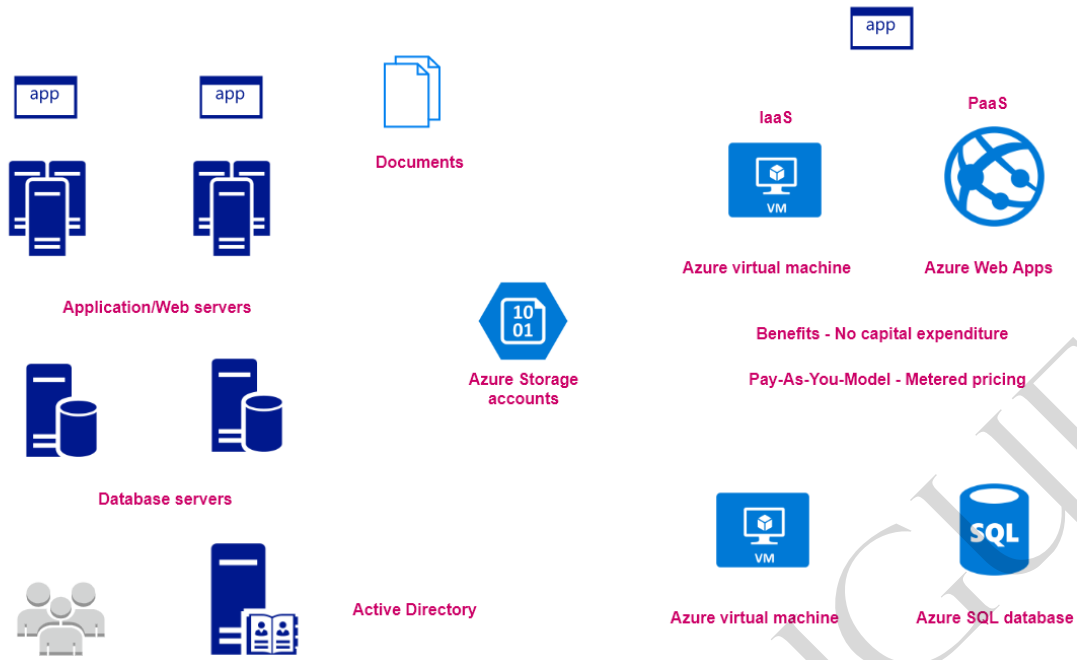
Some workloads will continue to remain in the on-premises data center

Applications in the on-premises data center must be able to talk to applications in Azure

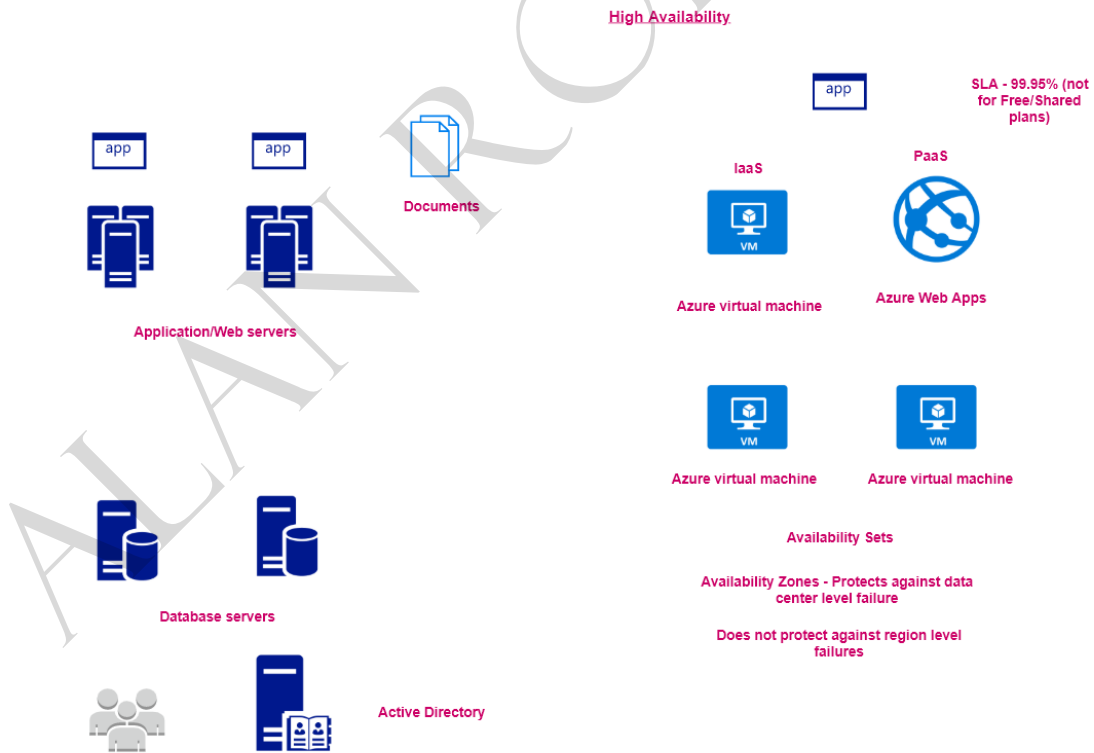
### Choosing the right cloud model



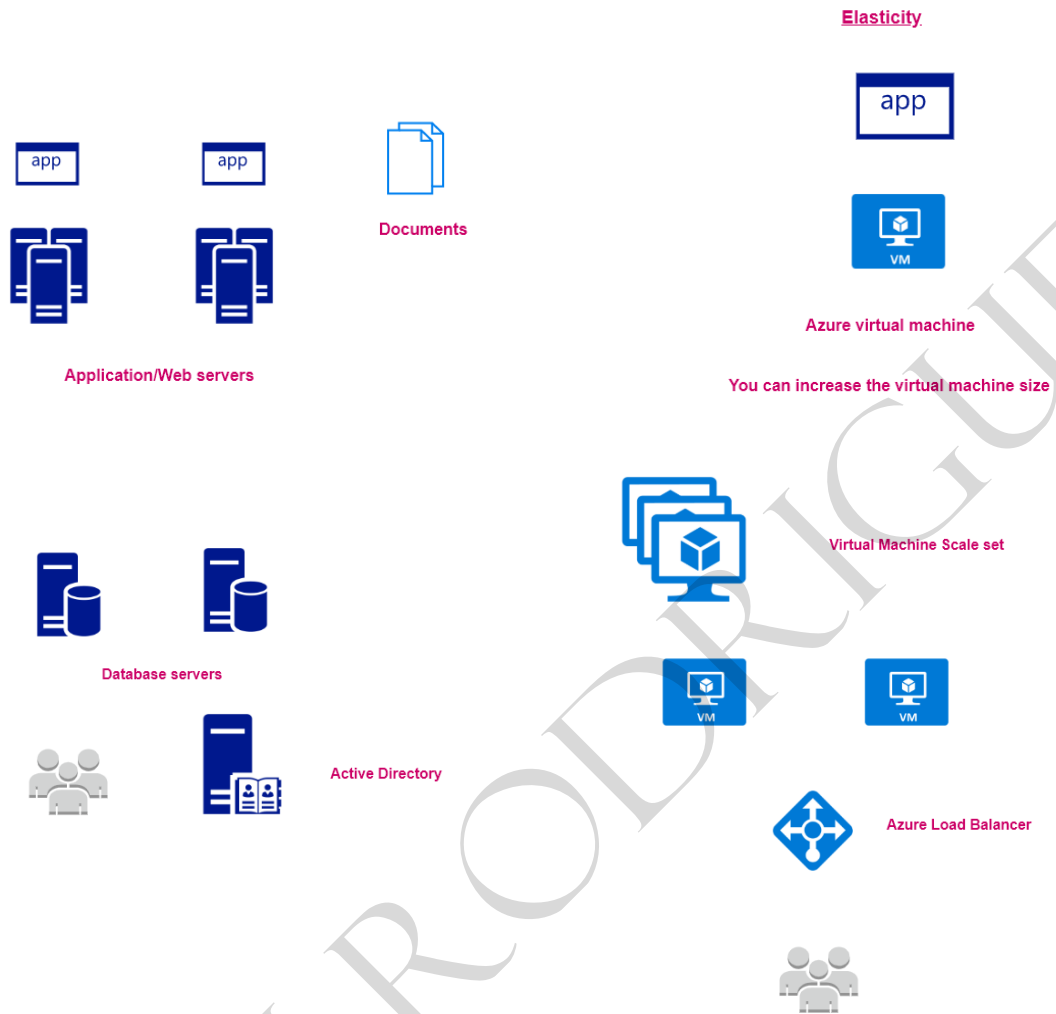
Storing user documents



## High Availability

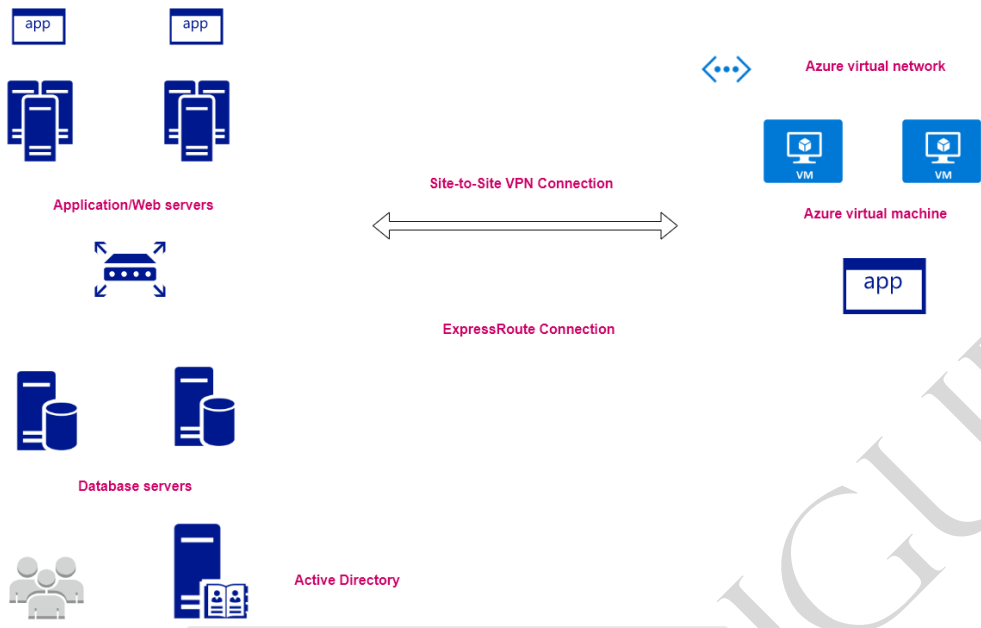


# Elasticity



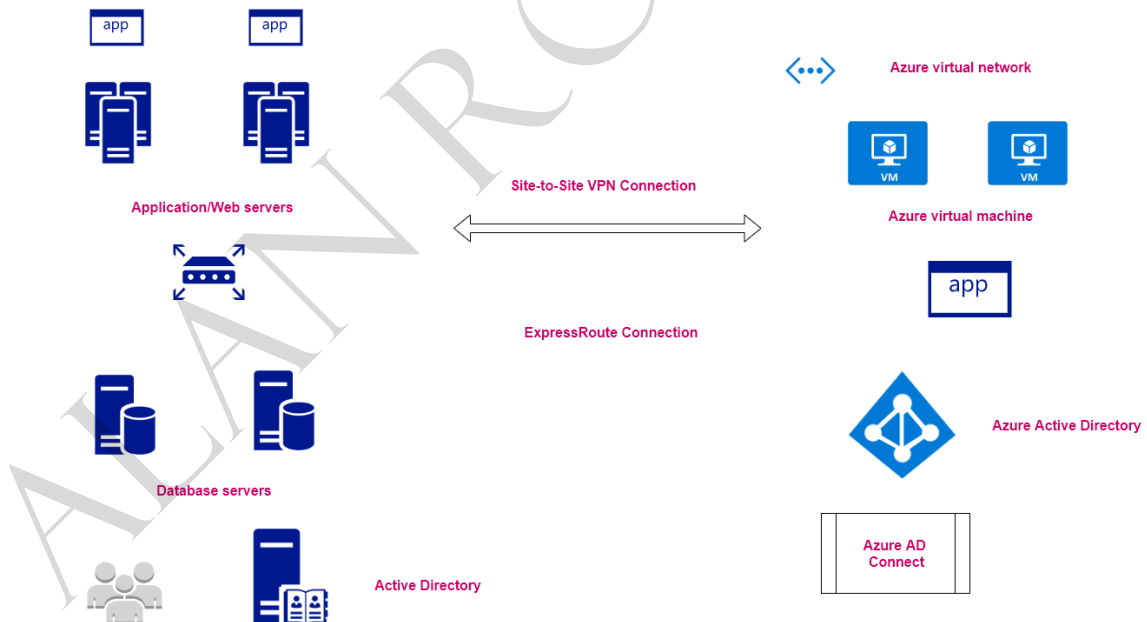
Connecting data center to Azure

Connecting your networks together



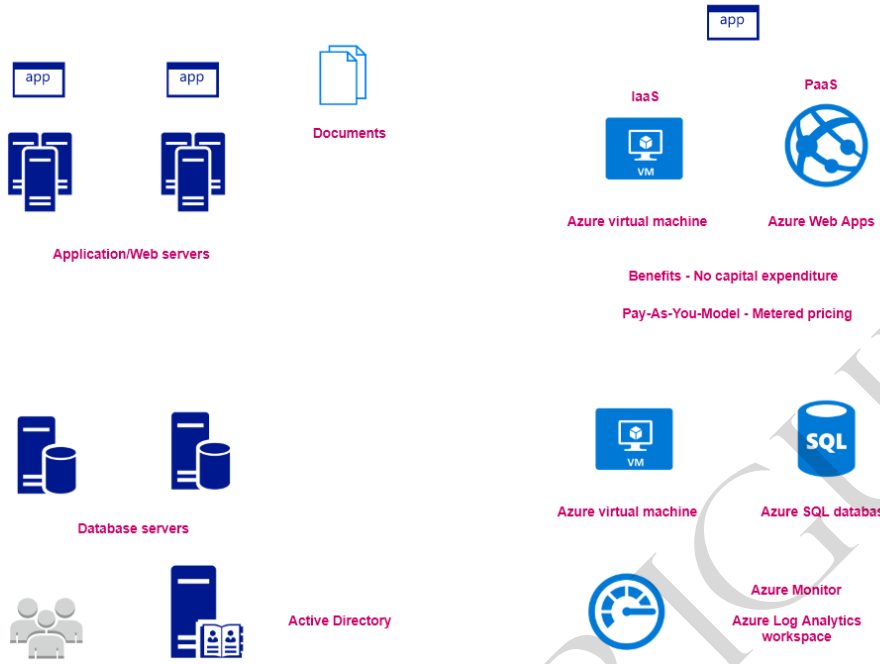
The user identities

Connecting your networks together



Monitoring your infrastructure

Monitoring your infrastructure



ALAN RODRIGUES