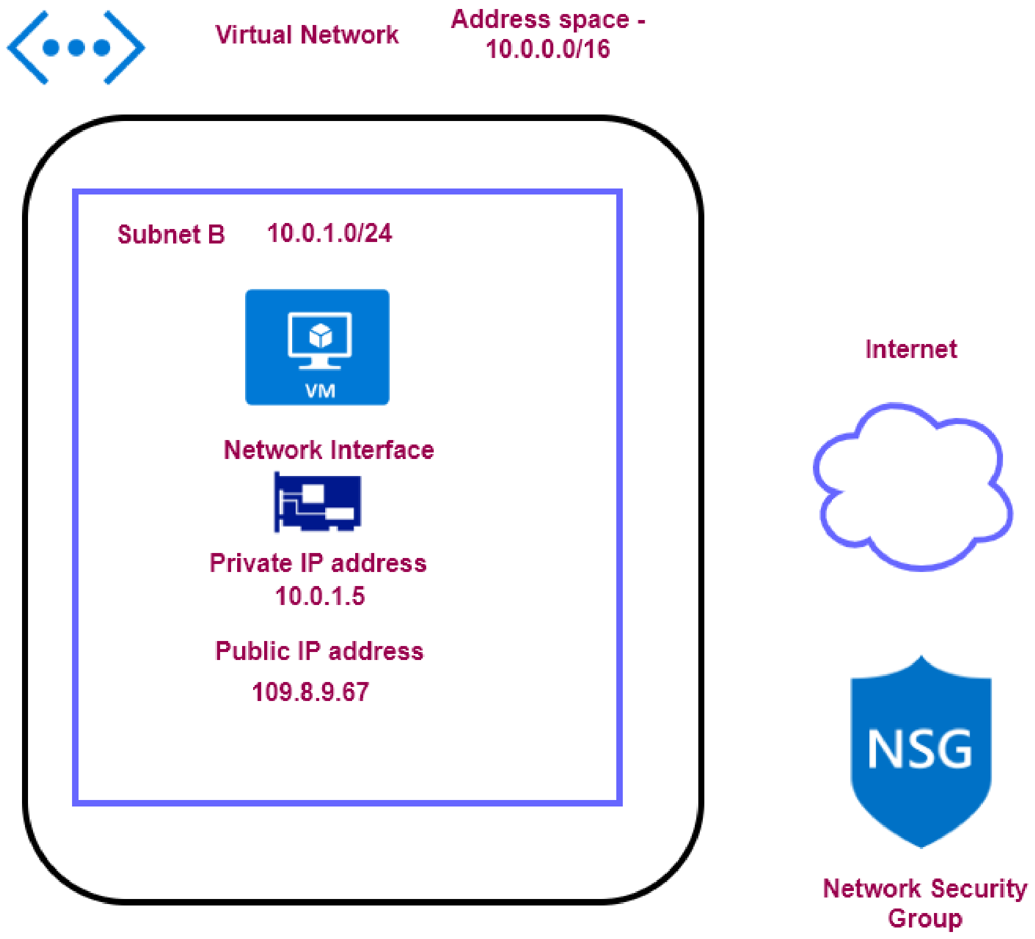
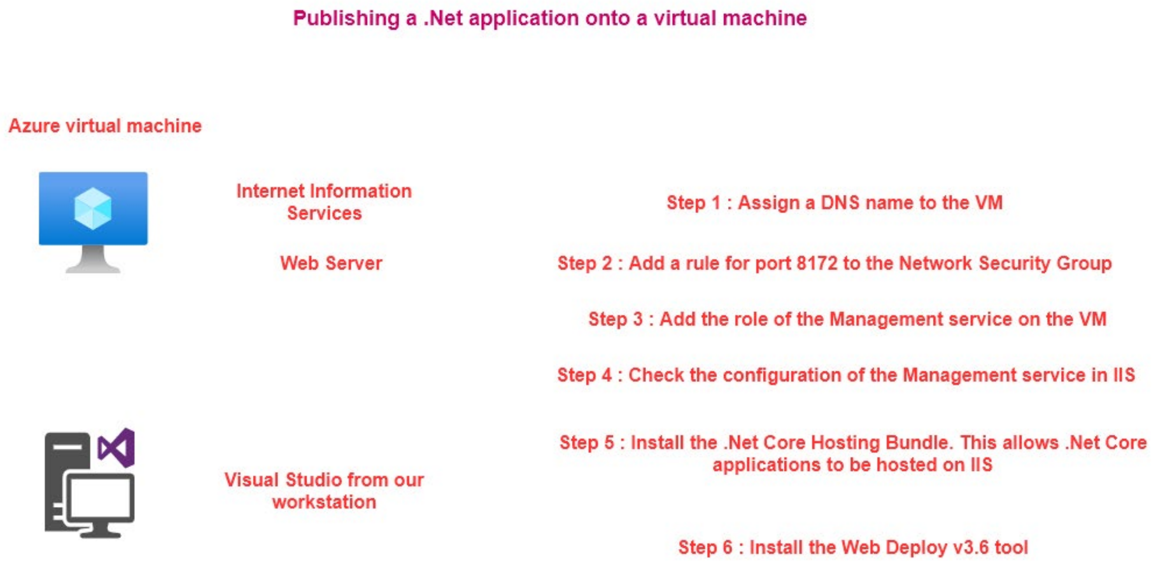
Design Monitoring

The basics about an Azure virtual machine

- The machine needs to be part of an Azure virtual network.
- The network is used to isolate workloads on the cloud
- The virtual machine has a network interface that is used for routing of traffic
- With the help of the public IP address, one can contact the VM over the Internet
- The NSG or Network Security Group is used to filter inbound and outbound traffic from the virtual machine



General steps for publishing a web application onto an Azure virtual machine



Publishing a .Net application onto a virtual machine

Azure virtual machine

Internet Information Services

Web Server

Visual Studio from our workstation

Step 1 : Assign a DNS name to the VM

Step 2 : Add a rule for port 8172 to the Network Security Group

Step 3 : Add the role of the Management service on the VM

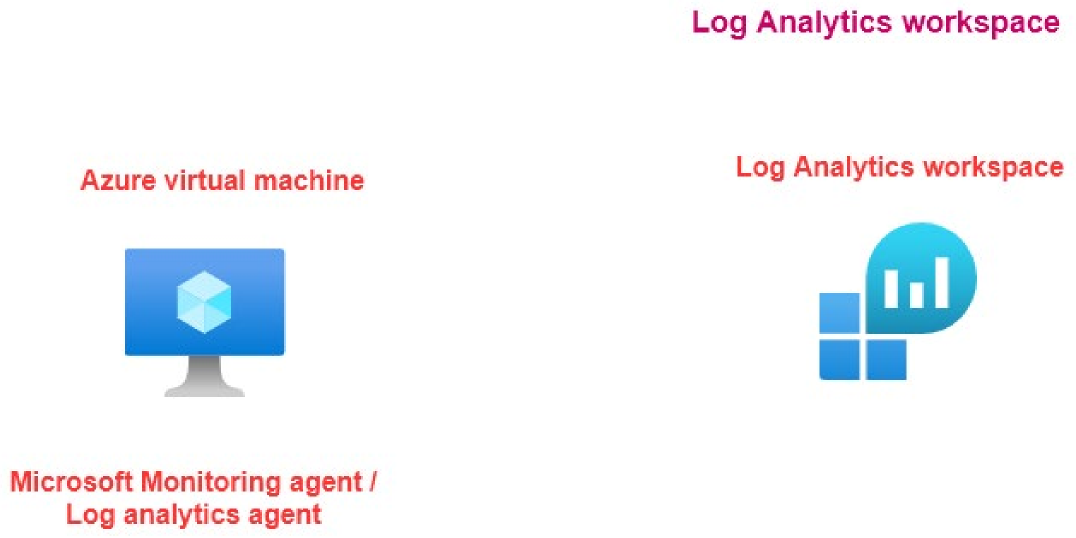
Step 4 : Check the configuration of the Management service in IIS

Step 5 : Install the .Net Core Hosting Bundle. This allows .Net Core applications to be hosted on IIS

Step 6 : Install the Web Deploy v3.6 tool

Log Analytics workspace

- The Log Analytics workspace is used as a central logging solution.
- You have to ensure the agent is installed on the virtual machine



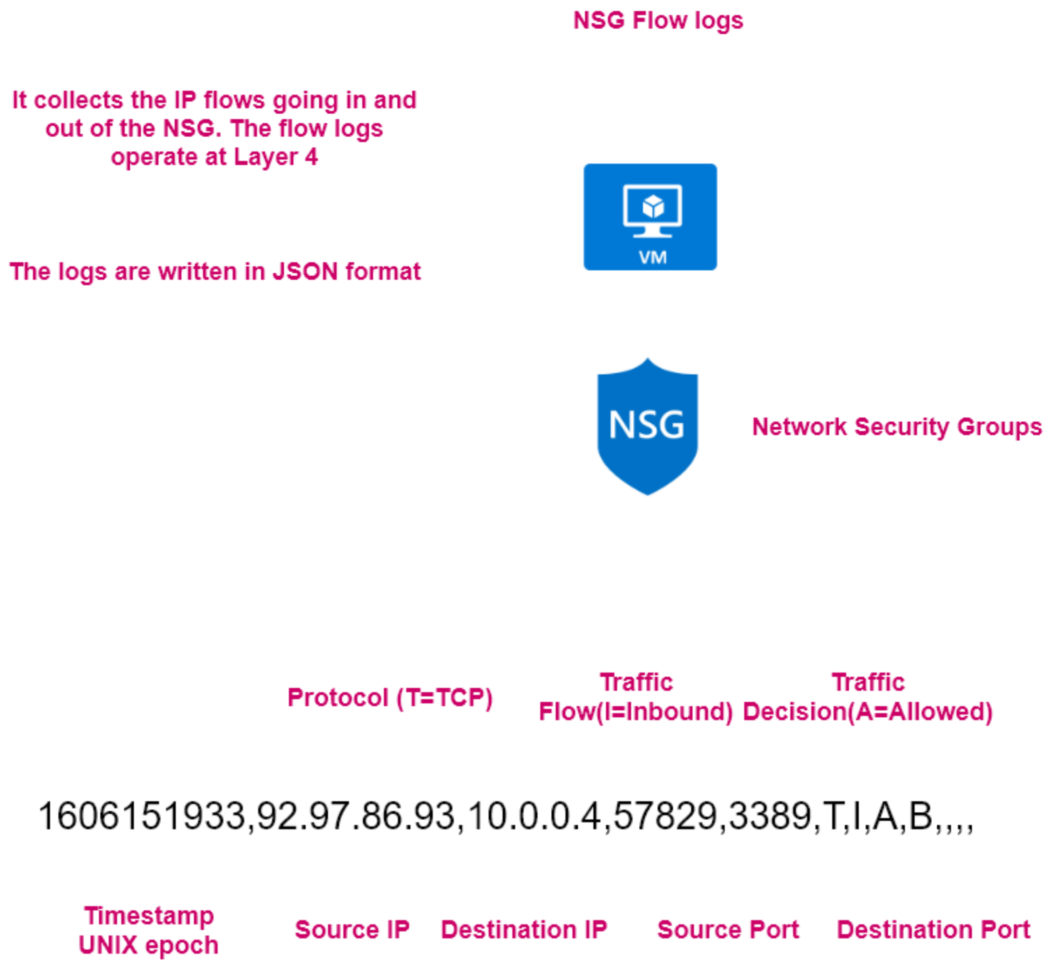
Log Analytics workspace

Azure virtual machine

Log Analytics workspace

Microsoft Monitoring agent / Log analytics agent

NSG Flow Logs



NSG Flow logs

It collects the IP flows going in and out of the NSG. The flow logs operate at Layer 4

The logs are written in JSON format

Network Security Groups

Protocol (T=TCP)

Traffic Flow(I=Inbound)

Traffic Decision(A=Allowed)

```
1606151933,92.97.86.93,10.0.0.4,57829,3389,T,I,A,B,,,,
```

Timestamp UNIX epoch

Source IP

Destination IP

Source Port

Destination Port

Application Insights

- Application Performance Management service for web developers.
- You can use this tool to monitor your applications.
- It can help developers detect anomalies in the application.
- It can help diagnose issues.
- It can also help understand how users use your application.
- It also helps you improve performance and usability of your application.

- **How does it work**
- You install a small instrumentation package within your application.
- You can see the statistics of your application locally in Visual Studio as you run your application.
- You can also use the Application Insights resource in Azure to monitor your application.

- **What are the different aspects monitored by Application Insights**
- Request rates, the response times and failure rates – This is done at the page level.
- Exception recorded by your application.
- Page views and their load performance as reported from the user's browser.
- User and session counts.
- Performance counters of the underlying Windows or Linux Machines.
- Diagnostic trace logs from your application.
- Any custom events or metrics that the developer writes themselves in the code.

- Understanding how your users use the application
- **Funnels** – You can create a funnel from one stage to another stage of your application.
- You can then see how users are progressing through the stages of the funnel.
- **User Flows** – This helps visualize how users navigate between pages in your site. This can help answer question such as
  - Does the user navigate away from a page on your site

  - What do users click on a page on your site
  - Where are the places where users churn most on your site
  - Are there places where users repeat the same action over and over

- **Impact** – This helps decide if a page is having an impact on your application.
- It can help answer the question as to whether the page load time is impacting how many people convert on a page in the application.
- **Retention** – This helps you understand how many users return to your application.
- It can also help understand if users are able to perform certain tasks in your application.

Smart Detection and Continuous Export in Application Insights

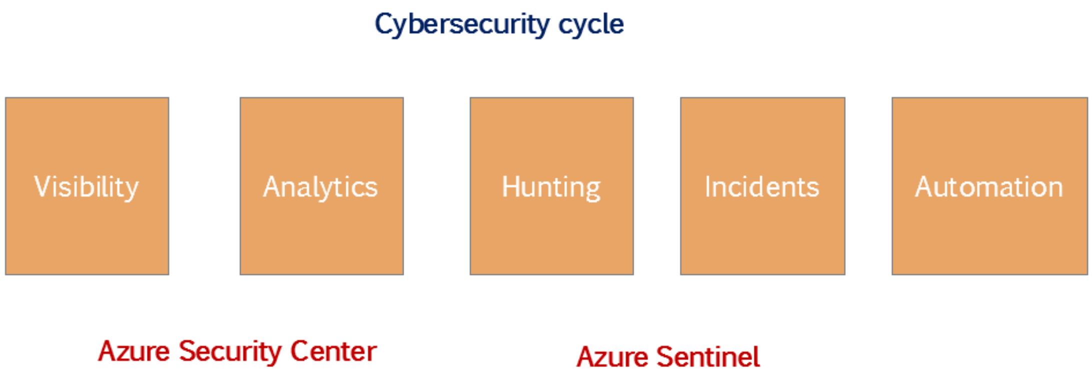
- This is an in-built feature that is available in Application Insights.
- Based on the telemetry data that is sent onto Application Insights, it can detect potential performance problems and failure anomalies in the web application.
- It uses machine learning to look at the data and then send alerts based on different conditions
- Continuous Export - This allows you to send the data collected by Application Insights into an Azure storage account.

Azure Sentinel

- This is a cloud service that provides a solution for SEIM (Security Information Event Management) and SOAR (Security Orchestration Automated Response)

- This provides a solution that helps in the following
- Collection of data – Here you can collect data across all users, devices, applications and your infrastructure. The infrastructure could be located on-premise and on the cloud.
- It helps to detect undetected threats.
- It helps to hunt for suspicious activities at scale.
- It helps to respond to incident rapidly
- Once you start using Azure Sentinel, you can start collecting data using a variety of connectors.
- You have connectors for a variety of Microsoft products and other third-party products as well.
- You can then use in-built workbooks to get more insights on the collected data

Azure Sentinel vs Azure Security Center



Cybersecurity cycle

Visibility

Analytics

Hunting

Incidents

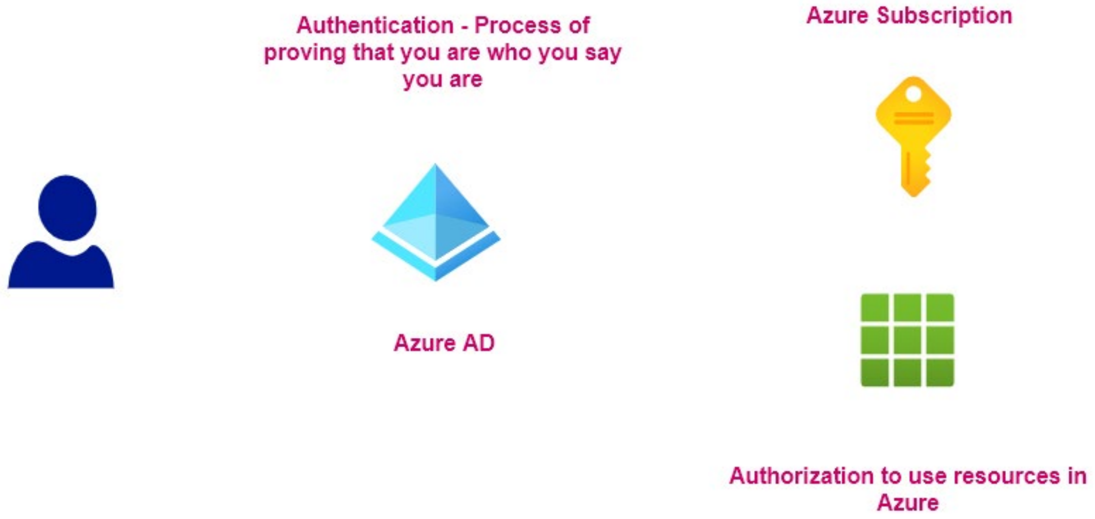
Automation

Azure Security Center

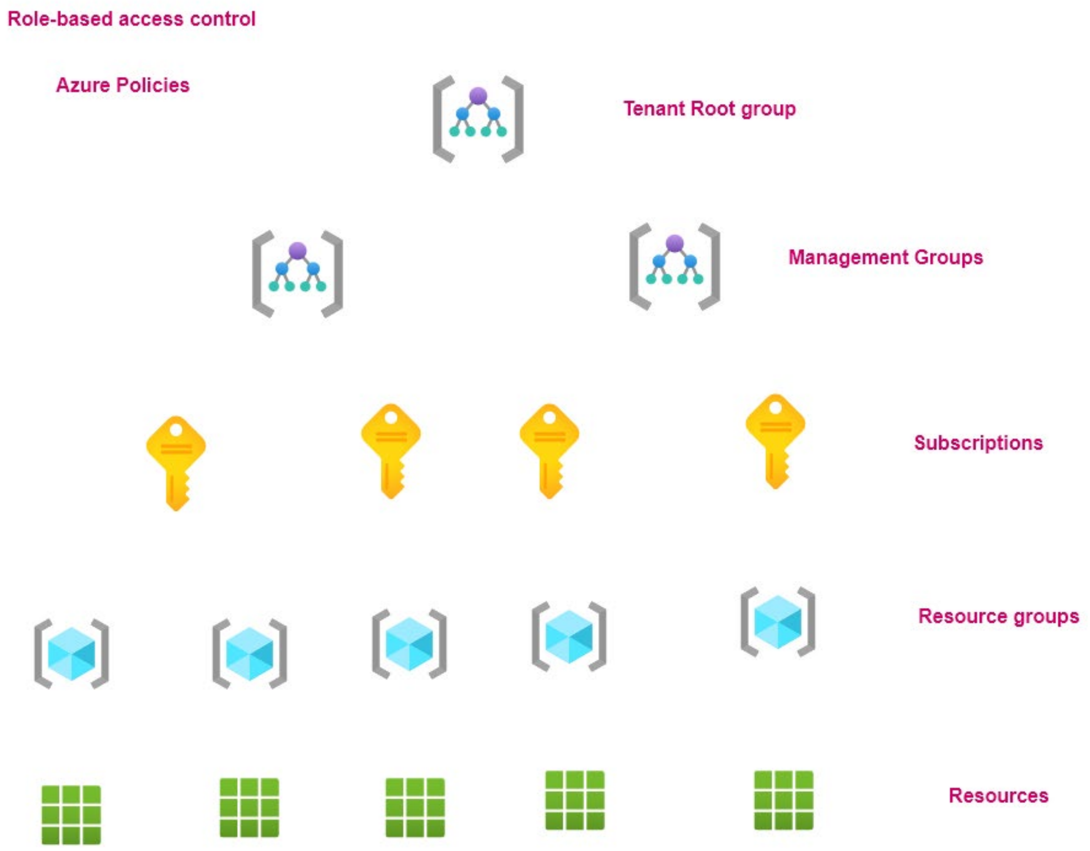
Azure Sentinel

Design Identity and Security

Authentication and Authorization


Authentication - Process of proving that you are who you say you are
Azure AD
Azure Subscription
Authorization to use resources in Azure

Authorization hierarchy



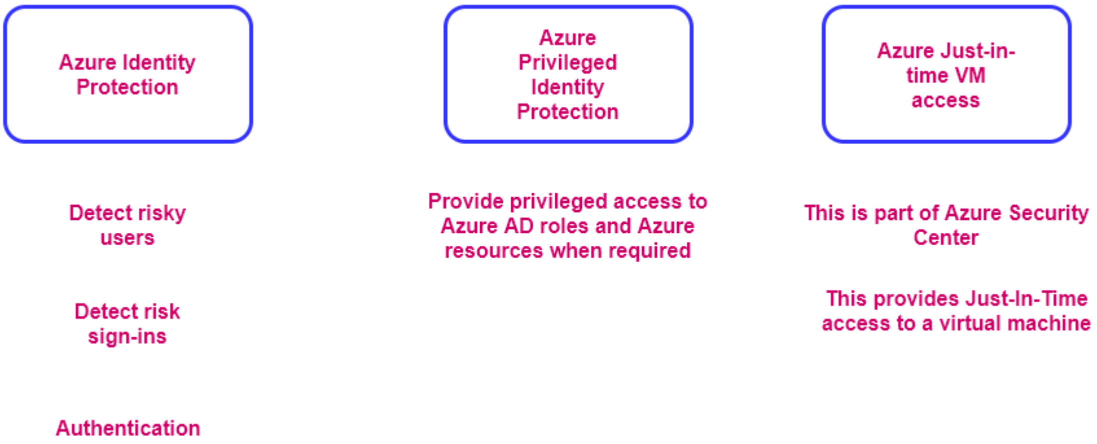
Azure Privileged Identity Management

- Using this service you can carry out the following activities
- Provide just-in-time privileged access to Azure AD and Azure resources.
- Assign time-bound access to resources using start and end dates.
- Require approval to activate privileged roles.
- Enforce multi-factor authentication to activate any role.
- Get notifications when privileged roles are activated.
- Conduct access reviews to ensure users still require the roles.
- This features requires the use of Azure AD Premium P2 licenses

Azure AD Identity Protection

- This is a tool that automates and remediates identity-based risks.
- Here Microsoft uses its in-built intelligence system to detect any identity-based risks.
- Different types of risks that can be detected
- **Anonymous IP address** – This happens when a user signs in from an anonymous IP address.
- **Atypical travel** – This happens if a user sign's in from a location that is not normally used by a user for the sign-in process.
- **Unfamiliar sign-in properties** – Here the sign-in properties are not the same as normally seen for the user.

Difference between Azure Identity Protection, Azure Privileged Identity Management and Just-In-Time VM access



Azure Identity Protection

Detect risky users

Detect risk sign-ins

Authentication

Azure Privileged Identity Protection

Provide privileged access to Azure AD roles and Azure resources when required

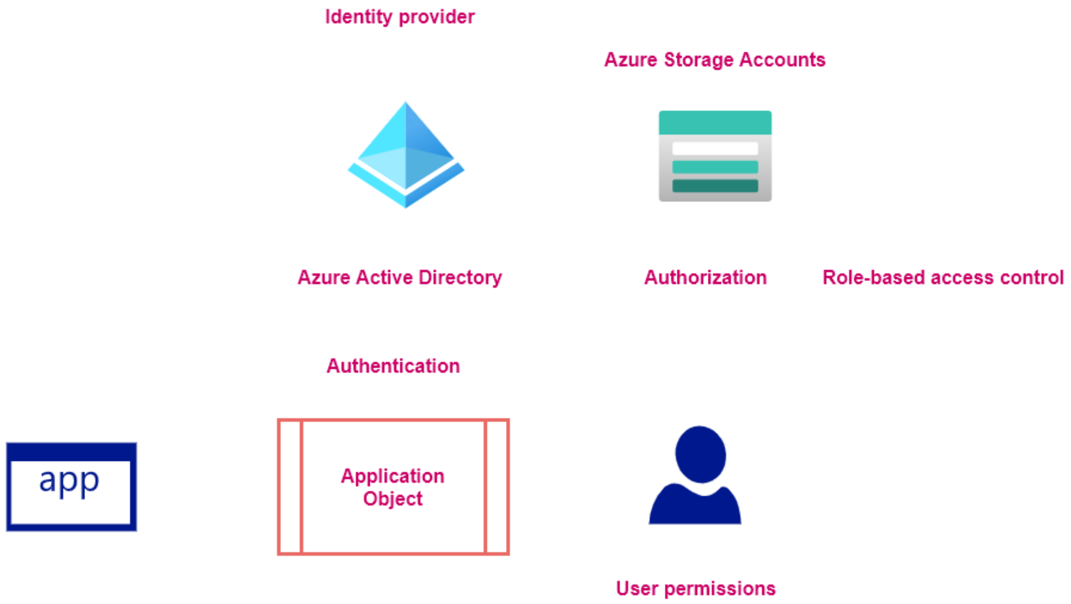
Azure Just-in-time VM access

This is part of Azure Security Center

This provides Just-In-Time access to a virtual machine

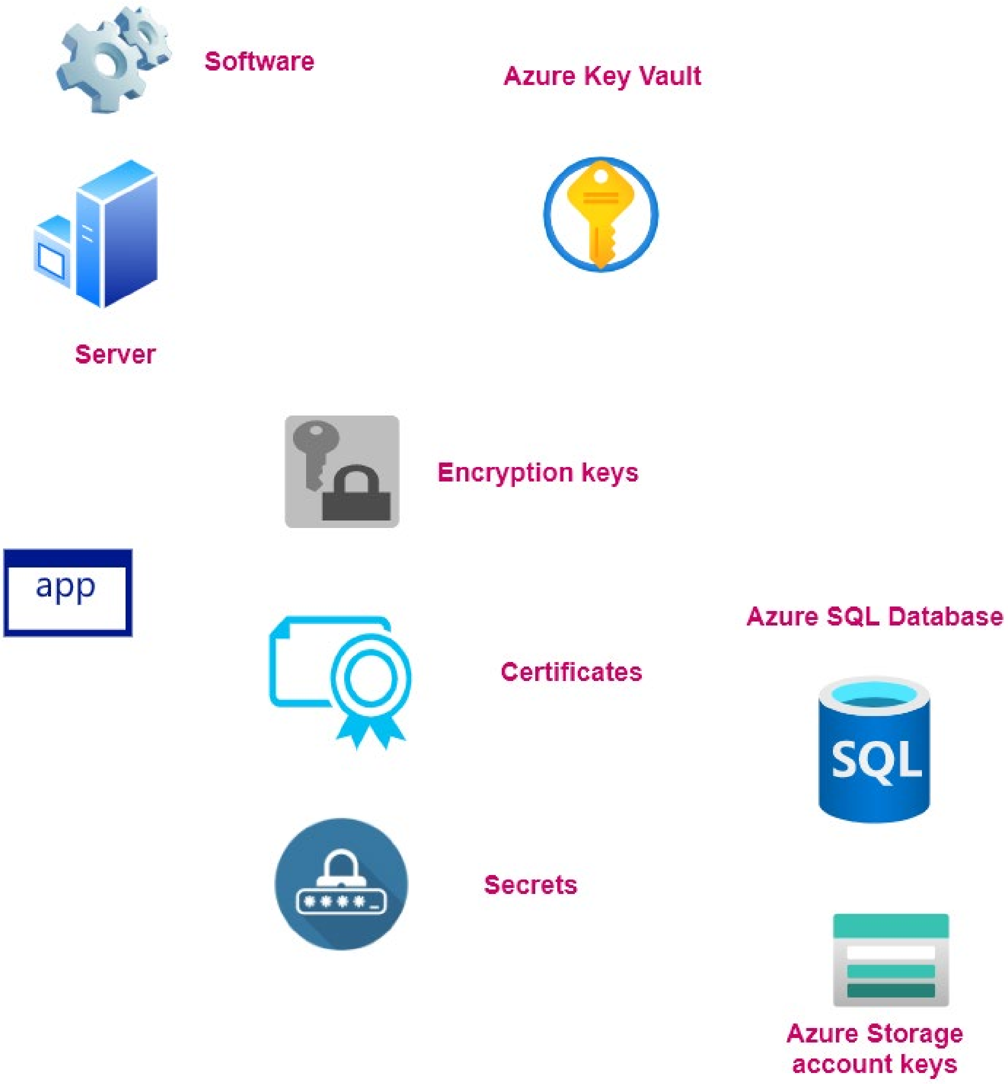
Application Objects

Use Application Objects defined in Azure AD to give access to resources for your application



Azure Key Vault

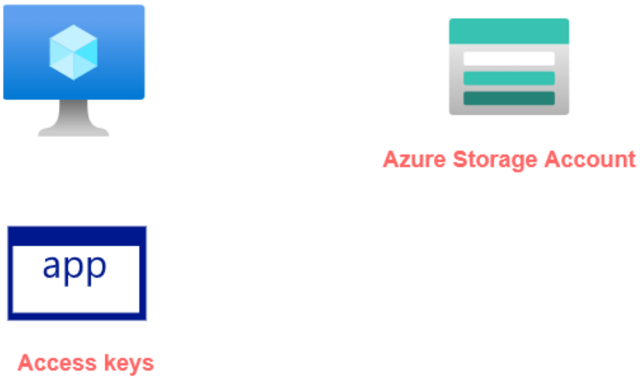
Use this service to securely store and manage the lifecycle of your secrets, encryption keys and certificates



Managed Identities

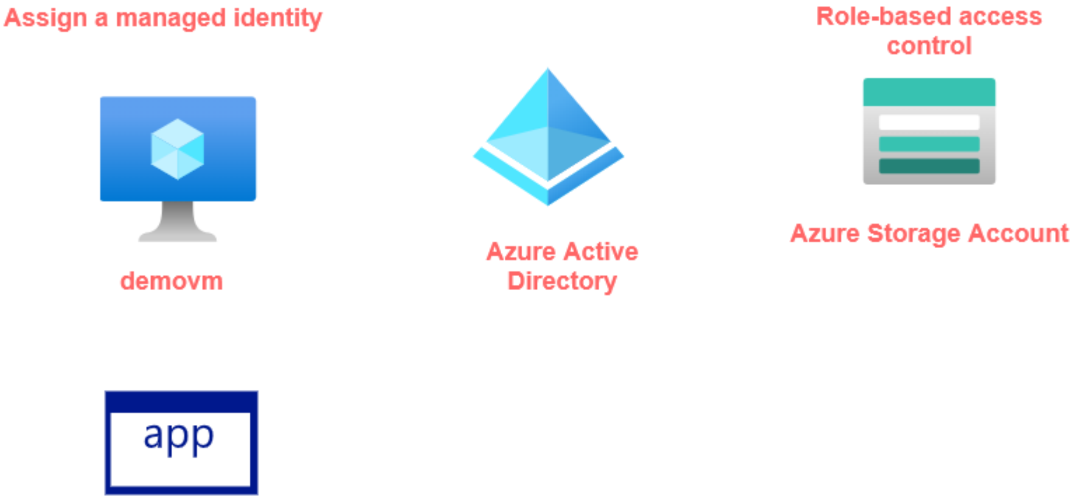
Managed Identities

This helps Azure resources to authenticate to services that support Azure AD authentication



Azure Storage Account

Access keys



Assign a managed identity

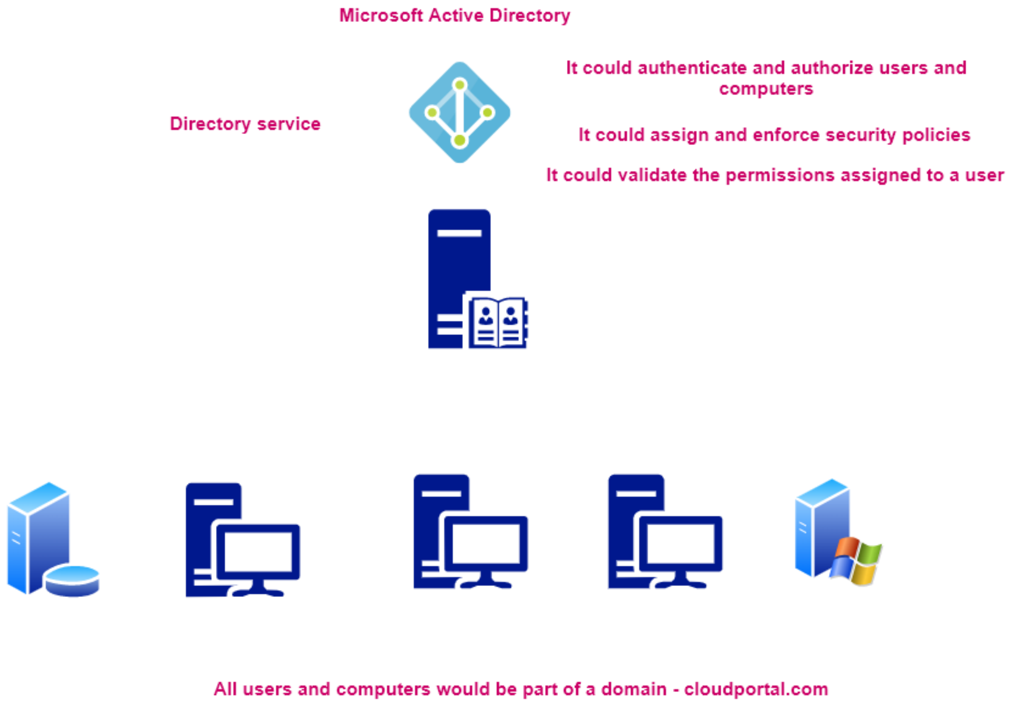
Role-based access control

demovm

Azure Active Directory

Azure Storage Account

Microsoft Active Directory



Microsoft Active Directory

Directory service

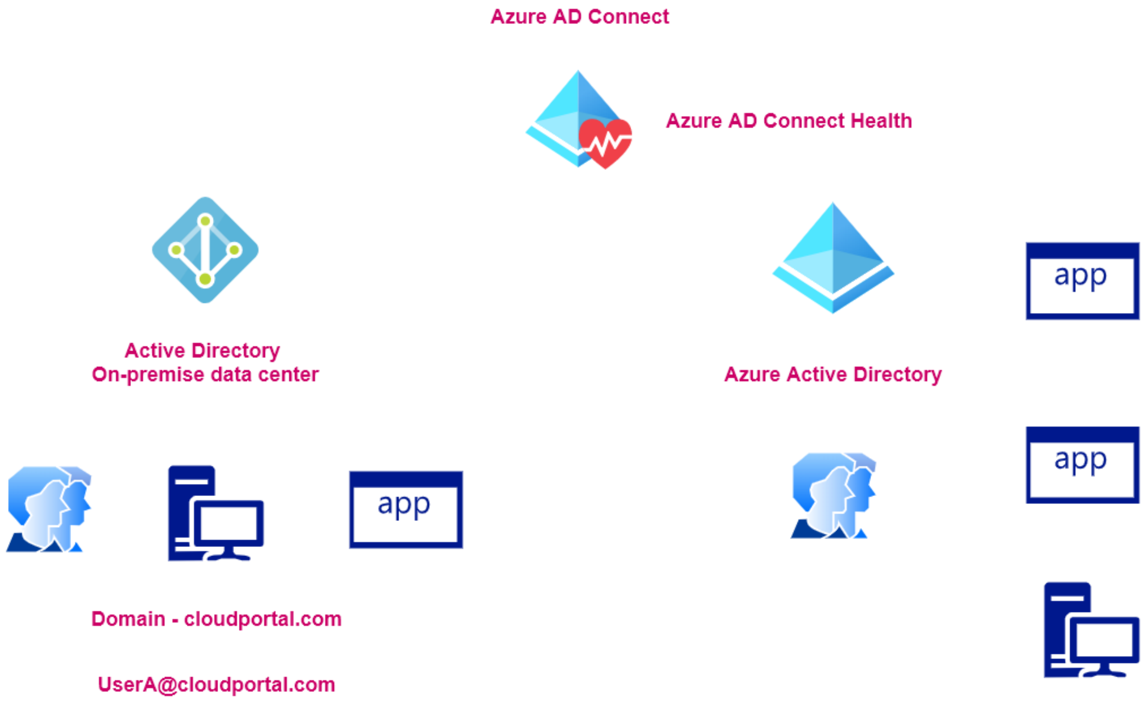
It could authenticate and authorize users and computers

It could assign and enforce security policies

It could validate the permissions assigned to a user

All users and computers would be part of a domain - cloudportal.com

Review of Azure AD Connect



Azure AD Connect

Azure AD Connect Health

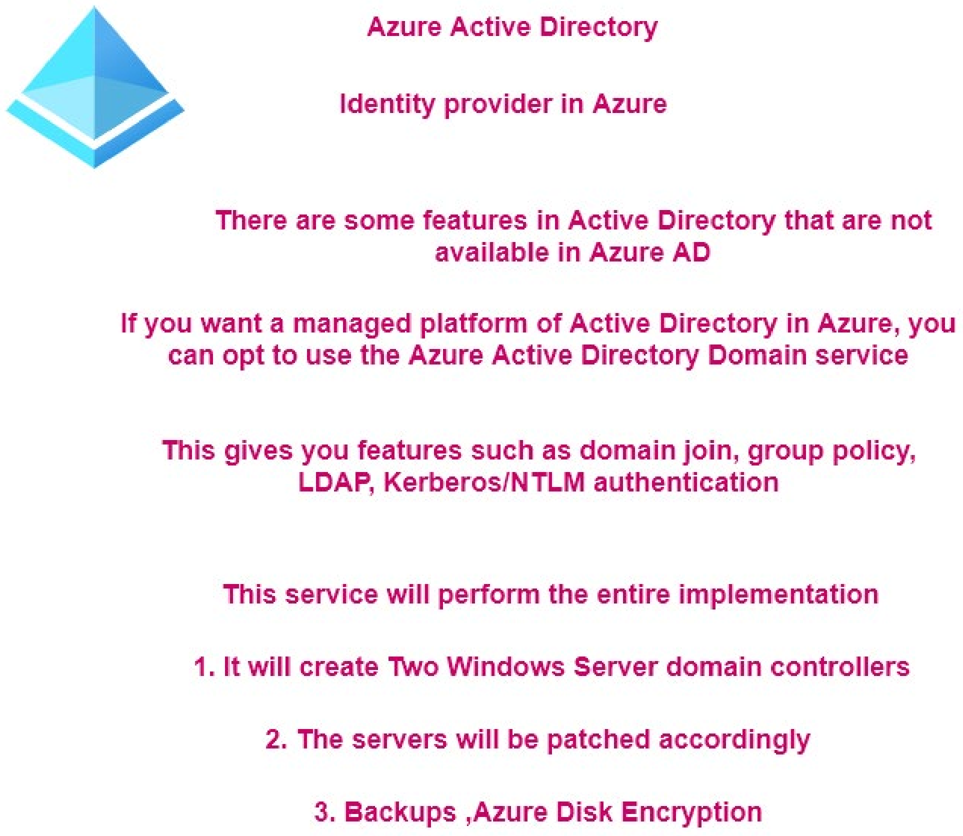
Active Directory
On-premise data center

Azure Active Directory

Domain - cloudportal.com

UserA@cloudportal.com

Azure Active Directory Domain services



Azure Active Directory

Identity provider in Azure

There are some features in Active Directory that are not available in Azure AD

If you want a managed platform of Active Directory in Azure, you can opt to use the Azure Active Directory Domain service

This gives you features such as domain join, group policy, LDAP, Kerberos/NTLM authentication

This service will perform the entire implementation

1. It will create Two Windows Server domain controllers

2. The servers will be patched accordingly

3. Backups ,Azure Disk Encryption

Design Data Storage

The different storage options

The different data stores

Azure Storage Accounts

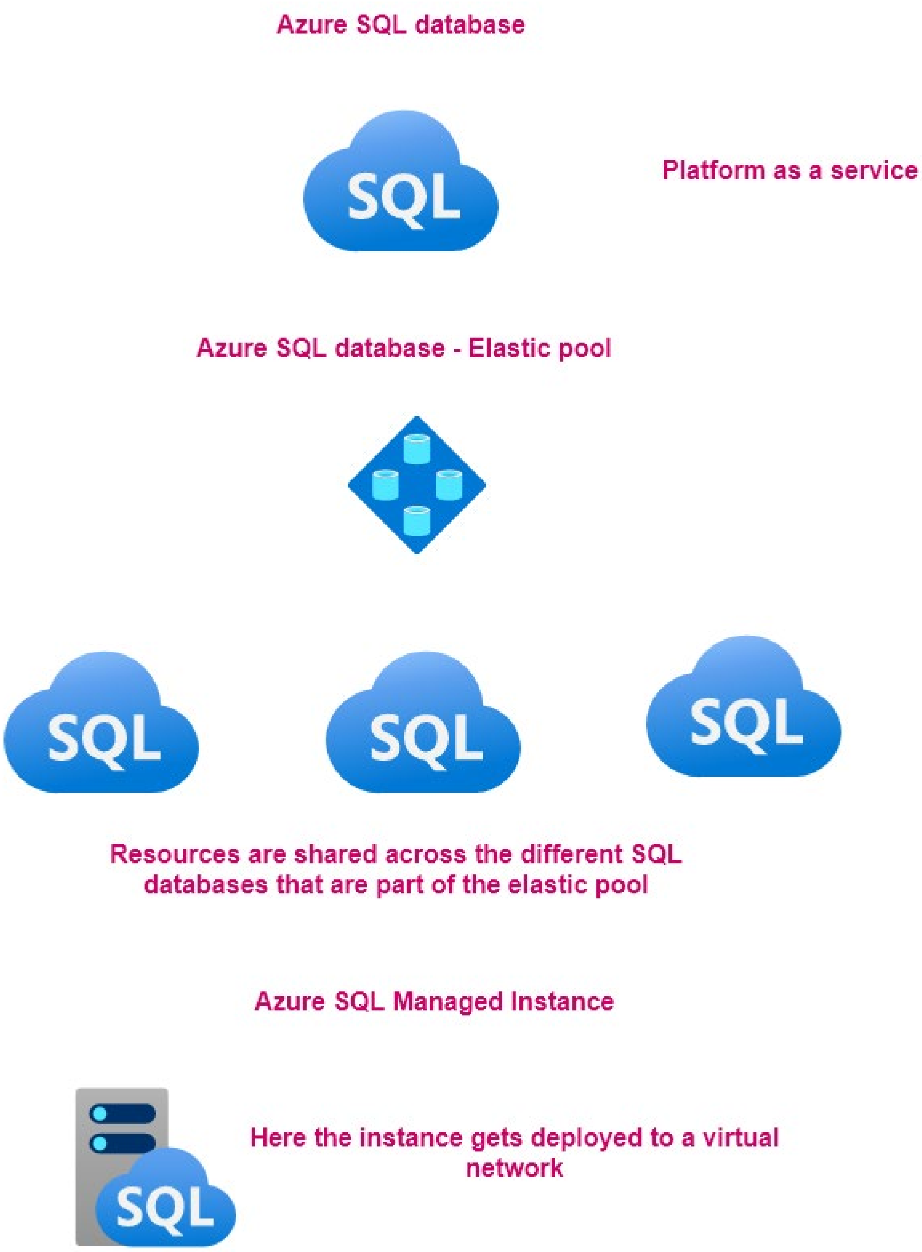
Blob storage	Objects - Videos, images etc
File shares	Files shares that can be accessed via the Server Message Block protocol
Tables	Simple NoSQL data store

SQL Database

Oracle	Microsoft SQL Server	MySQL database

You have control over the VM

You can install any version of the database software you want



Azure SQL database

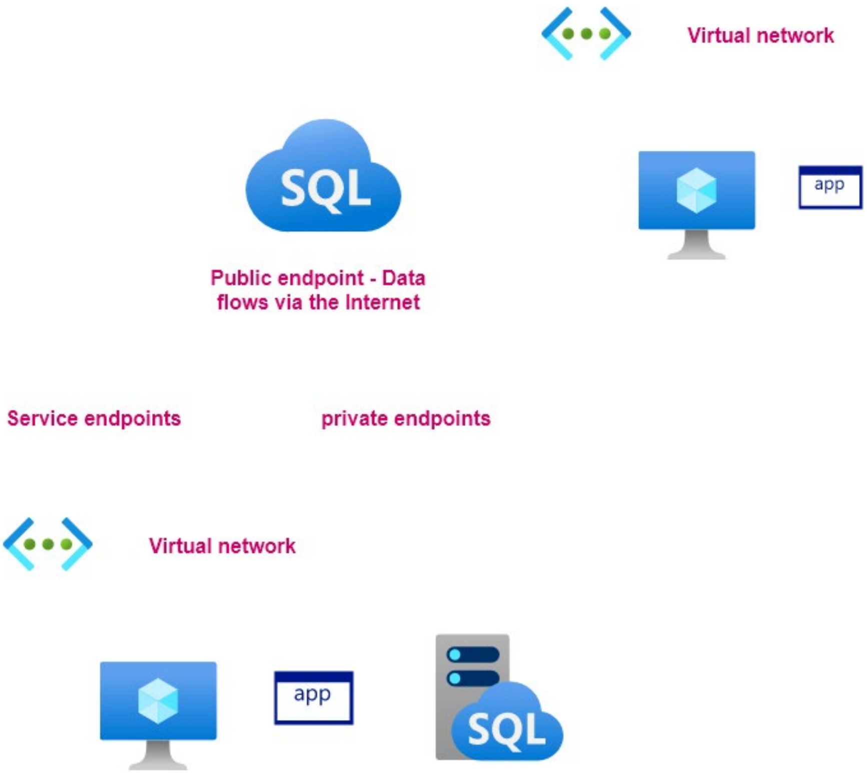
Platform as a service

Azure SQL database - Elastic pool

Resources are shared across the different SQL databases that are part of the elastic pool

Azure SQL Managed Instance

Here the instance gets deployed to a virtual network



Virtual network

Public endpoint - Data flows via the Internet

Service endpoints

private endpoints

Virtual network

Azure SQL Managed Instance

Azure Cosmos DB

Fully managed NoSQL data store

SQL API

Table API

Cassandra API

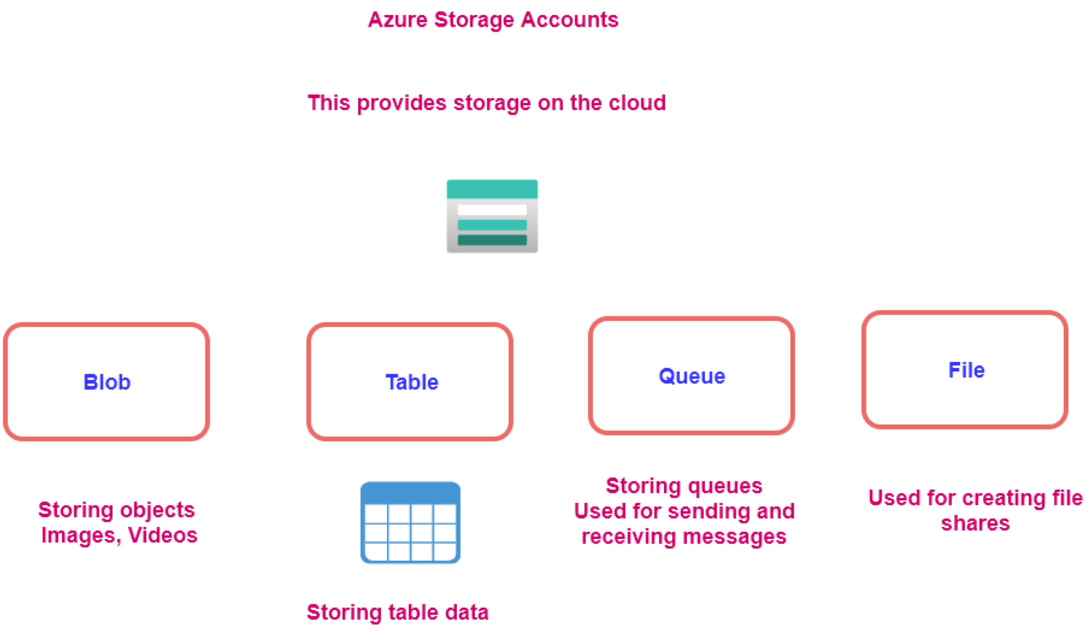
MongoDB API

Gremlin API

Azure Cache for Redis

In-memory data store

Azure Storage Accounts



Azure Storage Accounts

This provides storage on the cloud

Blob

Table

Queue

File

Storing objects
Images, Videos

Storing table data

Storing queues
Used for sending and
receiving messages

Used for creating file
shares

How to access the services - Security
- Authorization

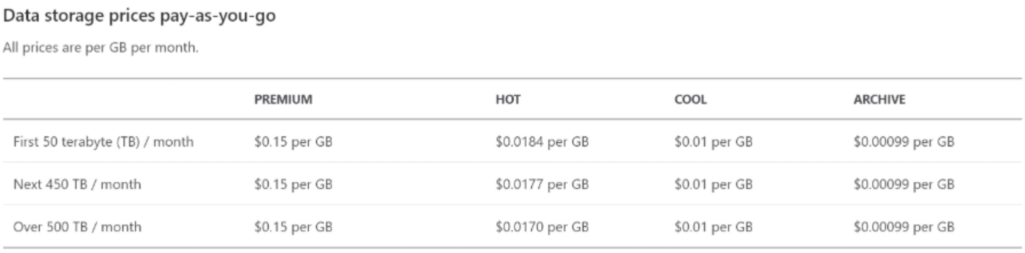
Access Keys

Shared Access
Signatures

Azure Active
Directory

Azure Storage Account tiers

Azure Storage Accounts

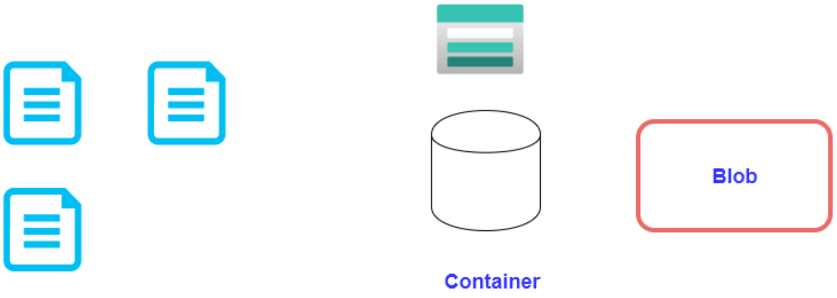


Data storage prices pay-as-you-go

All prices are per GB per month.

	PREMIUM	HOT	COOL	ARCHIVE
First 50 terabyte (TB) / month	$0.15 per GB	$0.0184 per GB	$0.01 per GB	$0.00099 per GB
Next 450 TB / month	$0.15 per GB	$0.0177 per GB	$0.01 per GB	$0.00099 per GB
Over 500 TB / month	$0.15 per GB	$0.0170 per GB	$0.01 per GB	$0.00099 per GB

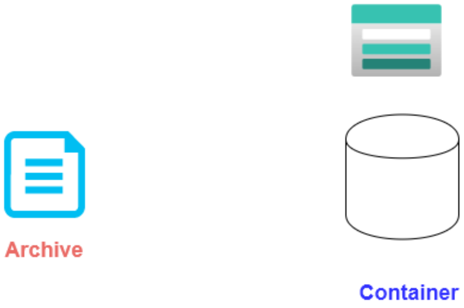
When a company starts storing millions of objects , then the storage price makes a difference



Access tier

Hot Cool Archive

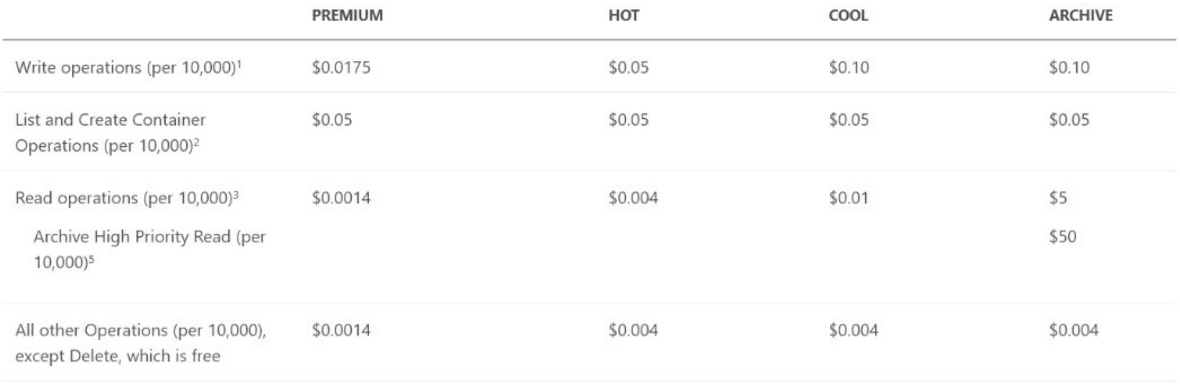
The Archive can only be enabled at the individual blob level



You have to rehydrate the file to access the file

Here you need to change the access tier of the file to either Hot or Cool to access the file

It takes time to rehydrate the file



	PREMIUM	HOT	COOL	ARCHIVE
Write operations (per 10,000)[1]	$0.0175	$0.05	$0.10	$0.10
List and Create Container Operations (per 10,000)[2]	$0.05	$0.05	$0.05	$0.05
Read operations (per 10,000)[3]	$0.0014	$0.004	$0.01	$5
Archive High Priority Read (per 10,000)[5]				$50
All other Operations (per 10,000), except Delete, which is free	$0.0014	$0.004	$0.004	$0.004

Early Deletion Fee

Cool Access tier - This is used for data that is accessed infrequently and stored for at least 30 days

Archive Access tier - This is used for data that is rarely accessed and stored for at least 180 days

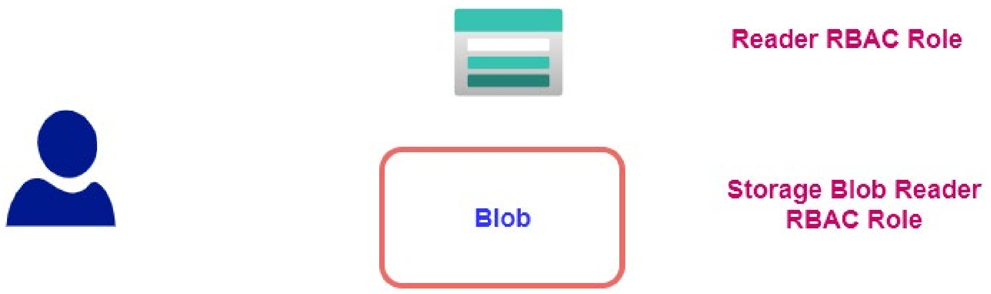
If you have a blob in the Cool Access tier and you change the access tier to the Hot access tier earlier than 30 days , then you are charged an early deletion fee

If you have a blob in the Cool Access tier and you change the access tier to the Hot access tier after just 10 days, then you are still charged costs for the extra 20 days of the Cool Access tier

Using Azure AD for authentication of blobs

Azure Storage Accounts

This provides storage on the cloud



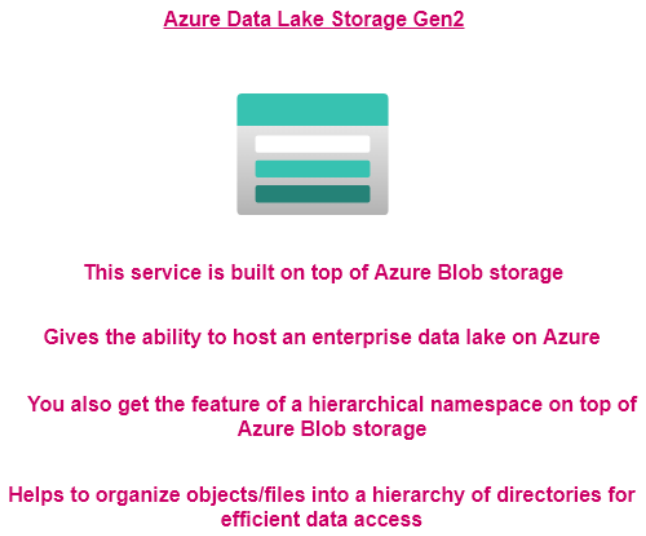
Reader RBAC Role

Blob

Storage Blob Reader RBAC Role

Storing objects
Images, Videos

Azure Data Lake Gen2 Storage accounts



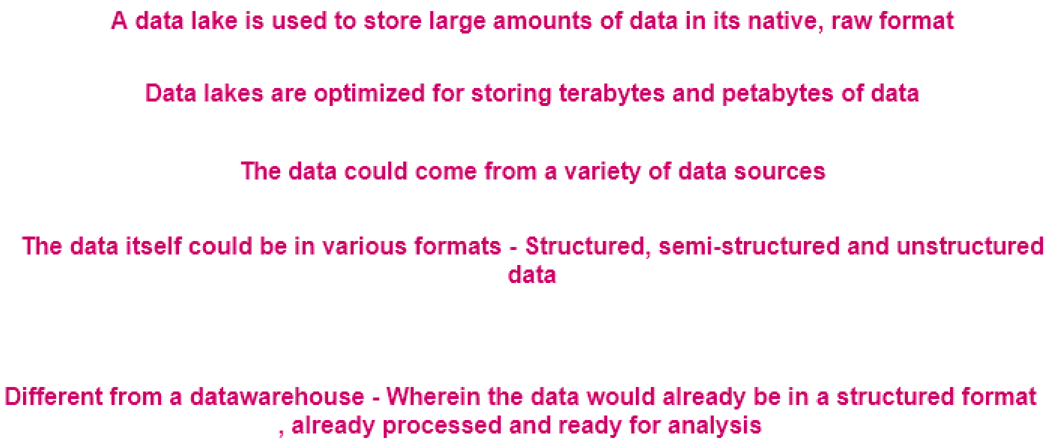
Azure Data Lake Storage Gen2

This service is built on top of Azure Blob storage

Gives the ability to host an enterprise data lake on Azure

You also get the feature of a hierarchical namespace on top of Azure Blob storage

Helps to organize objects/files into a hierarchy of directories for efficient data access



A data lake is used to store large amounts of data in its native, raw format

Data lakes are optimized for storing terabytes and petabytes of data

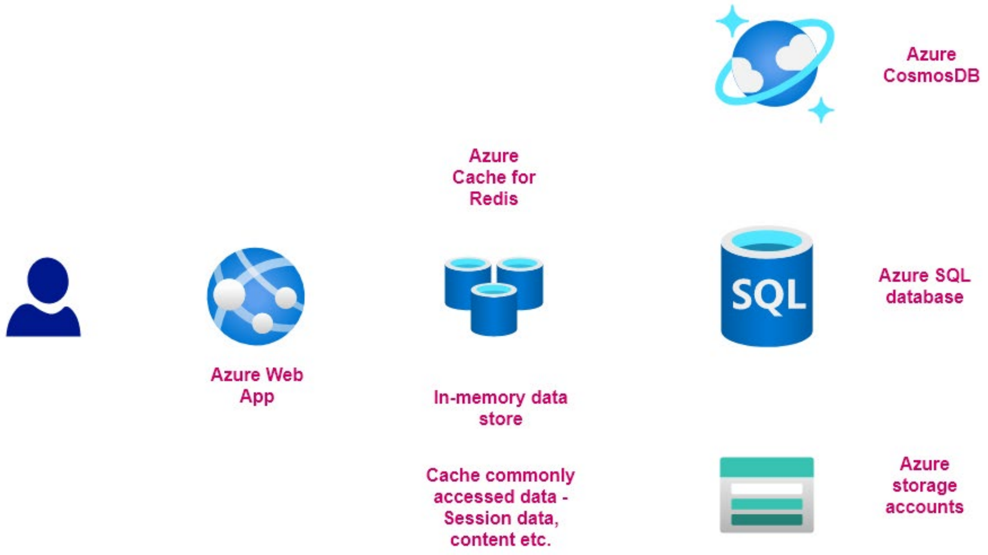
The data could come from a variety of data sources

The data itself could be in various formats - Structured, semi-structured and unstructured data

Different from a datawarehouse - Wherein the data would already be in a structured format , already processed and ready for analysis

Azure Cache for Redis

Your in-memory data store



Azure SQL Database – Different deployment options

- You can use the Infrastructure as a service facility wherein you deploy Microsoft SQL Server on an Azure Virtual machine.
- This will give you complete administrative access over the virtual machine.
- Here you can also use the pay-as-you-go model when using SQL server on an Azure virtual machine.
- This provides an easy option for migrating your on-premise SQL Server workloads.
- Here you can install the version of SQL Server that you require.
- And then migrate the data onto the instance on the Azure virtual machine.
- Then you have the Platform as a service wherein you can use the Azure SQL database service.
- Here the underlying compute infrastructure is managed by Azure.
- Here you also get an SLA of 99.995%

- With Azure SQL database server, you can choose from a variety of pricing tiers.
- Here you can also make use of features such as Automated backup, Automated tuning, simplified patching etc.
- Azure SQL Managed Instance – This is an ideal option also for migrating existing SQL Server workloads onto Azure.
- SQL Managed Instance has near 100% compatibility with the latest SQL Server (Enterprise Edition) database engine.
- You can also get native Virtual Network Integration.
- You can also use the Hybrid benefits to use your own licenses to save on costs.

Azure SQL Server – Data Masking

- Here the data in the database table can be limited in its exposure to non-privileged users.
- You can create a rule that can mask the data.
- Based on the rule you can decide on the amount of data to expose to the user.
- There are different masking rules.
- **Credit Card masking rule** – This is used to mask the column that contain credit card details. Here only the last four digits of the field are exposed.
- **Email** – Here first letter of the email address is exposed. And the domain name of the email address is replaced with XXX.com.
- **Custom text**- Here you decide which characters to expose for a field.
- **Random number**- Here you can generate a random number for the field

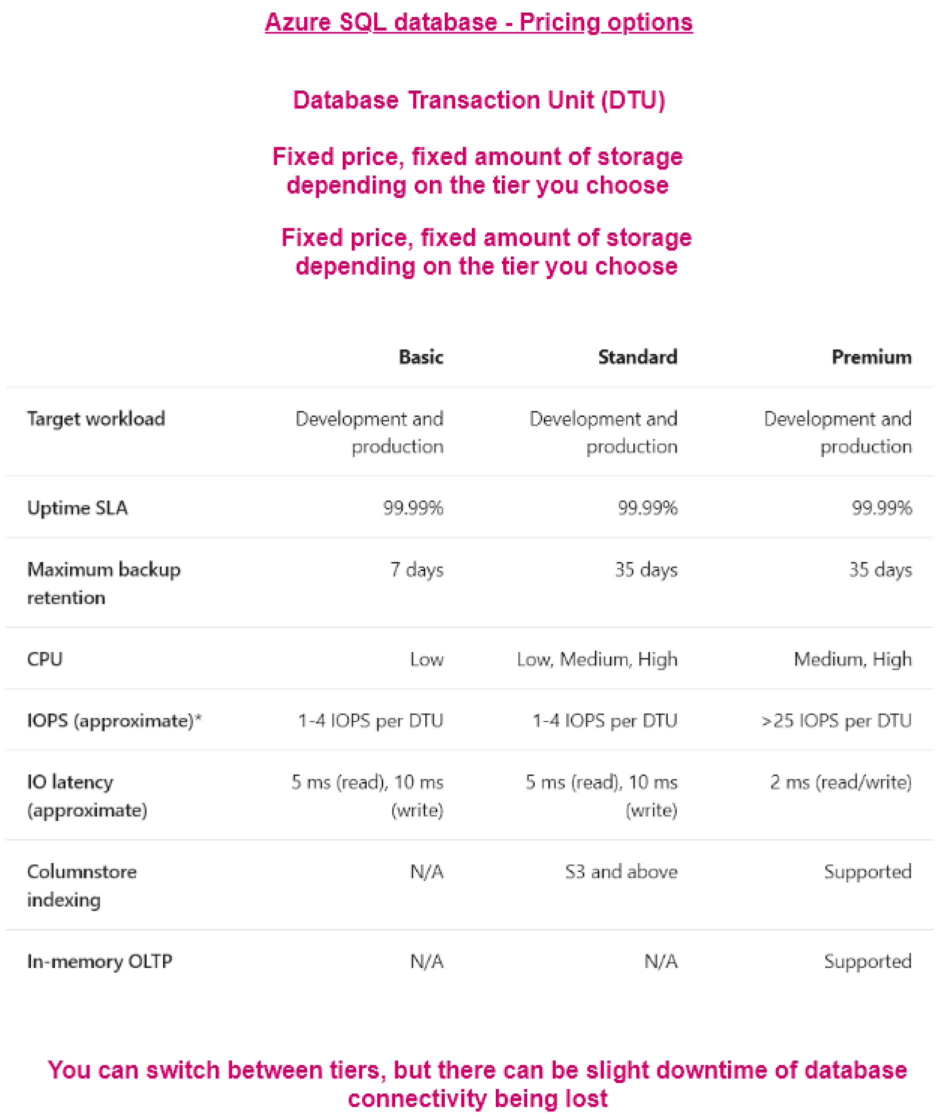
Azure SQL Database – Transparent Data Encryption

- **Transparent data encryption.**
- Here the database data , any associated backups and log files are all encrypted for you.
- When data is fetched from the database , it is automatically decrypted.
- This is automatically enabled for Azure SQL Databases (Note:- Not for Azure SQL Managed Instance).
- You can use the key provided by Azure for the encryption.
- Or you can create your own key in the Azure Key vault service.

Azure SQL Server – Always Encrypted

- **Azure SQL Server – Always Encrypted**
- This is used to protect sensitive data in your database.
- Here the data is protected at rest, when it is moved from the client and the server and when the data is in use.
- When you use the "Always Encrypted" feature, the sensitive data will not appear as plaintext.
- You can enable the "Always Encrypted" feature with the help of SQL Server Management studio
- To use the Azure key vault service
- Ensure that the user has the following permissions -
create, get, list, sign, verify, wrapKey, and unwrapKey permissions
- During the encryption process , it will ask you to login into Azure.
- If the user does not have the right permissions, the encryption process will fail.
- Once the encryption is complete , the application can make use of decryption techniques to fetch the data from the database.

Azure SQL Database – Different pricing options



Azure SQL database - Pricing options

Database Transaction Unit (DTU)

Fixed price, fixed amount of storage depending on the tier you choose

Fixed price, fixed amount of storage depending on the tier you choose

	Basic	Standard	Premium
Target workload	Development and production	Development and production	Development and production
Uptime SLA	99.99%	99.99%	99.99%
Maximum backup retention	7 days	35 days	35 days
CPU	Low	Low, Medium, High	Medium, High
IOPS (approximate)*	1-4 IOPS per DTU	1-4 IOPS per DTU	>25 IOPS per DTU
IO latency (approximate)	5 ms (read), 10 ms (write)	5 ms (read), 10 ms (write)	2 ms (read/write)
Columnstore indexing	N/A	S3 and above	Supported
In-memory OLTP	N/A	N/A	Supported

You can switch between tiers, but there can be slight downtime of database connectivity being lost

v-Core-based purchasing model

Here you can decide on the number of vCores and size of the database

You can also use the Hybrid benefit model to use existing licences to save on cost.

Serverless

Here the compute can scale based on demand

You also have an auto-pause feature that can pause the database when it is not being used. This can save on compute costs.

Hyperscale

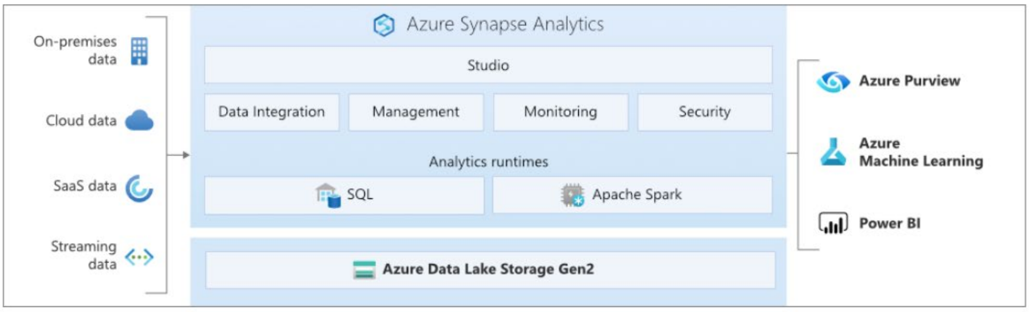
Here compute and storage are seperate

You can scale storage up to 100 TB

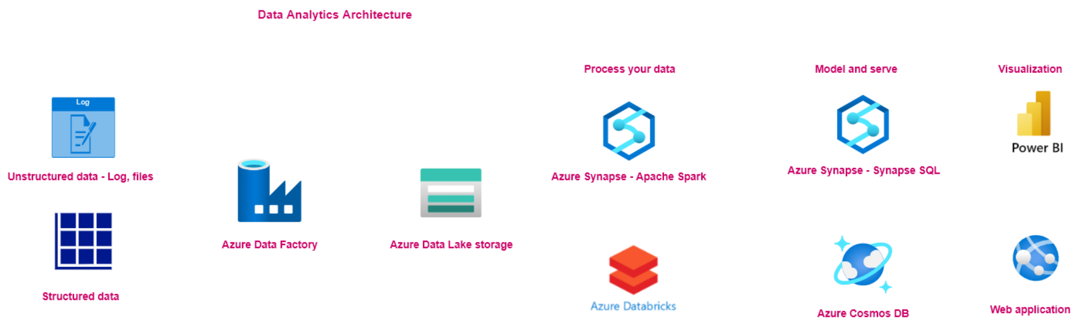
Azure Synapse Analytics

Azure Synapse Analytics

Helps to gain insights to your data warehouses and big data systems

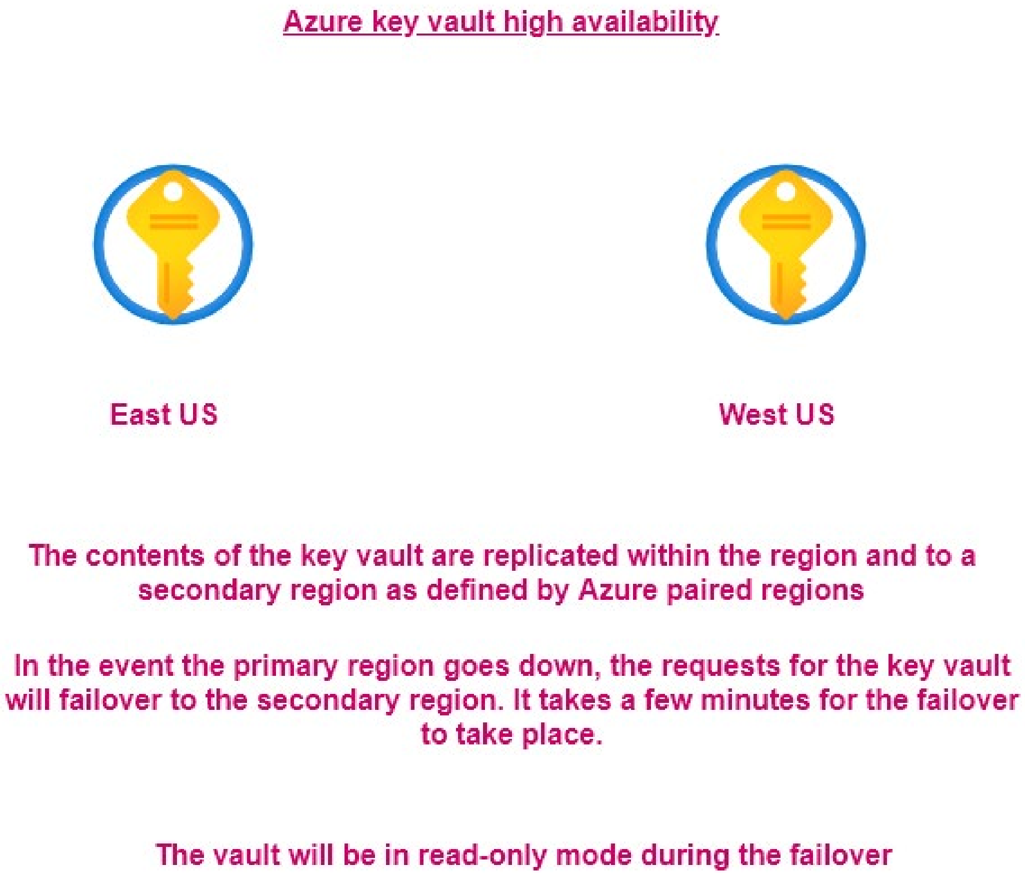


You can build your data warehouses using a Synapse SQL pool - Serverless and dedicated



Design Business Continuity

Azure Key vault – High availability



Azure key vault high availability

The contents of the key vault are replicated within the region and to a secondary region as defined by Azure paired regions

In the event the primary region goes down, the requests for the key vault will failover to the secondary region. It takes a few minutes for the failover to take place.

The vault will be in read-only mode during the failover

Azure SQL Database – Backup

Azure SQL Database backup

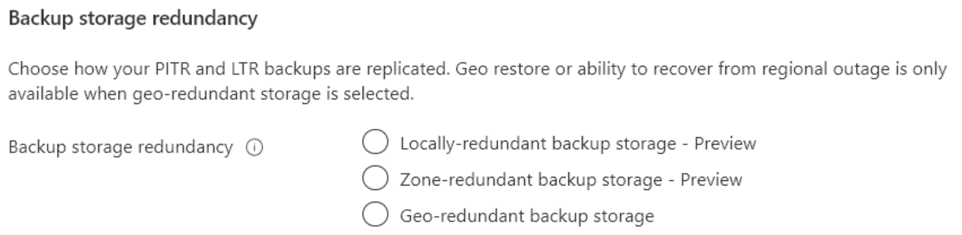
The backup feature is available for Azure SQL database and SQL Managed Instance

Full backups are taken every week

Differential backups - Every 12-14 hours

Transaction log backups every 5-10 minutes

You can also configure availability for the backups itself



Backup storage redundancy

Choose how your PITR and LTR backups are replicated. Geo restore or ability to recover from regional outage is only available when geo-redundant storage is selected.

Backup storage redundancy ⓘ

○ Locally-redundant backup storage - Preview

○ Zone-redundant backup storage - Preview

○ Geo-redundant backup storage

Performing a restore

You can perform a point-in-time restore of an existing database on the same server as the original database

You can perform a point-in-time restore of a deleted database on the same server

You can perform a Geo-restore to another geographic region if the primary region is not available

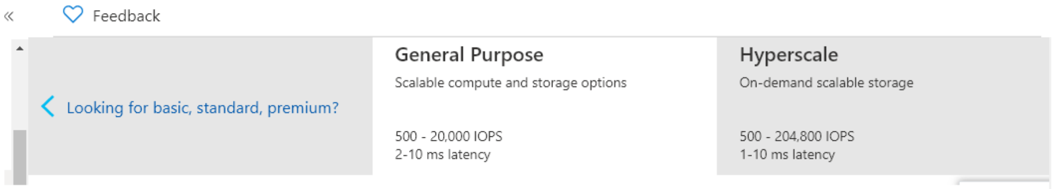
Long-term retention

Here backups can be stored in Azure Storage accounts for a duration of up to 10 years.

Sometimes backups are required for a long time for regulatory or compliance purposes.

Azure SQL Database - High availability

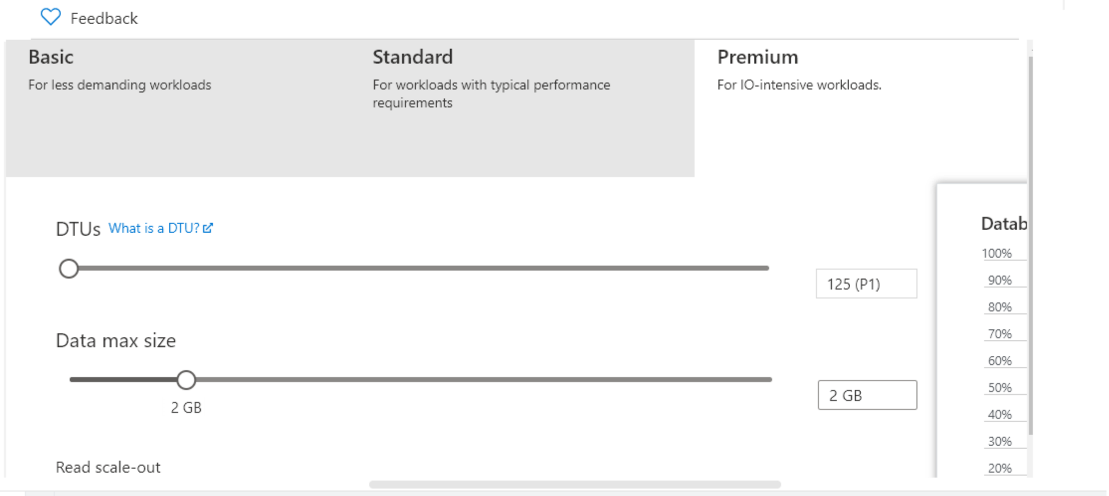
With Zone-redundancy, the databases are replicated across Azure Availability Zones



Looking for basic, standard, premium?

General Purpose
Scalable compute and storage options
500 - 20,000 IOPS
2-10 ms latency

Hyperscale
On-demand scalable storage
500 - 204,800 IOPS
1-10 ms latency



Basic
For less demanding workloads

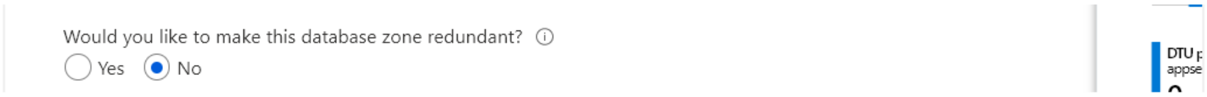
Standard
For workloads with typical performance requirements

Premium
For IO-intensive workloads.

DTUs What is a DTU?
125 (P1)

Data max size
2 GB
2 GB

Read scale-out



Would you like to make this database zone redundant?
○ Yes ● No

With Zone-redundancy, the databases are replicated across Azure Availability Zones

Here data gets replicated to nodes in different data centers

Here the data is replicated synchronously

This is also available with the Azure SQL Serverless tier

Azure SQL Database – Active geo-replication

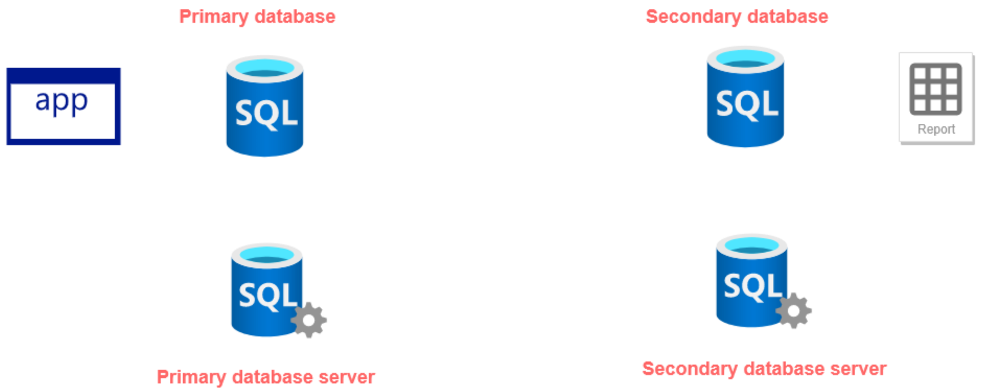
Azure SQL - Active geo-replication

This feature allows you to create a readable secondary database

This database would be based on a primary database

The secondary database can on a server in the same or different data center

This is not supported for Azure SQL Managed Instance

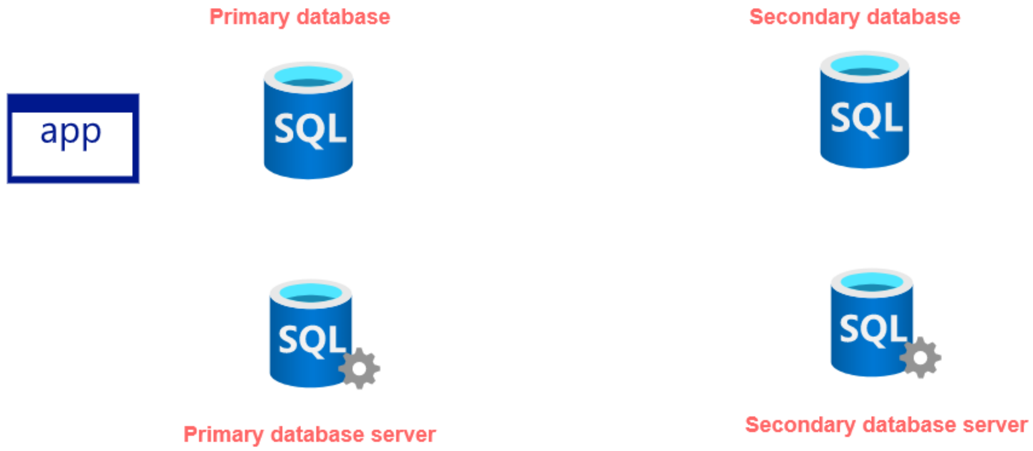


Primary database

Secondary database

Primary database server

Secondary database server



Primary database

Secondary database

Primary database server

Secondary database server

Failover

Here the failover need to be initiated manually by the user or application

When you do a failover, you have to understand there could be a small data loss if the data in the primary has not been replicated to the secondary

Azure SQL Database – Auto-failover groups

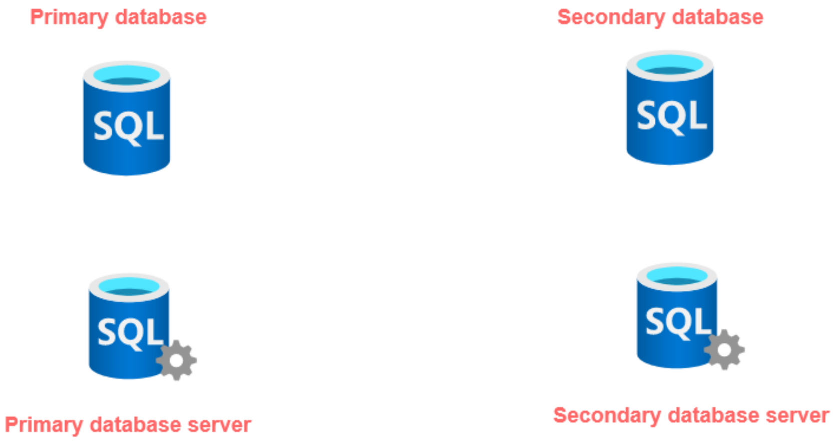
Auto-failover groups

This is a feature that is built on top of Active-Geo replication

This feature is available for Azure SQL Managed Instance

Here you can replicate and failover a group of databases on a server

The failover can be done manually or automatically via a policy

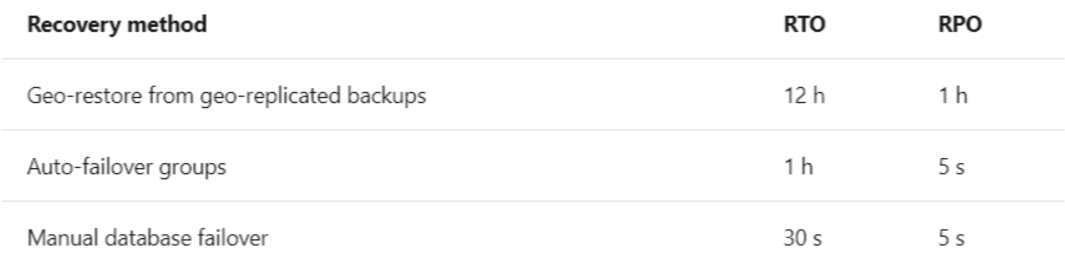


Primary database

Secondary database

Primary database server

Secondary database server



Recovery method	RTO	RPO
Geo-restore from geo-replicated backups	12 h	1 h
Auto-failover groups	1 h	5 s
Manual database failover	30 s	5 s

https://docs.microsoft.com/en-us/azure/azure-sql/database/business-continuity-high-availability-disaster-recover-hadr-overview

With Automatic failover you don't need to change the connection string in the application

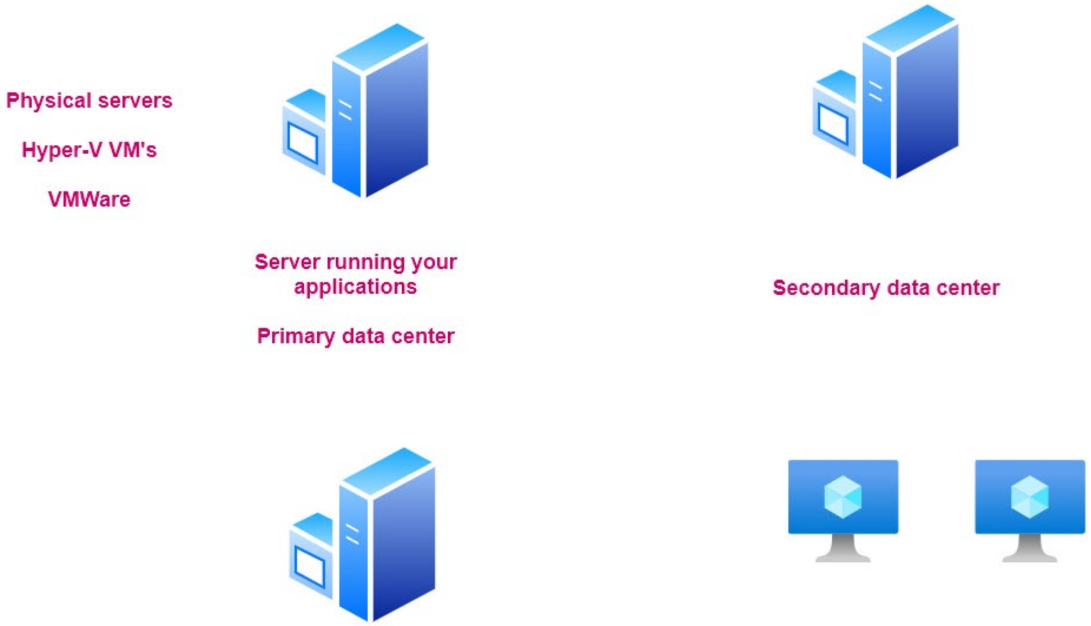
The secondary server has to be in a different region

Azure Site Recovery Review

Azure Site Recovery

Used for business continuity and for disaster recovery

Ensures your apps and workloads are running when there are planned or unplanned outages



Physical servers

Hyper-V VM's

VMWare

Server running your applications

Primary data center

Secondary data center

Server running your applications

Primary data center

Servers in Azure

VM in Azure

VM in Azure

The replication frequency is high , being as low as every 30 seconds for Hyper-V VMs

Hence the RPO is low. And because you can switch over quickly, the RTO is also low

You can run planned failovers with zero-data loss

Or unplanned failovers with minimal data loss

Hyper-V Replication

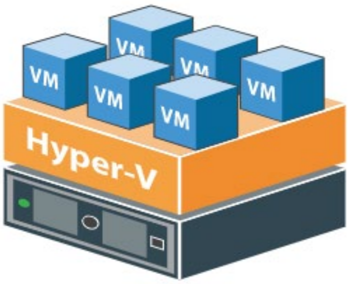
Azure - An Azure subscription, Azure storage account and Azure virtual network

The replicated data from the on-premises VM workloads is stored in the storage account

Azure Site Recovery only holds the metadata that is needed to orchestrate the replication

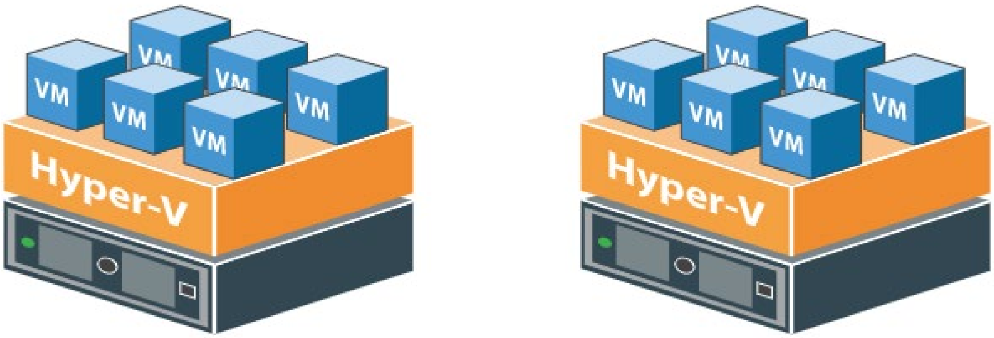
If the failover is happening to Azure VM's, the VM's are created with the replicated data when the failover occurs

Hyper-V - The Azure Site Recovery Provider and agent must be installed on each standalone Hyper-V host or on each Hyper-V cluster node

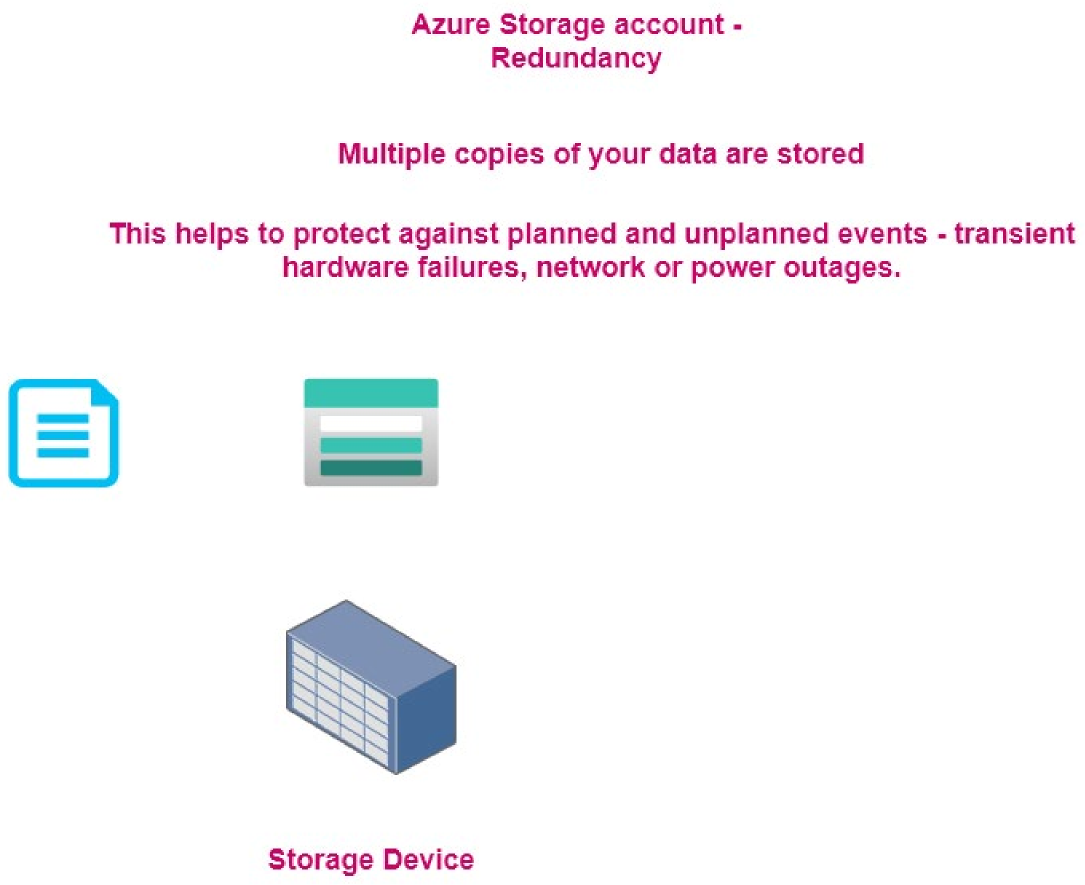


Standalone Hyper-V host

Hyper-V cluster



Azure Storage Redundancy

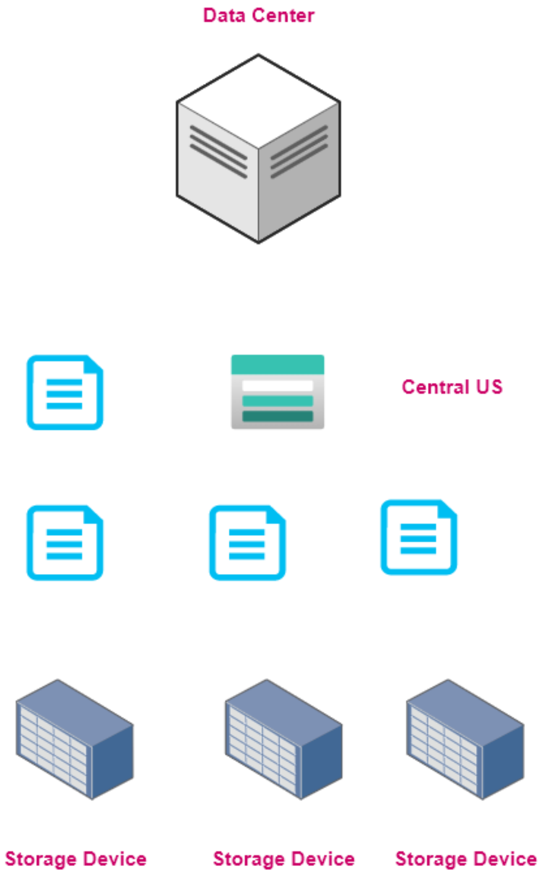


Azure Storage account -
Redundancy

Multiple copies of your data are stored

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

Locally-redundant storage



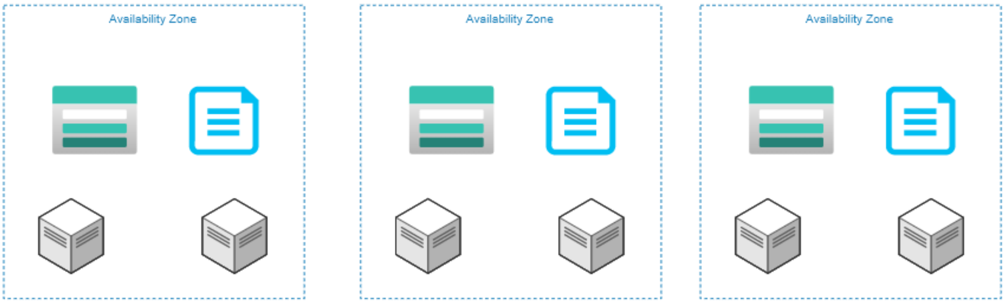
Here three copies of your data are made

It helps to protect against server rack of drive failures

Zone-redundant storage

This helps to protect against data center level failures

Here data is replicated synchronously across three Azure availability zones

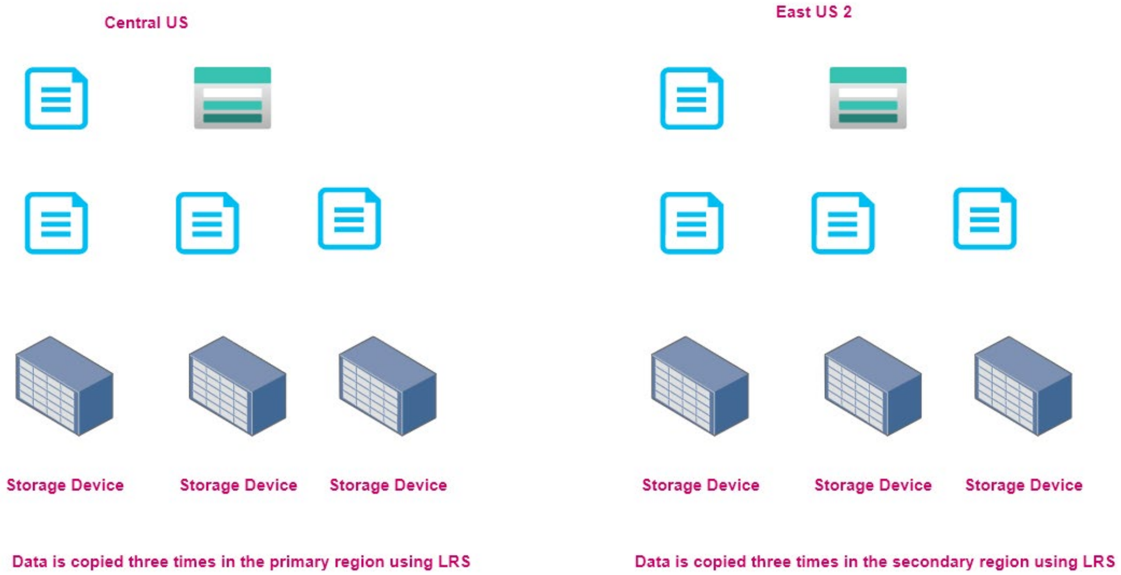


Central US

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

Geo-redundant storage

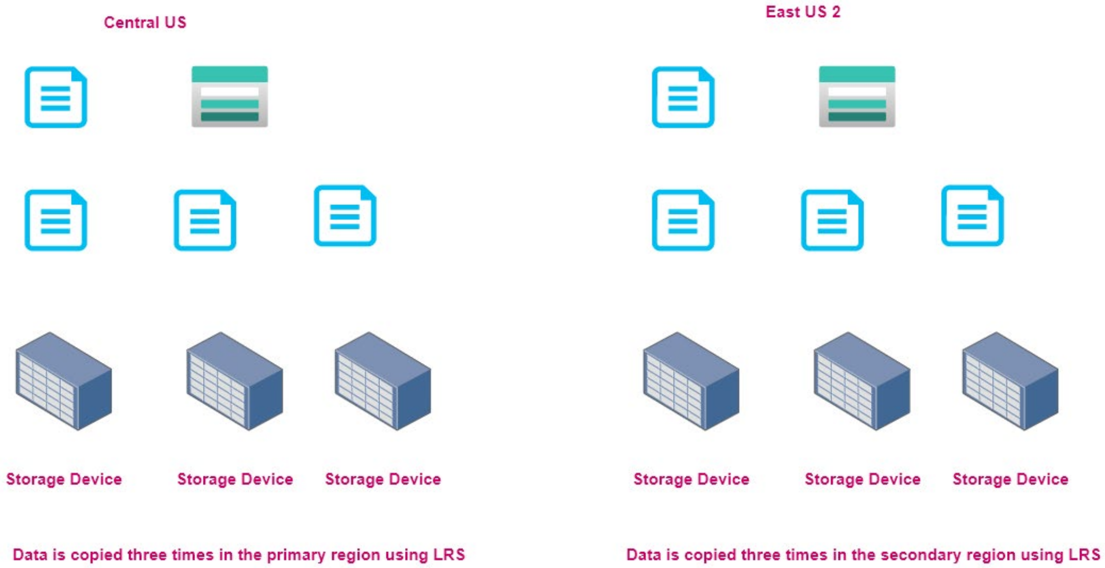
Here data is replicated to another region



Data is copied three times in the primary region using LRS

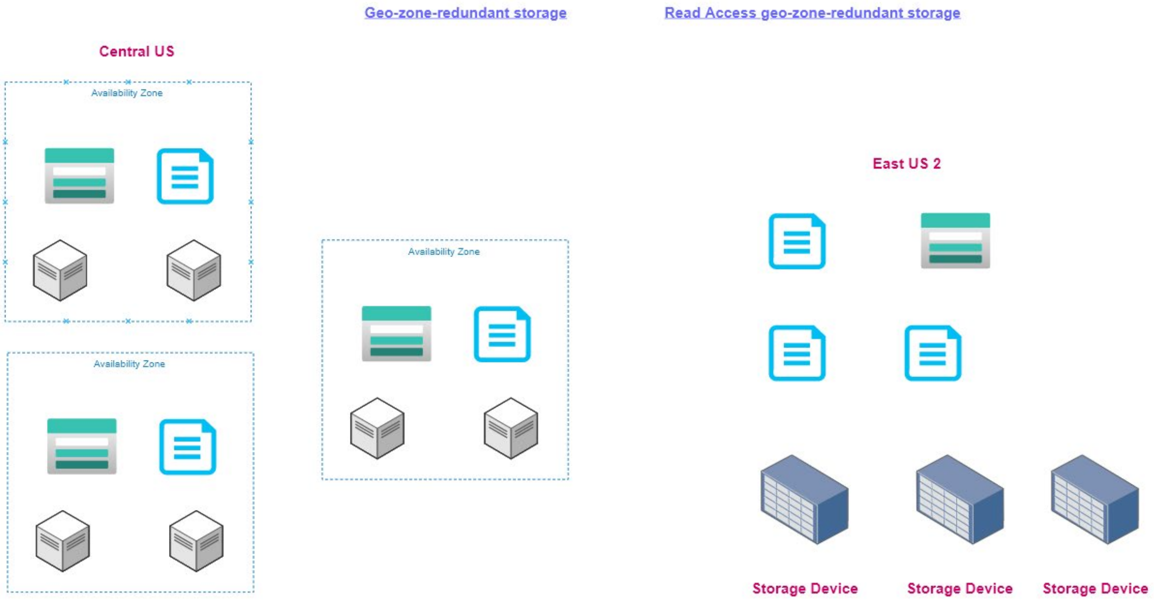
Data is copied three times in the secondary region using LRS

Read-access geo-redundant storage



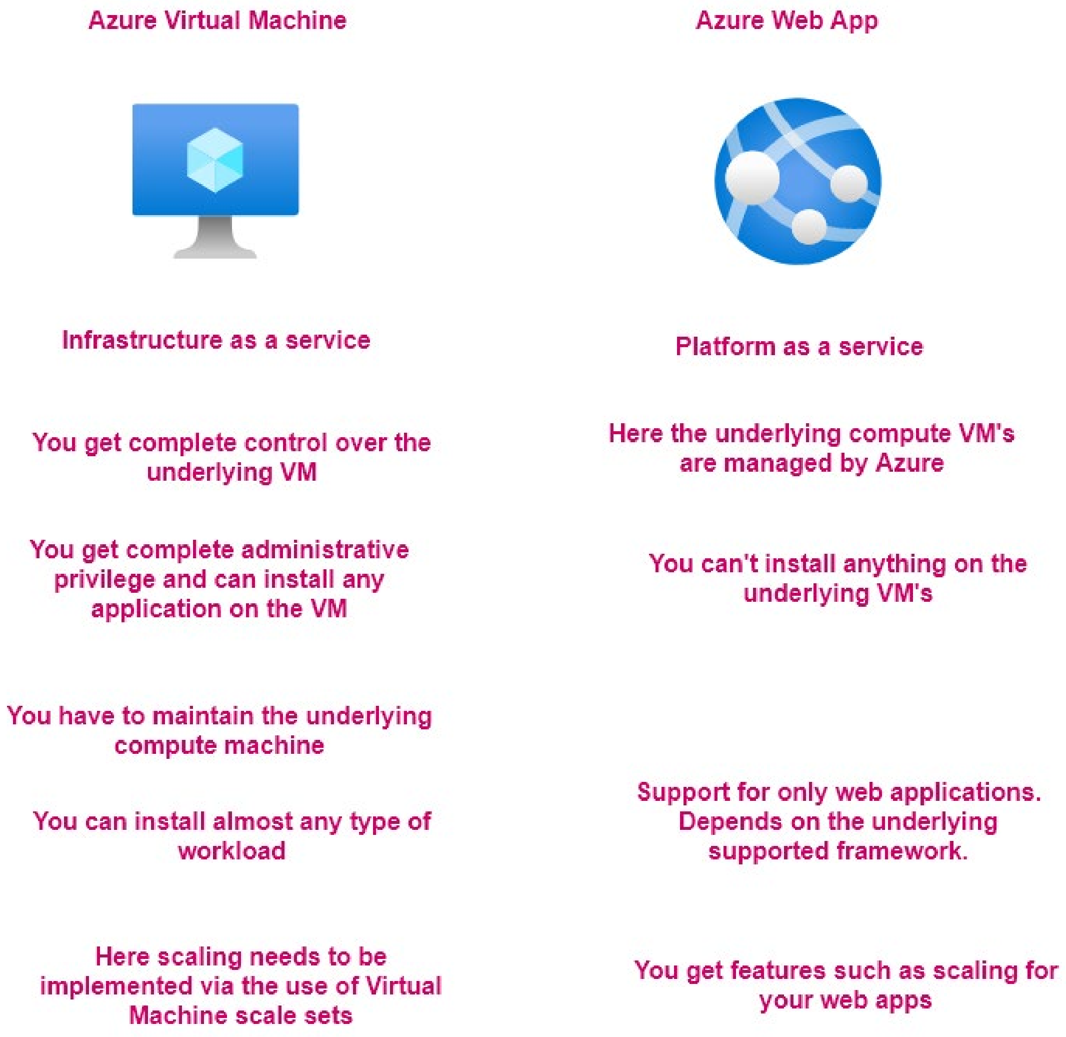
Data is copied three times in the primary region using LRS

Data is copied three times in the secondary region using LRS



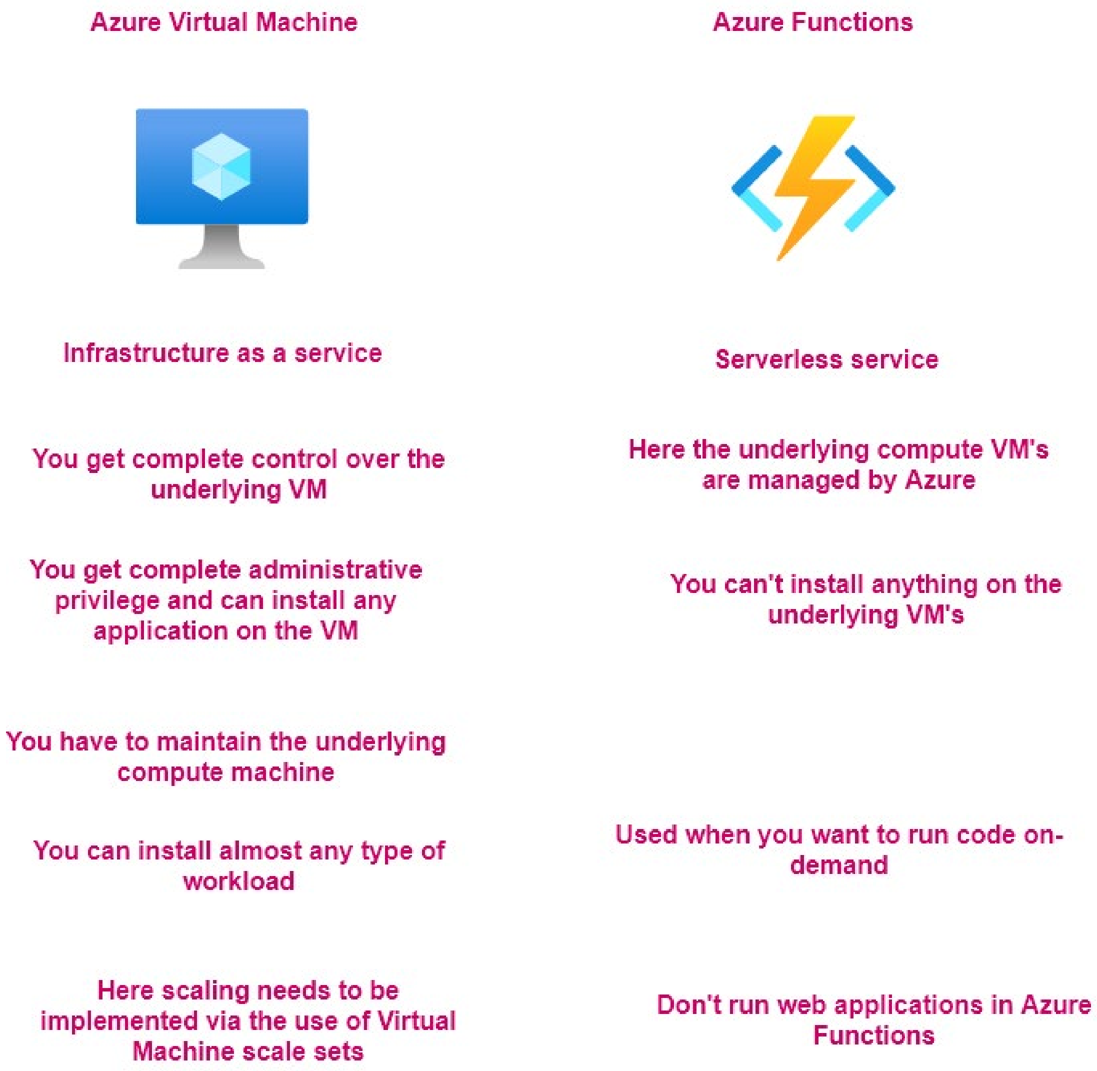
Design Infrastructure

Azure Virtual Machines vs Azure Web Apps



Azure Virtual Machine	Azure Web App
Infrastructure as a service	Platform as a service
You get complete control over the underlying VM	Here the underlying compute VM's are managed by Azure
You get complete administrative privilege and can install any application on the VM	You can't install anything on the underlying VM's
You have to maintain the underlying compute machine	
You can install almost any type of workload	Support for only web applications. Depends on the underlying supported framework.
Here scaling needs to be implemented via the use of Virtual Machine scale sets	You get features such as scaling for your web apps

Azure Virtual Machines vs Azure Functions



Azure Virtual Machine

Infrastructure as a service

You get complete control over the underlying VM

You get complete administrative privilege and can install any application on the VM

You have to maintain the underlying compute machine

You can install almost any type of workload

Here scaling needs to be implemented via the use of Virtual Machine scale sets

Azure Functions

Serverless service

Here the underlying compute VM's are managed by Azure

You can't install anything on the underlying VM's

Used when you want to run code on-demand

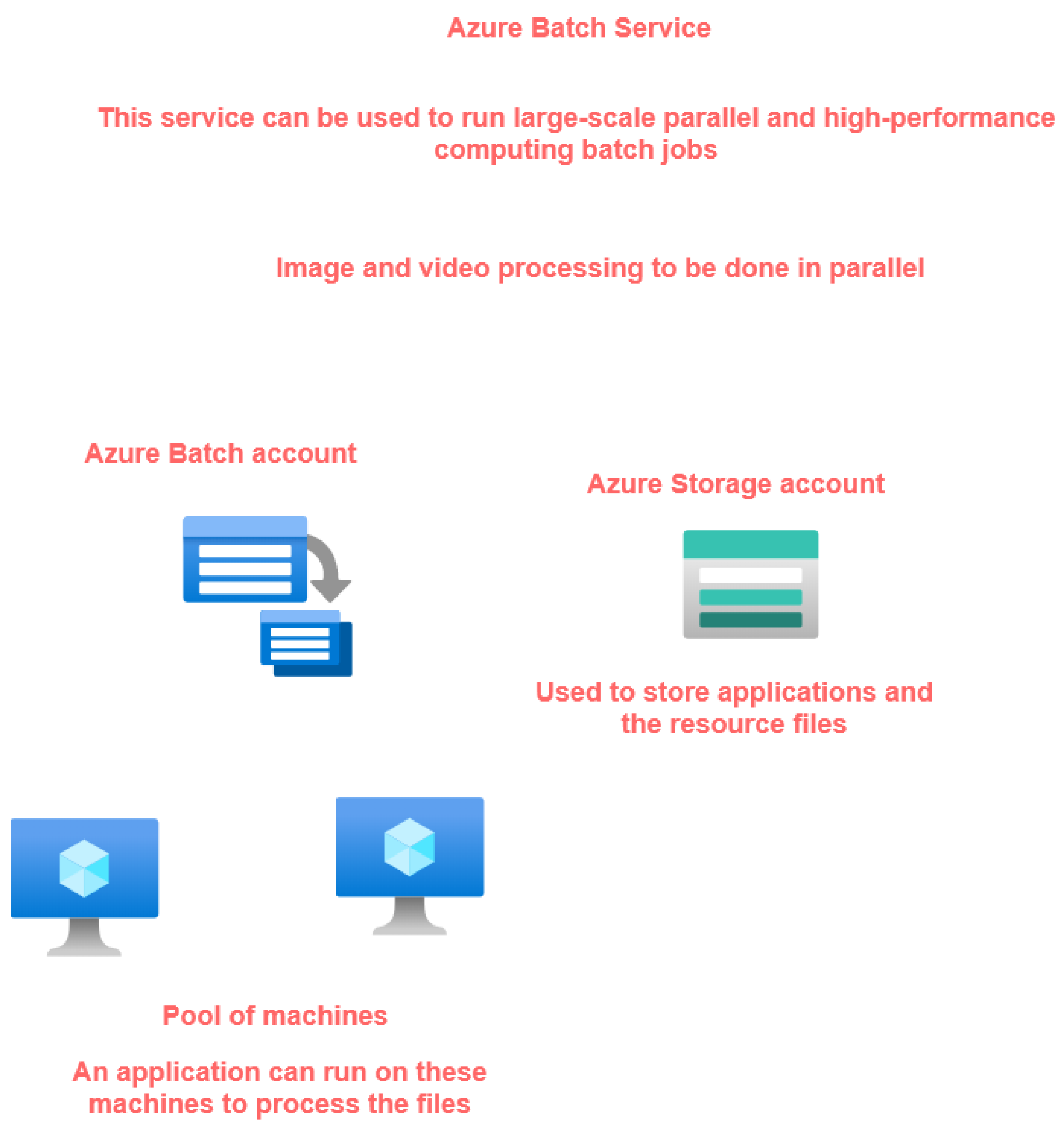
Don't run web applications in Azure Functions

The different virtual machine sizes

- **General Purpose**
- Av2-series VMs – These are best suited for entry level workloads for development and test environments.
- DCsv2 – These virtual machines have the latest processor technology that can be used to protect the confidentiality and integrity of data and code. It enables customers to build secure enclave-based applications that can protect code and data while its in use.
- **Compute Optimized**

- Fsv2-series – These give a higher CPU-to-memory ratio. These instances are good for medium traffic web servers, network appliances and application servers.
- **Memory optimized**
- These give a high memory-to-CPU ratio. This is good for hosting relational database servers, caching-based application and in-memory analytics.
- Ev3, Esv3 series
- M series – This provides a high vCPU count – up to 128 vCPUs and high memory – up to 3.8 TiB.
- **Storage optimized**
- These give high disk throughput and IO, this is ideal for Big Data applications, SQL , NoSQL databases, data warehousing – Lsv2-series

The Azure Batch service

- 

  Azure Batch Service

  This service can be used to run large-scale parallel and high-performance computing batch jobs

  Image and video processing to be done in parallel

  Azure Batch account

  Azure Storage account

  Used to store applications and the resource files

  Pool of machines

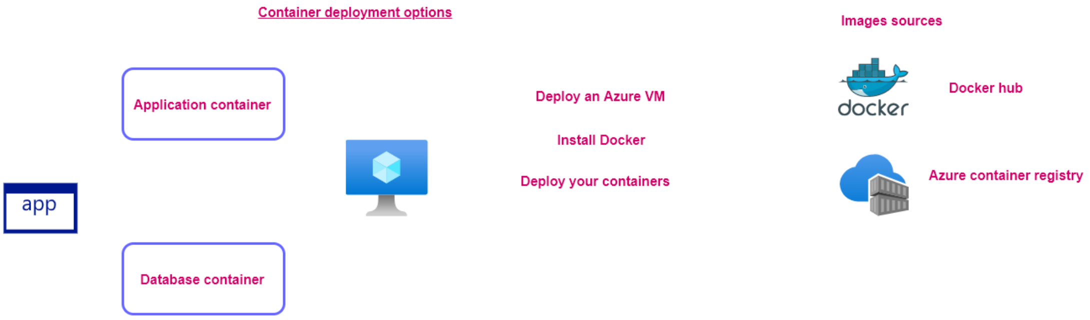
  An application can run on these machines to process the files

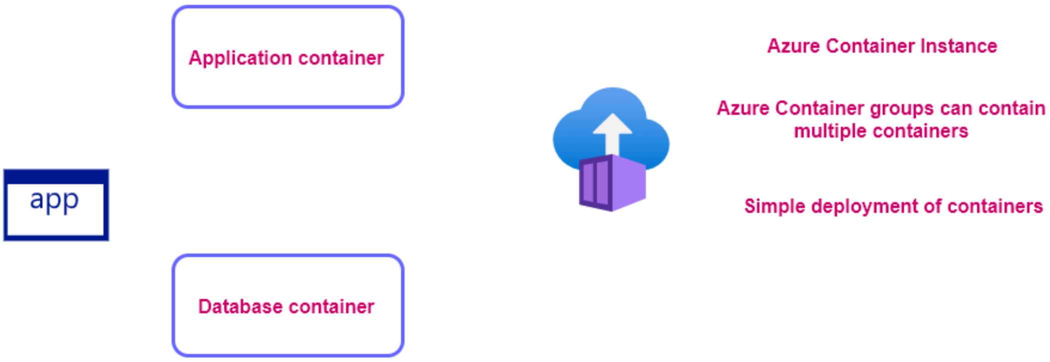
  Nodes are used in the Azure Batch account to run the applications that would process your workloads.

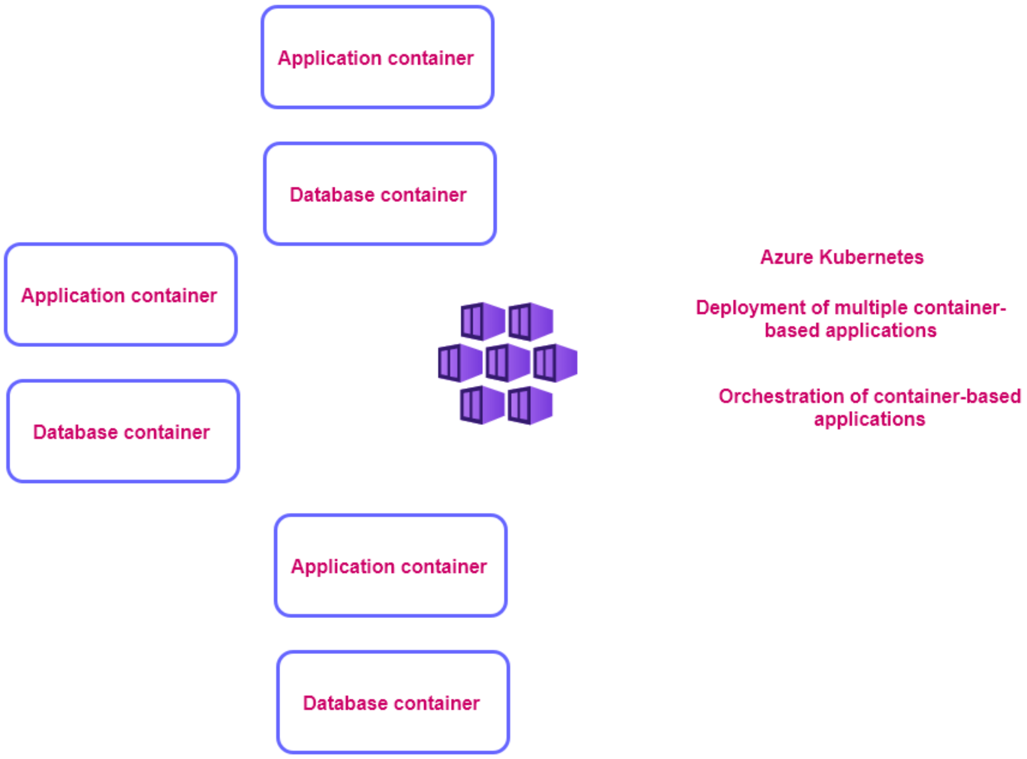
- The nodes are run in a pool that are defined in the Azure Batch account.
- Scripts or executables can run on the nodes.
- Executables or scripts include *.exe, *.cmd, *.bat, and PowerShell scripts (for Windows) and binaries, shell, and Python scripts (for Linux).
- You can have two types of nodes
- **Dedicated nodes** – These are reserved nodes that can guarantee that the jobs will run on the nodes.

- **Low-priority nodes** – These are less expensive , but they depend on the surplus capacity that is available in Azure.

Different Container deployment options




Application container
app
Database container
Azure Container Instance
Azure Container groups can contain multiple containers
Simple deployment of containers



Application container

Database container

Application container

Database container

Application container

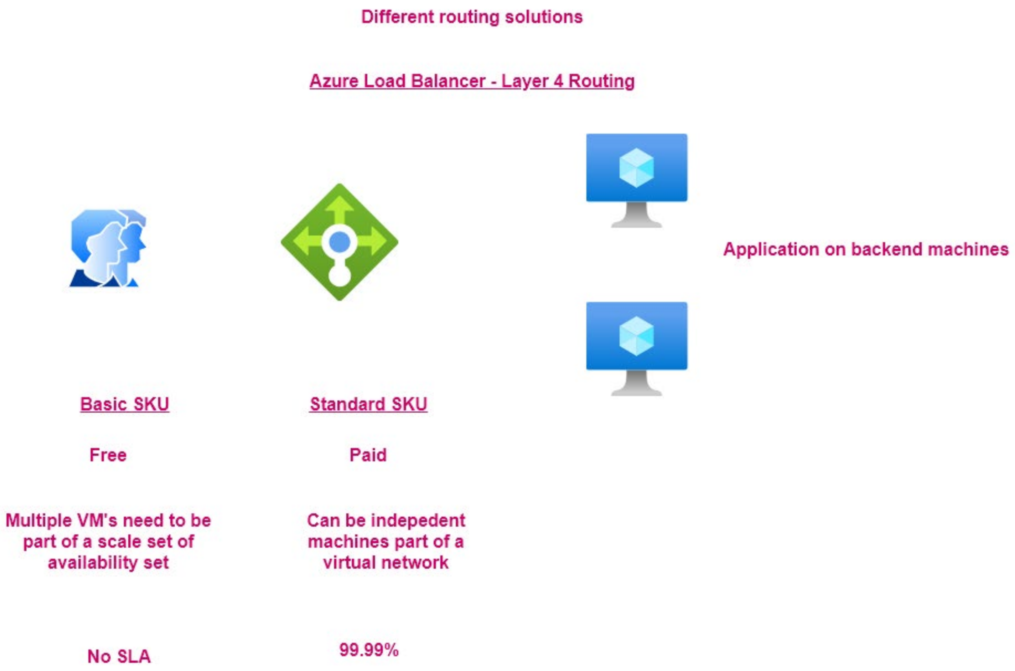
Database container

Azure Kubernetes

Deployment of multiple container-based applications

Orchestration of container-based applications

Different network routing solutions



Different routing solutions

Azure Load Balancer - Layer 4 Routing

Application on backend machines

Basic SKU	Standard SKU
Free	Paid
Multiple VM's need to be part of a scale set of availability set	Can be indepedent machines part of a virtual network
No SLA	99.99%

Azure Application Gateway - Layer 7 Routing

Application on backend machines

URL Routing

https://cloudportalhub.com/images

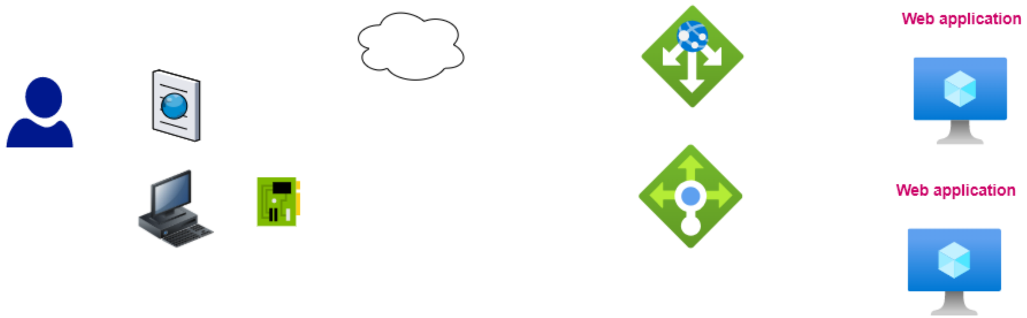
https://cloudportalhub.com/videos

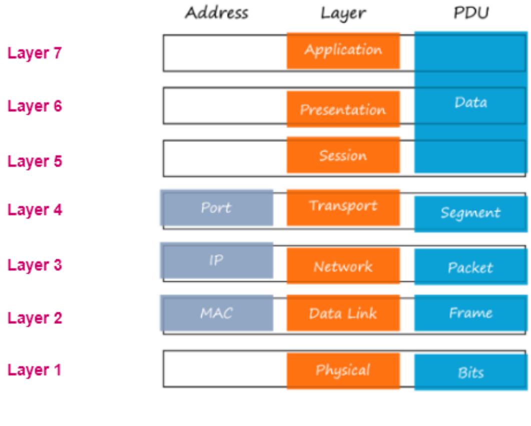
SSL Termination

Multiple web site routing

	Address	Layer	PDU
Layer 7		Application	Data
Layer 6		Presentation	
Layer 5		Session	
Layer 4	Port	Transport	Segment
Layer 3	IP	Network	Packet
Layer 2	MAC	Data Link	Frame
Layer 1		Physical	Bits

OSI model

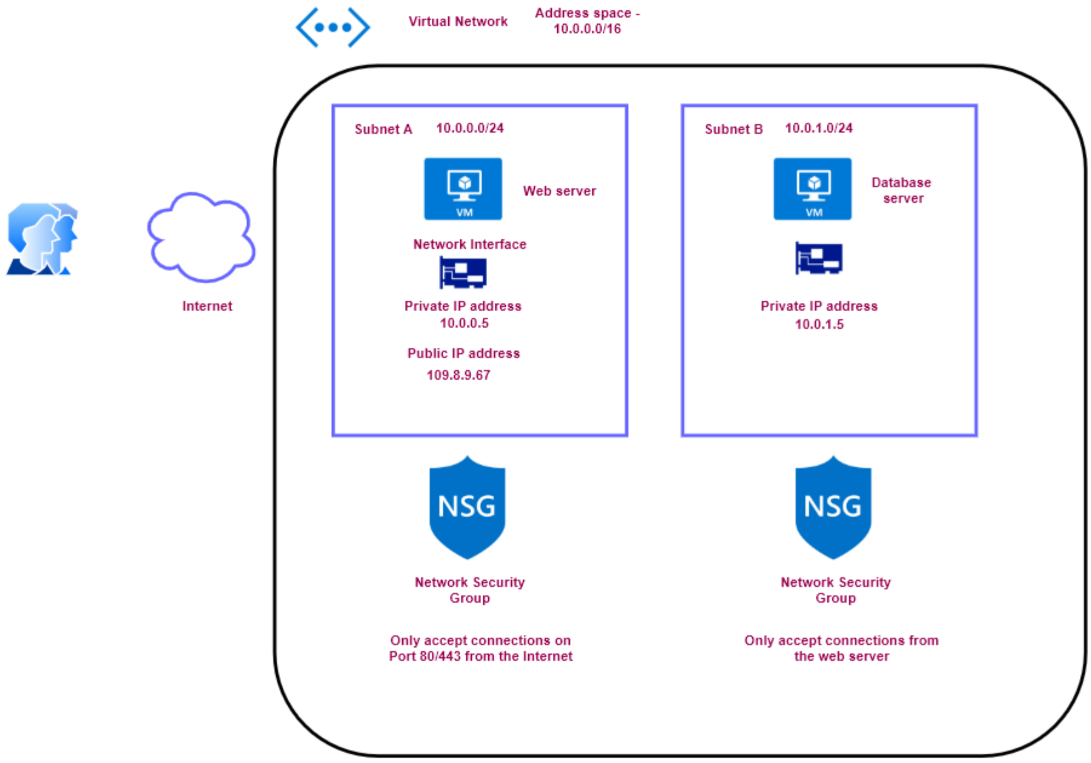




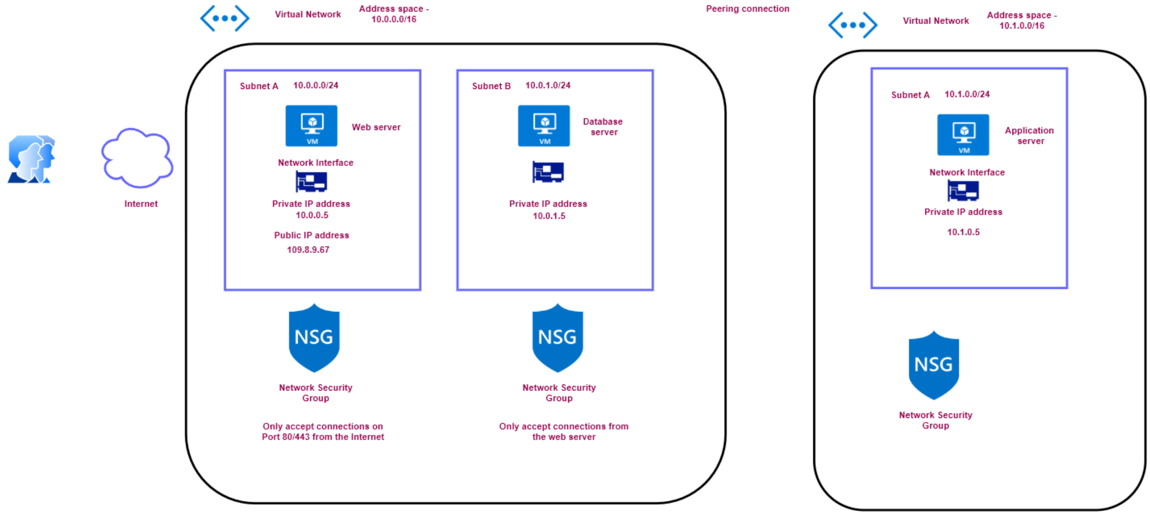
	Address	Layer	PDU
Layer 7		Application	Data
Layer 6		Presentation	
Layer 5		Session	
Layer 4	Port	Transport	Segment
Layer 3	IP	Network	Packet
Layer 2	MAC	Data Link	Frame
Layer 1		Physical	Bits

OSI model

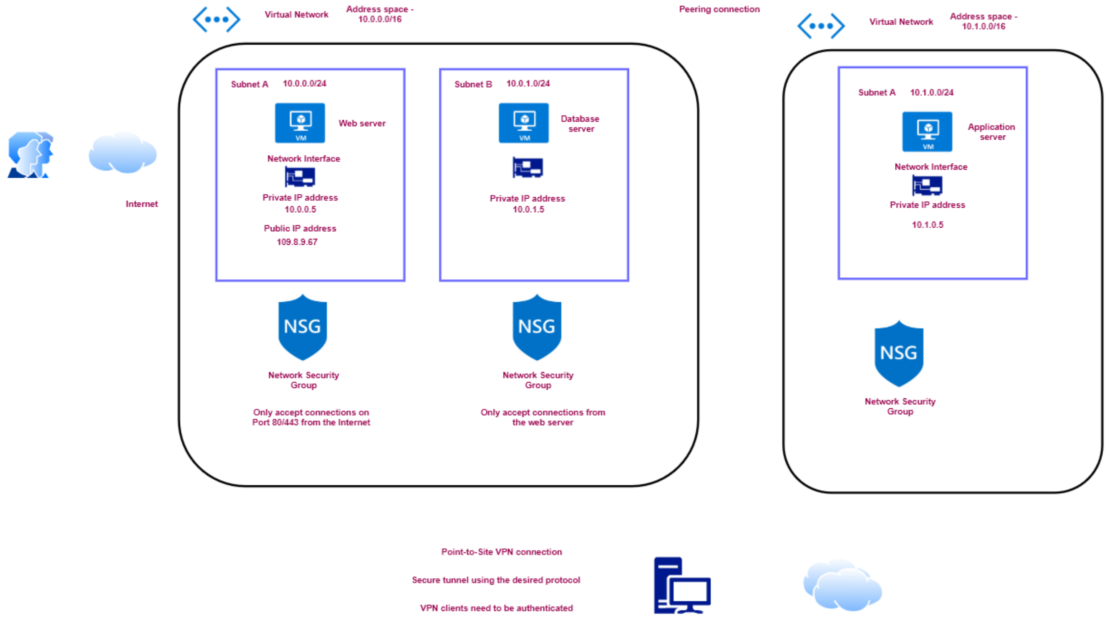
Review – Azure virtual networks


Virtual Network
Address space - 10.0.0.0/16
Internet
Subnet A 10.0.0.0/24
VM
Web server
Network Interface
Private IP address 10.0.0.5
Public IP address 109.8.9.67
Subnet B 10.0.1.0/24
VM
Database server
Private IP address 10.0.1.5
NSG
Network Security Group
Only accept connections on Port 80/443 from the Internet
NSG
Network Security Group
Only accept connections from the web server

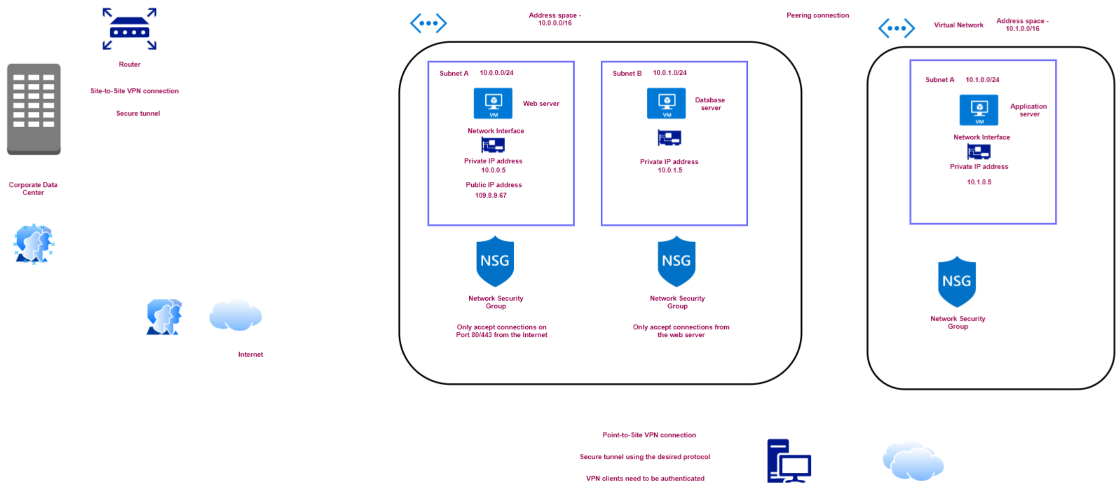
Review – Azure virtual network peering



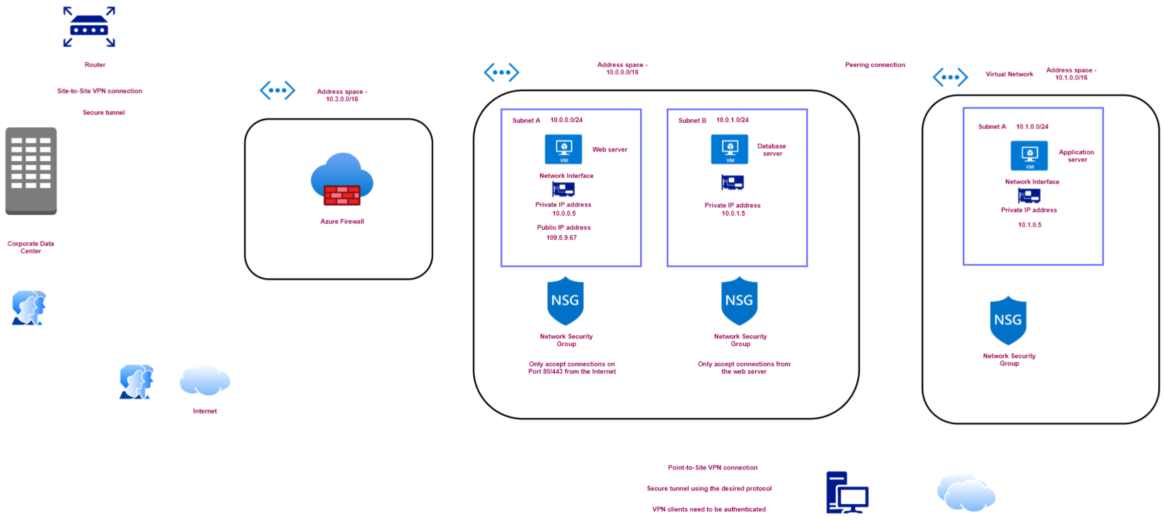
Review – Point-to-Site VPN connections


Virtual Network
Address space - 10.0.0.0/16
Peering connection
Virtual Network
Address space - 10.1.0.0/16
Internet
Subnet A 10.0.0.0/24
Web server
VM
Network Interface
Private IP address 10.0.0.5
Public IP address 109.8.9.67
Subnet B 10.0.1.0/24
Database server
VM
Private IP address 10.0.1.5
NSG
Network Security Group
Only accept connections on Port 80/443 from the Internet
NSG
Network Security Group
Only accept connections from the web server
Subnet A 10.1.0.0/24
Application server
VM
Network Interface
Private IP address
10.1.0.5
NSG
Network Security Group
Point-to-Site VPN connection
Secure tunnel using the desired protocol
VPN clients need to be authenticated

Review – Site-to-Site VPN connections


Router
Site-to-Site VPN connection
Secure tunnel
Corporate Data Center
Internet
Address space - 10.0.0.0/16
Subnet A 10.0.0.0/24
Web server
VM
Network Interface
Private IP address 10.0.0.5
Public IP address 109.8.9.67
Subnet B 10.0.1.0/24
Database server
VM
Private IP address 10.0.1.5
NSG
Network Security Group
Only accept connections on Port 80/443 from the Internet
NSG
Network Security Group
Only accept connections from the web server
Peering connection
Virtual Network
Address space - 10.1.0.0/16
Subnet A 10.1.0.0/24
Application server
VM
Network Interface
Private IP address
10.1.0.5
NSG
Network Security Group
Point-to-Site VPN connection
Secure tunnel using the desired protocol
VPN clients need to be authenticated

Review – Azure Firewall


Router
Site-to-Site VPN connection
Secure tunnel
Corporate Data Center
Internet
Address space - 10.3.0.0/16
Azure Firewall
Address space - 10.0.0.0/16
Subnet A 10.0.0.0/24
Web server
VM
Network Interface
Private IP address 10.0.0.5
Public IP address 109.8.9.67
Subnet B 10.0.1.0/24
Database server
VM
Private IP address 10.0.1.5
NSG
Network Security Group
Only accept connections on Port 80/443 from the Internet
NSG
Network Security Group
Only accept connections from the web server
Peering connection
Virtual Network
Address space - 10.1.0.0/16
Subnet A 10.1.0.0/24
Application server
VM
Network Interface
Private IP address
10.1.0.5
NSG
Network Security Group
Point-to-Site VPN connection
Secure tunnel using the desired protocol
VPN clients need to be authenticated

Azure Network Watcher

- This service provides tools to monitor, diagnose , view metrics, and enable or disable logs for resources in an Azure virtual network.
- It is used to monitor the network for your Infrastructure as a service.
- This tool is not intended for monitoring your PaaS solutions or for Web Analytics.

- **<u>Connection Monitor</u>**

- This provides a unified end-to-end connection monitoring in Azure Network Watcher.
- This supports both Azure and hybrid setups as well.
- With this tool you can get better visibility into network performance.
- It supports connectivity checks based on HTTP, TCP, ICMP.

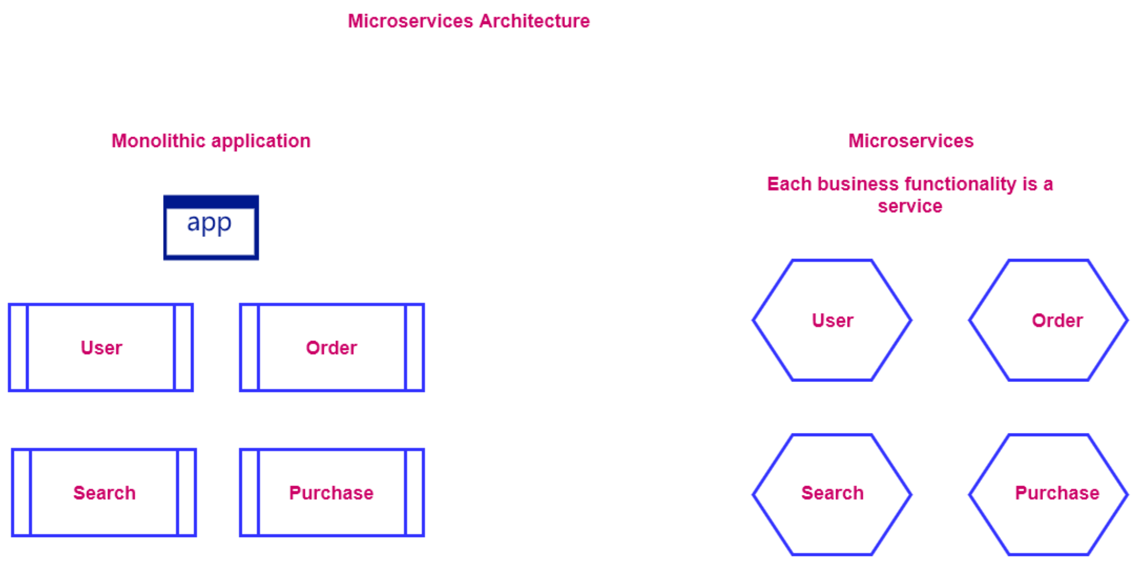
- **IP flow verify – Detecting traffic filtering problems**
- This tool can be used to check if a packet has been allowed or denied access to or from a virtual machine.
- You can choose to check the packet flow based on Protocol (TCP,UDP) , Local and Remote IP address and Port number.
- This tool basically looks at the rules in the Network Security Groups assigned to the subnet or the virtual machine NIC.
- You can use this tool to confirm whether a rule in the Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

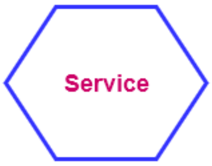
- **Next Hop – Detecting virtual machine routing problems**
- This tool can be used to check if traffic is being sent to the destination based on the routes associated with the network interface.
- You can get the Next hop type ; IP address and Route table being used to route traffic.
- You can use this to understand whether traffic is being routed to the intended destination.

- **Packet Capture**
- This can be used to capture traffic to and from a virtual machine.

- **Network Security Group Logging**
- This tool gives more information on the ingress and egress IP traffic flowing via a Network Security Group.
- Here the flow logs are written in JSON format.
- **Traffic Analysis**
- This provides visibility into the user and application activity
- This tool analyzes the Network Watcher network security groups flow logs
- It then provides more insights into the traffic flow

Microservices Architecture





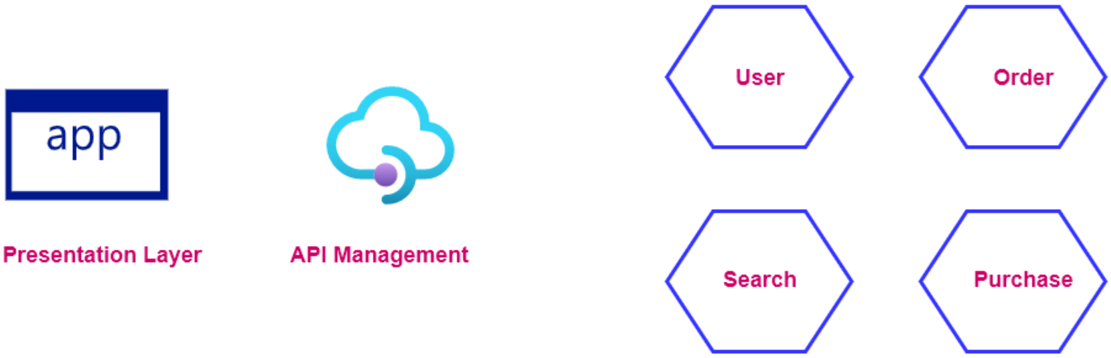
Each service is self-contained

Each service implements a specific business function

Each service has a seperate codebase that is managed by a small development team

It should be easy to update the service independently without breaking the entire application that consumes the service

Each service normally persists its own data



Advantages

Agile

Smaller code base

Mix and match technologies

Fault isolation

Disadvantages

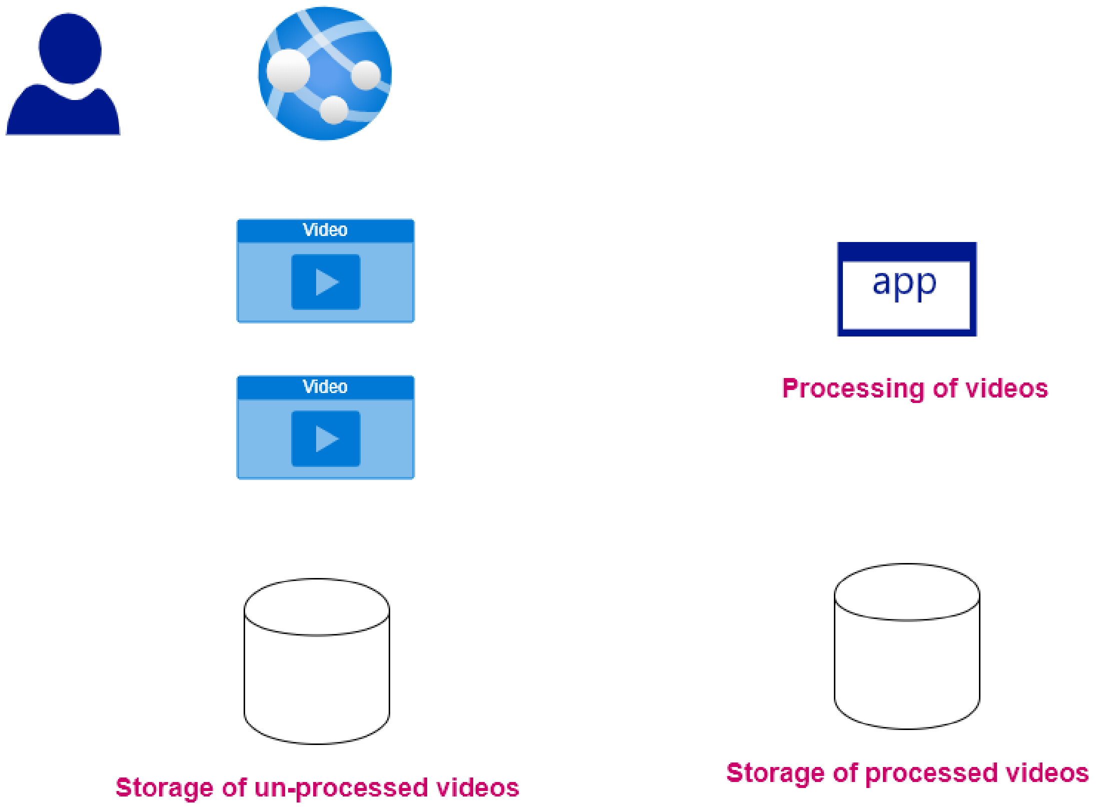
Complexity

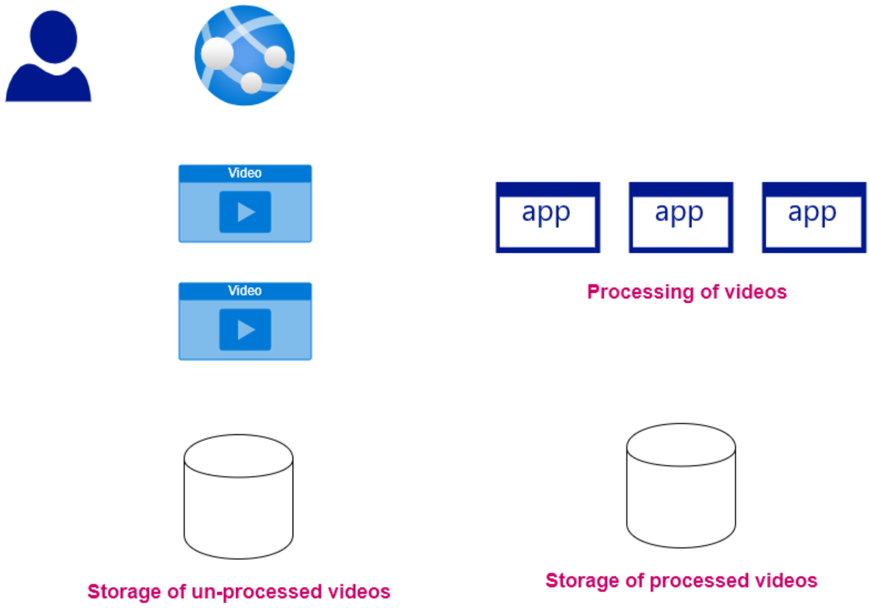
Testing

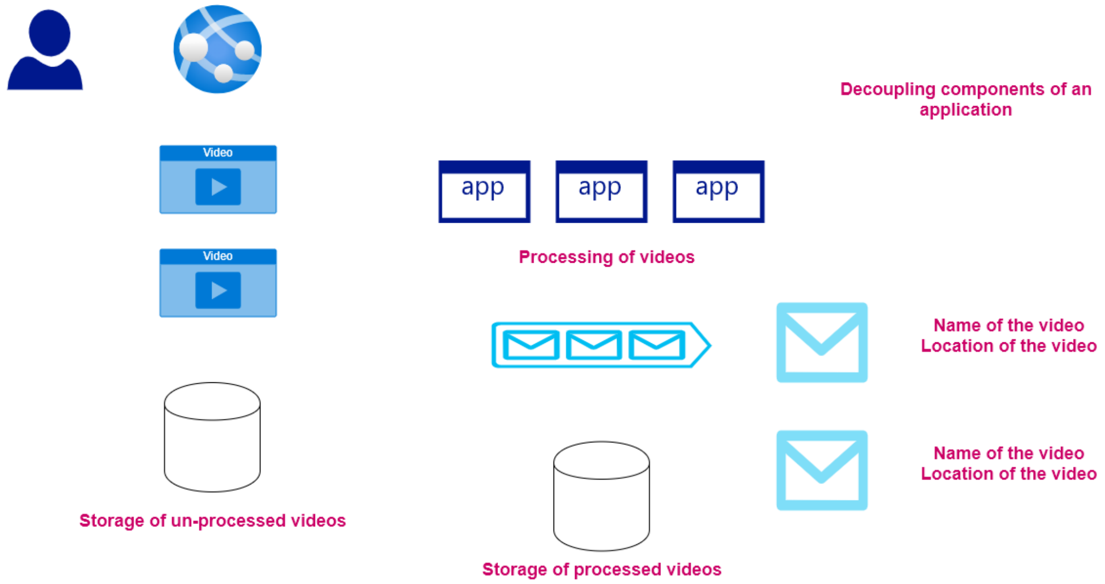
Governance

Data Integrity

The need of a queue service


Video
Video
app
Processing of videos
Storage of un-processed videos
Storage of processed videos


Video
Video
app
app
app
Processing of videos
Storage of un-processed videos
Storage of processed videos



Decoupling components of an application

Processing of videos

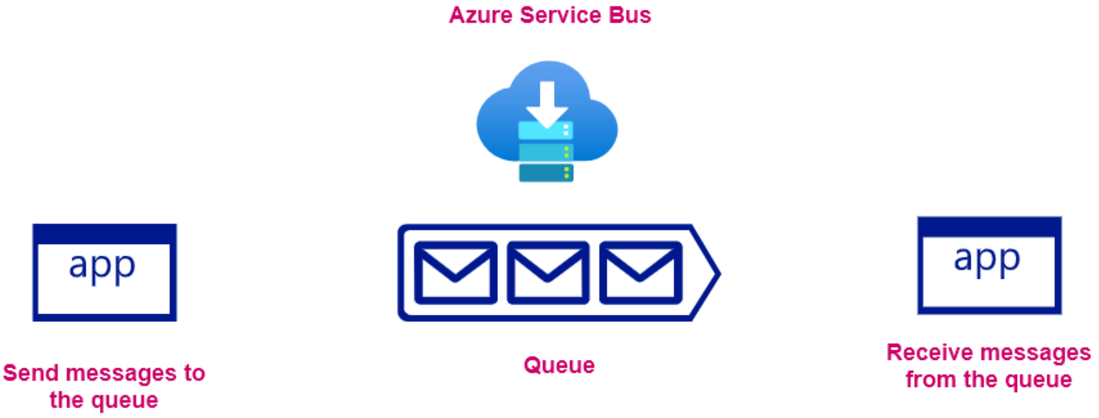
Name of the video
Location of the video

Name of the video
Location of the video

Storage of un-processed videos

Storage of processed videos

Review – Azure Service Bus

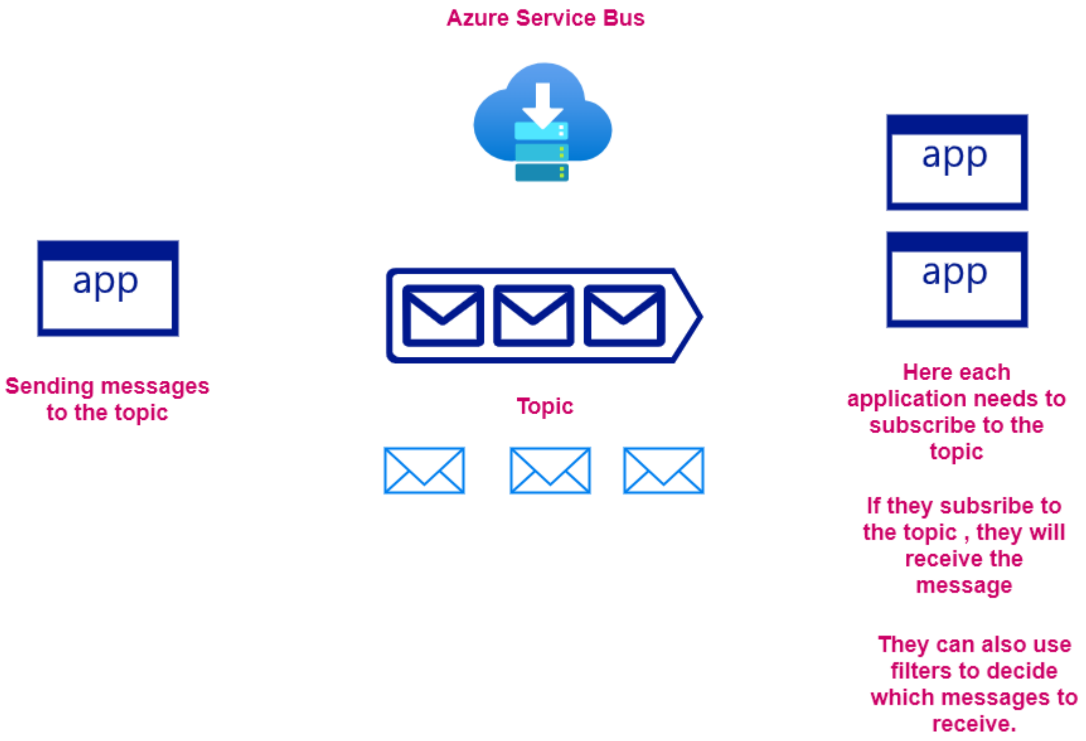


Azure Service Bus

Send messages to the queue

Queue

Receive messages from the queue



Azure Service Bus

Sending messages to the topic

Topic

Here each application needs to subscribe to the topic

If they subsribe to the topic , they will receive the message

They can also use filters to decide which messages to receive.

Review – Azure Logic Apps

Azure Logic Apps

Azure Functions

Developers define logic to perform some steps

When an administrative action is performed on a virtual machine

Email an administrator

Azure Event Hubs

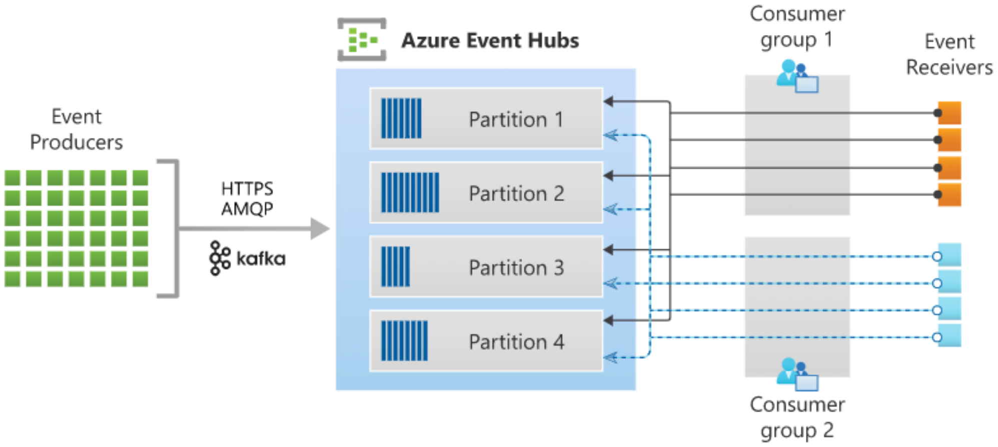
What are Azure Event Hubs

This is a big data streaming platform

This service can receive and process millions of events per second

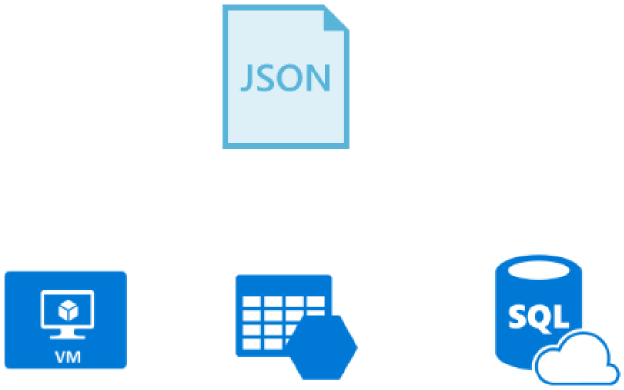
You can stream log data , telemetry data, any sort of events to Azure Event Hubs

Event Hubs Architecture

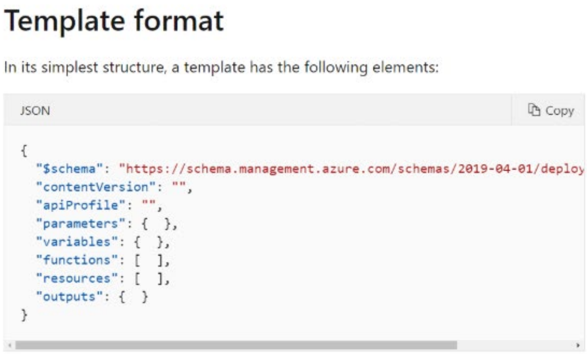


https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-features

ARM Templates review



https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-syntax



Template format

In its simplest structure, a template has the following elements:

JSON

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploy
  "contentVersion": "",
  "apiProfile": "",
  "parameters": {  },
  "variables": {  },
  "functions": [  ],
  "resources": [  ],
  "outputs": {  }
}
```

Version of the template language being used

Version of the template

Collection of API version for resource types

Values that can be provided during deployment

Values that can reused in the template

Resource that need to be deployed

Values that can be retrived after resource deployment

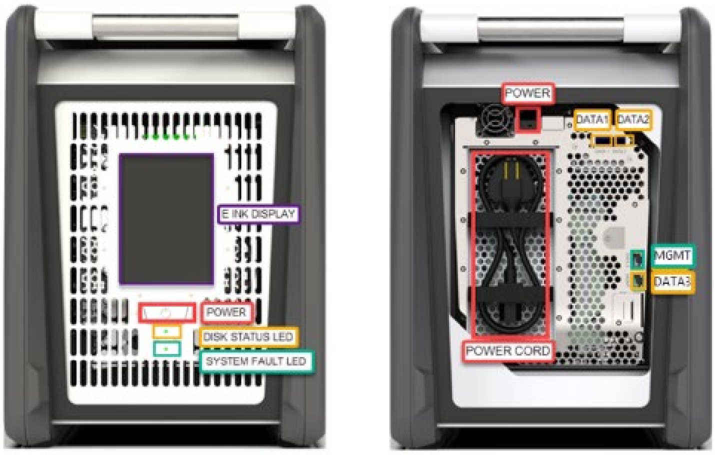
Azure Data Box

Azure Data Box

Transfer a large data set to Azure

Migrating large data sets onto Azure

https://docs.microsoft.com/en-us/azure/databox/data-box-overview



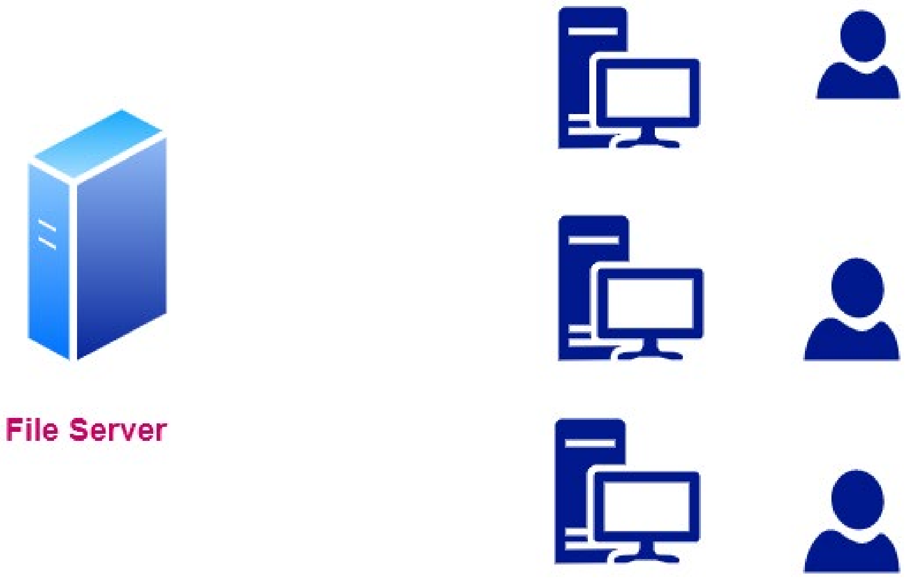
Data Box front view (left) and back view (right)

Data Box device - This device will get shipped to you

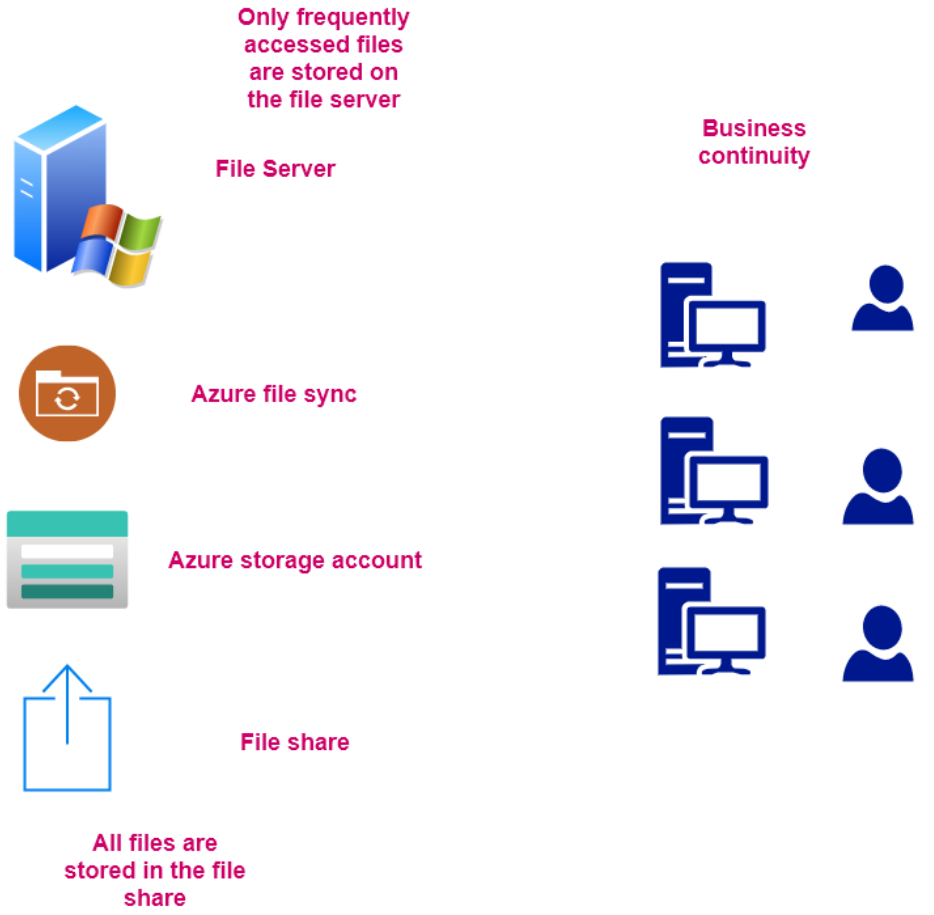
You the copy the data locally onto the device

Ship the device back to Microsoft and the engineers will copy the data onto Azure

Azure File Sync Service



File Server



Only frequently accessed files are stored on the file server

File Server

Azure file sync

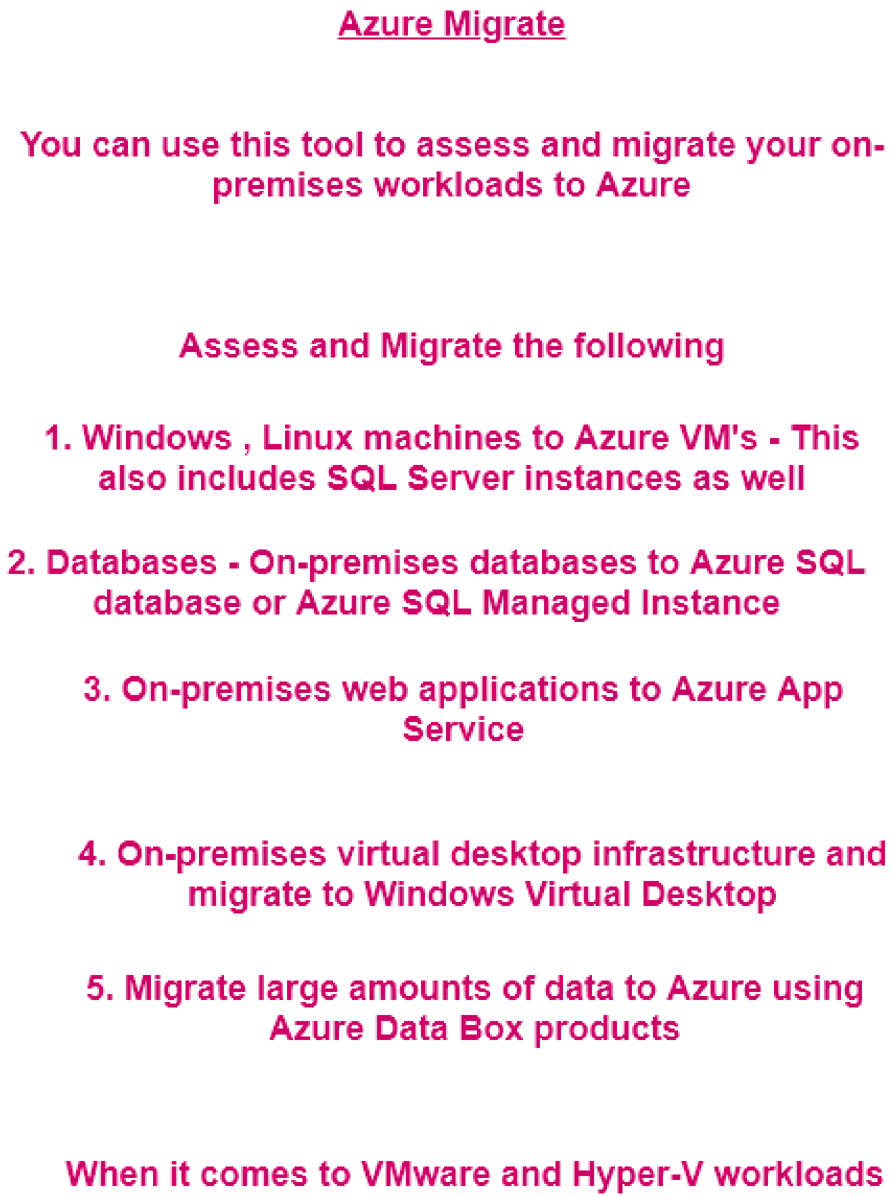
Azure storage account

File share

All files are stored in the file share

Business continuity

Review – Azure Migrate



Azure Migrate

You can use this tool to assess and migrate your on-premises workloads to Azure

Assess and Migrate the following

1. Windows , Linux machines to Azure VM's - This also includes SQL Server instances as well

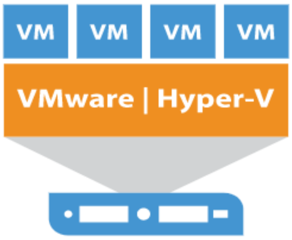
2. Databases - On-premises databases to Azure SQL database or Azure SQL Managed Instance

3. On-premises web applications to Azure App Service

4. On-premises virtual desktop infrastructure and migrate to Windows Virtual Desktop

5. Migrate large amounts of data to Azure using Azure Data Box products

When it comes to VMware and Hyper-V workloads



1. It can check whether the on-premises servers are ready for migration

2. It can estimate the size of Azure VM's that would be required for your on-premises workloads

3. You also get an estimation of cost for running the servers in Azure.

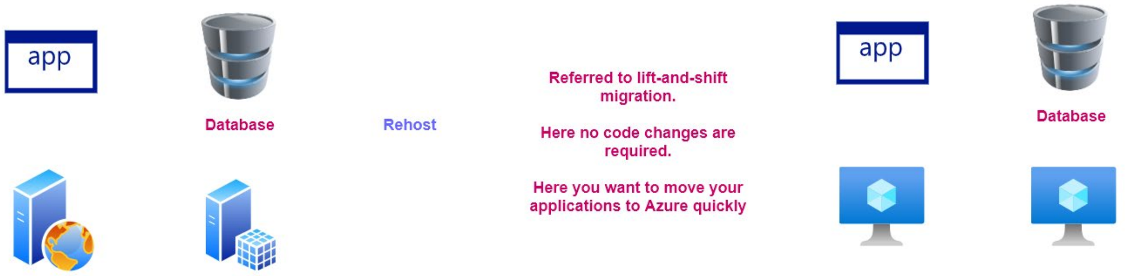
Azure Site Recovery should be used for disaster recovery scenarios

Core difference between Azure Migrate and Azure Site Recovery

Azure Migrate should be used for Migration purposes

Migration Patterns

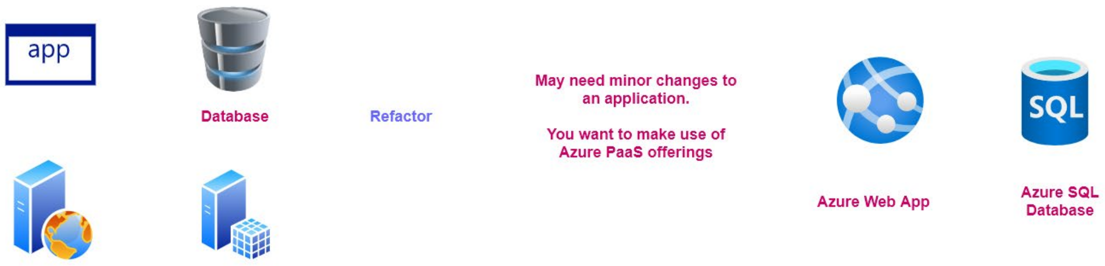
Migration Patterns



Referred to lift-and-shift migration.

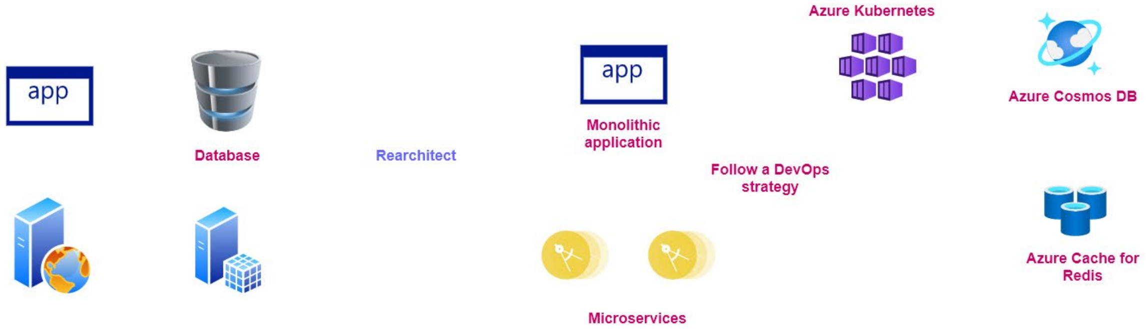
Here no code changes are required.

Here you want to move your applications to Azure quickly



May need minor changes to an application.

You want to make use of Azure PaaS offerings



Database

Rearchitect

Monolithic application

Azure Kubernetes

Azure Cosmos DB

Follow a DevOps strategy

Azure Cache for Redis

Microservices

Rebuild

Rebuild the application from scratch

Follow a DevOps strategy

Use Azure cloud services

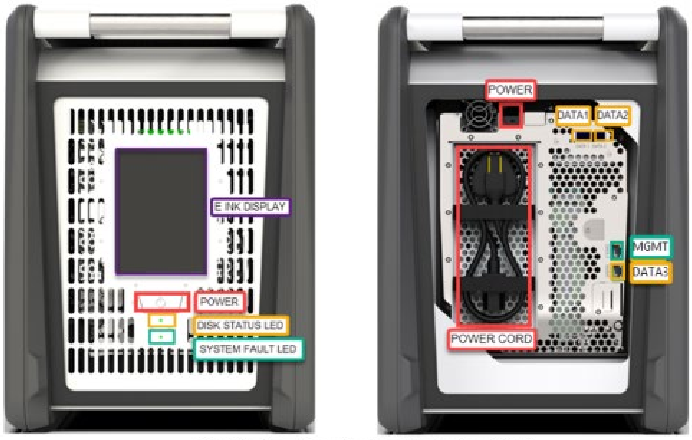
Data Migrations

Data Migrations

Migrate a large SQL Server database to Azure

Use Azure Data Factory to migrate your initial set of data

Use Azure Data Factory to migrate data until the cutoff period



Data Box front view (left) and back view (right)

Use Azure Data Factory to migrate data until the cutoff period

Azure Data Factory - SSIS-Runtime

Run your SSIS workloads in Azure