

# AZ-304



## Microsoft Azure Architect Design

# Program

- 1. Design Authentication and Authorization**
- 2. Design a Network Solution**
- 3. Storage**
- 4. Design a Compute Solution**
- 5. Design a Database Solution**

# Introduction

# Azure Architecture Design Concepts



This course covers several fundamental design concepts of:

- Important architecture concepts
- Requirements, analysis, and design
- Optimizing solutions

# AZ-304 pillars

## Foundational Knowledge

The *Azure Architect Design Fundamentals* course covers several architecture fundamentals topics, which can help you in your AZ-304 learning journey.

**AZ-304**

Azure Architect Design

Security

Scalability

Reliability

Efficiency

**Foundation**

Azure Architecture Design Concepts

# AZ-304 Exam



**The AZ-304 has several business case scenario questions.**

**There will be approximately 40 - 60 questions.**



**You are allowed 120 minutes to take the AZ-304.**

**No time limit for scenario questions.**



# Design Authentication and Authorization

# Authentification and Authorization

## Why is Identity and Access Management (IAM) important?

---

In cloud-focused architecture, identity is a large percentage of the security available. Traditional (legacy) security measures become less effective when we implement shared services that are accessed across multiple provider networks and/or the internet.

# Identity and Access Management

## Useful tips for your IAM environment:



### Single Enterprise Directory

Establish a single enterprise directory for identity management. For IT and security at the least!



### Synchronize Identity Systems

Use Azure AD Connect to sync your Azure AD with exiting on-premises authoritative Active Directory.



### Do NOT:

Synchronize On-Premises Admin accounts to cloud identity providers. High privileged accounts **don't sync by default** in Azure AD Connect.

# Identity and Access Management

## Useful tips for your IAM environment:



### Block Legacy Authentication

Use conditional access to block legacy protocols. Disable legacy protocols for internet-facing services.



### Use Modern Password Protection

Don't rely on passwords with just a mix of character types and minimum lengths. Use and enforce MFA practices as well as strong password rules.



### Use Cross-Platform Credential Management

Azure AD can be used to authenticate Windows, Linux, Azure, O365, AWS and Google services, and third-party software.

## How Multi-Factor Authentication Works

Azure MFA requires two or more elements for full authentication.

### Something You Know

A password or an answer to a security question.

### Something You Possess

A mobile app or a token-generating device.

### Something You Are

Typically a biometric property, fingerprint or a face scan.

# Multi-Factor Authentication

How do you get it?



Azure AD Premium or  
Microsoft 365 Business

Both of these offerings  
support MFA using  
Conditional Access policies



Azure AD Free or  
standalone O365 licenses

Uses pre-created Conditional  
Access baseline policies



Azure AD  
Global Admins

Global Administrator  
accounts have Azure MFA  
capabilities built-in

## Azure MFA is enforced with Conditional Access policies.

These are If-THEN statements

Common access requests that might require MFA:

- IF a specific cloud app is accessed
- IF a user is accessing a specific network
- IF a user is registering a new device on your network
- IF a user is in a particular geographic area



# Supported Authentication Methods

You can use the following methods for Azure MFA:

Always support more than one method so that you have a backup.

## Mobile app

Such as the Microsoft Authenticator app. OATH verification code is changed every 30 seconds. Note, it's useable in China on Android devices.



## Call to a phone

Azure calls a supplied phone number. User approves the authentication using the phone keypad.



## Text message to a phone

A text with a verification code is sent to a mobile phone. User then enters the code into the sign-in interface.



Azure AD Identity Protection is the easiest way to register a MFA method. Requires licenses.

# Steps for securing your identity structure

1 Strengthen credentials

2 Reduce your attack surface

3 Automate threat response

4 Use Cloud intelligence

5 Enable end-user self-service

Note: Most of the recommendations only apply to applications configured to use Azure AD as their identity provider.

# Strengthen credentials

## Use strong authentication methods

Azure AD's security defaults enforce MFA for all users and blocks legacy protocol sign-ins. Super easy! Enable with one click.

## Turn off traditional complexity and expiration rules

- Use Azure AD's dynamic banned password feature.
- Require passwords of at least 8 characters.
- Disable expiration rules.
- Disable character-composition requirements.

## Protect against leaked credentials

- Azure AD has a leaked credentials report that reports ID/password pairs exposed to the "dark web" - but only if you enable password hash sync!
- AD FS Smart Lockout - protects against brute force attacks.
- Use Windows Hello for strong two-factor authentication on PCs and mobile devices.

# Reduce Attack Surface

## Block invalid authentication in AD FS

Apps using legacy authentication — POP3, IMAP4, SMTP — are easily compromised. Set up SharePoint and Exchange Online to use modern auth methods. If you have Azure AD Premium, use Conditional Access policies to block legacy authentication.

## Restrict user consent operations

- Consider disabling user consent operations to help minimize risk.
- Use application assignment and conditional access to restrict users to specific applications.

## Implement Azure AD Privileged Identity Management

- Identify and manage users assigned to admin roles.
- Remove unused roles and those with excessive privilege.
- Protect privileged roles with multi-factor authentication.
- Establish rules that ensure privileged roles are granted as-needed.

# Automate Threat Response

## Use Azure AD Identity Protection

If a user's ID is determined to be "at risk" by the Identity Protection system, that ID can be automatically flagged and set to require a password change.

A "sign-in risk" is the likelihood of someone other than an account holder trying to log in. If the risk is medium or above, set the policy to force MFA or block access.

# Use Cloud Intelligence

## Monitor Azure AD

Use Azure logging and auditing to get audit activity reports in the Azure AD portal.

Monitor AD FS with Azure AD Connect Health for hybrid environments.

Azure ID Identity Protection offers two reports that should be monitored daily:

**Risky sign-in & Risky user**

# Enable End-User Self-Service

## Azure AD self-service password reset (SSPR)

Allow users to reset or unlock their accounts. SSPR includes detailed reporting and saves you time!

## Azure AD access reviews

Manage access package and group memberships as well as privileged role assignments to maintain security standards.

## Azure AD entitled management

Assign non-admins the ability to configure access for their teams. O365, Teams, security groups, application roles, and access package catalogs.

# Key Features of Azure Seamless Single Sign-On



## User Experience

Users are automatically signed in to both on-premises and cloud-based applications.



## Web Browser Support

Works on all major browsers that support Kerberos authentication. From Window 7 to 10, Server 2012 R2 and above, and Mac OS X.



## FREE!

You don't need any paid versions of Azure AD to use SSO.



## Easy to deploy

- Can be rolled out via group policy.
- Works with password hash sync or Pass-through Authentication.



## Opportunistic

If SSO fails, user sign-in goes back to a standard login page.



## Non-windows Registration

Register non-Windows 10 devices with Azure AD without the need for Azure AD FS infrastructure.

# Azure Seamless Single Sign-On

## Before you recommend Azure Seamless SSO...

### Does it work everywhere?

Azure Seamless SSO does **NOT** work in Azure Germany and the Microsoft Azure Government cloud.

### Does Seamless SSO support Alternate ID for the username?

Seamless SSO supports \*Alternate ID\* as the username when configured in Azure AD Connect. However, not all O365 apps support \*Alternate ID\*.

### What sign-in methods work with Seamless SSO?

Both password hash synchronization and Pass-through Authentication work with SSO. However, Seamless SSO does **NOT** work with Active Directory Federation Services (ADFS).



# AD Join vs Seamless SSO

## The difference between Azure AD Join and Seamless SSO

### AD JOIN

VS.

### SEAMLESS SSO

Offers SSO to users with devices registered to Azure AD. Said devices do not necessarily have to join the domain.

Works without Azure AD FS. Non-Windows 10 devices can use version 2.1 or later of the Workplace Join client.

**If you have both enabled, AD Join will take precedence over Seamless SSO.**

# The difference between Azure AD Join and Seamless SSO

## The difference between Azure AD Join and Seamless SSO

AD JOIN

VS.

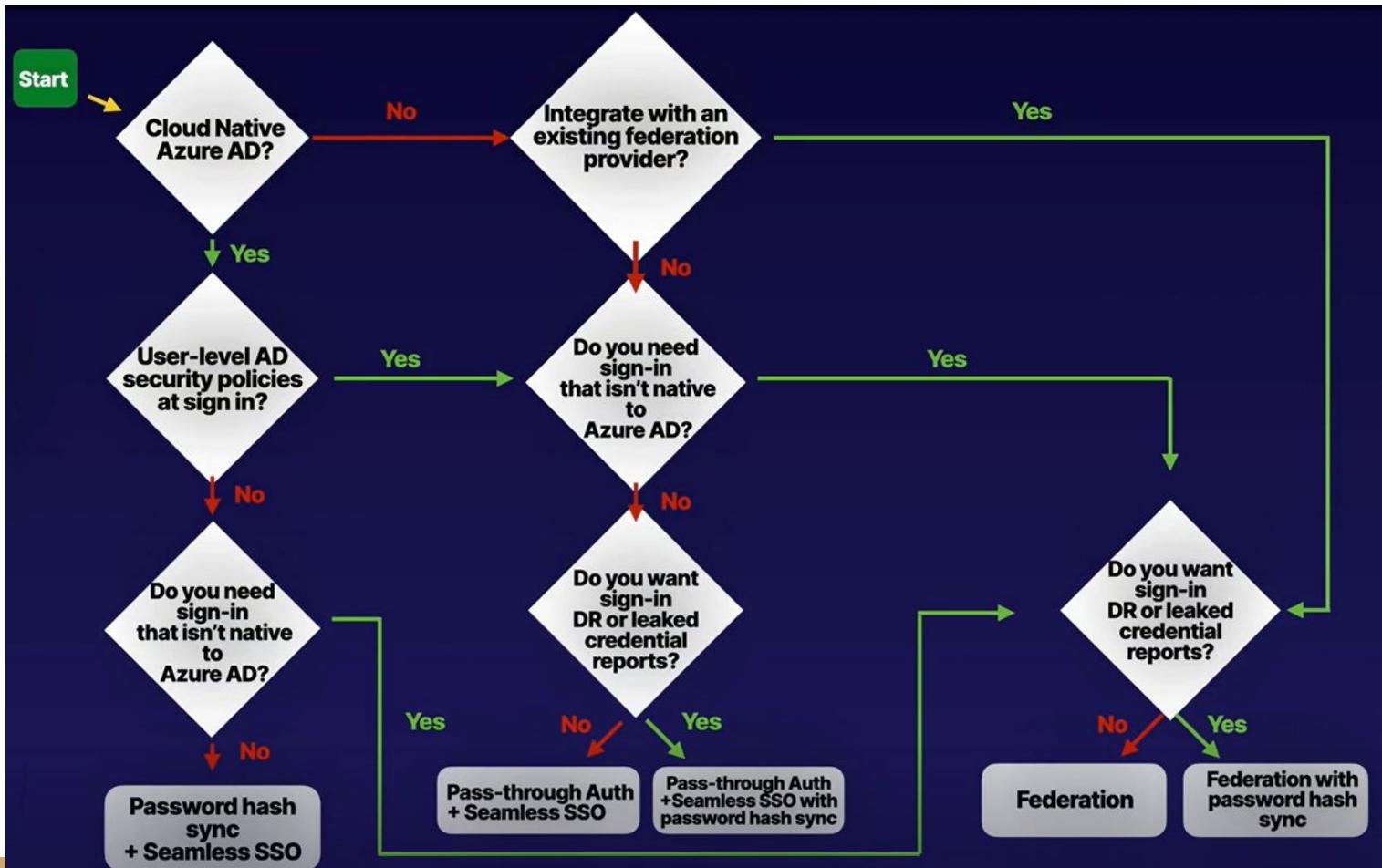
SEAMLESS SSO

Offers SSO to users with devices registered to Azure AD. Said devices do not necessarily have to join the domain.

Works without Azure AD FS. Non-Windows 10 devices can use version 2.1 or later of the Workplace Join client.

If you have both enabled, AD Join will take precedence over Seamless SSO.

# Hybrid Identity Decision Tree



# Hybrid Identity Decision Tree

## Some details on decision tree questions:

- Azure AD can handle sign-in for users without relying on on-premises resources.
- Azure AD can hand off user sign-in to a provider such as AD FS.
- To apply user-level AD security policies, Azure AD requires some on-premises components.

## Sign-in features not natively supported by Azure AD:

- Sign-in using smart cards or certificates
- Sign-in using on-premise MFA server
- Sign-in using third-party authentication
- Multi-site on-premises authentication

**Note: Azure AD Identity Protection requires password hash sync regardless of sign-in method.**



# Hybrid Identity Decision Tree

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
<b>Where does authentication happen?</b>	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
<b>What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?</b>	None	One server for each additional authentication agent
<b>What are the requirements for on-premises Internet and networking beyond the provisioning system?</b>	None	Outbound Internet access from the servers running authentication agents
<b>Is there a TLS/SSL certificate requirement?</b>	No	No
<b>Is there a health monitoring solution?</b>	Not required	Agent status provided by Azure Active Directory admin center
<b>Do users get single sign-on to cloud resources from do- main-joined devices within the company network?</b>	Yes with Seamless SSO	Yes with Seamless SSO
<b>What sign-in types are supported?</b>	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID
<b>What are the multifactor authentication options?</b>	Azure MFA Custom Controls with Conditional Access	Azure MFA Custom Controls with Conditional Access
<b>What are the Conditional Access options?</b>	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

# Hybrid Identity Decision Tree

## Some details on decision tree questions:

- Azure AD can handle sign-in for users without relying on on-premises resources.
- Azure AD can hand off user sign-in to a provider such as AD FS.
- To apply user-level AD security policies, Azure AD requires some on-premises components.

## Sign-in features not natively supported by Azure AD:

- Sign-in using smart cards or certificates
- Sign-in using on-premise MFA server
- Sign-in using third-party authentication
- Multi-site on-premises authentication

**Note: Azure AD Identity Protection requires password hash sync regardless of sign-in method.**



# Comparing Authentication Methods

Consideration	Password hash synchronization + Seamless SSO	Pass-through Authentication + Seamless SSO
<b>Where does authentication happen?</b>	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent
<b>What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?</b>	None	One server for each additional authentication agent
<b>What are the requirements for on-premises Internet and networking beyond the provisioning system?</b>	None	Outbound Internet access from the servers running authentication agents
<b>Is there a TLS/SSL certificate requirement?</b>	No	No
<b>Is there a health monitoring solution?</b>	Not required	Agent status provided by Azure Active Directory admin center
<b>Do users get single sign-on to cloud resources from do- main-joined devices within the company network?</b>	Yes with Seamless SSO	Yes with Seamless SSO
<b>What sign-in types are supported?</b>	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID	UserPrincipalName + password Windows-Integrated Authentication by using Seamless SSO Alternate login ID
<b>What are the multifactor authentication options?</b>	Azure MFA Custom Controls with Conditional Access	Azure MFA Custom Controls with Conditional Access
<b>What are the Conditional Access options?</b>	Azure AD Conditional Access, with Azure AD Premium	Azure AD Conditional Access, with Azure AD Premium

# B2B - What Is It?

## **Business to Business!**

Azure AD B2B allows the partner organization to use their own identity management solution.

- Organizations use their own identities and credentials; Azure AD is not required.
- No management of external accounts or passwords.
- No account synchronization or lifecycle management required.
- Guest accounts are created when an external user redeems their access invitation.

## Functions of Azure AD B2B

Apps and services are shared via Conditional Access policies.

Application and group owners can manage their own guest users.

Azure AD supports external identity providers (Google, Facebook, etc.).

B2B allows for an external user to utilize the self-service sign-up for application access.

# Summary



## IAM - Identity & Access Management

- Single enterprise directory
- Block legacy auth methods
- Use modern password protection
- Cross-platform credential management



## MFA

- Supported by Azure AD Premium or 365 Business
- Enforced with Conditional Access policies
- Auth via mobile app, phone call, or text message



## Securing your Identity Structure

- Strengthen credentials
- Reduce attack surface
- Automate threat response
- Use Cloud Intelligence
- Enable end-user self-service

# Summary



## Seamless Single Sign-on

- Password hash sync and Pass-through Auth work with SSO
- Does not work in Government Cloud
- Free!
- Deployed via group policy



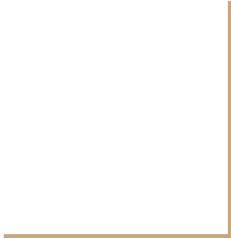
## Hybrid Identity

- Look at your environment to determine auth method.
- Know the difference between password hash synchronization and Pass-through Authentication



## B2B Integration

- Identities and credentials are handled by external organization
- Apps/services are shared via Conditional Access policies
- Azure AD is not required



# Design a Network Solution

# Design a Network Solution

## Considerations when planning your Virtual Network...

**Do any organizational security requirements exist for isolating traffic into separate Virtual Networks or for isolating Virtual Networks into separate regions/subscriptions?**

**How many network interfaces and private IP addresses do you require in a virtual network? (Remember limits!)**

**Do you have any organizational administration requirements for resources in different Virtual Networks?**

**Do you want to connect the Virtual Network to another Virtual Network or on-premises network?**

# Design a Network Solution

## Considerations for subnets...

Some Azure service resources (such as VPN Gateways) require and create their own subnets. Make sure you've allowed space for this.

Azure routes traffic between all subnets in a Virtual Network. Deploy resources to different subnet if routing traffic through a Network Virtual Appliance (NVA).

Network Security Groups (NSGs) can be assigned to subnets to control subnet traffic.

Use service endpoints on subnets to limit access to resources like SQL DBs or Storage Accounts.

# Design a Network Solution

## Considerations for network security...

Filter network traffic between resources using NSGs, NVAs, or both. Use NVAs to create a perimeter network (aka: DMZ) between your Azure resources and the internet.

Application Security Groups (ASGs) apply traffic rules to VMs in the same subnet directly to network interfaces.

Default NSGs allow all traffic to flow between all resources in a Virtual Network.

Change default outbound traffic rules via a route table to force traffic flow through an NVA or a VPN Gateway.

# Design a Network Solution

## Connectivity

### Peering:

**Virtual Networks can be in the same, or different, supported Azure regions.**

**Virtual Networks can be in different subscriptions (even those in different AD Tenants).**

### VPN Gateway:

**Used to connect a Virtual Network to your on-premises network using site-to-site VPN or ExpressRoute.**

**Combining peering and a VPN Gateway to create hub and spoke networks.**

### Name Resolution:

**Azure DNS cannot resolve name of resource in a peered network. Deploy a DNS server or use Azure DNS private domains to resolve names for peering.**

**Name resolution between virtual and on-premises networks also requires a DNS server.**

# Design a Network Solution

## Permissions and Policy

Permissions are assigned to a scope in the following hierarchy:

- Management Group
- Subscription
- Resource Group
- Resource

To work with Virtual Networks, use the Owner, Contributor, or Network Contributor roles.

Azure Policy can define and enforce rules over resources to maintain compliance. For example, they can require the use of NSGs or restrict network resource creation to specific regions.

Policies are applied in the following hierarchy:

- Management Group
- Subscription
- Resource group
- Resource

# Name Resolution in Azure Virtual Networks

## Name Resolution in Azure Virtual Networks

1

Azure DNS private zones

2

Azure-provided name resolution

3

Your own DNS Server

This might forward queries to an Azure-provided DNS server.

# Name Resolution in Azure Virtual Networks

## Scenarios for Name Resolution

-  **Name resolution between VMs located in the same Virtual Network, or Azure Cloud Services role instances in the same cloud service.**  
Azure DNS private zones or Azure-provided name resolution.
-  **Name resolution between VMs in different Virtual Networks or role instances in different cloud services.**  
Azure DNS private zones or your DNS server forwarding queries between networks.
-  **Name resolution from an Azure App Service using Virtual Network integration to role instances or VMs in the same network.**  
Your DNS servers forwarding queries between networks.

# Name Resolution in Azure Virtual Networks

## Scenarios for Name Resolution

✓ **Name resolution from App Service's Web Apps to VMs in the same Virtual Network.**

Your DNS servers forwarding queries between networks.

✓ **Resolution of on-premises computer and service names from VMs or role instances in Azure.**

Your DNS server: on-premises datacenter, local read-only datacenter, or a DNS secondary synced via zone transfer.

## Design a Network Solution

# Scenarios for Name Resolution

✓ **Resolution of Azure hostnames from on-premises computers.**

Forward queries to your DNS proxy server in the corresponding Virtual Network.

✓ **Reverse DNS for internal IP addresses.**

Azure DNS private zones, Azure-provided name resolution, or your own DNS server.

✓ **Name resolution between VMs or role instances located in different cloud services, NOT in a Virtual Network.**

Cannot do this outside a Virtual Network.

# Understanding Azure-Based Name Resolution

## AZURE-PROVIDED NAME RESOLUTION

**Provides only basic authoritative DNS capabilities. DNS zone names and records are automatically managed.**

*Want more control? Use your own DNS servers or Azure DNS private zones!*

- Azure provides internal name resolution for VMs and role instances within the same Virtual Network or cloud service.
- VMs and instances in a cloud service share the same DNS suffix, so a hostname is sufficient. No FQDN required.
- Virtual Networks deployed via the classic deployment model give different DNS suffixes to different cloud services.
- Virtual Networks deployed using the Azure Resource Manager model keeps the DNS suffix consistent across all VMs in a Virtual Network, FQDN not needed.

**Note:** DNS names can be assigned to both VMs and NICs.

# Solutions for Hybrid Networks



HYBRID NETWORKS

**Microsoft says,  
“Use ExpressRoute!”**

ExpressRoute is Azure’s primary solution for extending on-premises networks over a private connection (NSX-T uses it.).

ExpressRoute extends beyond Azure, allowing connections to other Microsoft services, such as Office 365.

# ExpressRoute Connectivity Types

1

## CloudExchange Via Colocation

Cross-connect to Azure by using the Ethernet exchange provided by your colocation facility.

2

## Point-to-Point

Connect your on-premises data centers and offices to Azure via a point-to-point Ethernet link.

3

## Any-to-Any

Connect your WAN to Azure using an IP VPN provider. Gives all WAN connected offices/data centers an equivalent connection to Azure.

# Hybrid Networks

## Considerations for using ExpressRoute...

### Benefits:

- Uses layer 3 connectivity and security standards.
- Can support up to 100 Gbps bandwidth.
- Suited for high-speed and critical business operations.

### Considerations:

- Somewhat complex, requires collaboration with your ISP.
- On-premise installation of high-bandwidth routers required.
- ISP manages the ExpressRoute circuit.
- Does not support the Hot Standby Router Protocol (HSRP), instead use a Border Gateway Protocol (BGP).
- Layer 3, requires a Network Security Appliance for threats.
- Network Security Appliances should be placed between your ISP edge routers and your on-premises network.
- Connectivity monitoring requires the Azure Connectivity Toolkit.

## Recommend Implementations for Secure Hybrid Networks

### Setting up a Perimeter Network

---

Protect your Azure Virtual Network with a perimeter network architecture. This works with either a VPN Gateway or an Azure ExpressRoute connection.

# Components of the Perimeter Network



On-premises  
network



Azure Firewall



Azure Virtual  
Network



NSGs



Gateway

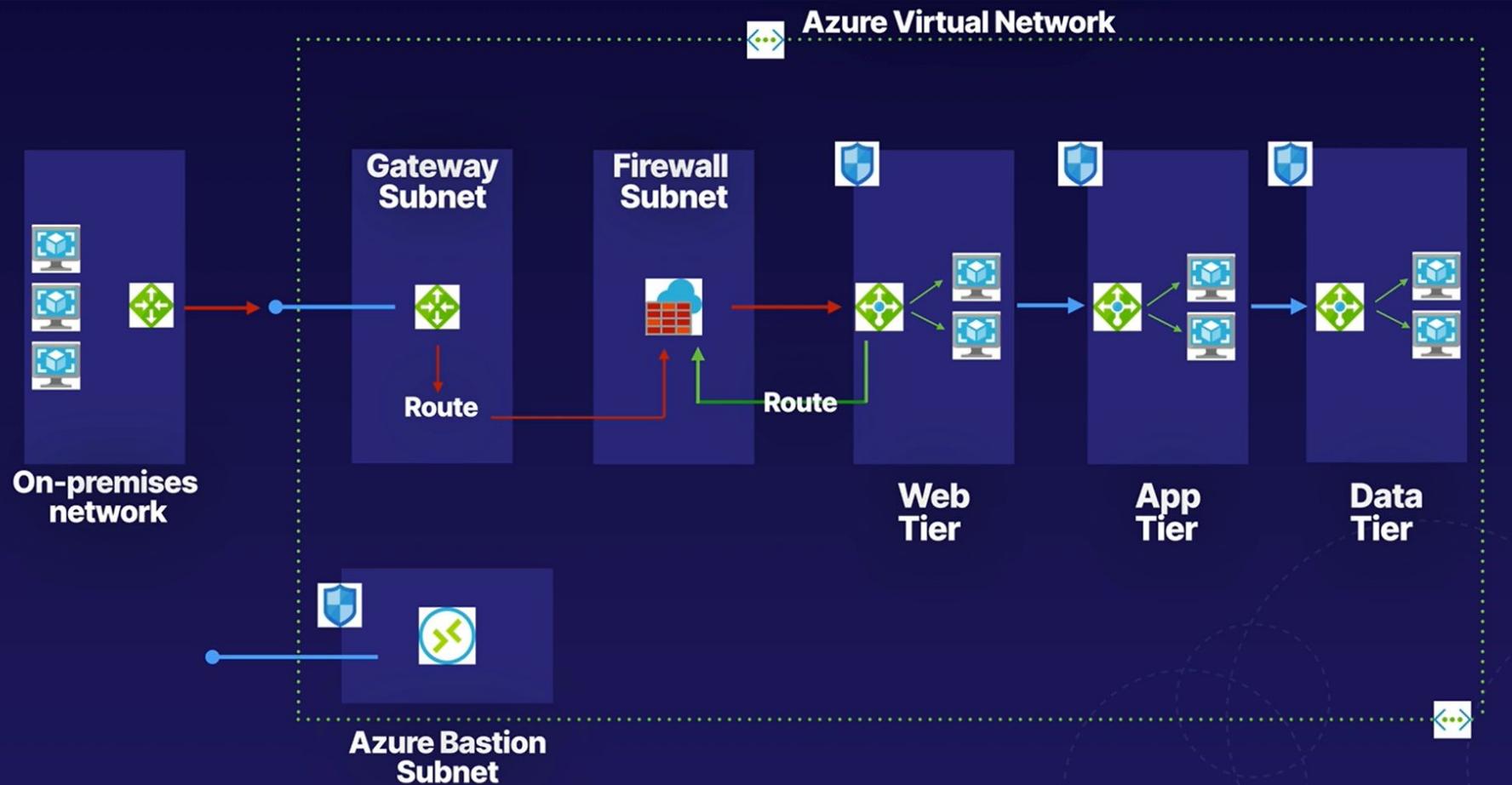


Virtual Network  
routes



Azure Bastion

# Secure Hybrid Network



# Secure Hybrid Network

## SECURITY CONSIDERATIONS:

Routing on-premises users through the firewall.

Use NSGs to block/pass traffic between application tiers.

---

Be sure to organize your Virtual Network assets in the same resource group. This will work for both organizational purposes as well as security.

Assign RBAC roles to resource groups to restrict access to resources.

# Summary

## Planning Virtual Networks

What to keep in mind:

### Handling Name Resolution

- Azure private zones
- Azure-provided name resolution
- Customer-managed DNS (your own)

### Azure Name Resolution

What it does and doesn't do.

### Hybrid Networks

aka: ExpressRoute

### Securing a Hybrid Network

Perimeter Network



**Storage**

# Choosing a storage Tier

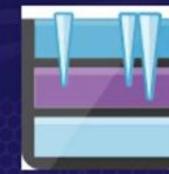
## Blob Storage Tiers



Hot



Cool



Archive

# Choosing a storage Tier

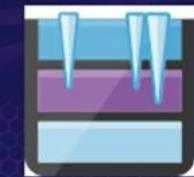
## Storage Cost



Hot



Cool



Archive

\$\$\$



\$

# Choosing a storage Tier

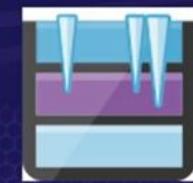
## Transaction Cost (read/writes)



Hot



Cool



Archive

\$



\$\$\$

# Choosing a storage Tier

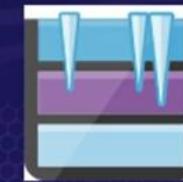
## Access Delay



Hot



Cool



Archive



# Choosing a storage Tier

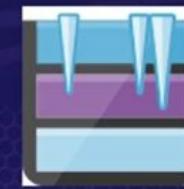
## Early Deletion Fee



Hot



Cool



Archive



# Choosing a storage Tier

## Best Uses



Hot



Cool



Archive

- Actively changing data
- Recent backups

- Older backups
- Storage

- Long-term backups
- Archive data
- Static/historical/compliance (e.g. HIPAA)

# Choosing a Storage Tier

# Choosing a Storage Tier

**Hot, Cool, and Archive Storage**

**Storage Cost**

**Access Delay**

**Transaction Cost**

**Early Deletion Fee for Cool and Archive**

**Best Uses:**

- **Hot – Actively changing data**
- **Cool – Backups & Storage**
- **Archive – Long-term & Historical data**

# Support Tiering for Storage Accounts

## Performance



Standard

Premium

# Support Tiering for Storage Accounts

## Types of Storage Accounts



- General-purpose v2
- General-purpose v1 (Legacy)
- BlockBlobStorage
- FileStorage
- BlobStorage (Legacy)

# Support Tiering for Storage Accounts

## General-purpose (v2)



**Blobs**

**Files**

**Tables**

**Queues**

# Support Tiering for Storage Accounts

## BlockBlobStorage



**Blobs**

**Files**

**Tables**

**Queues**

# Support Tiering for Storage Accounts

## FileStorage



**Blobs**

**Files**

**Tables**

**Queues**

# Support Tiering for Storage Accounts

## Replication

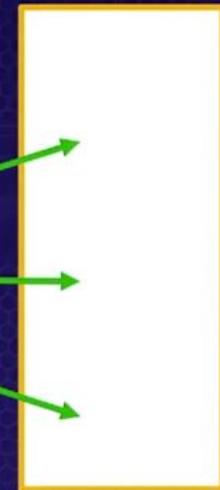
Type of  
Replication



Secondary  
Region



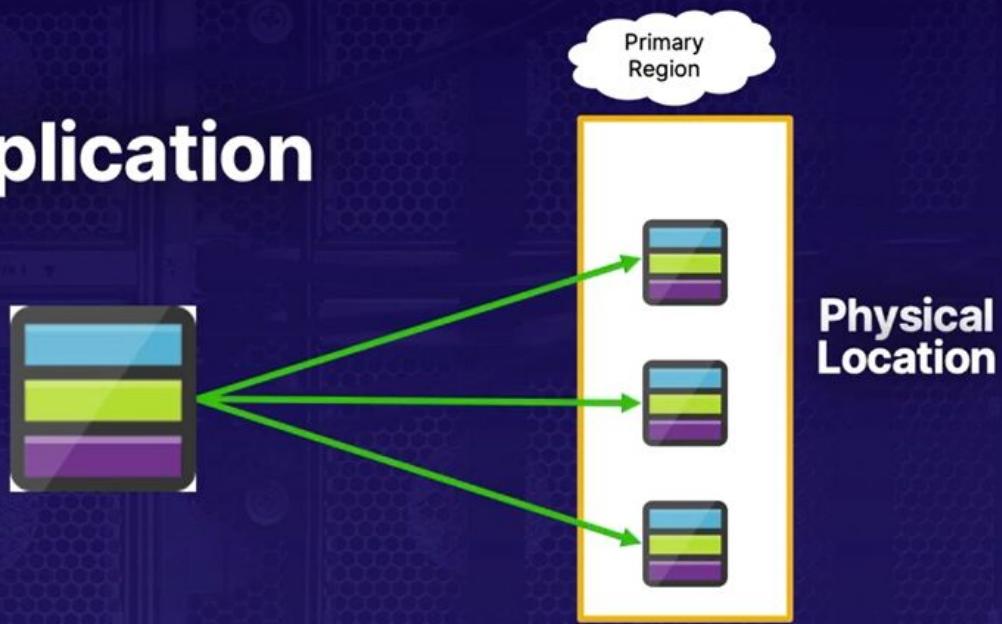
Primary  
Region



# Support Tiering for Storage Accounts

## Replication

Locally  
Redundant  
Storage  
(LRS)

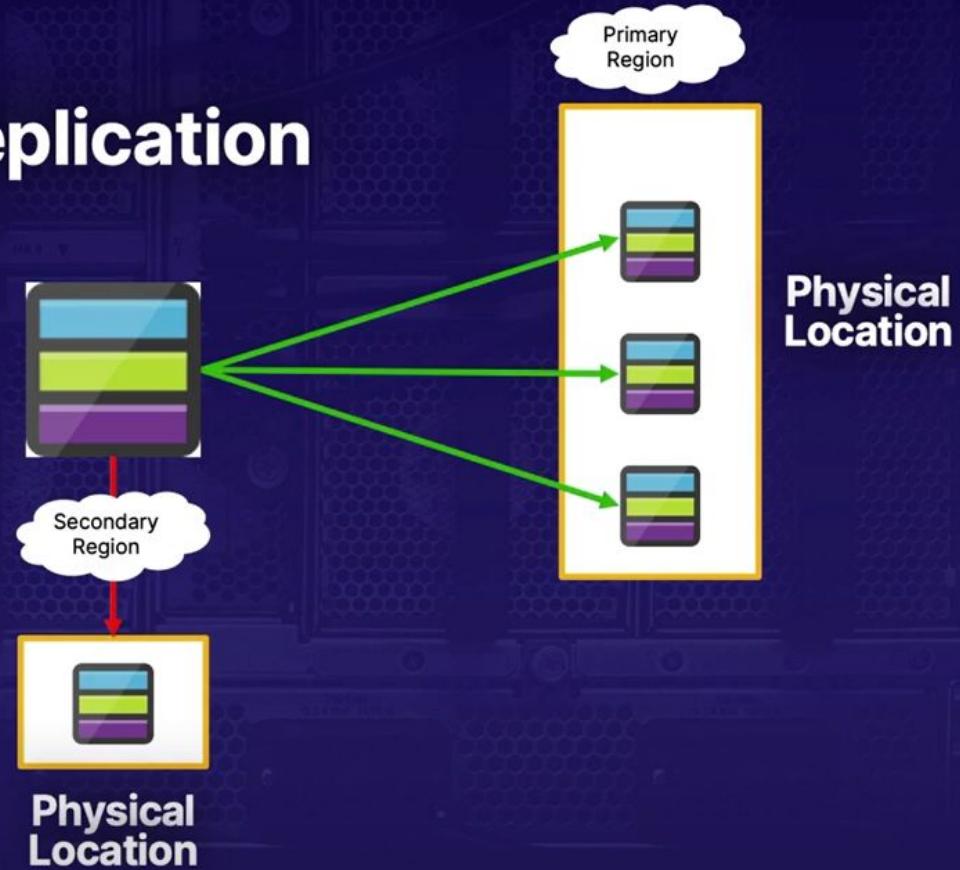


# Support Tiering for Storage Accounts

## Replication

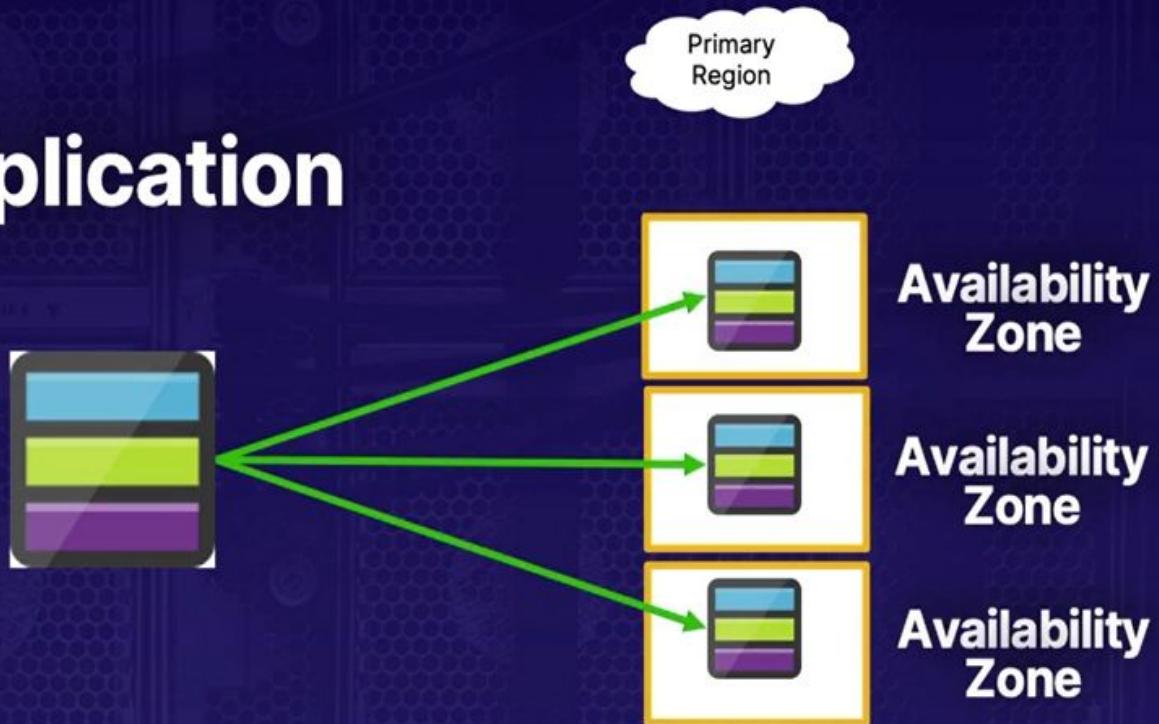
Geo-  
Redundant  
Storage  
(GRS)

Correction: Geo-redundant storage (GRS) makes 3 copies of your data using LRS within the same location at the primary region. In the secondary region, the data is copied 3x by LRS. In total, GRS/RA-GRS makes 6 copies of your data.



# Support Tiering for Storage Accounts

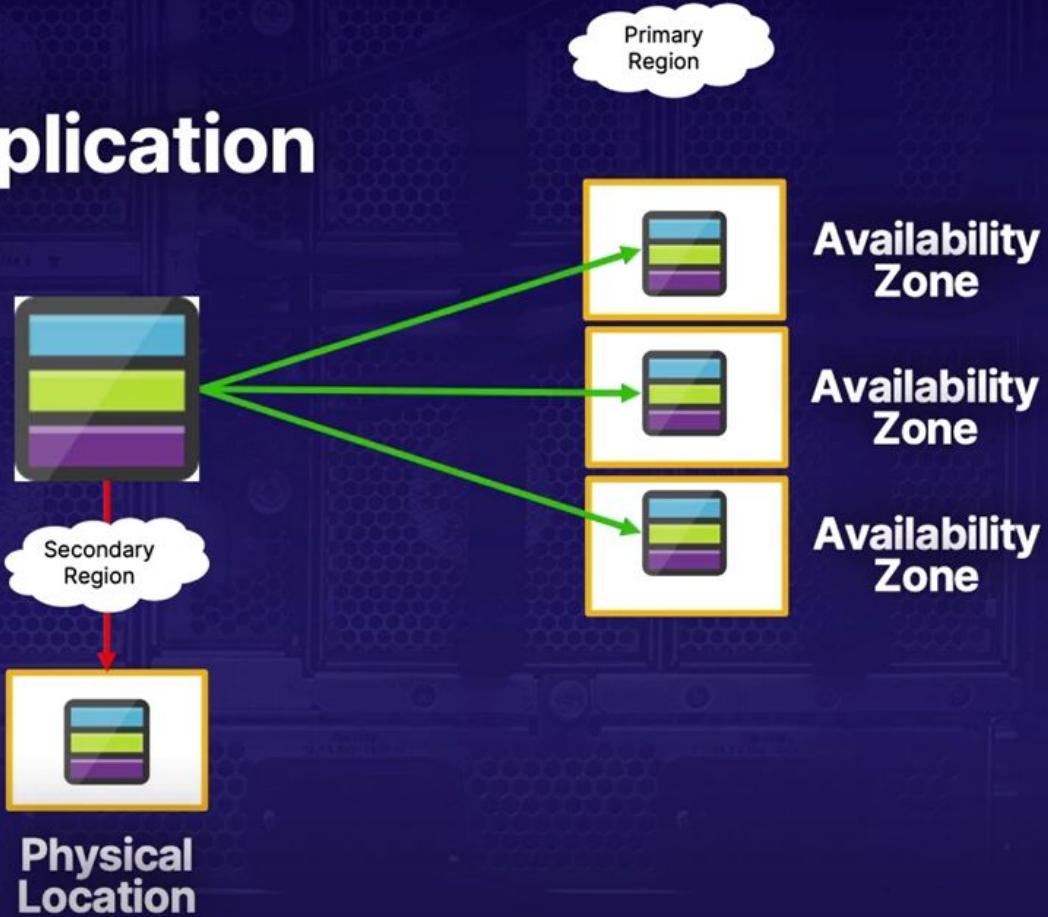
## Replication



# Support Tiering for Storage Accounts

## Replication

**Geo-zone-  
Redundant  
Storage  
(GZRS)**



# Support Tiering for Storage Accounts

# Support Tiering for Storage Accounts

**Recap: Hot, Cool, and Archive Storage**

**Performance – Standard & Premium**

**Types of Storage Accounts**

- General-purpose v2
- BlockBlobStorage
- FileStorage
- Legacy

**Replication - GRS, LRS, ZRS, GZRS**

# Recommended Storage Management Tools

## Recommended Storage Management Tools

### Tool Types:

- Graphical User Interface (GUI)
- Command Line
- Scripting

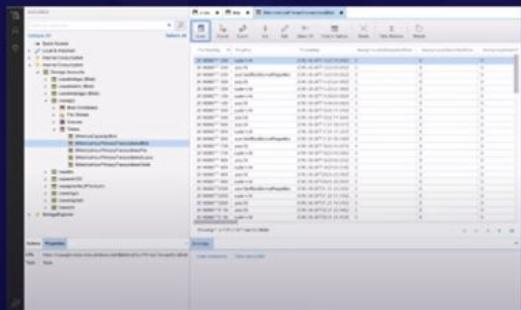
Azure Storage Explorer

Visual Studio Cloud Explorer

# Tool Types - Recommended Storage Management Tools



## Graphical User Interface (GUI)



## Command Line

A screenshot of the Azure Cloud Shell terminal. It shows the terminal prompt 'mark@Azure:-\$ |' and the output of a command: 'Bash Requesting a Cloud Shell. Succeeded. Connecting terminal... Welcome to Azure Cloud Shell Type "az" to use Azure CLI Type "help" to learn about Cloud Shell'. The background is dark with light-colored text.

## Scripting

A screenshot of a PowerShell window showing two examples of blob download scripts. The first script uses the Get-AzStorageBlobContent cmdlet to download 'Image001.jpg' from a specific container to a local destination. The second script does the same for 'Image002.png'. Both scripts include parameters for Container, Destination, and Context.

```
# download first blob
Get-AzStorageBlobContent -Blob "Image001.jpg" ` 
    -Container $containerName ` 
    -Destination "D:\_TestImages\Downloads\" ` 
    -Context $ctx

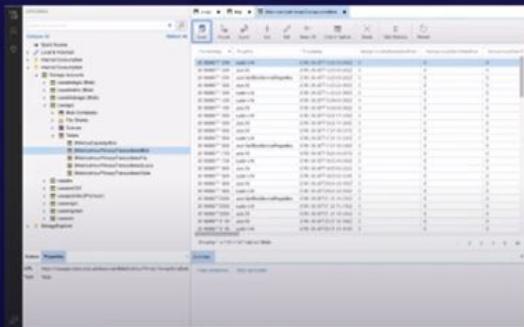
# download another blob
Get-AzStorageBlobContent -Blob "Image002.png" ` 
    -Container $containerName ` 
    -Destination "D:\_TestImages\Downloads\" ` 
    -Context $ctx
```

# Tool Types - Recommended Storage Management Tools

## Recommended Storage Management Tools



- Azure Portal
  - Azure Storage Explorer
  - Visual Studio Cloud Explorer



- Azure CLI



- PowerShell
  - .NET
  - Java
  - Python
  - Go
  - PHP
  - Ruby
  - Xamarin



# Azure Storage Explorer

## Recommended Storage Management Tools

- **Blobs, Files, Queues, Tables**
- **Azure Cosmos DB**
- **Azure Data Lake**
- **Virtual Machine Disks**

The screenshot shows the Azure Storage Explorer interface. On the left, the 'EXPLORER' pane displays a hierarchical tree of storage resources under 'Storage Accounts'. The 'Tables' node is expanded, showing several table entities. On the right, a detailed table view for the '\$MetricsHourPrimaryTransactionsBlob' table is shown, listing 100 items from July 12, 2019. The table has columns for PartitionKey, RowKey, Timestamp, and three error count columns. Below the table, the 'Actions' and 'Properties' tabs are visible, along with a URL and Type entry. The 'Activities' pane at the bottom shows a history of operations.

PartitionKey	RowKey	Timestamp	AnonymousAuthorizationError	AnonymousClientOtherError	AnonymousClientTl
20190807T1200	system>All	2019-08-07T13:23:16.905Z	0	0	0
20190807T1200	user>All	2019-08-07T13:23:00.262Z	0	0	0
20190807T1200	user.GetBlobServiceProperties	2019-08-07T13:23:00.262Z	0	0	0
20190807T1300	user>All	2019-08-07T14:23:24.066Z	0	0	0
20190807T1300	system>All	2019-08-07T14:23:24.066Z	0	0	0
20190807T1400	system>All	2019-08-07T15:59:56.992Z	0	0	0
20190807T1400	user>All	2019-08-07T15:59:56.992Z	0	0	0
20190807T1500	system>All	2019-08-07T16:22:11.879Z	0	0	0
20190807T1500	user>All	2019-08-07T16:22:11.884Z	0	0	0
20190807T1600	user>All	2019-08-07T17:21:06.547Z	0	0	0
20190807T1600	system>All	2019-08-07T17:21:37.242Z	0	0	0
20190807T1600	user.GetBlobServiceProperties	2019-08-07T17:21:06.546Z	0	0	0
20190807T1700	user>All	2019-08-07T18:23:46.057Z	0	0	0
20190807T1700	system>All	2019-08-07T18:23:46.057Z	0	0	0
20190807T1800	user>All	2019-08-07T19:20:58.332Z	0	0	0
20190807T1800	system>All	2019-08-07T19:20:58.334Z	0	0	0
20190807T1900	user>All	2019-08-07T20:24:26.566Z	0	0	0
20190807T1900	system>All	2019-08-07T20:24:26.562Z	0	0	0
20190807T2000	user.GetBlobServiceProperties	2019-08-07T21:21:46.345Z	0	0	0
20190807T2000	system>All	2019-08-07T21:22:13.415Z	0	0	0
20190807T2000	user>All	2019-08-07T21:21:46.345Z	0	0	0
20190807T2100	user>All	2019-08-07T22:21:26.186Z	0	0	0
20190807T2100	system>All	2019-08-07T22:21:26.191Z	0	0	0

# Tool Types - Recommended Storage Management Tools

## Recommended Storage Management Tools

- Multiple Subscriptions
- Azure
- Azure Stack
- Government Cloud

The screenshot shows the Azure Storage Explorer interface. On the left, the Explorer sidebar lists various storage resources under categories like Quick Access, Internal Consumption, and External Storage. A specific item, '\$MetricsHourPrimaryTransactionsBlob', is selected and highlighted in blue. On the right, a large table displays detailed information for this blob, including PartitionKey, RowKey, Timestamp, and error metrics. Below the table, a message indicates 'Showing 1 to 100 of 357 cached items'. At the bottom, there are tabs for Actions and Properties, and a preview pane showing the URL of the blob.

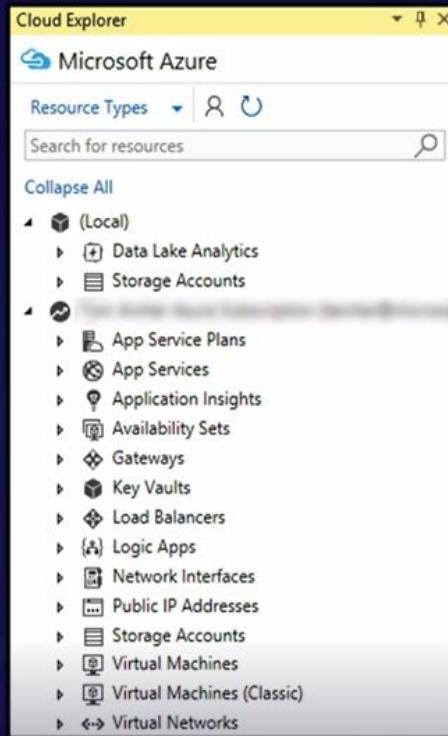
PartitionKey	RowKey	Timestamp	AnonymousAuthorizationError	AnonymousClientOtherError	AnonymousClientTotal
20190807T1200	system>All	2019-08-07T13:23:16.906Z	0	0	0
20190807T1200	user>All	2019-08-07T13:23:00.262Z	0	0	0
20190807T1200	user.GetBlobServiceProperties	2019-08-07T13:23:00.262Z	0	0	0
20190807T1300	user>All	2019-08-07T14:23:24.966Z	0	0	0
20190807T1300	user.GetBlobServiceProperties	2019-08-07T14:23:24.966Z	0	0	0
20190807T1400	system>All	2019-08-07T15:59:56.062Z	0	0	0
20190807T1400	user>All	2019-08-07T15:59:56.062Z	0	0	0
20190807T1400	user.GetBlobServiceProperties	2019-08-07T15:59:56.062Z	0	0	0
20190807T1500	system>All	2019-08-07T16:22:11.876Z	0	0	0
20190807T1500	user>All	2019-08-07T16:22:11.884Z	0	0	0
20190807T1600	user>All	2019-08-07T17:21:06.547Z	0	0	0
20190807T1600	user.GetBlobServiceProperties	2019-08-07T17:21:06.547Z	0	0	0
20190807T1700	user>All	2019-08-07T18:23:46.067Z	0	0	0
20190807T1700	user.GetBlobServiceProperties	2019-08-07T18:23:46.067Z	0	0	0
20190807T1800	user>All	2019-08-07T19:20:58.332Z	0	0	0
20190807T1800	system>All	2019-08-07T19:20:58.334Z	0	0	0
20190807T1900	user>All	2019-08-07T20:24:26.560Z	0	0	0
20190807T1900	system>All	2019-08-07T20:24:26.562Z	0	0	0
20190807T2000	user.GetBlobServiceProperties	2019-08-07T21:21:46.345Z	0	0	0
20190807T2000	user>All	2019-08-07T21:22:13.415Z	0	0	0
20190807T2000	user.GetBlobServiceProperties	2019-08-07T21:21:46.345Z	0	0	0
20190807T2100	user>All	2019-08-07T22:21:26.186Z	0	0	0
20190807T2100	system>All	2019-08-07T22:21:26.191Z	0	0	0

# Tool Types - Recommended Storage Management Tools

## Recommended Storage Management Tools



- **Built on Azure Resource Manager Stack**
- **View Resources and Groups**
- **Inspect Properties**
- **Perform Key Developer Diagnostics within Visual Studio**



# Summary

# Choosing a Storage Tier

## Key Learning Outcomes

Microsoft Exam Expectation:  
Choose between storage tiers

### Hot, Cool, and Archive

- Oven, Fridge, and Freezer

### Differences

- Storage Cost
- Access Delay
- Transaction Cost
- Early Deletion Fee

### Best Uses

- Actively changing data
- Backups and Storage
- Long-term and historical

# Summary

## Support Tiering of Storage Accounts

Key Learning Outcomes

Microsoft Exam Expectation:  
Choose between storage tiers

### Performance

- Standard
- Premium

### Types of Storage Accounts

- General Purpose
- BlockBlob
- FileStorage
- Legacy

### Replication

- LRS
- ZRS
- GRS
- GZRS

# Summary

## Recommended Storage Management Tools

### Key Learning Outcomes

**Microsoft Exam Expectation:**  
Recommend storage management tools

### Tool Types

- GUI
- Command Line
- Scripting

### Azure Storage Explorer

- Universal Tool

### Visual Studio Cloud Explorer

- Perform Developer Diagnostics

# Summary

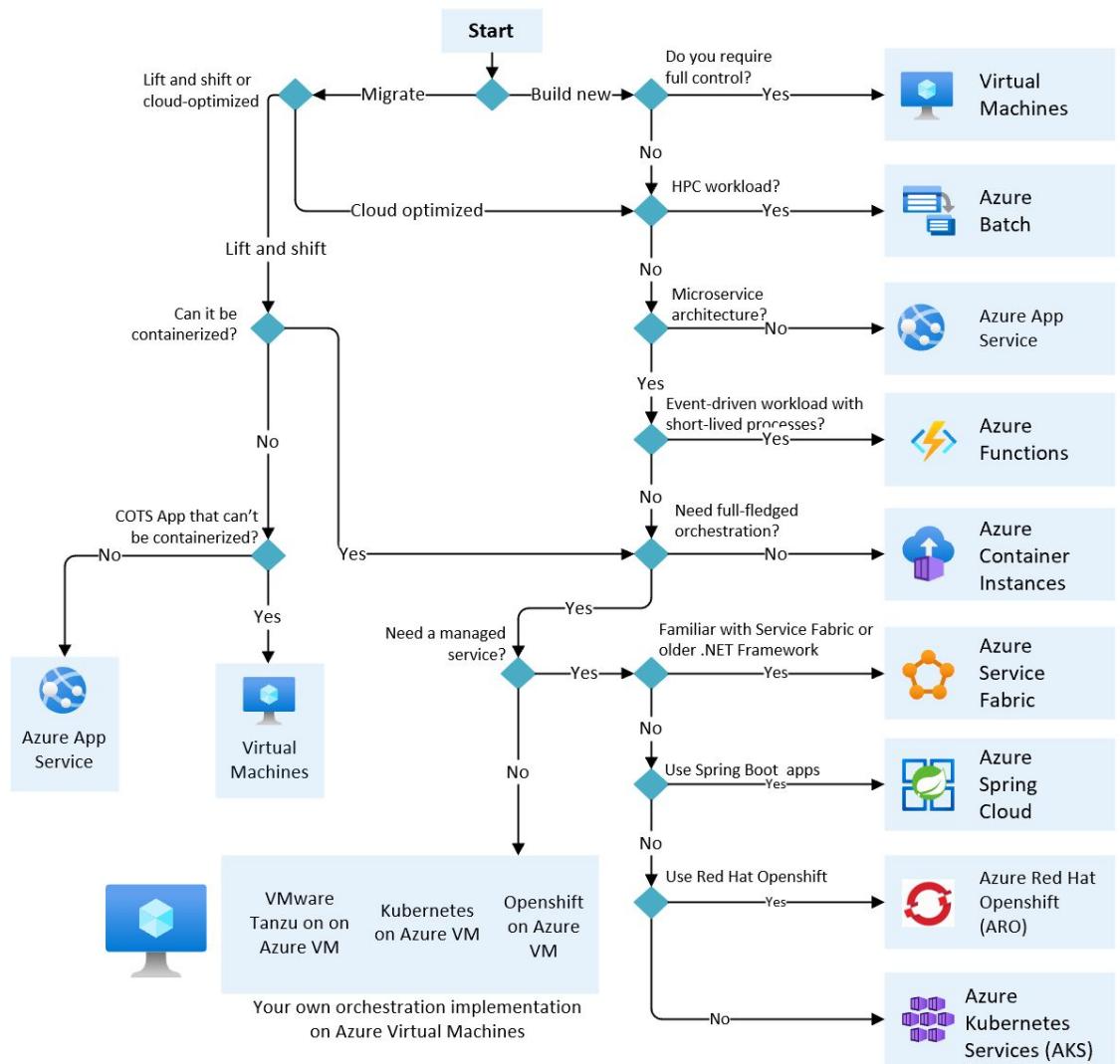
## Storage Redundancy

Keep a close eye on the regions end users need to access an application.

Sometimes "Read-Access" isn't so apparent!

# Design a Compute Solution

# Choose an Azure compute service for your application



# Choosing an Azure Compute Service

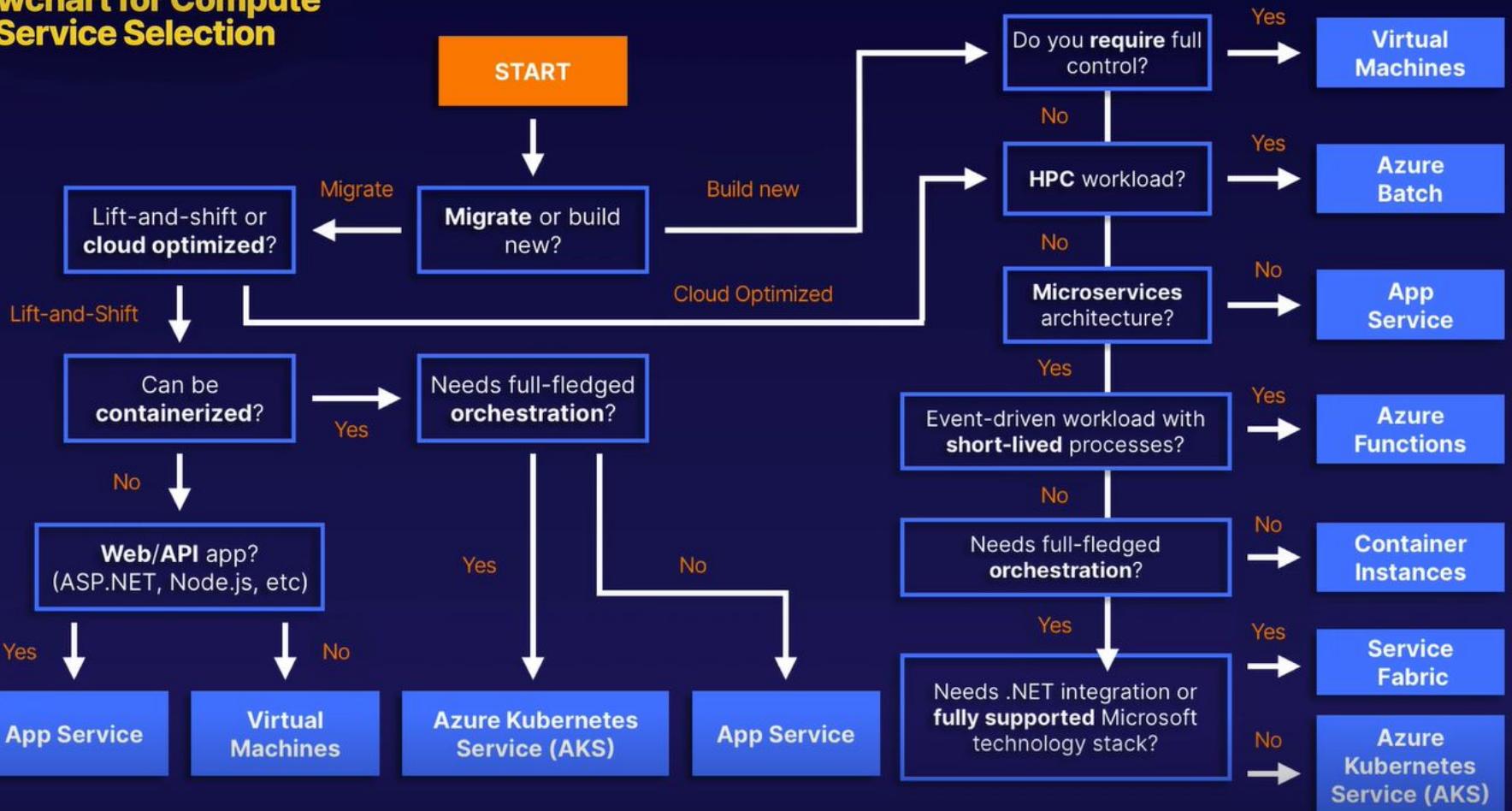
**Compute: hosting model for the computing resources on which your application runs.**

---

As with all planning and review activities, you'll need to know your end goal.  
Always choose services with performance, availability, and cost in mind.

# Choosing an Azure Compute Service

## **Flowchart for Compute Service Selection**



# Choosing a Compute Service

## Hosting Models:

### Infrastructure as a Service (IaaS)

Provision VMs and associated network/storage components.

### Platform as a Service (PaaS)

Managed hosting - deploy app without VMs or dedicated networking.

### Functions as a Service (FaaS)

Deploy code and the service runs it. e.g. Azure Functions

SaaS: considered a subset of PaaS

# Choosing an Azure Compute Service

## Features:

**Virtual Machines:**  
'nuff said.

**Kubernetes (AKS):**  
service for running  
containerized apps



**App Service:**  
for hosting web apps, RESTful APIs,  
mobile back-ends, or automated  
business processes.

**Container Instances:**  
quick and simple container  
setup. No VMs required.  
Includes Service Fabric

**Batch:**  
service for running large-  
scale parallel and high-  
performance computing  
(HPC) operations.

**Functions:**  
Azure Functions as a  
Service (FaaS)

# Determine Compute Options for Microservices

## Microservices - What are they?

Applications are composed of small, independent modules which communicate using well-defined API contracts. These modules are decoupled “building blocks” that generally implement a single purpose function.

## How does this apply to compute design?

You'll want to design an environment suited to the operations that your microservices will accomplish.

# Choosing an Azure Compute Option for Microservices

**Two of the most popular approaches:**

**SERVERLESS**

**vs.**

**SERVICE ORCHESTRATOR**

Azure Functions:

Deploy your code and the hosting service puts it onto a VM to execute.

Service Bus queues, Event Hub events, message processing...

AKS & Service Fabric:

"Kubernetes APIs as a service" - limited to containers.

Service Fabric packages, deploys, and manages microservices. Can also run processes (binary executables).

# Containers

## Relevant Benefits of Containers for Microservices

Containers are not the same as microservices and are not strictly necessary.

### Portability

Container images are standalone packages without libraries/dependencies, making them easy to deploy.



### Density

Containers are lightweight compared to running full VMs due to shared OS resources.



### Resource Isolation

You can limit the CPU/memory that is available to a container. This helps limit runaway processes.



# Serverless

## SERVERLESS (FUNCTIONS AS A SERVICE)

No need to manage VMs or  
Virtual Network infrastructure.

Types of triggers can include schedules, HTTP,  
Blob storage, Event Hub events, Azure Queue  
storage, and Service Bus queues.

# So, Which to choose

**When choosing between an orchestrator and a serverless approach, keep these factors in mind:**

## Manageability

**Serverless** - platform manages all compute resources.

**Orchestrator** - you'll need to consider load balancing, CPU and memory usage, as well as networking.

## Flexibility and Control

**Orchestrator** - lots of control over configuring and managing your services and the cluster.

**Serverless** - less control since many details are abstracted.

## Portability

All orchestrators (Kubernetes, DC/OS, Docker Swarm, and Service Fabric) can run on-premises or in multiple public clouds.

## Application Integration

**Serverless** - architecture can be challenging to manage. Logic Apps can help coordinate a set of functions.

## Cost

**Orchestrator** - you pay for the VMs in the cluster.

**Serverless** - pay only for actual compute resources consumed.

In both cases, factor in the costs of other services (storage, databases, messaging, etc.).

## Scalability

Azure Functions scales automatically.

**Orchestrator** - scale by increasing the number of service instances in the cluster. You can also add VMs.

# Choosing Kubernetes

**As mentioned before, consider green field or lift-and-shift when evaluating AKS**

## Identity and security management

Configure an AKS cluster to integrate with Azure AD and use existing IDs and groups.

## Cluster node upgrades

AKS manages Kubernetes software upgrades. Cordons of nodes one by one and drains them before upgrading.

## Integrated logging and monitoring

AKS includes Azure Monitor for containers. Custom Kubernetes installs normally required a monitoring solution needing install and config.

## GPU enabled nodes

AKS supports GPU enabled node pools for compute or graphic intensive workloads.

## Auto Cluster node and pod scaling

AKS supports two scaling options: Horizontal pod autoscaler or cluster autoscaler.

# Choosing Kubernetes

**As mentioned before, consider green field or lift-and-shift when evaluating AKS**

## Storage volume support

AKS supports both static and dynamic storage volumes. Pods can attach/reattach to these volumes as they are created or rescheduled on different nodes.

## Ingress with HTTP app routing support

Do your apps need to be publicly available? HTTP application routing allows easy access to deployed apps.

## Docker image support

AKS supports the Docker file image format.

## Virtual network support

An AKS cluster can easily be deployed into an existing virtual network.

## Private container registry

Do you need a private container registry? AKS integrates with Azure Container Registry. You can also use other public or private container repos.

# When & why to use ACI (Azure Container Instances)

**Do you have a task that can operate in an isolated container?  
e.g. - simple apps, task automation, or build jobs**

**Fast startup times, compared to VMs.**

**Container access: ACI allows container groups to be exposed to the internet via IP Address and FQDN.**

**Available command shell via HTTPS/TLS**

**Hypervisor-level security: ACI guarantees your container-held app is as isolated as a VM.**

**Persistent Storage: direct mount of Azure File shares to an instance**

**Remember: If you need full container orchestration, automatic scaling, cross-container service discovery, or coordinated application upgrades, then you need to be using AKS**

# When & why to use ACI (Azure Container Instances)

**Custom sizing: adjust your Instance to meet the needs of your application.**

**Linux and Windows support: ACI can run both operating systems with the same API.**

**Co-scheduled groups: multi-container groups that share a host machine, local network, storage, and lifecycle . Combine main app container with supporting role containers.**

**Virtual network deployment: put container instances into an Azure virtual network as you would a VM, with the same benefits.**

---

**Remember: If you need full container orchestration, automatic scaling, cross-container service discovery, or coordinated application upgrades, then you need to be using AKS**

# Design a Compute Solution

## Solutions to provision your Azure compute infrastructure...

**Use automation to provision and  
manage compute resources.**

For each VM you deploy, you normally have to manually do the following:

Configure the VM: tier, SKU, IP address, disk, etc.

Configure the OS: set OS level firewalls, partitions, security, etc.

Install Software: anti-malware, agents, backup software, etc.

Apply Updates: an important part of every OS install.

# Automation Tools

## ARM Templates

You know them, you love them!

## Custom Scripts

Useful for post-deployment configuration, software install, or other configuration tasks.

## Desired State Configuration

Maintain standards for VM states.

# Automation Tools

## Automation State Configuration

Manage and deploy DSC configurations.

### Chef

On-premises or cloud deployment tool.  
Typically hosted.  
Recipes can add the Chef extension to  
ARM templates.

### Terraform

Open-source infrastructure-as-code (IAC) tool.  
Multi-cloud functional.  
Can run directly from the Azure CLI.

# Compute Solution Design



## Choose the Service

IaaS, PaaS, FaaS

Containers, VMs, AKS, Apps,  
Batch, Functions



## Containers

Azure Container Instances,  
AKS



## Microservices

Serverless or Orchestrated



## Automated Provisioning

Standard built-in Azure  
and third-party tools to  
deploy resources



# Design a Database Solution



# Selecting a Database Platform - Types of Data



## Structured

- Azure SQL Database
- MySQL
- PostgreSQL on Azure
- Data Lake



## Semi-Structured (NoSQL)

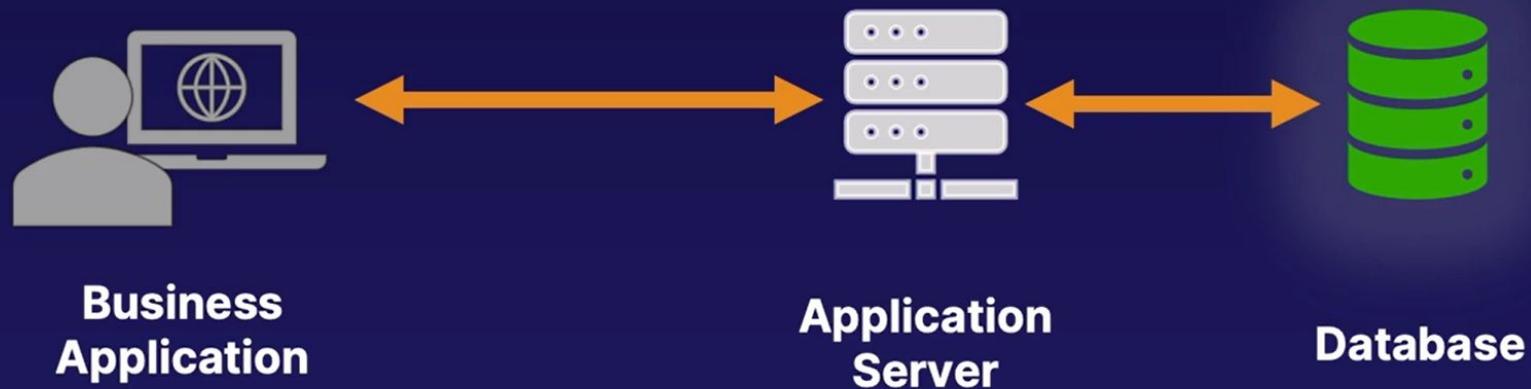
- Azure Cosmos DB
- Data Lake



## Unstructured

- Table storage
- Blob storage
- File storage

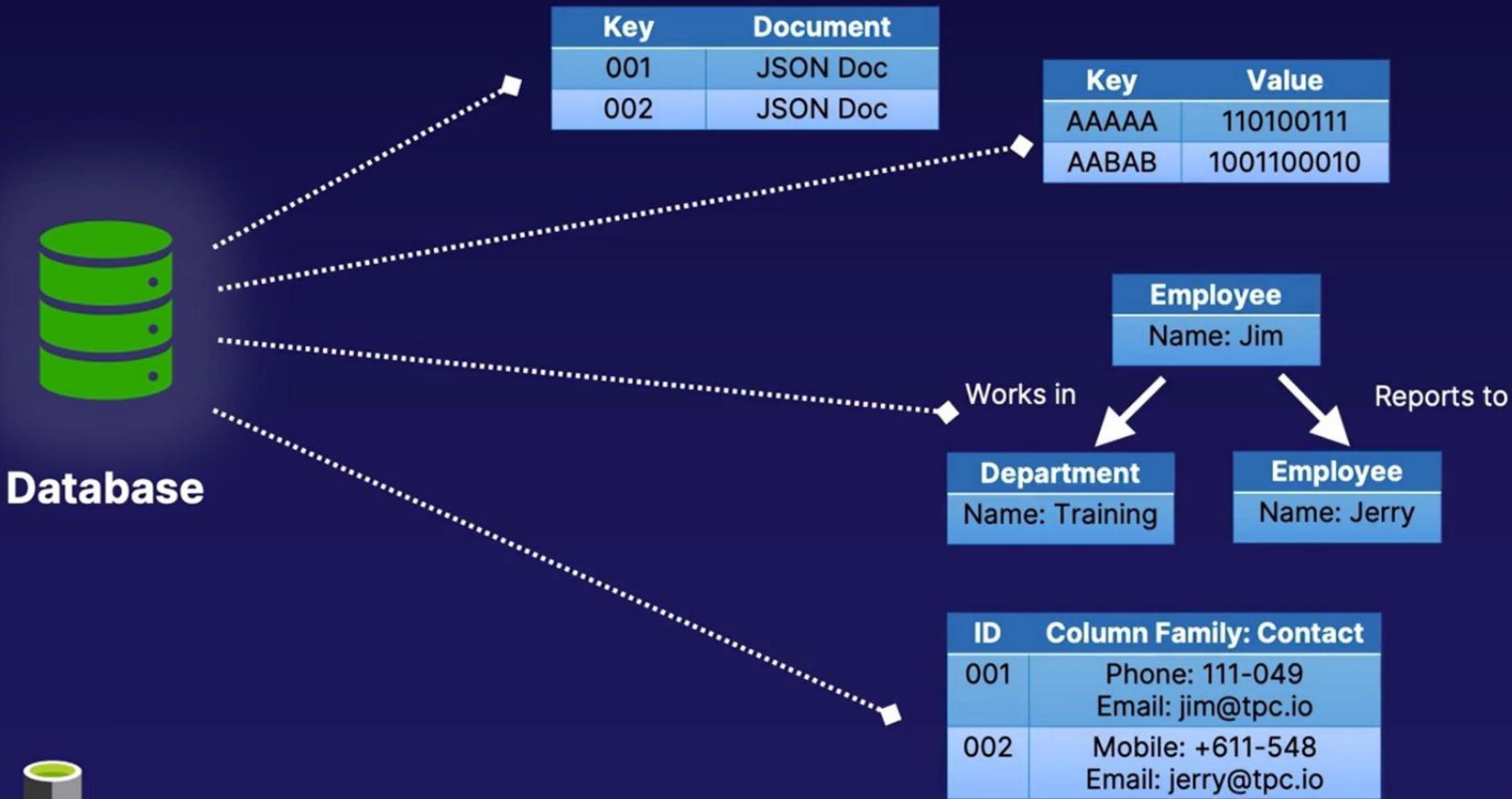
# Structured Data: Relational Database



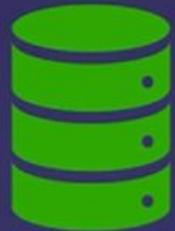
# Structured Data: Relational Database



# Non-Relational Data Models



# Non-Relational Data Models



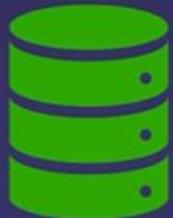
**Document  
Databases**



Key	Document
001	JSON Doc
002	JSON Doc

```
{  
  "id": "5d6aa83bc0220",  
  "name": "Tom's Dog",  
  "imgUrlBase": "www.tpc..."  
}
```

# Non-Relational Data Models



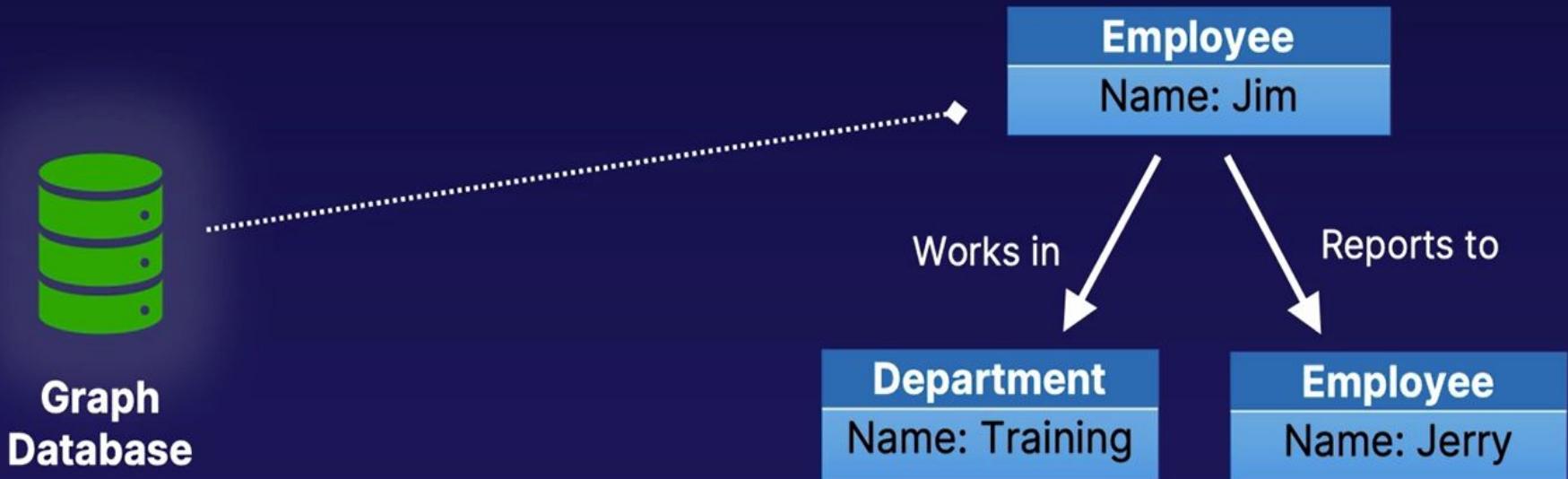
**Key Value  
Stores**

Optimized for:

- Simple lookups only
- Lookup by key

Key	Value
AAAAAA	110100111
AABAB	1001100010

# Non-Relational Data Models



# Non-Relational Data Models

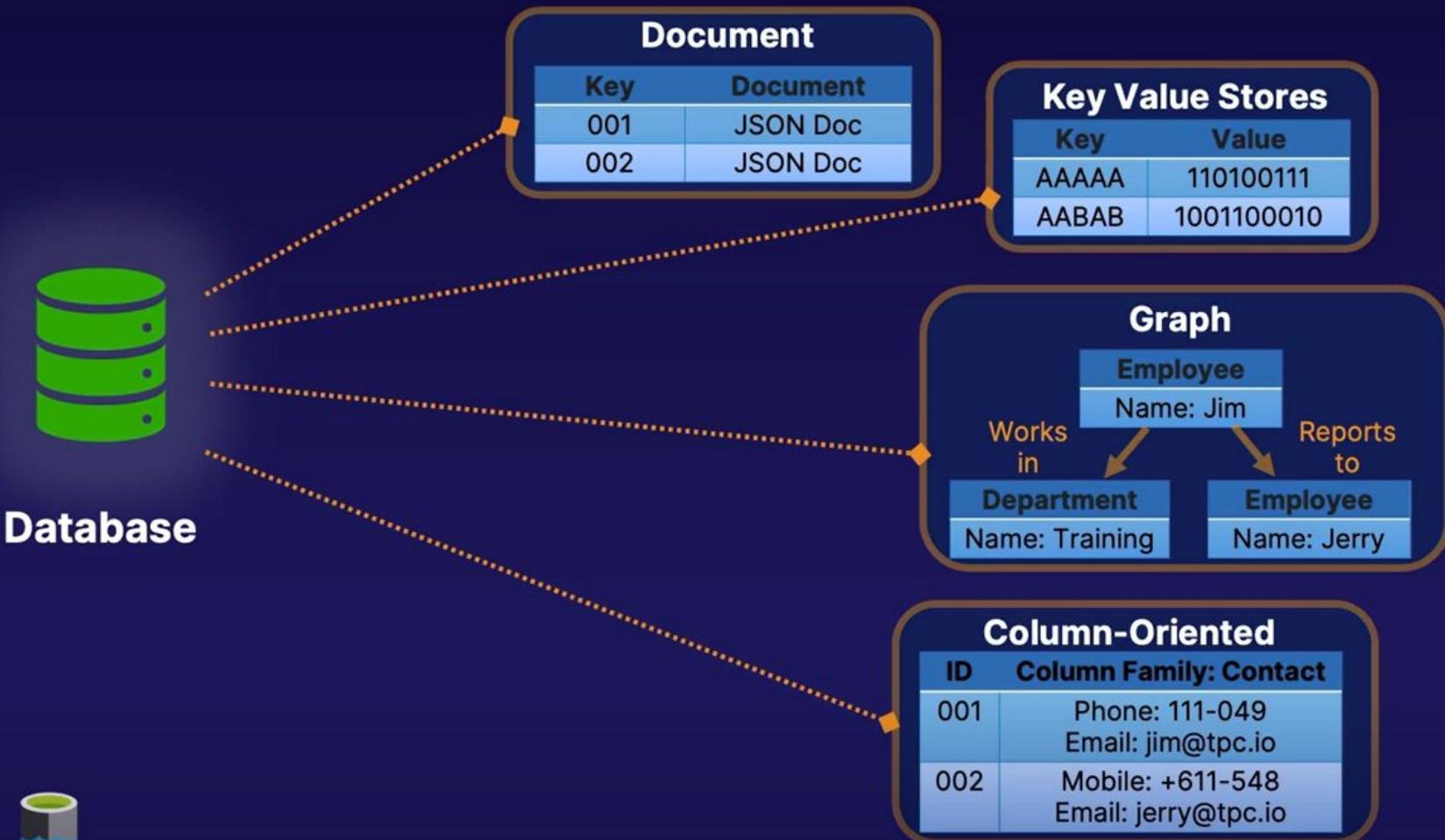


## Column-Oriented Databases

ID	Column Family: Contact
001	Phone: 111-049 Email: jim@tpc.io
002	Mobile: +611-548 Email: jerry@tpc.io

- Arranged by columns and rows
- Rows contain families of data

# Non-Relational Data Models



# Selecting a Database Platform

### Types of Data

- Structured, Semi-Structured, Unstructured

### Relational Databases

### Non-relational Data Models

- Document, Key Value Stores, Graph, Column-Oriented

# Azure Data Storage Solutions - Type of Storage



**Cosmos DB**



**Azure SQL**



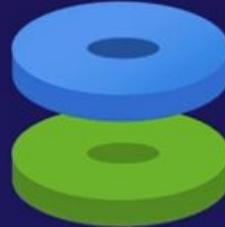
**Data Lake**



**Blob**



**Files**



**Disk**



**Queue**

# Types of Storage



Cosmos DB

- Globally Distributed
- Supports Schema-Less Data

# Types of Storage



Data Lake

- Structured + Unstructured
- Object Storage + Big Data
- Analysis

# Types of Storage



Azure Blob

- **Unstructured**
- **Highly Scalable**

# Types of Storage



Queue

- **Large Numbers of Messages**
- **Decoupled Component**
- **Scaling Web App, Mobile App, and Services**

# Types of Storage

# Azure Data Storage Solutions

## Types of Storage

### Cosmos DB

- Globally distributed
- Schema-less supported

### Data Lake

- Structured and Unstructured
- Object Storage
- Big Data
- Analysis

### Azure SQL Database

Blob, Queue, Files, Disk

# Database Service Tier Sizing

## Types of Azure SQL Databases

- SQL Virtual Machines
- Azure SQL Managed Instances
- SQL Databases

## DTU vs. vCore Models

## Elastic Pools

## Sizing Models

## Database Servers

# First Time Replication Provisioning



## SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.



## SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.



## SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

## SaaS Solution

## PaaS Solution

## IaaS Solution

- Single database, elastic pool, database server
- Single instance
- Select image of SQL and Windows/Linux Server versions

# SQL Virtual Machines

Basics Disks Networking Management Advanced SQL Server settings Tags Review + create



## SQL virtual machines

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.



## Select a VM size



Search by VM size...

Display cost : **Monthly**

vCPUs : All

RAM (GiB) : All

+ Add filter

↗ Most used sizes by Azure users

Showing 363 VM sizes. | Subscription: Visual Studio Enterprise | Region: South Central US | Current size: Standard\_D2\_v2 | Image 2019

VM Size ↑↓	Family ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS
------------	-----------	----------	--------------	---------------	----------

↙ Most used by Azure users

The most used sizes by users in Azure

DS1_v2 ↗	General purpose	1	3.5	4	3200
D2s_v3 ↗	General purpose	2	8	4	3200
B2s ↗	General purpose	2	4	4	1280
B1s ↗	General purpose	1	1	2	320
B2ms ↗	General purpose	2	8	4	1920
B1ms ↗	General purpose	1	2	2	640
DS2_v2 ↗	General purpose	2	7	8	6400
B4ms ↗	General purpose	4	16	8	2880
D4s_v3 ↗	General purpose	4	16	8	6400

# Azure SQL Managed Instances

Basics

Networking

Additional settings

Tags

Review + create

## Service tier

Select from the latest vCore service tiers available for Azure SQL Managed Instance including General Purpose and Business Critical. [Learn more](#)

Service tier i

- General Purpose (4-80 vCores, 32 GB-8 TB storage capacity, Fast storage) - for most production workloads
- Business Critical (4-80 vCores, 32 GB-4 TB storage capacity, Super fast storage) - for IO-intensive and compute-intensive workloads

## Compute Hardware

Configure compute hardware that will run your Azure SQL Managed Instance. [Learn more](#)

Hardware generation i

Gen5

vCores i



Storage in GB i



## SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.



# Azure SQL Managed Instances

Basics

Networking

Additional settings

Tags

Review + create



## SQL managed instances

Best for most migrations to the cloud. Lift-and-shift ready.

**vCores: 4 - 80**

**Storage: 32GB - 4/8 TB**

### Service tier

Select from the latest vCore service tiers available for Azure SQL Managed Instance including General Purpose and Business Critical. [Learn more](#)

Service tier (i)

- General Purpose (4-80 vCores, 32 GB-8 TB storage capacity, Fast storage)  
- for most production workloads
- Business Critical (4-80 vCores, 32 GB-4 TB storage capacity, Super fast storage) - for IO-intensive and compute-intensive workloads

# SQL Databases - Single Database

[Basics](#)[Networking](#)[Additional settings](#)[Tags](#)[Review + create](#)

## SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

### Basic

For less demanding workloads

### Standard

For workloads with typical performance requirements

### Premium

For IO-intensive workloads.

### 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

### Business Critical

High transaction rate and high resiliency

5,000 - 204,800 IOPS  
1-2 ms latency

# SQL Databases - Single Database Sizing Models

**DTU**

(Database Transaction Unit)

**Bundled compute,  
storage, and I/O**

Simple, preconfigured  
resource options

**vs.**

**vCore**

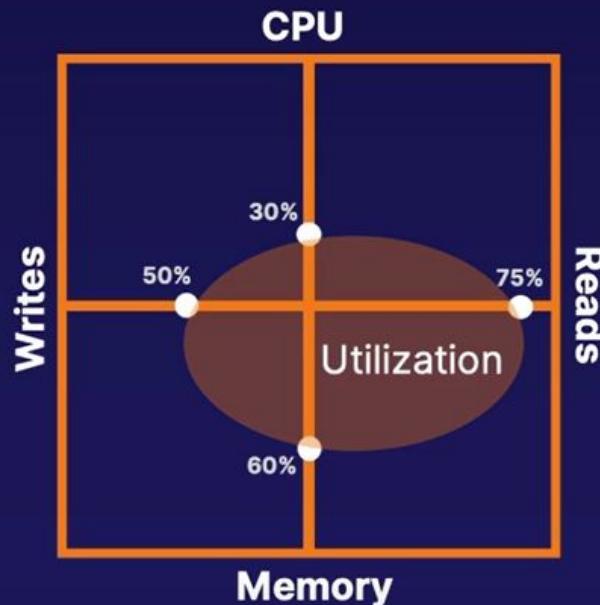
**Choose compute and  
storage resources**

Flexibility, control, and  
transparency

## Database Transaction Unit

Bundled compute, storage, and I/O

- Represents resources assigned to the database
- CPU, memory, and read-write rates
- Compare the power across performance levels
- Simplifies talking about performance



# SQL Databases - Single Database Sizing Models

## DTU Model

vs.

## vCore Model

1

### Basic

Less demanding workloads

1

### General Purpose

Scalable compute and storage options

2

### Standard

Typical performance requirements

2

### Hyperscale

On-demand scalable storage

3

### Premium

I/O-intensive workloads

3

### Business Critical

High transaction rate and high resiliency

# SQL Databases - Single Database Sizing Models

## DTU Model

1

**Basic**

2

**Standard**

3

**Premium**

DTU	5
Data Max Size	100 MB – 2 GB

DTU	10 - 3000
Data Max Size	100 MB – 250 GB

DTU	125 - 4000
Data Max Size	100 MB – 1 TB

# SQL Databases - Single Database Sizing Models

## vCore Model

### 1 General Purpose

IOPS	500 – 20,000
Latency	2 – 10 ms
vCores	2 - 80
Data Max Size	1 GB – 4 TB

Replicas    1 Read-Write

### 2 Hyperscale

IOPS	500 – 204,800
Latency	1 – 10 ms
vCores	2 - 80
Data Max Size	100 TB

Replicas    1 Read-Write  
0 – 4 Read-Scale

### 3 Business Critical

IOPS	5,000 – 204,800
Latency	1 – 2 ms
vCores	2 - 80
Data Max Size	1 GB – 4 TB

Replicas    3 Read-Write  
1 Read-Scale

# SQL Databases - Elastic Pools

## Share the Load

### Great because...

no per-database charge

eDTU or vCore models

### Best for...

managing/scaling  
multiple databases

varying/unpredictable  
usage demands



# SQL Databases - Elastic Pool Sizing Models

## eDTU Model

1

### Basic

<b>Pool</b>	<b>50 - 1600</b>
<b>Database</b>	<b>0 - 5</b>
<b>Data Max Size</b>	<b>4.88 - 156.25 GB</b>

2

### Standard

<b>Pool</b>	<b>50 - 3000</b>
<b>Database</b>	<b>0 - 10</b>
<b>Data Max Size</b>	<b>50 GB - 4 TB</b>

3

### Premium

<b>Pool</b>	<b>125 - 4000</b>
<b>Database</b>	<b>0 - 25</b>
<b>Data Max Size</b>	<b>50 GB - 4 TB</b>

# SQL Databases - Elastic Pool Sizing Models

## vCore Model

### 1 General Purpose

IOPS	500 – 20,000
Latency	2 – 10 ms
vCores	2 – 80
Data Max Size	1 GB – 4 TB

### 2 Hyperscale

IOPS	500 – 204,800
Latency	1 – 10 ms
vCores	2 – 80
Data Max Size	100 TB

### 3 Business Critical

IOPS	5,000 – 204,800
Latency	1 – 2 ms
vCores	2 – 80
Data Max Size	1 GB – 4 TB

Secondary Replicas	0 – 4
--------------------	-------

# SQL Databases - Database Server

???

**SQL databases**

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

- Single database
- Single database
- Elastic pool
- Database server

# Logical container for managing databases and elastic pools

## Product details

SQL Database Server  
by Microsoft

[Terms of use](#) | [Privacy policy](#)

### Estimated cost per month

No additional charges



# SQL Databases - Database Server

## Logical container for managing databases and elastic pools

+ Create database + New elastic pool + New Synapse SQL pool (data warehouse) ↓ Import database ✎ Reset password → Move ✎ Delete

 <b>Active Directory admin</b> Allows you to centrally manage identity and access to your Azure SQL databases. <b>NOT CONFIGURED</b>	 <b>Advanced data security</b> Data Discovery & Classification, Vulnerability Assessment and Advanced Threat Protection. <b>NOT CONFIGURED</b>	 <b>Automatic tuning</b> Monitors and tunes your database automatically to optimize performance. <b>CONFIGURED</b>
 <b>Auditing</b> Track database events and writes them to an audit log in Azure storage. <b>NOT CONFIGURED</b>	 <b>Failover groups</b> Automatically manages replication, connectivity and failover for a set of databases. <b>NOT CONFIGURED</b>	 <b>Transparent data encryption</b> Encryption at rest for your databases, backups, and logs. <b>SERVICE-MANAGED KEY</b>

## Logical container for managing databases and elastic pools

### Settings

- Quick start
- Failover groups
- Manage Backups
- Active Directory admin
- SQL databases
- SQL elastic pools
- Deleted databases
- Import/Export history
- DTU quota
- Properties
- Locks

### Security

- Auditing
- Firewalls and virtual networks
- Private endpoint connections
- Advanced data security
- Transparent data encryption

### Intelligent Performance

- Automatic tuning
- Recommendations

### Monitoring

- Logs

### Automation

- Tasks
- Export template

# Database Service Tier Sizing

## Types of Azure SQL Databases

- SQL Virtual Machines
- Azure SQL Managed Instances
- SQL Databases

## DTU vs. vCore Models

## Elastic Pools

## Sizing Models

## Database Servers

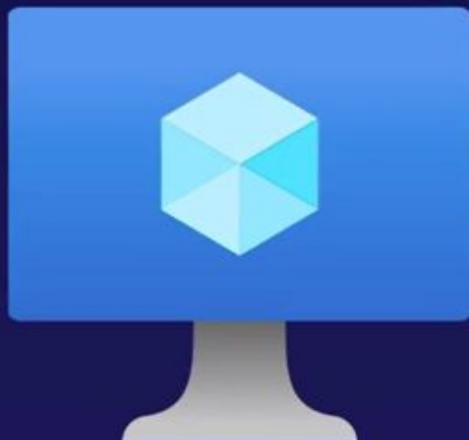
## Scaling Up and Down

- **Memory**
- **CPU**
- **Disk Space**



## Scaling Up

- Memory
- CPU
- Storage



## Scaling Down

- Memory
- CPU
- Storage



# Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling

## Scaling Out



↑ Number of VMs

# Dynamically Scale Azure SQL DB and SQL Managed Instances - Types of Scaling

## Scaling In

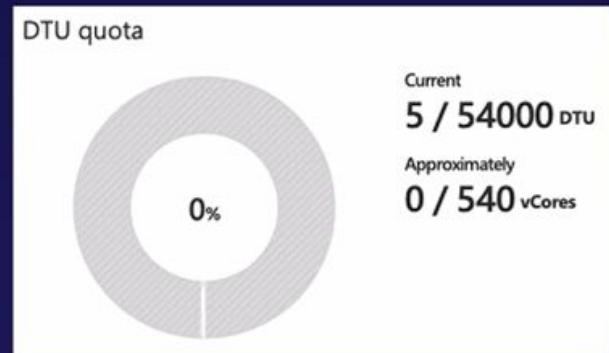


↓ **Number of VMs**

# Scaling with Azure SQL Database

## Scaling (DTU Model)

- DTU
- Data Max Size
- Read Scale Out



# Scaling with Azure SQL Database



Basic                      Standard                      Premium

For less demanding workloads              For workloads with typical performance requirements              For IO-intensive workloads.

DTUs [What is a DTU?](#)

125              250              500              1000              1750              4000              **125 (P1)**

Data max size

**100 MB**              1 TB              **100 MB**

Read scale-out

Enabled     Disabled

Would you like to make this database zone redundant? [?](#)

Yes     No

# Bonus: Automatic Tuning



## Intelligent Performance

⚡ Automatic tuning

📁 Recommendations

Option	Desired state	Current state
	<input type="radio"/> ON <input type="radio"/> OFF <input checked="" type="radio"/> INHERIT	<b>ON</b> Inherited from Azure defaults
	<input type="radio"/> ON <input type="radio"/> OFF <input checked="" type="radio"/> INHERIT	<b>OFF</b> Inherited from Azure defaults
	<input type="radio"/> ON <input type="radio"/> OFF <input checked="" type="radio"/> INHERIT	<b>OFF</b> Inherited from Azure defaults

# Bonus: Automatic Tuning

## Tuning Options

### 1 Create Index

- Identifies indexes that may improve performance
- Creates indexes
- Automatically verifies that performance has improved

### 2 Drop Index

- Identifies redundant and duplicate indexes (without unique indexes)
  - Identifies indexes not used for > 90 days
- \*Not compatible with apps using partition switching and index hints

### 3 Force Last Good Plan

- Identifies queries using execution plan that is slower than the previous good plan
- Queries using the last known good plan instead of regressed plan



# Dynamically Scale Azure SQL DB and SQL Managed Instances

## Types of Scaling

- Up/Down
- In/Out
- DTU Model/vCore Model

How to Scale using the Azure Portal

Automatic Tuning and Options

# Encrypting Data at Rest, in Transmission, and in Use

## ENCRYPTING DATA

### Transparent Data Encryption (TDE)



MAY 2017



FEBRUARY 2019

#### AT REST

Automatically encrypted by Storage Service Encryption (SSE) with 256-bit Advanced Encryption Standard (AES) cipher

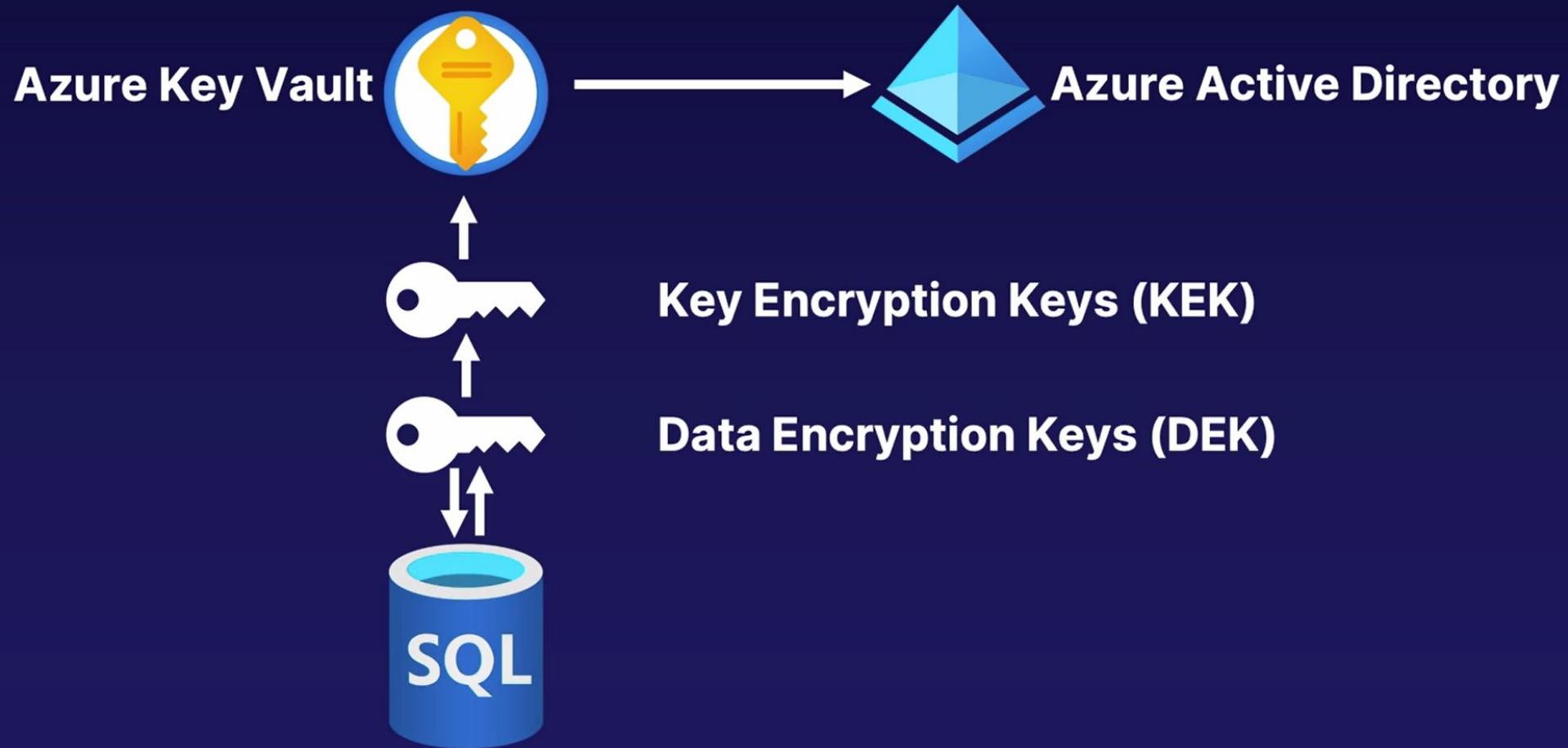
#### IN TRANSMISSION

Enable transport-level security by enabling **secure transfer**, and always use HTTPS

#### IN USE

Create an Azure Key Vault to Encrypt Databases in Use (lab)

# How Azure Key Vault Encrypts SQL



# Selecting a Database Platform

## Key Learning Outcomes

**Microsoft Exam Expectation:**  
Select an appropriate data platform  
based on requirements

### Structured

- Azure SQL
- MySQL
- PostgreSQL
- Relational DB

### Semi-Structured

- Cosmos DB
- Key Value Stores
- Document DB
- Graph DB
- Column Family

### Unstructured

- Blob
- File
- Data Lake

# Summary

# Azure Data Storage Solutions

## Key Learning Outcomes

**Microsoft Exam Expectation:**  
Select an appropriate data platform  
based on requirements

## Types of Storage

- Cosmos DB
- Azure SQL
- Data Lake
- Blob
- Queue
- Files
- Disk

## Cosmos DB

- Schema-less Data
- Globally Distributed

## Data Lake

- All Types of Data
- Object Storage
- Big Data and Analysis

# Summary

# Database Service Tier Sizing

## Key Learning Outcomes

**Microsoft Exam Expectation:**  
Recommend database service tier sizing

### SQL Types

- SQL Databases
- Managed Instances
- Virtual Machines

### DTU vs vCore

- vCore - Traditional Model
- DTU – Database Transactional Unit

### Elastic Pools

- Manage and scale multiple databases
- Manages both models

# Summary

## Dynamically Scaling SQL Managed Instances

Key Learning Outcomes

Microsoft Exam Expectation:  
Recommend a solution for database scalability

### Types of Scaling

- Up and Down
- In and Out

### DTU Scaling

- DTU
- Data Max Size
- Read Scale Out

### vCore Scaling

- vCores
- Data Max Size
- Replicas

# Summary

# Encrypting SQL Data

## Key Learning Outcomes

### Microsoft Exam Expectation:

Recommend a solution for encrypting data at rest, data in transmission, and data in use

#### At Rest

- Transparent Data Encryption (TDE)

#### In Transmission

- Transport Layer Security
- SSL Certificates

#### In Use

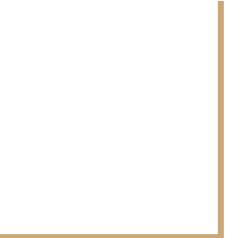
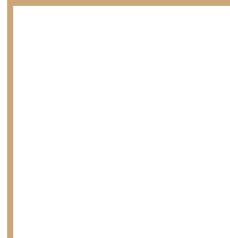
- Always Encrypted

## Quick Notes

SQL Managed Instances support Common Language Runtime (CLR)

Elastic Pools and Azure SQL Database servers can handle many databases

Deterministic supports more querying vs Randomized Encryption



**Thank you**