Cloud Computing

Caltech | Center for Technology & Management Education

# Post Graduate Program in Cloud

Powerd by simplilearn

Caltech | Center for Technology & Management Education

# AZ 304 – Microsoft Azure Architect Design

Powerd by simplilearn

# Design a Solution for Databases

# Learning Objectives

By the end of this lesson, you will be able to:

- Analyze an Appropriate Data Platform Based on Requirements
- Illustrate of Azure Data Storage
- Recommend Database Service Tier Sizing
- Implement a Solution for Database Scalability
- Configure a Solution for Encrypting Data

# A Day in the Life of an Azure Architect

You are working as a Cloud Database Architect and you have been given a project to choose the right candidate service for a relational database which can be used for an OLTP application. This solution should be also utilized to store data with long-term retention.

You need to ensure that during an adverse event like a catastrophic failure or natural disaster, the users are still able to read the data.

Your organization is also looking for a fully managed NoSQL database for modern app development that provides single-digit millisecond response times, automatic and rapid scalability, and guarantees speed at any size.

To achieve all of the above along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.

# Select an Appropriate Data Platform Based on Requirements

# Recommending the Right Data Store

There are different options to choose from among SQL and NoSQL databases

Relational database management systems

Key or Value stores

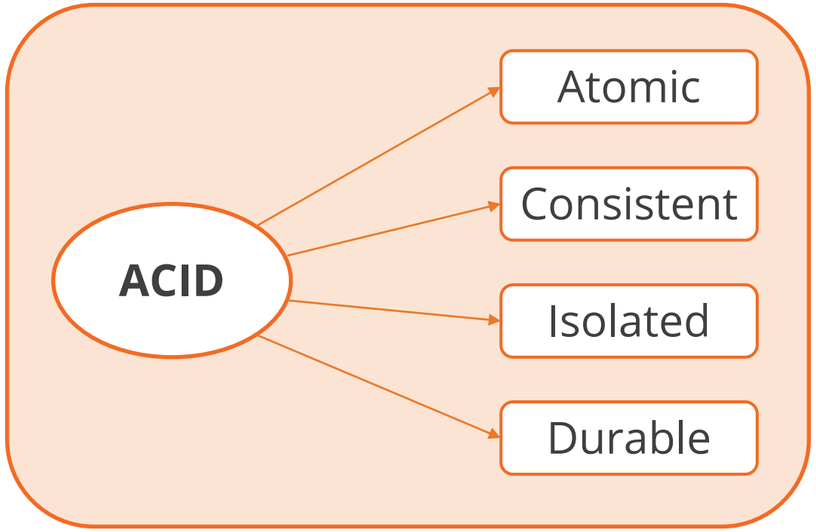

Graph databases

Document databases

# Relational Database Management Systems

Relational databases organize data as a series of two-dimensional tables with rows and columns.

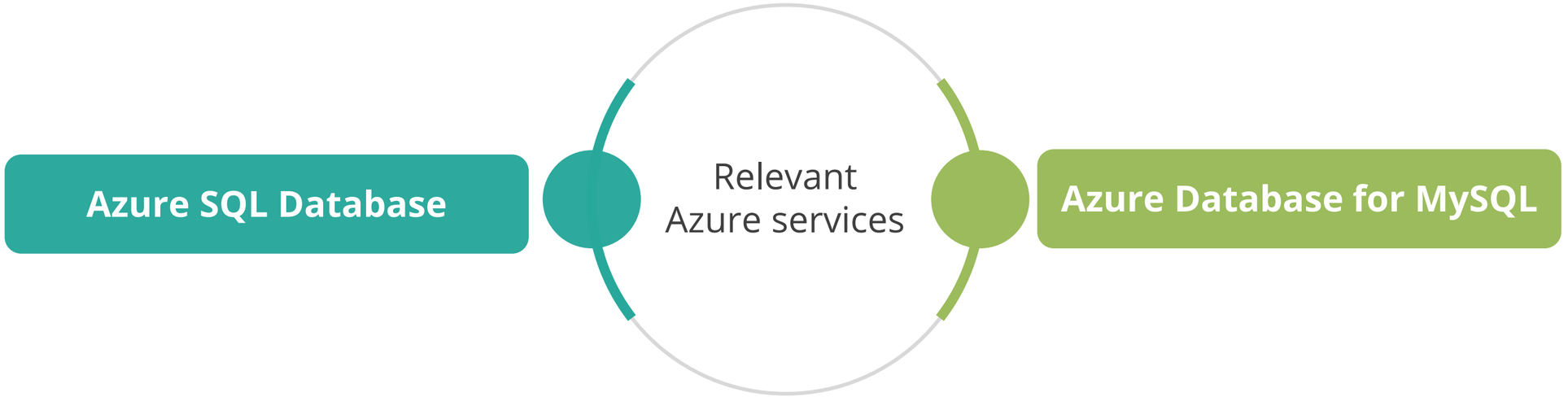
Each table has its own columns, and every row in a table has the same set of columns.




RDBMS implements a transactionally consistent mechanism that conforms to the ACID model for updating information.

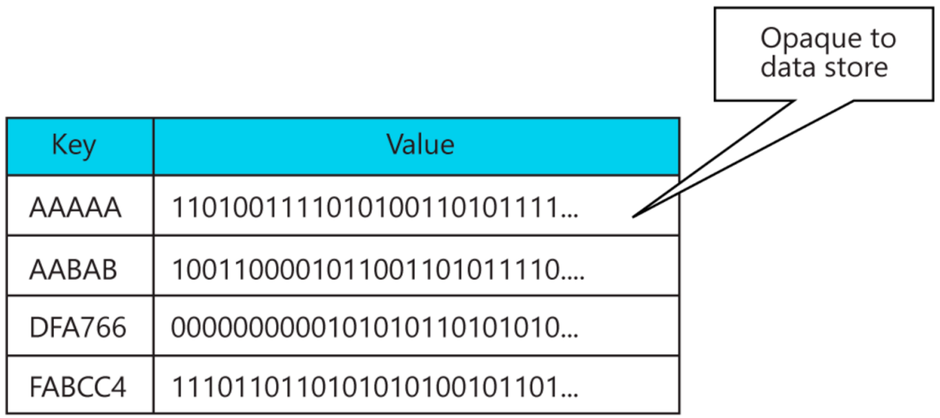
# Relational Database Management Systems

An RDBMS is useful when strong consistency guarantees are important.



# Key or Value Stores

A key or value store is a large hash table.




- Associate each data value with a unique key
- Most key or value stores only support simple query, insert, and delete operations.
- An application can store arbitrary data as a set of values,
- Some key or value stores impose limits on the maximum size of values

# Key or Value Stores

A key or value store is a large hash table.

These are the features of key or value stores.

Cosmos DB

Azure Cache for Redis

Azure Tables

# Document Databases

It is conceptually like a key or value store, except that it stores a collection of named fields and data.

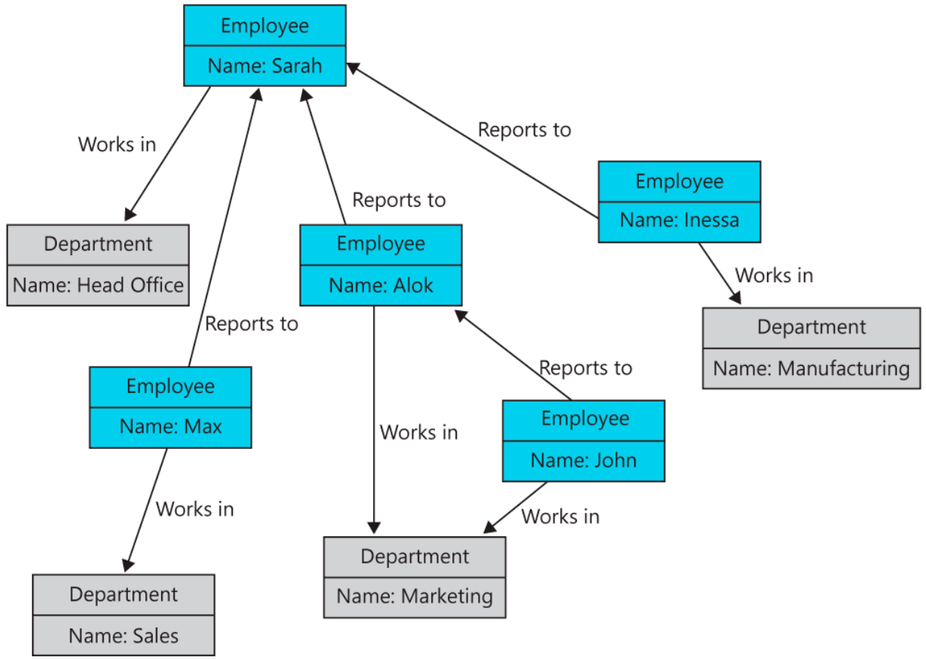
Data fields of a document can be encoded, including XML, YAML, JSON, and BSON.

| Key | Document |
|---|---|
| 1001 | {<br>“CustomerID”:99<br>“OrderItems”:[<br>{”ProductID”:2010,<br>“Quantity”:2,<br>“Cost”:520<br>},<br>{”ProductID”:4365,<br>“Quantity”:1,<br>“Cost”:18<br>}],<br>“OrderDate”:”04/01/2017”<br>} |
| 1002 | {<br>“CustomerID”:220<br>“OrderItems”:[<br>{”ProductID”:1825,<br>“Quantity”:1,<br>“Cost”:120<br>}],<br>“OrderDate”:”05/08/2017”<br>} |

- A document store does not require that all documents have the same structure
- **Relevant Azure services:** Cosmos DB

# Graph Databases

A graph database stores two types of information, nodes and edges.

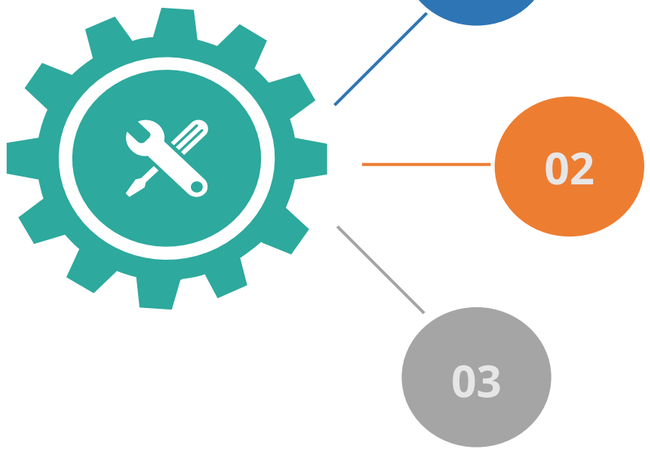



- Nodes are entities
- Edges which specify the relationships between nodes
- Both nodes and edges can have properties that provide information about that node
- Edges can also have a direction indicating the nature of the relationship
- **Relevant Azure services**: Cosmos DB

# Overview of Azure Data Storage

# Azure SQL Database

Azure SQL Database is a fully managed platform as a service (PaaS) database engine.



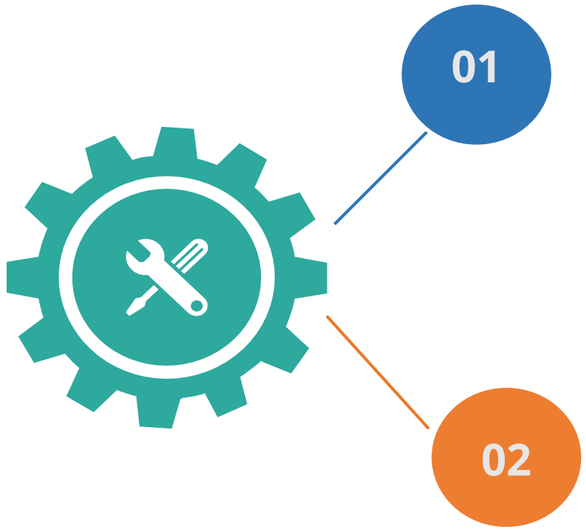

Provides High-performance, reliability, fully managed, and secure

Supports multiple programming languages

Migrates users existing SQL Server databases using the Azure Database Migration Service

# Azure SQL Database

Azure SQL Database deployment options for a database:

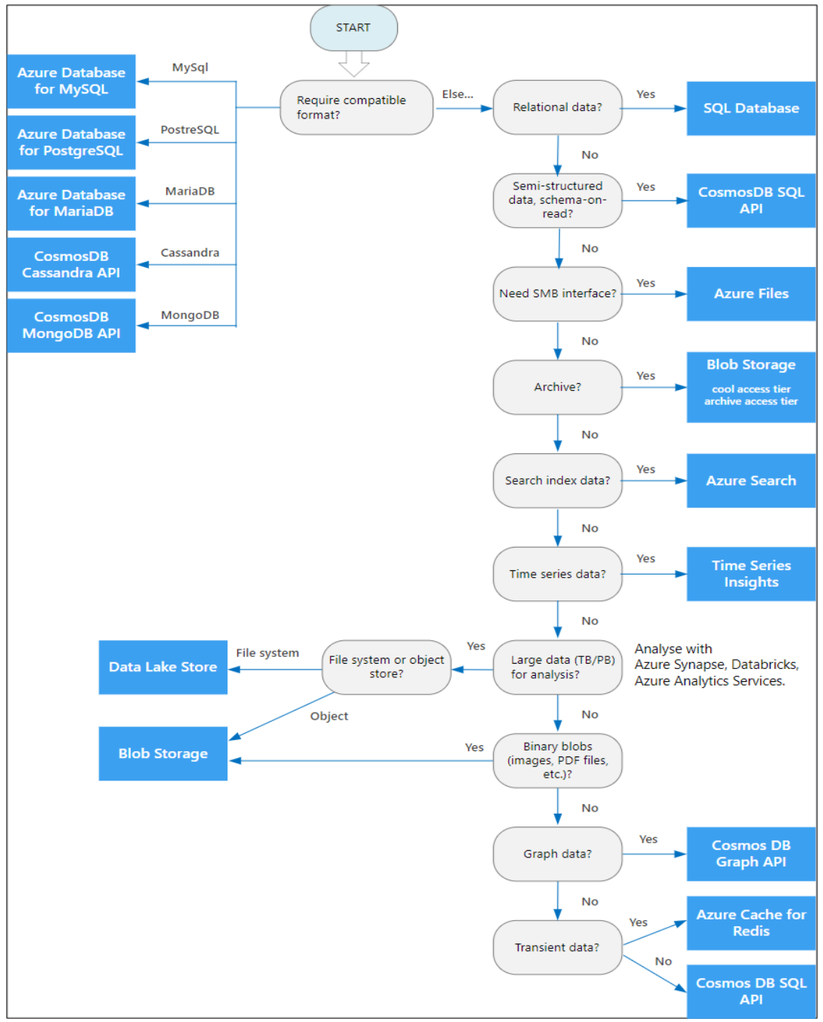



Single database represents a fully managed, isolated database

Elastic pool is a collection of single databases with a shared set of resources, such as CPU or memory

# Select a Candidate Data Store

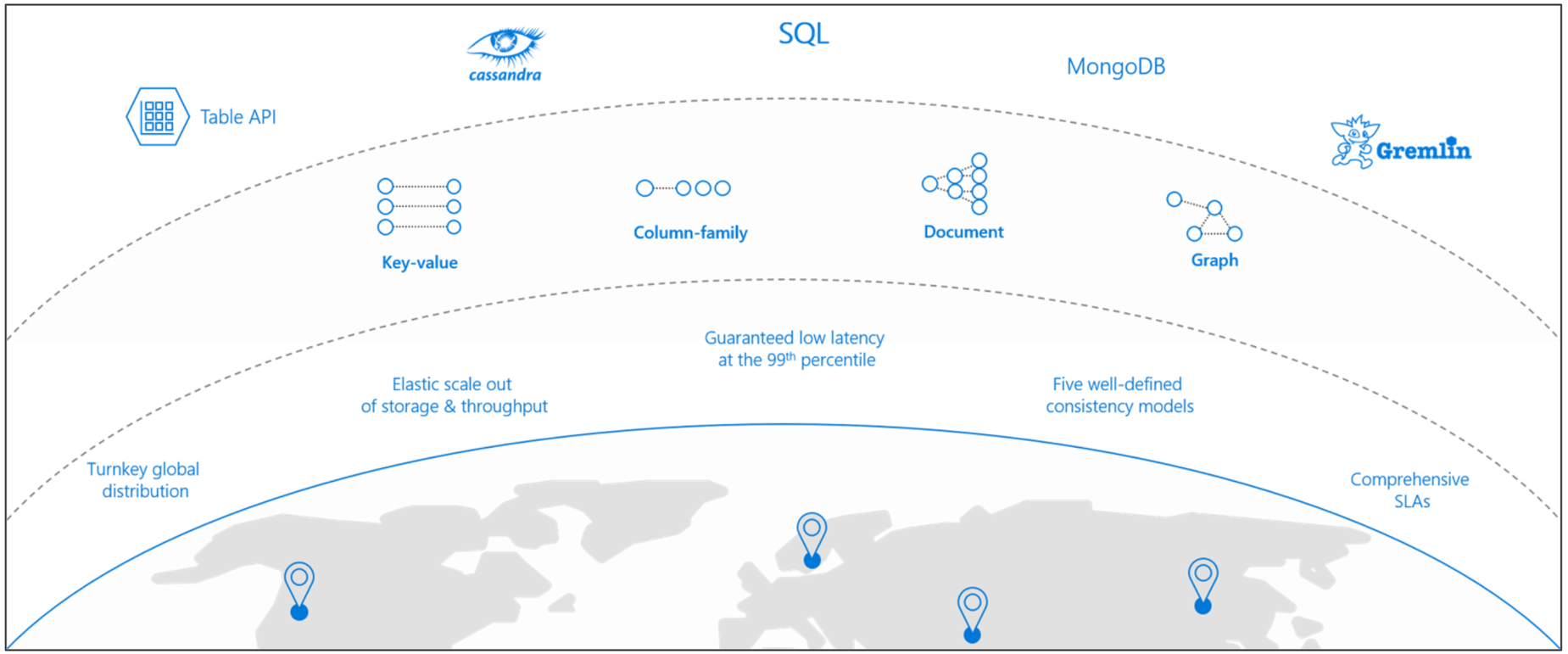
Azure offers several managed data storage solutions, each one provides different features and capabilities.




- If the application consists of multiple workloads, evaluate each workload separately.
- A complete solution may incorporate multiple data stores.

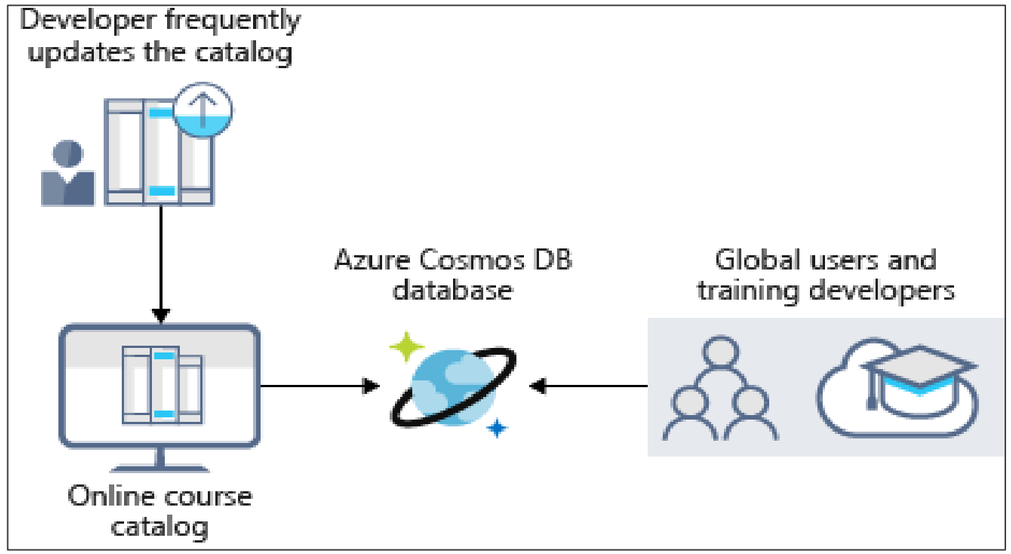
# Azure Cosmos DB

Azure Cosmos DB is a globally distributed and elastically scalable database.



# Azure Cosmos DB

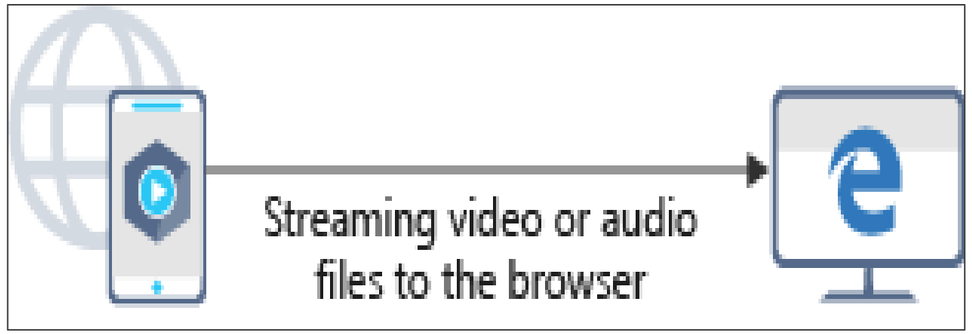
Azure Cosmos DB features:




- Geo-replication
- Elastic scaling of throughput and storage worldwide
- Five well-defined consistency levels

# Azure Blob Storage

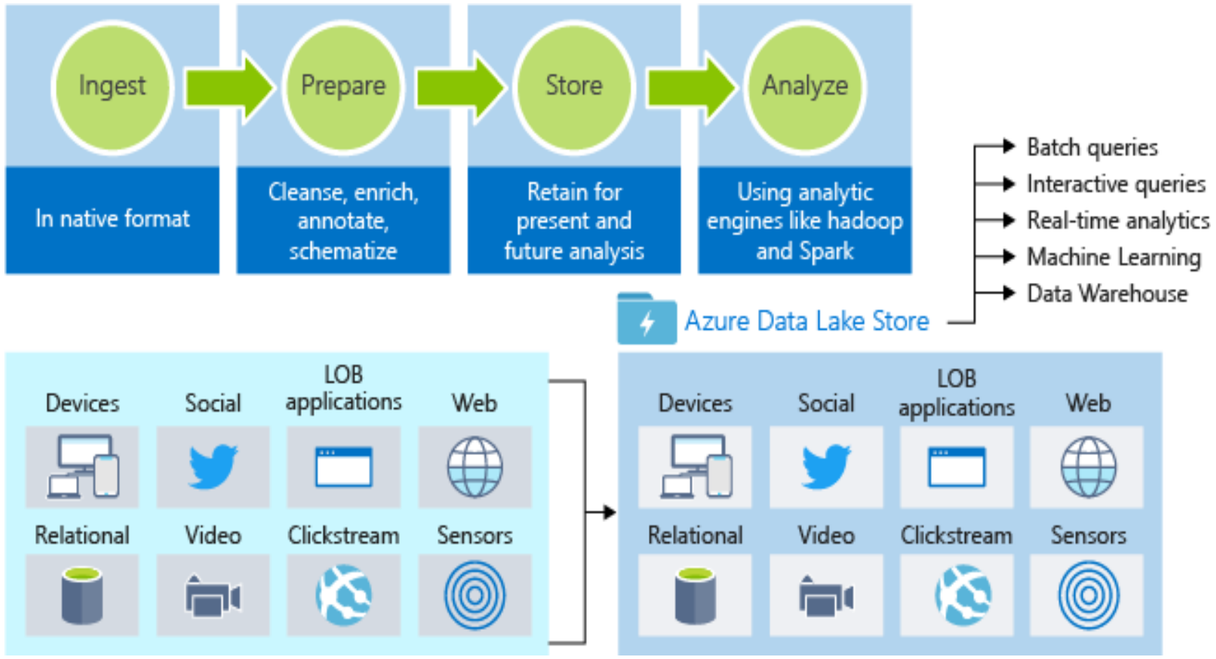
Azure Blob storage features:




- Azure Blob Storage is unstructured
- Highly scalable
- Thousands of simultaneous uploads
- Access Anywhere in the world

# Azure Data Lake Storage

Azure data lake storage features:




- Structured and unstructured data
- Hyperscale repository for big data analytic workloads
- No limits on account sizes, file sizes, or the amount of data

Hadoop accessed (available through HDInsight) using WebHDFS-compatible REST APIs

# Candidate Services

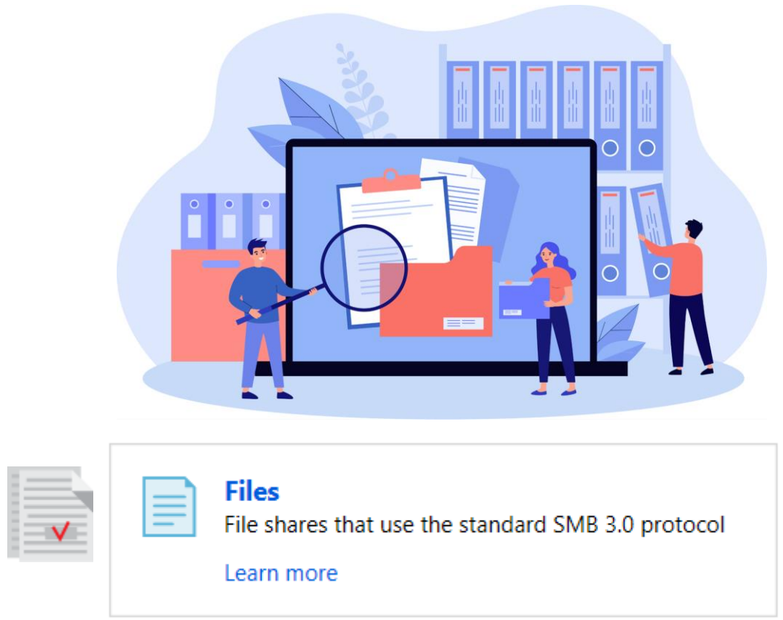
| Category | Azure Data Lake Storage Gen1 | Azure Blob Storage |
|---|---|---|
| **Purpose** | Optimized storage for big data analytics workloads | General purpose object store for a wide variety of storage scenarios |
| **Use Cases** | Batch, interactive, streaming analytics and machine learning data such as log files, IoT data, click streams, large datasets | Any type of text or binary data, such as application back end, backup data, media storage for streaming and general-purpose data |
| **Structure** | Hierarchical file system | Object store with flat namespace |
| **Authentication** | Based on Azure Active Directory Identities | Based on shared secrets - Account Access Keys and Shared Access Signature Keys. |
| **Authentication Protocol** | OAuth 2.0. Calls must contain a valid JWT (JSON Web Token) issued by Azure Active Directory | Hash-based Message Authentication Code (HMAC). Calls must contain a Base64-encoded SHA-256 hash over a part of the HTTP request. |
| **Authorization** | POSIX Access Control Lists (ACLs). ACLs based on Azure Active Directory Identities can be set at the file and folder level | For account-level authorization – Use Account Access Keys |
| | | For account, container, or blob authorization - Use Shared Access Signature Keys |

# Candidate Services

| Category | Azure Data Lake Storage Gen1 | Azure Blob Storage |
|---|---|---|
| **Auditing** | Available. | Available |
| **Encryption data at rest** | Transparent, Server side | Transparent, Server side / Client-Side encryption |
| **Developer SDKs** | .NET, Java, Python, Node.js | .NET, Java, Python, Node.js, C++, Ruby, PHP, Go, Android, iOS |
| **Analytics Workload Performance** | Optimized performance for parallel analytics workloads. High Throughput and IOPS | Optimized performance for parallel analytics workloads |
| **Size limits** | No limits on account sizes, file sizes, or number of files | For specific limits |
| **Geo-redundancy** | Locally redundant (multiple copies of data in one Azure region) | Locally redundant (LRS), zone redundant (ZRS), globally redundant (GRS), read-access globally redundant (RA-GRS). See here for more information |

# Azure Files

Managed file shares in the cloud that are accessible via SMB, these can be mounted concurrently by cloud or on-premises resources.

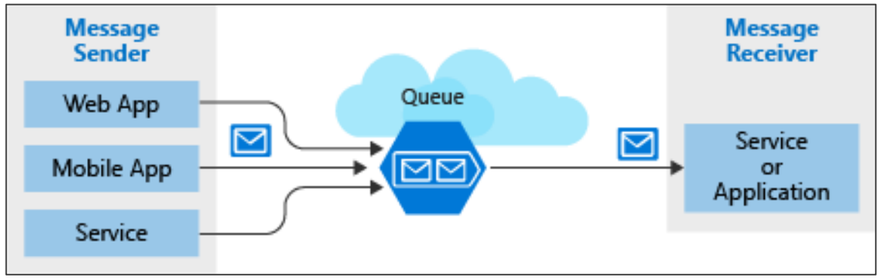



**Common uses:**

- Replace and supplement
- Lift and shift
- Azure File Sync
- Shared applications
- Diagnostic data
- Tools and utilities

# Azure Queues

These are the features and uses of azure queues:




## Azure queues features:

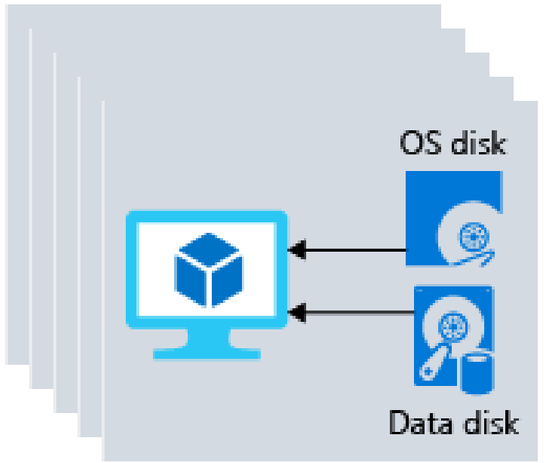
- Storing large numbers of messages
- Accessed from anywhere in the world
- Provides asynchronous message queueing

## Use queue storage to:

- Create a backlog of work
- Pass messages between services
- Distribute load
- Build resilience against component failures

# Disk Storage

These are the disk storage features:




- Provides disks for virtual machines, applications, and other services
- Persistent virtual hard disk storage
- Disks can be managed or unmanaged
- Solid-state drives (SSDs) and hard disk drives (HDDs)
- Standard SSD and HDD disks
- Premium SSD for mission-critical applications

# Assisted Practice

**Azure Cosmos DB**
**Duration: 10 Min.**

**Problem Statement:**

As an Azure Architect, you've been asked to provide your organization with a fully managed NoSQL database for modern app development that provides single-digit millisecond response times, automatic and rapid scalability, and guarantees speed at any size.

# Assisted Practice: Guidelines

Steps to create an Azure Cosmos DB account:

1. Login to your Azure Account
2. In the Policy pane, select Assignments and then click on Assign policy
3. Search for Azure Cosmos DB and select it
4. Creating an Azure Cosmos DB account

# Assisted Practice

**Azure SQL DB**
**Min.**

**Duration: 10**

**Problem Statement:**

As an Azure Architect, you've been asked to provide your company with an Azure database solution that can be utilized to store data with long-term retention.

# Assisted Practice: Guidelines

Steps to create an Azure SQL DB:

1. Login to the Azure portal at https://portal.azure.com
2. Select the SQL databases
3. Select the configurations as per the requirement
4. Select Next: Networking
5. Select Next: Additional settings

# Recommend Database Service Tier Sizing

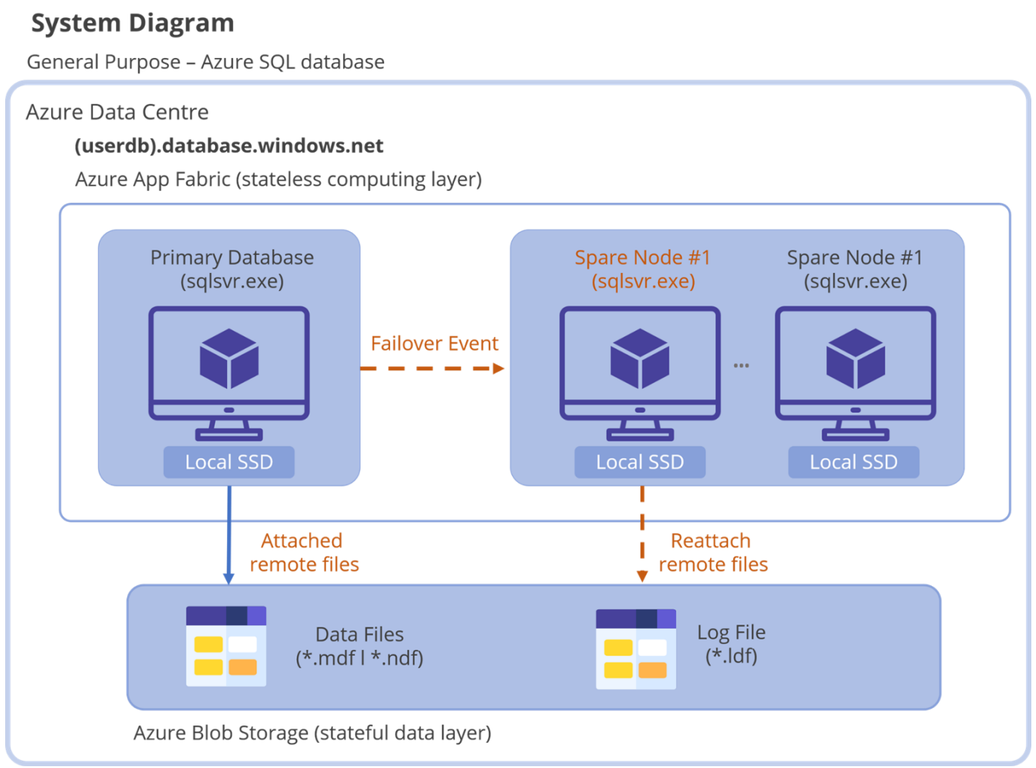
# Azure SQL Database and Azure SQL Managed Instance Service Tiers

The types of Azure SQL database & SQL managed instance service tiers are:

| General purpose | Business critical | Hyperscale |
| --- | --- | --- |
| Budget oriented workloads | Low latency workloads | Business workloads |

# General Purpose Service Tier for Azure SQL Database & Azure SQL Managed Instance

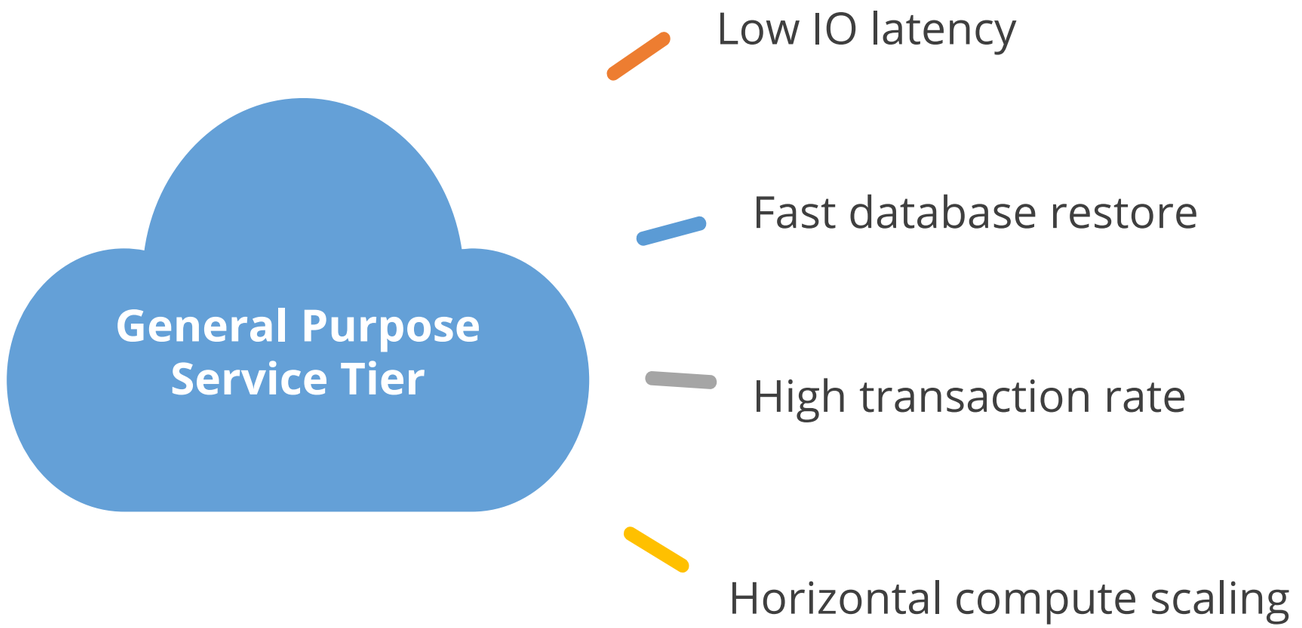
This service tier comes with 99% availability.




It is a default service tier that is suitable for most generic workloads.

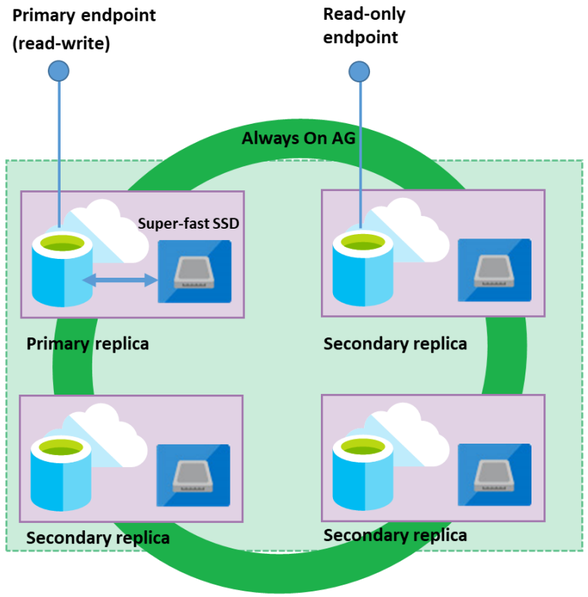
# General Purpose Service Tier for Azure SQL Database & Azure SQL Managed Instance

The benefits of General Purpose Service Tier are:



# Business Critical Tier for Azure SQL Database & Azure SQL Managed Instance

The Business Critical Tier is based on a cluster of database engine processes.

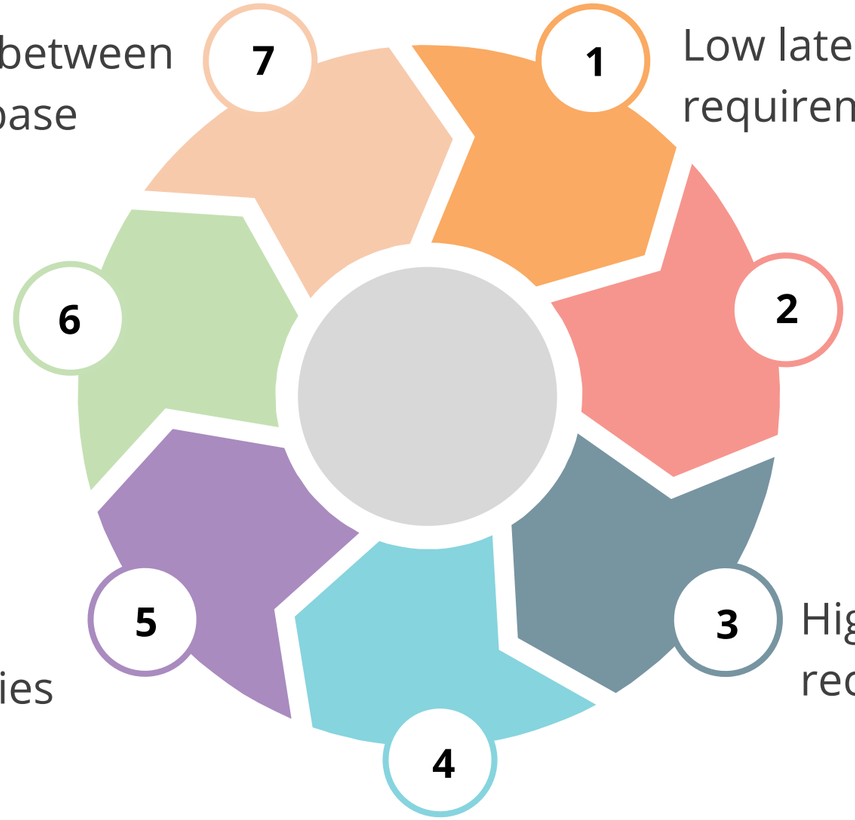



Business Critical service tier: collocated compute and storage

Premium availability is enabled in this service tier.

# Business Critical Tier for Azure SQL Database & Azure SQL Managed Instance

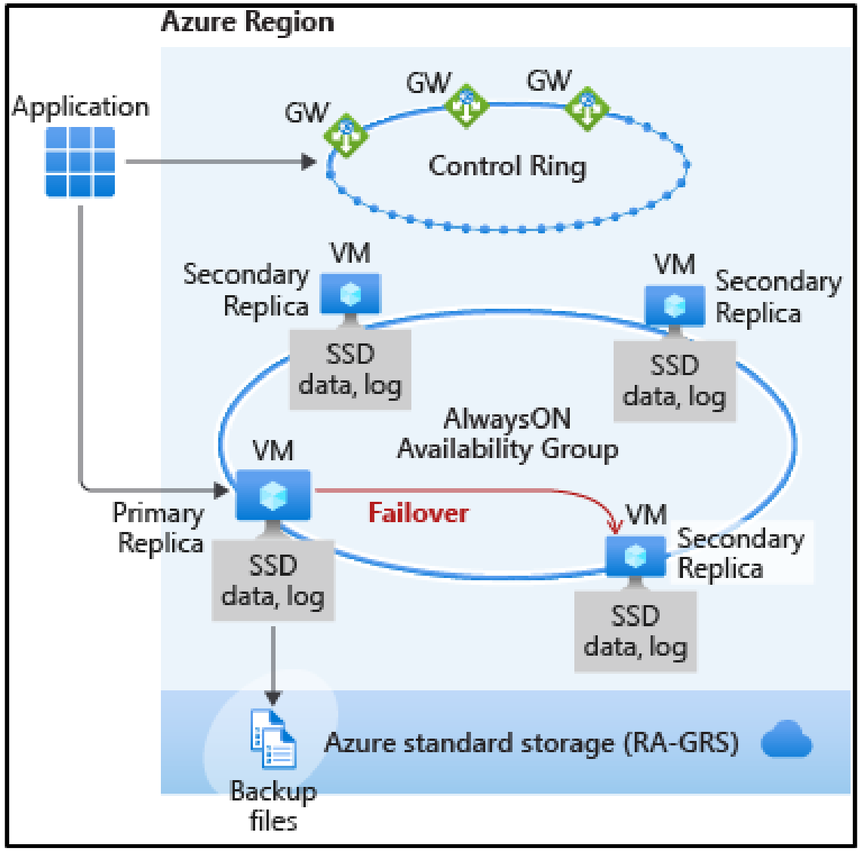
Business critical service tier can be chosen when there are:




1. Low latency requirements
2. Higher availability
3. Higher resiliency and faster recovery from failure
4. Fast geo-recovery
5. More time consumed in reporting and analytic queries
6. Long running transactions that modify data
7. Frequent communication between application and database

# Business Critical Service Tier Availability

Business critical high availability service tier is created when a four-node cluster is formed.




Source: https://docs.microsoft.com/

# Service Tier Comparison (Azure SQL and SQL Managed Instance)

The difference between the service tiers is given in the table below:

| Availability | Resource type | General Purpose | Business Critical | Hyperscale |
|---|---|---|---|---|
| Compute size | SQL database | 1 to 80 vCores | 1 to 80 vCores | 1 to 80 vCores |
| Storage size | SQL database | 5 GB - 4 TB | 5 GB - 4 TB | Upto 100 TB |
| TempDB size | SQL managed instance | 24 GB per vCore | Upto 4 TB | N/A |
| In-memory OLTP | SQL managed instance | N/A | Available | N/A |
| Database size | SQL database | 5 GB - 4 TB | Upto 100 TB | 5 GB - 4 TB |

# Service Tier Comparison (Azure SQL and SQL Managed Instance)

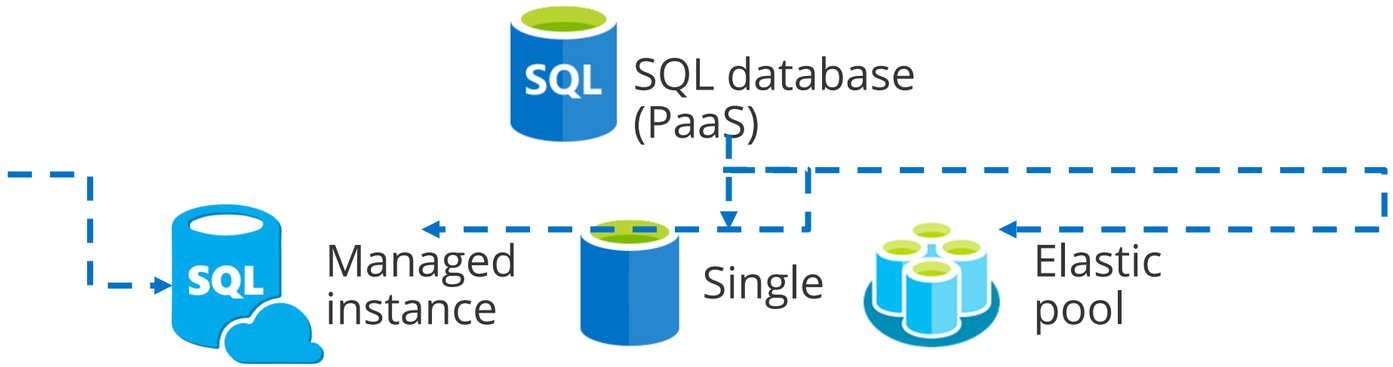
| General Purpose | Hyperscale | Business Critical |
|---|---|---|
| Least expensive | Less expensive | Most expensive |
| Latency 5-10 milliseconds | Scales compute resources up and down very quickly | Latency 1-2 milliseconds |
| 99.99 % availability | Instant backups and fast database restores | 99.95 % availability |
| Maximum size 4TB | Maximum size 100TB | Local SSDs on four-node cluster |

The service tier characteristics might be different in SQL database and SQL managed instance.

# Recommend a Solution for Database Scalability

# Dynamically Scale Azure SQL Database and Azure SQL Managed Instance

SQL database enables the users to change resources allocated to the databases.




SQL managed instance is a new deployment option that enables frictionless migration for SQL apps and modernization in a fully managed service.

# Dynamically Scale Azure SQL Database and Azure SQL Managed Instance

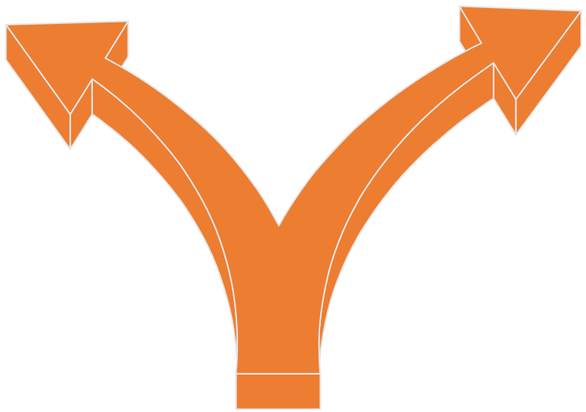
These are the benefits of Scaling:

- Is cost effective
- Is more versatile
- Mitigates performance issues
- Handles the incoming workload well

# Azure SQL Database and Azure SQL Managed Instance Pricing

Azure SQL database and SQL managed instance offers two types of purchasing model:

DTU-based purchasing model

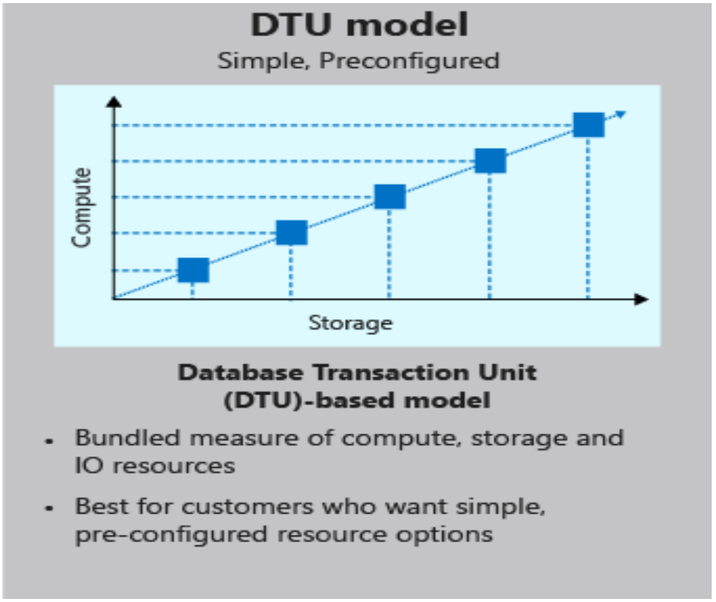


vCore-based purchasing model

**Purchasing model**

# The DTU-Based Purchasing Model

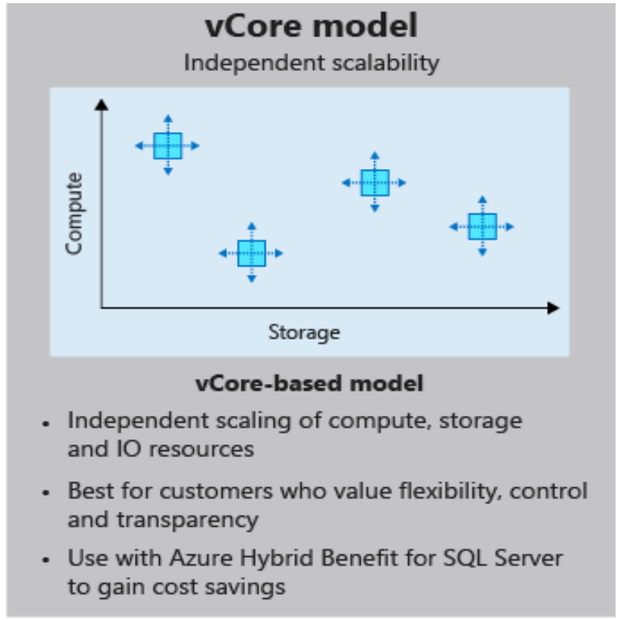
A Database Transaction Unit (DTU) is a composite metric that includes CPU, memory, reads, and writes.




The DTU-based purchase model provides a list of preconfigured compute resource bundles.

# The vCore-Based Purchasing Model

The vCore-based model helps in optimizing price.



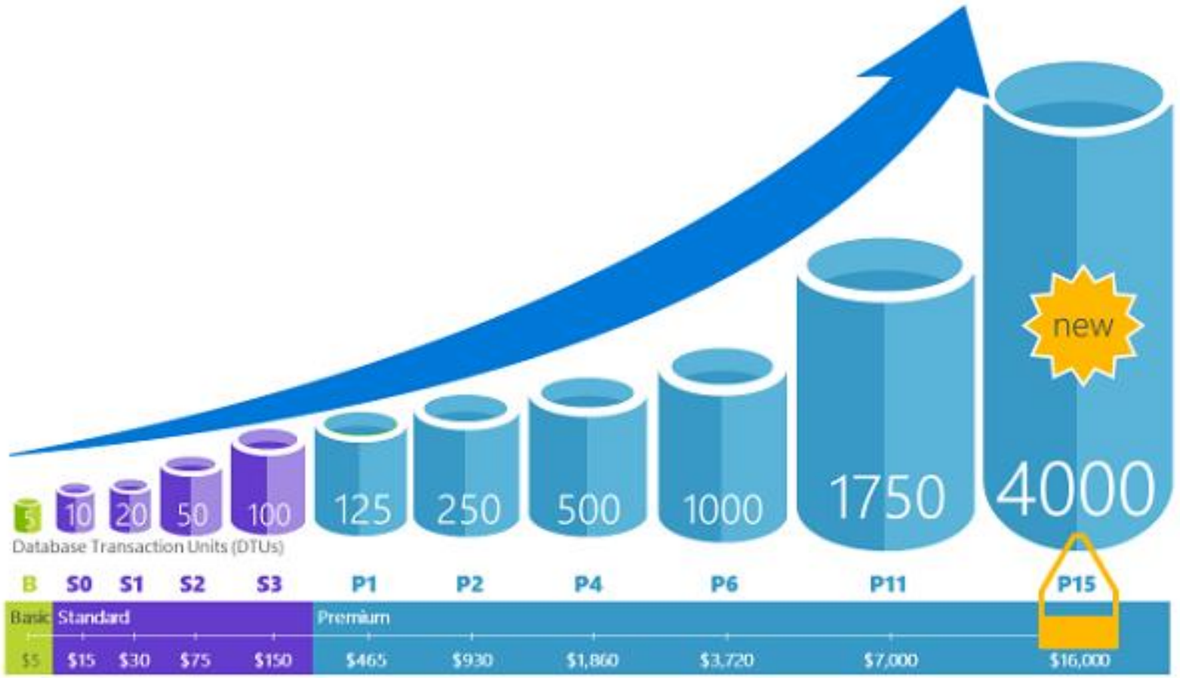

The vCore-based pricing strategy allows users to choose computing and storage resources individually.

# Scaling Azure SQL Database and Azure SQL Managed Instance

Scaling the database can be done via the Azure portal using a slider.

# Scale Single Databases in Azure SQL Database

Azure SQL Database allows the users to scale the databases dynamically.



# Scale Single Databases in Azure SQL Database

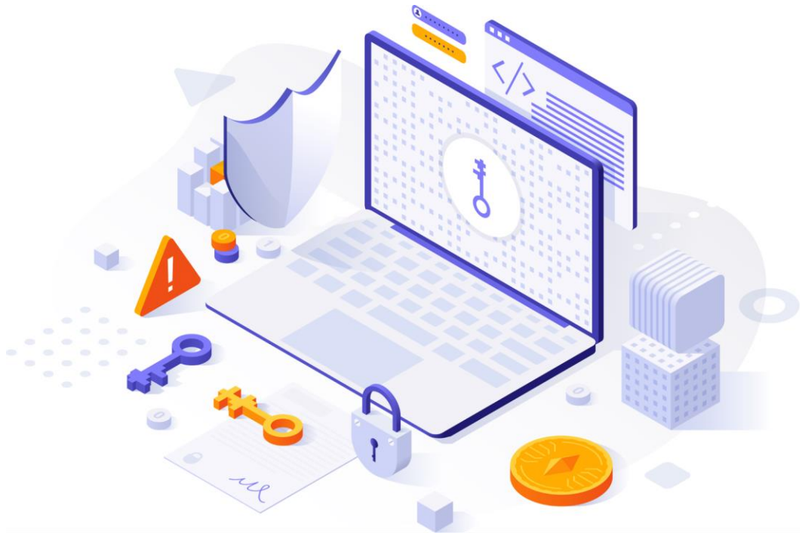
The user can determine the maximum number of resources that will be assigned to each database using either of the purchasing models.

The user can set a maximum resource limit for each group of databases in an elastic pool.

# Recommend a Solution for Encrypting Data

# Data Encryption

Encryption is the process of making data unreadable and unusable.

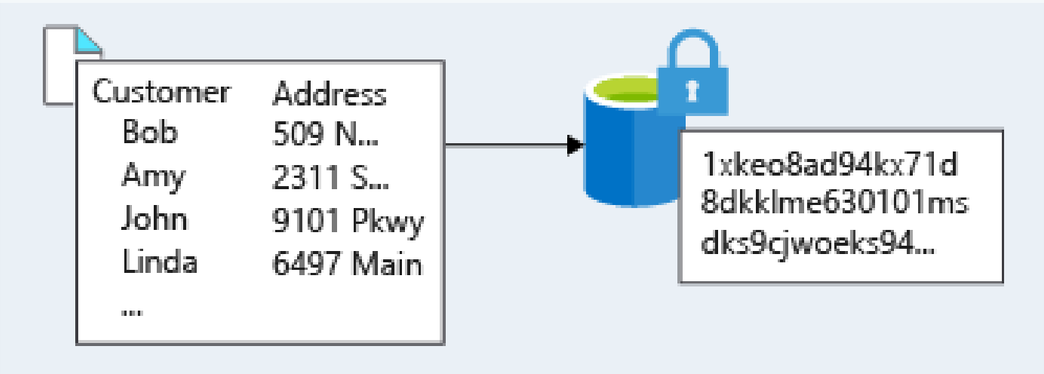


There are two top-level types of encryption:

- **Symmetric encryption:** Uses the same key to encrypt and decrypt the data
- **Asymmetric encryption:** Uses a public key and private key pair

# Encryption at Rest

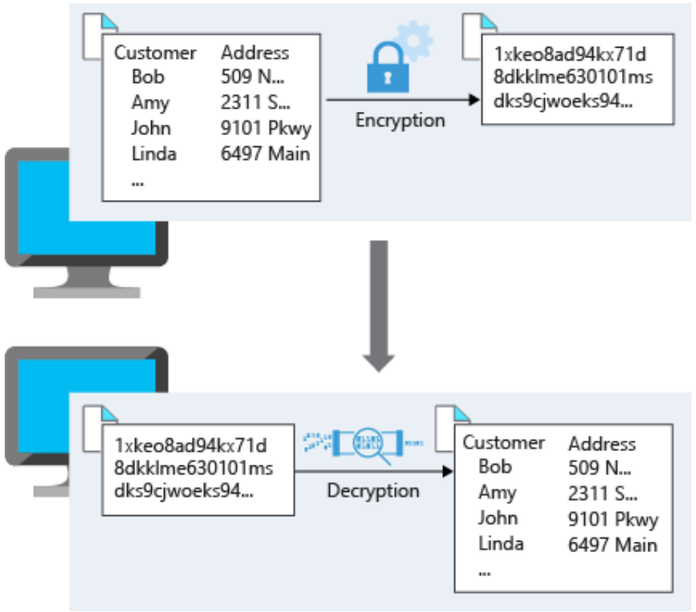
Data at rest is the data that has been stored on a physical medium.




- Unreadable without the keys and secrets
- Azure Disk Encryption uses Windows BitLocker, Linux dm-crypt
- Azure Storage and Azure SQL Database encrypt data at rest by default
- Use Azure Key Vault to maintain control of keys
- Encrypt drives before you write sensitive data

# Encryption in Transit

Encrypting data in transit protects the data from outside observers.




Microsoft uses Transport Layer Security (TLS) to protect data when it's traveling between the cloud services and customers.

# Identify and Classify Data

These are the built-in roles that identify and classify the data:

| Data Classification | Explanation | Example |
|---|---|---|
| Restricted | Data classified as restricted poses a significant risk if it's exposed, altered, or deleted. Strong levels of protection are required for this data. | Data containing SS numbers, CC numbers, and personal health records |
| Private | Data classified as private poses a moderate risk if it's exposed, altered, or deleted. Reasonable levels of protection are required for this data. Data that is not classified as restricted or public will be classified as private. | Personal records containing information such as address, phone numbers, and personal health records |
| Public | Data classified as public poses no risk if exposed, altered, or deleted. No protection is required for this data. | Public financial reports, public policies, and product documentation for customers |

# Encrypting Raw Storage

Azure Storage Service Encryption (SSE) for data at rest protects data to meet organizational security and compliance commitments.

# Encrypting Raw Storage

The Azure storage platform automatically encrypts data with 256-bit Advanced Encryption Standard (AES) in:

- All Azure Storage services including Azure Managed Disks, Azure Blob storage, Azure Files, Azure Queue storage, and Azure Table storage
- Both performance tiers (Standard and Premium)
- Both deployment models (Resource Manager and classic)

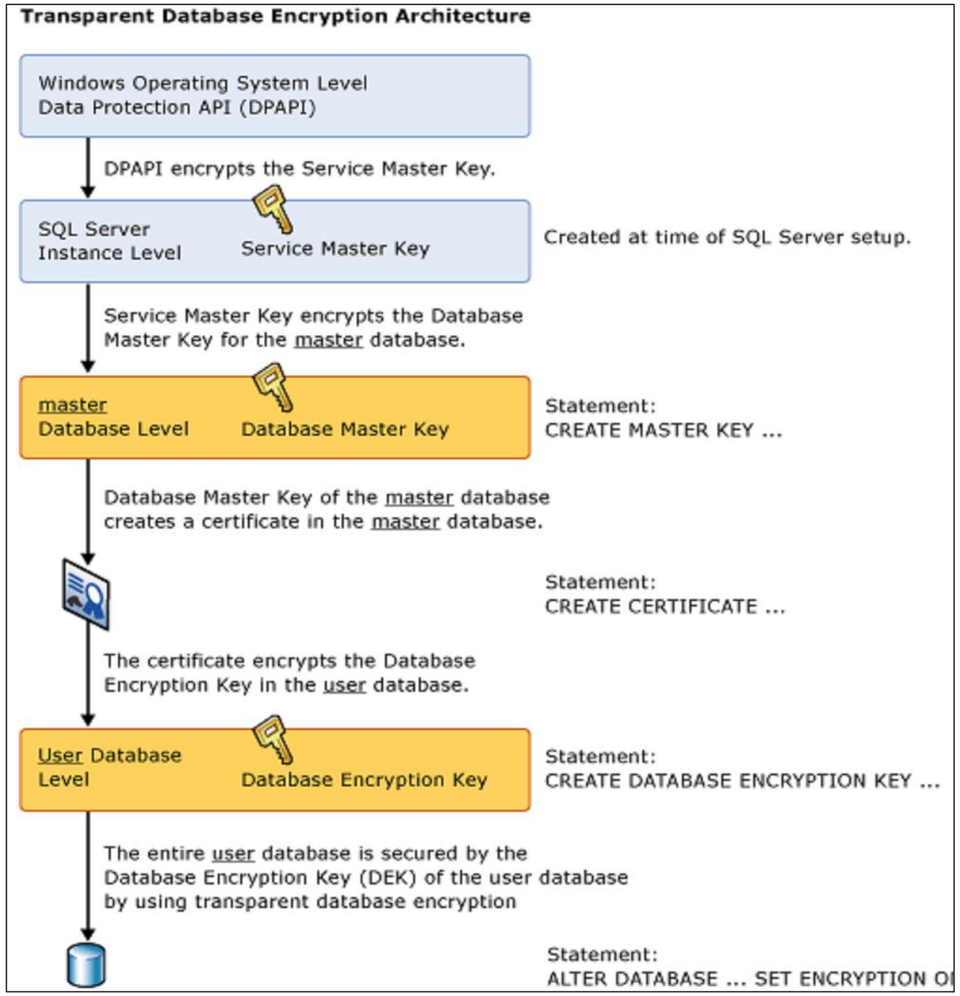
# Encrypting Virtual Machines

These points provide guidance for encrypting virtual machines:

- Azure Disk Encryption (ADE) encrypts Windows and Linux IaaS virtual machine disks
- ADE uses BitLocker on Windows and the DM-Crypt feature of Linux
- ADE is integrated with Azure Key Vault
- IaaS VMs are secured at rest by using industry-standard encryption
- IaaS VMs boot under customer-controlled keys and policies
- IaaS VMs can be audited in KeyVault

# Encrypting Databases

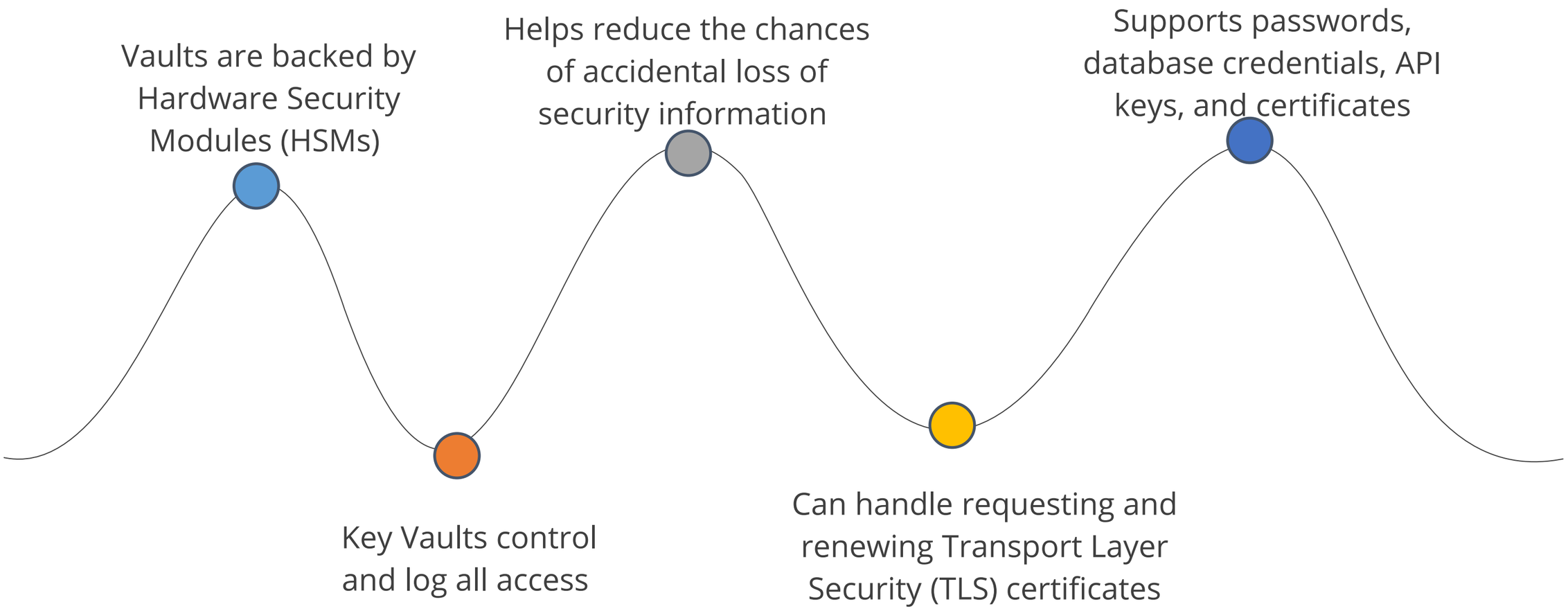
Transparent data encryption (TDE) helps protect the Azure SQL Database and Azure Data Warehouse.




## Features

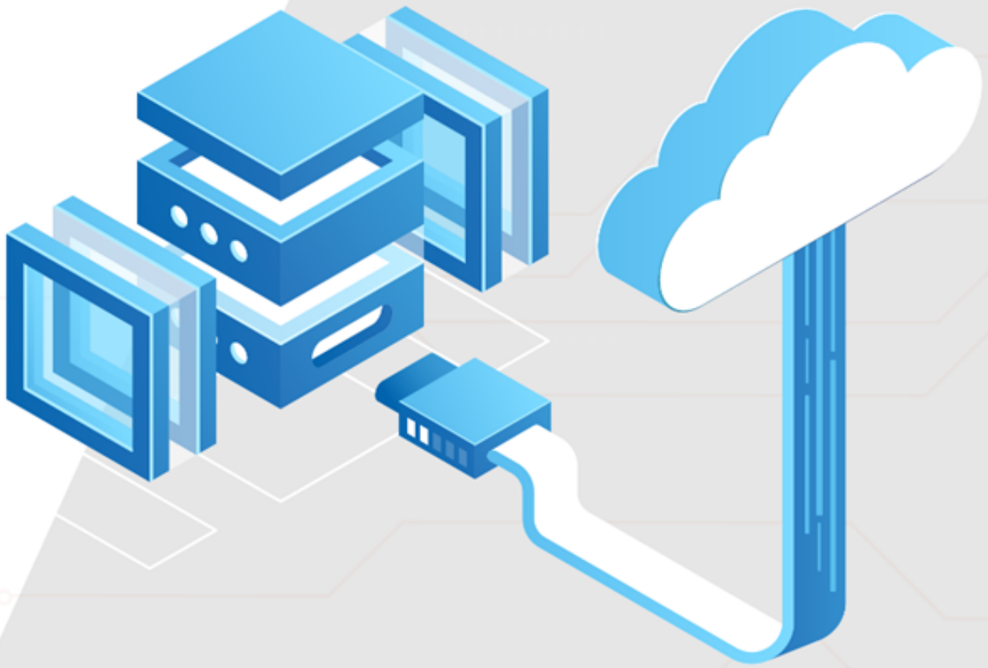
- Real-time encryption and decryption
- Enabled by default
- Uses symmetric key called the database encryption key
- Unique encryption key per logical SQL Server
- Bring-your-own-key is also supported with keys stored in Azure Key Vault

# Encrypting Secrets



# Key Takeaways

- Azure SQL Database is a fully managed platform as a service (PaaS) database engine.
- SQL managed instance is a new deployment option that enables frictionless migration for SQL apps and modernization in a fully managed service.
- Encrypting data in transit protects the data from outside observers and provides a mechanism for transmitting data while limiting risk of exposure
- Azure Storage Service Encryption (SSE) for data at rest protects data to meet organizational security and compliance commitments.



# Thank you