General Information

Sunday, June 5, 2022 11:44 AM

Course Official Website
https://docs.microsoft.com/en-us/learn/certifications/exams/az-305

Online Courseware
https://docs.microsoft.com/en-us/users/msftofficialcurriculum-4292/collections/zwm5cy2ownzz08

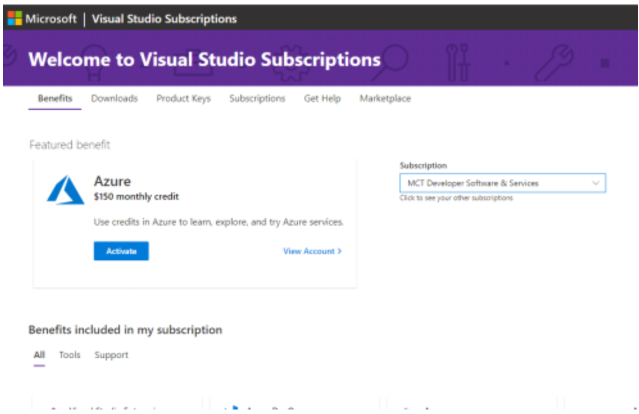
AZ-900 hands-on lab
https://microsoftlearning.github.io/AZ-900T0x-MicrosoftAzureFundamentals/

Github Version of this notes
https://github.com/Cyrus-Sir/hkjc-az-305

https://www.microsoft.com/en-US/cloudskillschallenge/build/registration/2022?wt.mc_id=rmskilling_az_usagecsc_inproduct_gdc

Free Azure

https://my.visualstudio.com/



Microsoft | Visual Studio Subscriptions

Welcome to Visual Studio Subscriptions

Featured benefit

Azure
$150 monthly credit

Use credits in Azure to learn, explore, and try Azure services.

Subscription: MCT Developer Software & Services

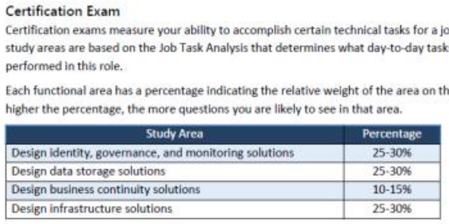
Click to see your other subscriptions

Benefits included in my subscription

Exam materials

Sunday, June 5, 2022 8:44 PM

Suggested study guide
https://www.thomasmaurer.ch/2021/10/az-305-study-guide-azure-solutions-architect



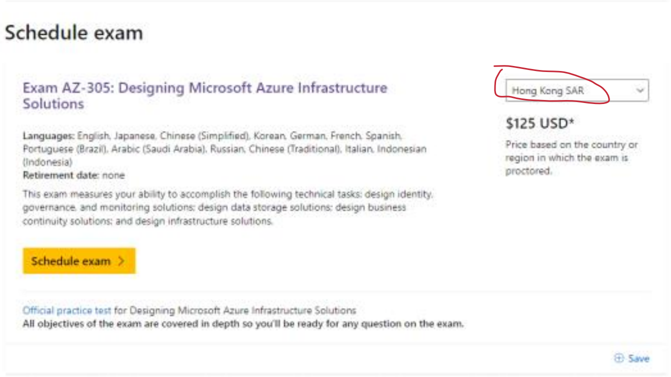
Certification Exam

Certification exams measure your ability to accomplish certain technical tasks for a job role. The study areas are based on the Job Task Analysis that determines what day-to-day tasks are performed in this role.

Each functional area has a percentage indicating the relative weight of the area on the exam. The higher the percentage, the more questions you are likely to see in that area.

Study Area	Percentage
Design identity, governance, and monitoring solutions	25-30%
Design data storage solutions	25-30%
Design business continuity solutions	10-15%
Design infrastructure solutions	25-30%

Exam



Schedule exam

Exam AZ-305: Designing Microsoft Azure Infrastructure Solutions

Languages: English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Arabic (Saudi Arabia), Russian, Chinese (Traditional), Italian, Indonesian (Indonesia)
Retirement date: none

This exam measures your ability to accomplish the following technical tasks: design identity, governance, and monitoring solutions; design data storage solutions; design business continuity solutions; and design infrastructure solutions.

Hong Kong SAR

$125 USD*

Price based on the country or region in which the exam is proctored.

Official practice test for Designing Microsoft Azure Infrastructure Solutions
All objectives of the exam are covered in depth so you'll be ready for any question on the exam.

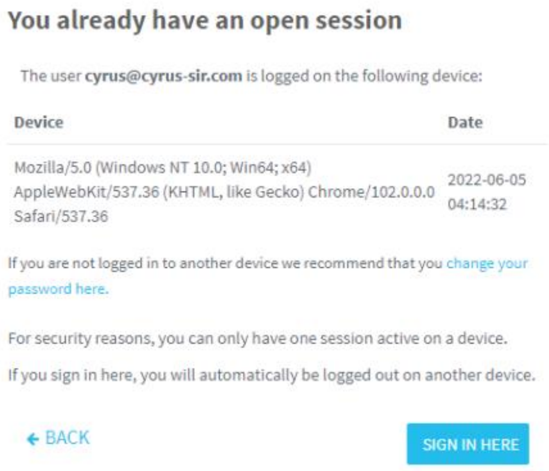
Practical Test (Cannot Share/Concurrent Login)

If you wants to have individual access, you can purchase from me, I have 40% off discount

https://marketplace.measureup.com/login

cyrus@cyrus-sir.com

When you see this, ask is there anyone is using in the WhatsApp Group, before you logout someone



You already have an open session

The user **cyrus@cyrus-sir.com** is logged on the following device:

Device	Date
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36	2022-06-05 04:14:32

If you are not logged in to another device we recommend that you change your password here.

For security reasons, you can only have one session active on a device.

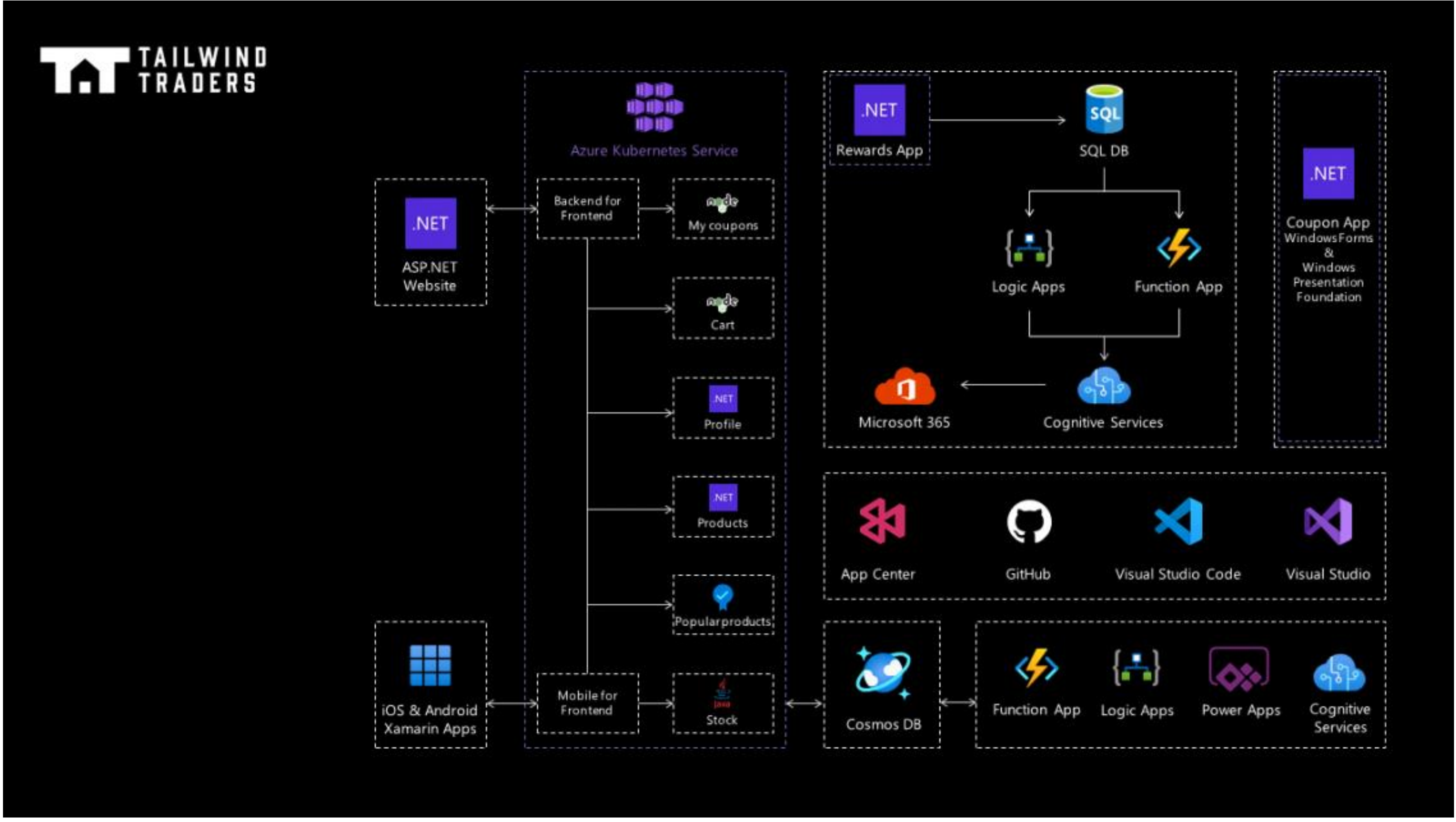
If you sign in here, you will automatically be logged out on another device.

Tailwind Traders

Monday, June 6, 2022 12:16 AM

Sample Application

https://github.com/microsoft/TailwindTraders



Tailwind

Sunday, June 5, 2022 3:29 PM

Case Study GitHub

https://github.com/MicrosoftLearning/AZ-305-DesigningMicrosoftAzureInfrastructureSolutions

Design a governance solution

Sunday, June 5, 2022 11:46 PM

Azure built-in roles
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Exercise

Title	URL
Create a management group	https://docs.microsoft.com/en-us/azure/governance/management-groups/create-management-group-portal
Manage your resources with management groups	https://docs.microsoft.com/en-us/azure/governance/management-groups/manage
Protect a storage account from accidental deletion by using a resource lock	https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/4-protect-storage-account-resource-lock
Restrict deployments to a specific location by using Azure Policy	https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/7-restrict-location-azure-policy
List access using Azure RBAC and the Azure portal	https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/4-list-access?source=learn
Grant access using Azure RBAC and the Azure portal	https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/5-grant-access
View activity logs for Azure RBAC changes	https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/6-view-activity-logs

Knowledge Check

Title	URL
Using Azure RBAC	https://docs.microsoft.com/en-us/learn/modules/secure-azure-resources-with-rbac/7-knowledge-check-rbac
Build a cloud governance strategy on Azure	https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/11-knowledge-check
Intro to Azure blueprints	https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-blueprints/5-knowledge-check
Describe core Azure architectural components	https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/knowledge-check

Case Study

Requirements

Tailwind Traders is planning on making some significant changes to their governance solution. They have asked for your help with recommendations and questions. Here are the specific requirements.

- Cost and accounting. Tailwind Traders has two core business units that handle Apparel and Sporting Goods. Each of the busin ess units has three departments: Product Development, Marketing, and Sales. Each business unit and subunit will track their Azure spend. At the same time, the Enterprise IT team will handle prov iding company-wide Azure cost reporting.
- New development project. The company has a new development project for customer feedback. The CFO wants to ensure all costs associated with the project are captured. For the testing phase, workloads should be hosted on lower cost virtual machines. The virtual machines should be named to indicate they are part of the project. Any instances of non-compliance with resource consistency rules should be automatically identified.

Tasks

1. Cost and accounting.
   - What are the different ways Tailwind Traders could organize their subscriptions and management groups? Which would be the b est to meet their requirements?

   https://app.diagrams.net/
2. New development project.
   - What are the different ways Tailwind Traders could track costs for the new development project?
   - How are you ensuring compliance with the requirements for virtual machine sizing and naming?

Design a compute solution

Sunday, June 5, 2022 11:46 PM

VM Size prefix meaning
https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series/

Create a virtual machine in the portal
https://microsoftlearning.github.io/AZ-900T0x-MicrosoftAzureFundamentals/Instructions/Walkthroughs/01-Create%20a%20virtual%20machine.html

Run your first Batch job with the Azure CLI
https://docs.microsoft.com/en-us/azure/batch/quick-create-cli
https://docs.microsoft.com/en-us/azure/batch/quick-create-portal

Run a parallel workload with Azure Batch using the .NET API
https://docs.microsoft.com/en-us/azure/batch/tutorial-parallel-dotnet

Create a Java app on Azure App Service
https://docs.microsoft.com/en-us/azure/app-service/quickstart-java?tabs=javase&pivots=platform-windows

Deploy a container instance in Azure using the Azure CLI
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-quickstart

Deploy an Azure Kubernetes Service cluster using the Azure CLI
https://docs.microsoft.com/en-us/azure/aks/learn/quick-kubernetes-deploy-cli

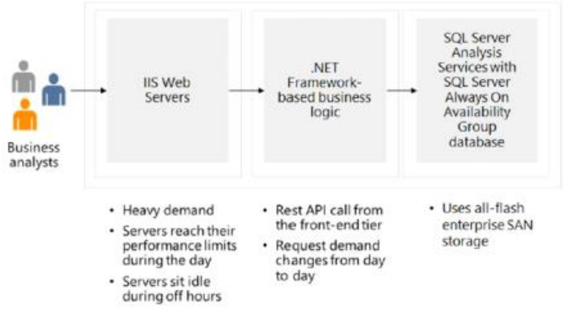
Create a C# function in Azure from the command line
https://docs.microsoft.com/en-us/azure/azure-functions/create-first-function-cli-csharp?tabs=azure-cli%2Cin-process

Module end labs

Create the social media tracker Logic App
https://docs.microsoft.com/en-us/learn/modules/route-and-process-data-logic-apps/4-ex-create-social-media-tracker

Case study

Requirements
Tailwind Traders would like to migrate their product catalog application to the cloud. This application has a traditional 3 -tier configuration using SQL Server as the data store. The IT team hopes you can help modernize the application. They have provided this diagram and several areas that could be improved.


Business analysts
IIS Web Servers
.NET Framework-based business logic
SQL Server Analysis Services with SQL Server Always On Availability Group database
• Heavy demand
• Servers reach their performance limits during the day
• Servers sit idle during off hours
• Rest API call from the front-end tier
• Request demand changes from day to day
• Uses all-flash enterprise SAN storage

- The front-end application is a .NET core-based web app. During peak periods 1750 customers visit the website each hour.
- The application runs on IIS web servers in a front-end tier. This tier handles all customer requests for purchasing products. During the latest holiday sale, the front -end servers reached their performance limits and page loads were lengthy. The IT team has considered adding more servers, but during off hours the servers are often idle.
- The middle tier hosts the business logic that processes customer requests. These requests are often for help desk support. Support requests are queued and lately the wait times have been exceptionally long. Customers are offered email rather than waiting for a representative. But many customers seem frustrated and are disconnectin g rather than waiting. Customer requests are 75-125 per hour.
- The back-end tier uses SQL Server database to store customer orders. Currently, the back-end database servers are performing well.
- While high availability is a concern, due to legal requirements the company must keep all the resources in a single region.

Task
- Front-end tier. Which Azure compute service would you recommend for the front-end tier? Explain why you decided on your solution.
- Middle tier. Which Azure compute service would you recommend for the middle tier? Explain why you decided on your solution.

Storage Account

Saturday, June 11, 2022 11:45 AM

Storage Account	Supported Services	Recommended usage
Standard general-purpose v2	Blob (including Data Lake Storage), Queue, and Table storage, Azure Files	Supports all the storage services: Blob, Azure Files, Queue, Disk (Page Blob), and Table.
Premium block blobs	Blob storage (including Data Lake Storage)	Premium block blobs are ideal for applications that require high transaction rates. Also ideal for situations that use smaller objects or require consistently low storage latency. This storage is designed to scale with your applications.
Premium file shares	Azure Files	Recommended for enterprise or high-performance scale applications. Use Premium file shares if you need a storage account that supports both SMB and NFS file shares.
Premium page blobs	Page blobs only	Premium high-performance page blob scenarios. Page blobs are ideal for storing index-based and sparse data structures like OS and data disks for virtual machines and databases.

Considerations

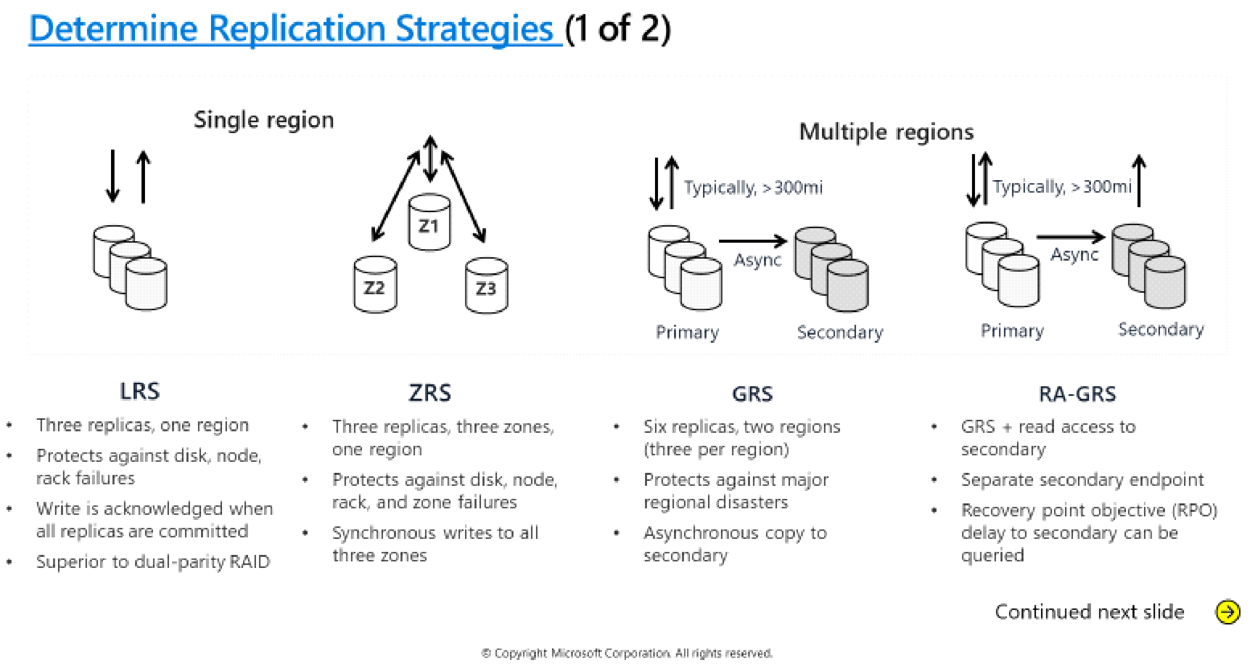
- Cost
- Compliance
- Location
- Replication requirements for different data nature
- Administrative overhead - Prevent deletion / update by date retention? By hold?
- Data sensitivity - Public / Private (Although can use VNet to protect)
- Data isolation - Retention policy differences?

Very important. Remember the endpoint for all storage account services

Storage service	Endpoint
Blob Storage	`https://<storage-account>.blob.core.windows.net`
Static website (Blob Storage)	`https://<storage-account>.web.core.windows.net`
Data Lake Storage Gen2	`https://<storage-account>.dfs.core.windows.net`
Azure Files	`https://<storage-account>.file.core.windows.net`
Queue Storage	`https://<storage-account>.queue.core.windows.net`
Table Storage	`https://<storage-account>.table.core.windows.net`

Redundancy

Saturday, June 11, 2022 11:52 AM



Determine Replication Strategies (1 of 2)

LRS

- Three replicas, one region
- Protects against disk, node, rack failures
- Write is acknowledged when all replicas are committed
- Superior to dual-parity RAID

ZRS

- Three replicas, three zones, one region
- Protects against disk, node, rack, and zone failures
- Synchronous writes to all three zones

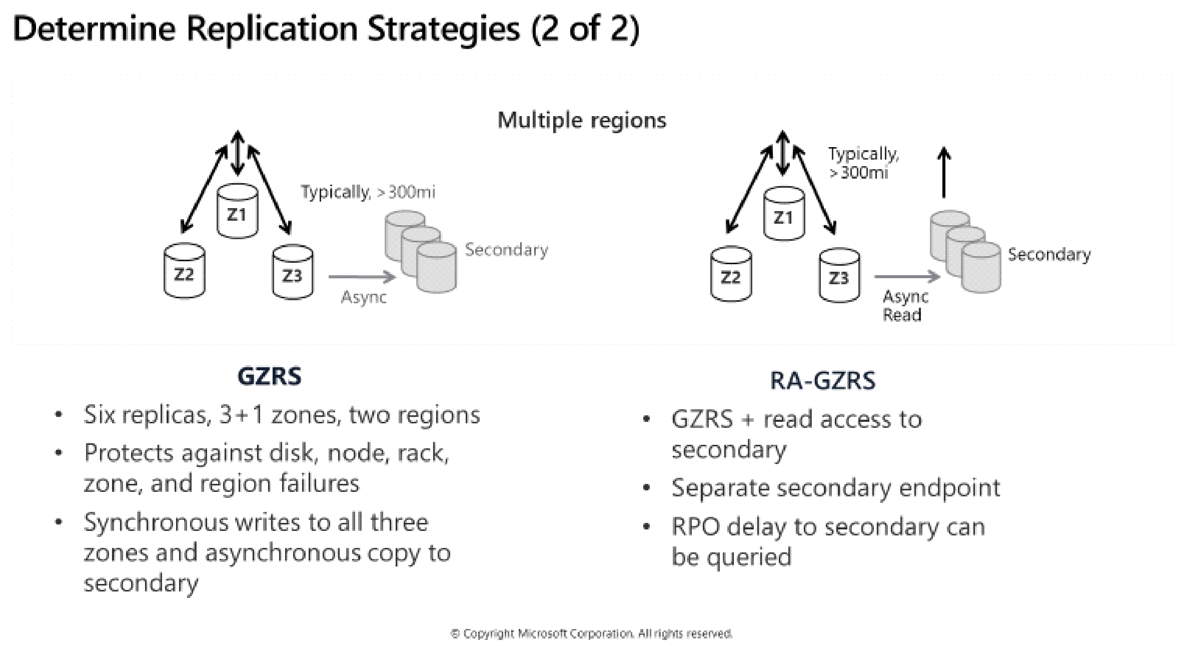
GRS

- Six replicas, two regions (three per region)
- Protects against major regional disasters
- Asynchronous copy to secondary

RA-GRS

- GRS + read access to secondary
- Separate secondary endpoint
- Recovery point objective (RPO) delay to secondary can be queried

Continued next slide



Determine Replication Strategies (2 of 2)

GZRS

- Six replicas, 3+1 zones, two regions
- Protects against disk, node, rack, zone, and region failures
- Synchronous writes to all three zones and asynchronous copy to secondary

RA-GZRS

- GZRS + read access to secondary
- Separate secondary endpoint
- RPO delay to secondary can be queried

Blob Storage

Saturday, June 11, 2022 11:58 AM

Access Tier	**Immutable Storage Policy**
Premium blob storage	Legal hold policies
Hot, cool, and archive access tiers	Time-based retention policies

Feature	**Premium**	**Hot tier**	**Cool tier**	**Archive tier**
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum storage duration	N/A	N/A	30 days	180 days Subject to early deletion charge
Latency (time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours
Use case	Date that small and requires frequent + fast updates Analytical Data	Application Data	Short-term backup Disaster recovery datasets Older media content wouldn't be viewed frequently but must be available immediately	Secondary backups Legally required compliance information

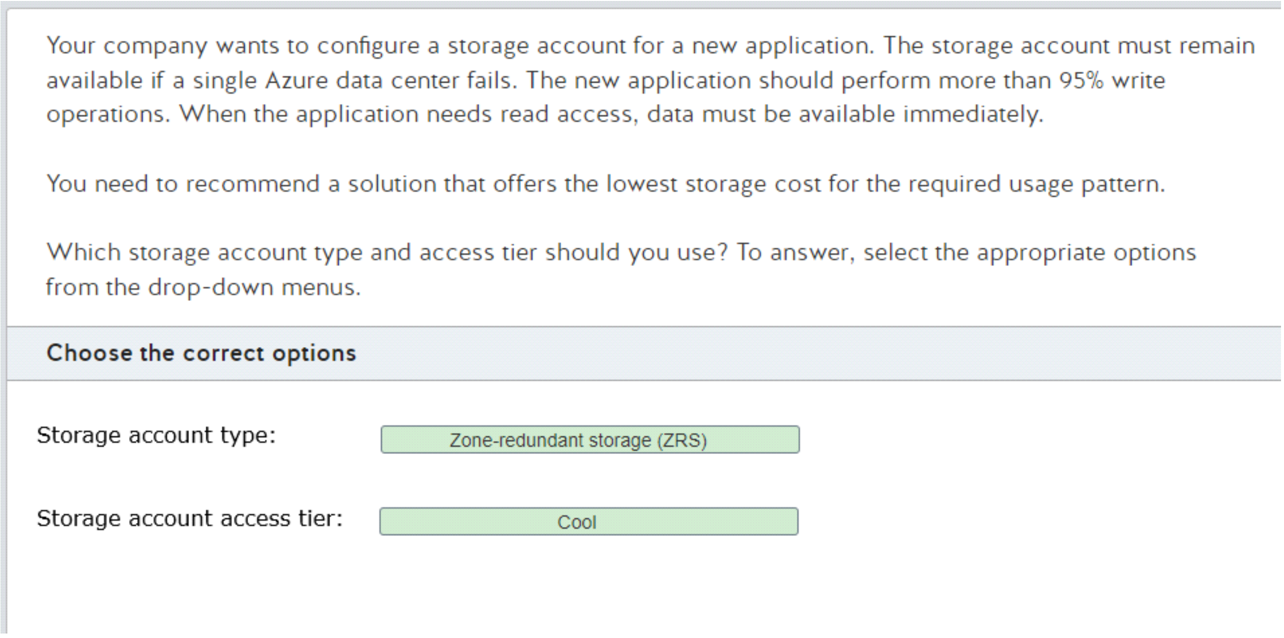
Time-based retention policies

- Before expire : can create and read data / Not update & delete
- After expire : can delete, but not edit

Legal hold policies

- Hold : can create + read; Not update + delete
- Unhold : do everything

Is this correct?



Your company wants to configure a storage account for a new application. The storage account must remain available if a single Azure data center fails. The new application should perform more than 95% write operations. When the application needs read access, data must be available immediately.

You need to recommend a solution that offers the lowest storage cost for the required usage pattern.

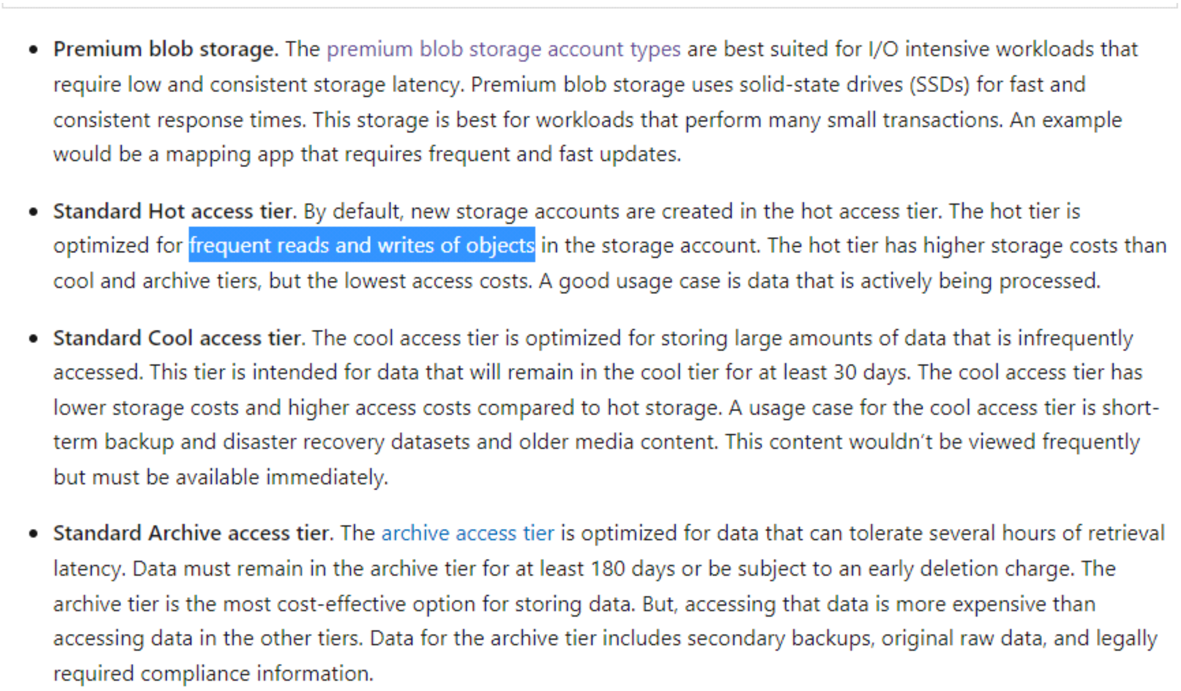
Which storage account type and access tier should you use? To answer, select the appropriate options from the drop-down menus.

Choose the correct options

Storage account type: Zone-redundant storage (ZRS)

Storage account access tier: Cool

Hints



- **Premium blob storage.** The premium blob storage account types are best suited for I/O intensive workloads that require low and consistent storage latency. Premium blob storage uses solid-state drives (SSDs) for fast and consistent response times. This storage is best for workloads that perform many small transactions. An example would be a mapping app that requires frequent and fast updates.
- **Standard Hot access tier**. By default, new storage accounts are created in the hot access tier. The hot tier is optimized for frequent reads and writes of objects in the storage account. The hot tier has higher storage costs than cool and archive tiers, but the lowest access costs. A good usage case is data that is actively being processed.
- **Standard Cool access tier**. The cool access tier is optimized for storing large amounts of data that is infrequently accessed. This tier is intended for data that will remain in the cool tier for at least 30 days. The cool access tier has lower storage costs and higher access costs compared to hot storage. A usage case for the cool access tier is short-term backup and disaster recovery datasets and older media content. This content wouldn't be viewed frequently but must be available immediately.
- **Standard Archive access tier**. The archive access tier is optimized for data that can tolerate several hours of retrieval latency. Data must remain in the archive tier for at least 180 days or be subject to an early deletion charge. The archive tier is the most cost-effective option for storing data. But, accessing that data is more expensive than accessing data in the other tiers. Data for the archive tier includes secondary backups, original raw data, and legally required compliance information.

Azure Files

Saturday, June 11, 2022 11:26 AM

Performance level	Latency	IOPS	Bandwidth
Standard	Double-digit ms	10,000 IOPS	300-MBps
Premium	Single-digit ms	100,000 IOPS	5-GBps

Premium only support ZRS storage in some region only

Storage tier	Usage
Premium	File shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency. Used for the most intensive IO workloads. Suitable workloads include databases, web site hosting, and development environments. Can be used with both Server Message Block (SMB) and Network File System (NFS) protocols.
Transaction optimized	Used for transaction heavy workloads that don't need the latency offered by premium file shares. File shares are offered on the standard storage hardware backed by hard disk drives (HDDs).
Hot	Storage optimized for general purpose file sharing scenarios such as team shares. Offered on standard storage hardware backed by HDDs.
Cool	Cost-efficient storage optimized for online archive storage scenarios. Offered on storage hardware backed by HDDs.

File Sync Cloud Tier and Policy

https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-cloud-tiering-policy
https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-cloud-tiering-overview

Key points

- Volume free space policy
- Date policy
- Windows Server data deduplication
- Cloud tiering heatmap
- Proactive recalling

File Sync Labs

https://docs.microsoft.com/en-us/azure/storage/file-sync/file-sync-extend-servers

Azure Disk

Saturday, June 11, 2022 12:08 PM

Detail	Ultra-disk	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max throughput	2,000 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	160,000	20,000	6,000	2,000

Disks encryption

- Azure Disk Encryption
  Encrypt the VHD
  Only the VM that own the disk can access the disk image
  DM-Crypt for Linux / BitLocker for Windows
  ADE Prerequisites
  a. Create a key vault.
  b. Set the key vault access policy to support disk encryption.
     i. Disk encryption - Required for Azure Disk encryption.
     ii. Deployment – Used by Compute Resource when defined in deployment
     iii. Template deployment – used by template deployment
  c. Use the key vault to store the encryption keys for ADE.

- Server-Side Encryption (encryption-at-rest)
  Encrypt physical disks in the data center
  When the data is accessed from the disk, it's decrypted and loaded into memory

- Encryption at host
  VM host encrypt the disk and put the encrypted data into Azure Storage

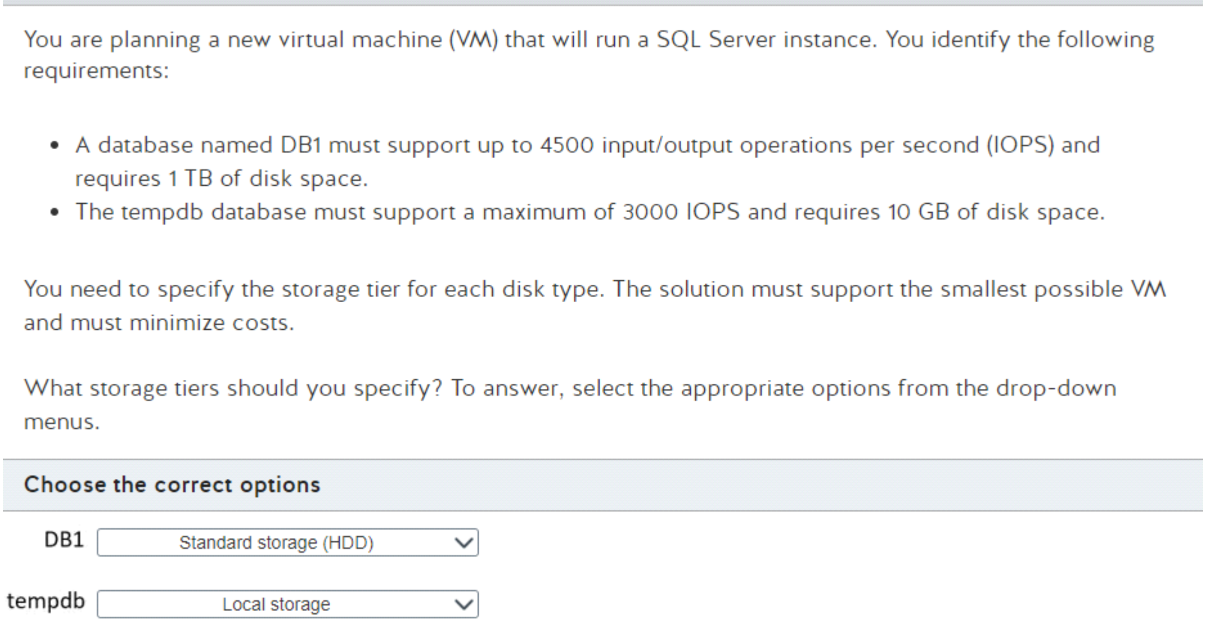
Different type of Disk

https://docs.microsoft.com/en-us/learn/modules/choose-the-right-disk-storage-for-vm-workload/2-managed-unmanaged-local-disk-storage

https://docs.microsoft.com/en-us/learn/modules/choose-the-right-disk-storage-for-vm-workload/3-disk-types-for-virtual-machines

Anything went wrong?

My answer is incorrect. Which one is incorrect? *(In fact I choose the wrong answer because I overlook the keyword in answer)* ☹



You are planning a new virtual machine (VM) that will run a SQL Server instance. You identify the following requirements:

- A database named DB1 must support up to 4500 input/output operations per second (IOPS) and requires 1 TB of disk space.
- The tempdb database must support a maximum of 3000 IOPS and requires 10 GB of disk space.

You need to specify the storage tier for each disk type. The solution must support the smallest possible VM and must minimize costs.

What storage tiers should you specify? To answer, select the appropriate options from the drop-down menus.

Choose the correct options

DB1: Standard storage (HDD)

tempdb: Local storage

Storage security

Saturday, June 11, 2022 2:21 PM

Use Shared Access Signatures

- Remember to SAS meaning. Try to generate a SAS by yourself

BlobEndpoint=https://cyrus822az305demo.blob.core.windows.net/;

QueueEndpoint=https://cyrus822az305demo.queue.core.windows.net/;

FileEndpoint=https://cyrus822az305demo.file.core.windows.net/;

TableEndpoint=https://cyrus822az305demo.table.core.windows.net/;

SharedAccessSignature=

sv=2021-06-08&

ss=bft&

srt=so&

sp=rwdlacuitfx&

se=2022-06-18T14:51:14Z&

st=2022-06-11T06:51:14Z&

sip=10.8.8.63-10.8.8.70&

spr=https&

sig=zsdmzledXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Enable firewall policies and rules

Restrict network access using service endpoints

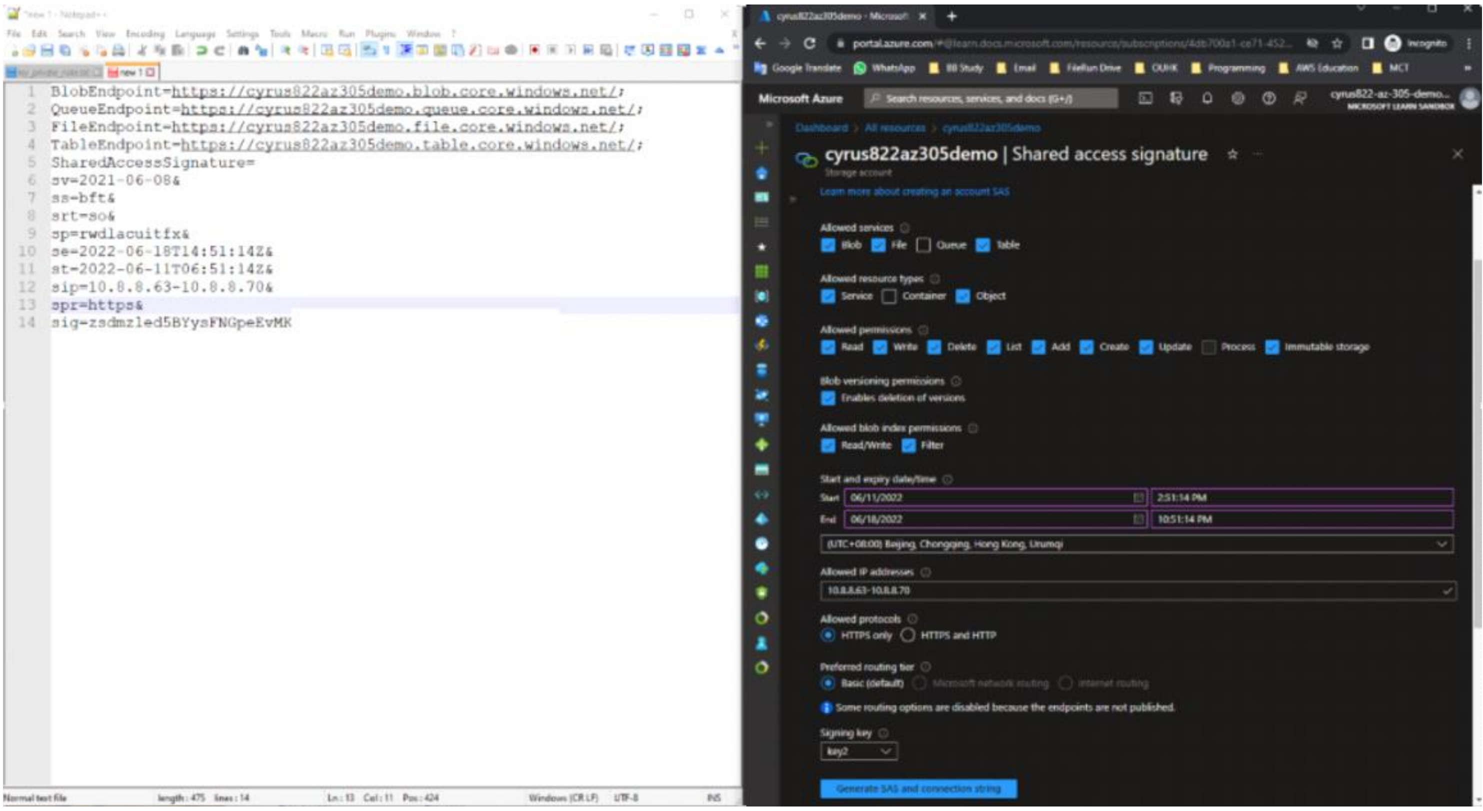
- Enable private IP addresses in the VNet to reach the service endpoint
- Enables on-premises networks to access resources using NAT IP addresses

Use private endpoints (Private Link)

Enable secure transfer

Use Customer-managed keys

- Customer-managed keys must be stored in Azure Key Vault



```
BlobEndpoint=https://cyrus822az305demo.blob.core.windows.net/;
QueueEndpoint=https://cyrus822az305demo.queue.core.windows.net/;
FileEndpoint=https://cyrus822az305demo.file.core.windows.net/;
TableEndpoint=https://cyrus822az305demo.table.core.windows.net/;
SharedAccessSignature=
sv=2021-06-08&
ss=bft&
srt=so&
sp=rwdlacuitfx&
se=2022-06-18T14:51:14Z&
st=2022-06-11T06:51:14Z&
sip=10.8.8.63-10.8.8.70&
spr=https&
sig=zsdmzled5BYysFNGpeEvMK
```

cyrus822az305demo | Shared access signature

Storage account

Learn more about creating an account SAS

Allowed services: ☑ Blob ☑ File □ Queue ☑ Table

Allowed resource types: ☑ Service □ Container ☑ Object

Allowed permissions: ☑ Read ☑ Write ☑ Delete ☑ List ☑ Add ☑ Create ☑ Update □ Process ☑ Immutable storage

Blob versioning permissions: ☑ Enables deletion of versions

Allowed blob index permissions: ☑ Read/Write ☑ Filter

Start and expiry date/time

Start: 06/11/2022 2:51:14 PM

End: 06/18/2022 10:51:14 PM

(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Allowed IP addresses: 10.8.8.63-10.8.8.70

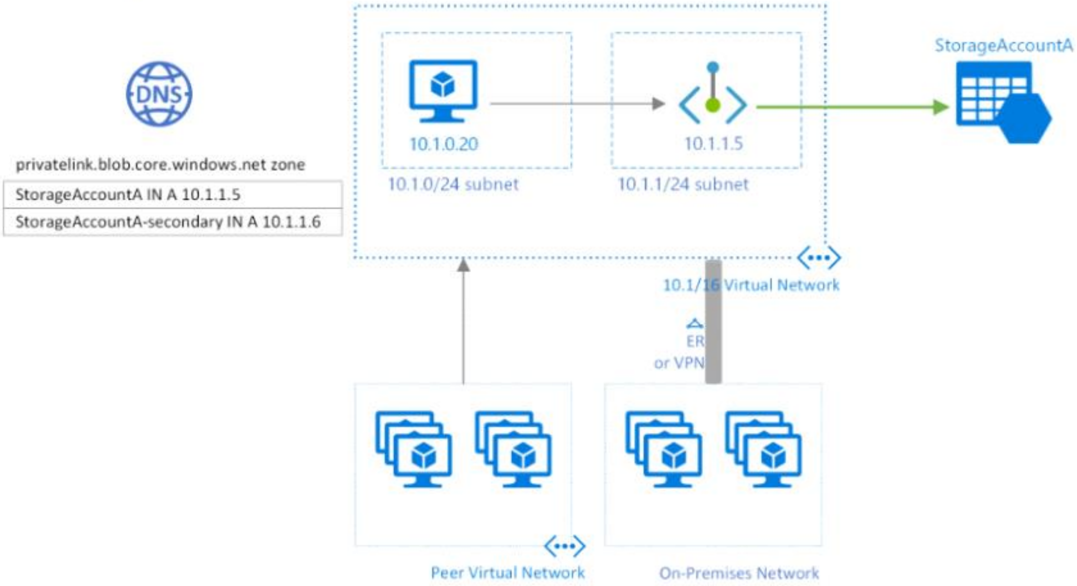
Allowed protocols: ● HTTPS only ○ HTTPS and HTTP

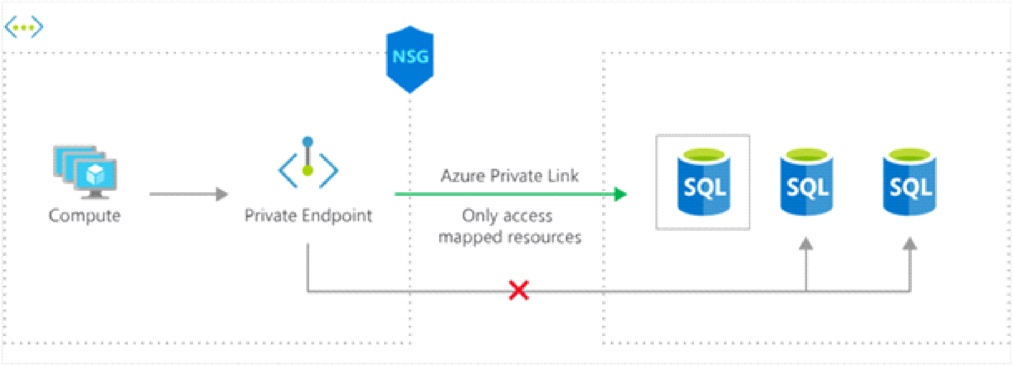
Preferred routing tier: ● Basic (default) ○ Microsoft network routing ○ Internet routing

Some routing options are disabled because the endpoints are not published.

Signing key: key2

Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > All resources > cyrus822az305demo
cyrus822-az-305-demo...
MICROSOFT LEARN SANDBOX
Generate SAS and connection string


privatelink.blob.core.windows.net zone
StorageAccountA IN A 10.1.1.5
StorageAccountA-secondary IN A 10.1.1.6
10.1.0.20
10.1.0/24 subnet
10.1.1.5
10.1.1/24 subnet
StorageAccountA
10.1/16 Virtual Network
ER
or VPN
Peer Virtual Network
On-Premises Network


NSG
Compute
Private Endpoint
Azure Private Link
Only access
mapped resources
SQL
SQL
SQL

Exercise

Saturday, June 11, 2022 4:37 PM

Disk Security

https://docs.microsoft.com/en-us/learn/modules/secure-your-azure-virtual-machine-disks/7-knowledge-check

Azure SQL DB

Saturday, June 11, 2022 4:10 PM

Decision Making Flow

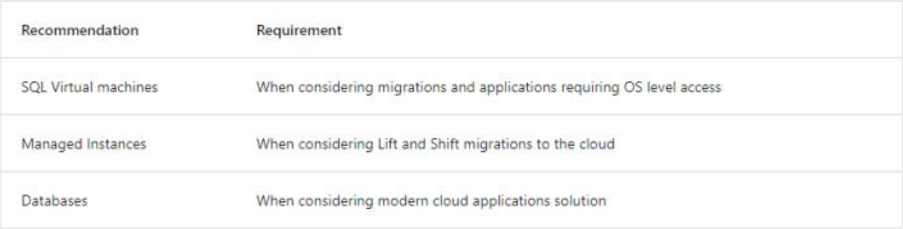
Deployment Model > Purchase Model > Service Tier

Features comparison: Azure SQL Database and Azure SQL Managed Instance

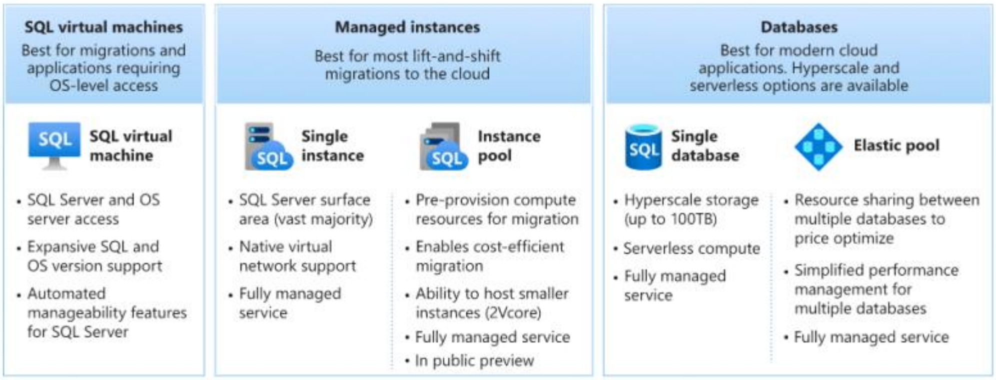
https://docs.microsoft.com/en-us/azure/azure-sql/database/features-comparison?view=azuresql

Deployment Model

- SQL Server on Azure VMs
- Managed instances:
  - Single instances
  - Instance pool
- Databases:
  - Single database
  - Elastic pool



Recommendation	Requirement
SQL Virtual machines	When considering migrations and applications requiring OS level access
Managed Instances	When considering Lift and Shift migrations to the cloud
Databases	When considering modern cloud applications solution



SQL virtual machines

Best for migrations and applications requiring OS-level access

SQL virtual machine

- SQL Server and OS server access
- Expansive SQL and OS version support
- Automated manageability features for SQL Server

Managed instances

Best for most lift-and-shift migrations to the cloud

Single instance

- SQL Server surface area (vast majority)
- Native virtual network support
- Fully managed service

Instance pool

- Pre-provision compute resources for migration
- Enables cost-efficient migration
- Ability to host smaller instances (2Vcore)
- Fully managed service
- In public preview

Databases

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

Single database

- Hyperscale storage (up to 100TB)
- Serverless compute
- Fully managed service

Elastic pool

- Resource sharing between multiple databases to price optimize
- Simplified performance management for multiple databases
- Fully managed service

Azure SQL feature

- Very large databases (currently up to 100TB)
- Autoscaling for unpredictable workloads (serverless)

Elastic pool feature

- Buy compute + storage, share across multiple DB
- Each database can use the resources they need, within the limits you set, depending on current load
- Billed for each hour a pool exists at the highest eDTU or vCores

Provisioned + vCore

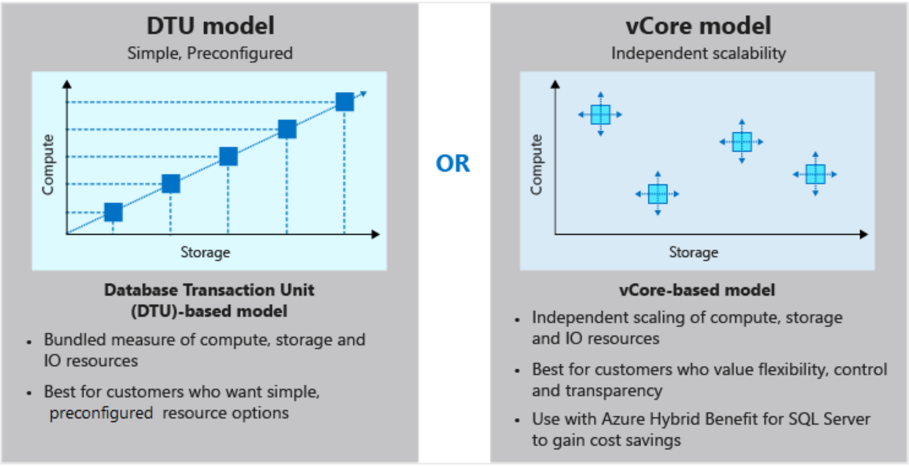
==> Hybrid Benefit ==> Save money

Pricing model

https://docs.microsoft.com/en-us/azure/azure-sql/database/purchasing-models?view=azuresql

DTU limits

https://docs.microsoft.com/en-us/azure/azure-sql/database/resource-limits-dtu-single-databases?view=azuresql



DTU model

Simple, Preconfigured

Database Transaction Unit (DTU)-based model

- Bundled measure of compute, storage and IO resources
- Best for customers who want simple, preconfigured resource options

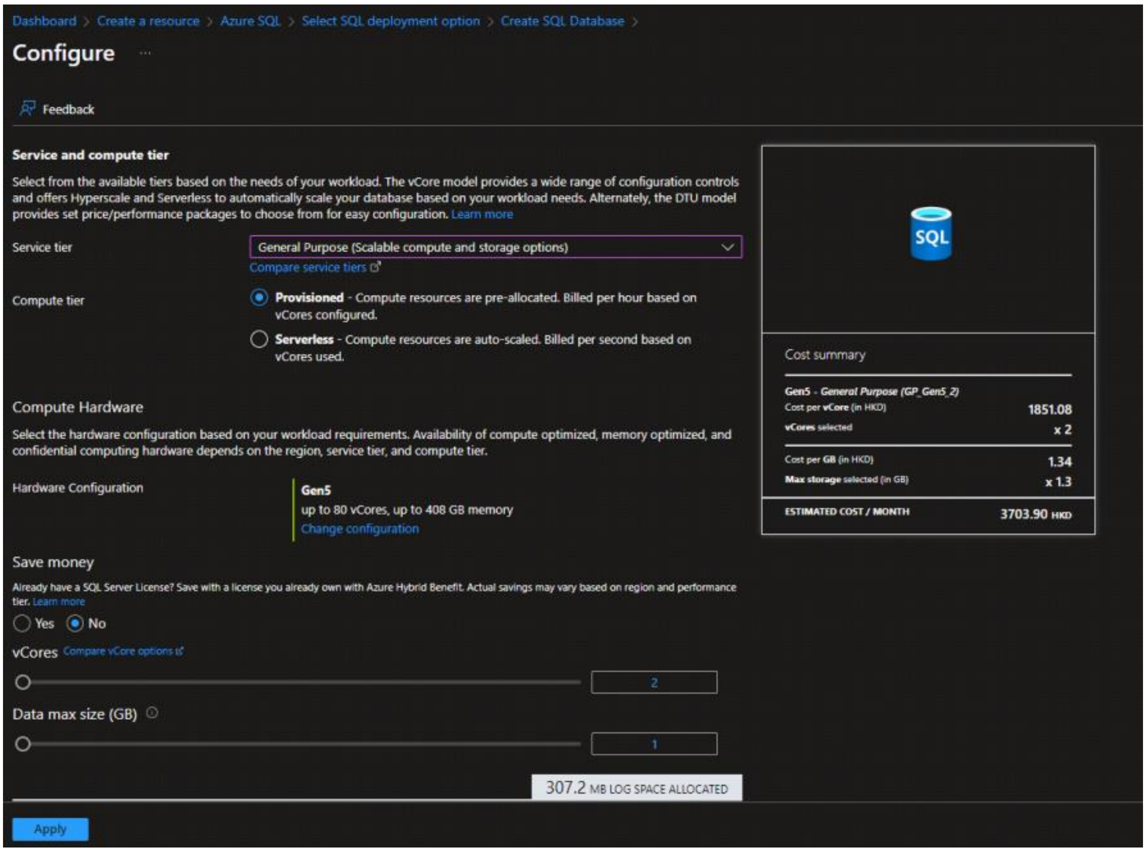
OR

vCore model

Independent scalability

vCore-based model

- Independent scaling of compute, storage and IO resources
- Best for customers who value flexibility, control and transparency
- Use with Azure Hybrid Benefit for SQL Server to gain cost savings



Dashboard > Create a resource > Azure SQL > Select SQL deployment option > Create SQL Database >

Configure

Feedback

Service and compute tier

Select from the available tiers based on the needs of your workload. The vCore model provides a wide range of configuration controls and offers Hyperscale and Serverless to automatically scale your database based on your workload needs. Alternately, the DTU model provides set price/performance packages to choose from for easy configuration. Learn more

Service tier: General Purpose (Scalable compute and storage options)

Compare service tiers

Compute tier:

● **Provisioned** - Compute resources are pre-allocated. Billed per hour based on vCores configured.

○ **Serverless** - Compute resources are auto-scaled. Billed per second based on vCores used.

Compute Hardware

Select the hardware configuration based on your workload requirements. Availability of compute optimized, memory optimized, and confidential computing hardware depends on the region, service tier, and compute tier.

Hardware Configuration: **Gen5**
up to 80 vCores, up to 408 GB memory
Change configuration

Save money

Already have a SQL Server License? Save with a license you already own with Azure Hybrid Benefit. Actual savings may vary based on region and performance tier. Learn more

○ Yes ● No

vCores Compare vCore options

2

Data max size (GB)

1

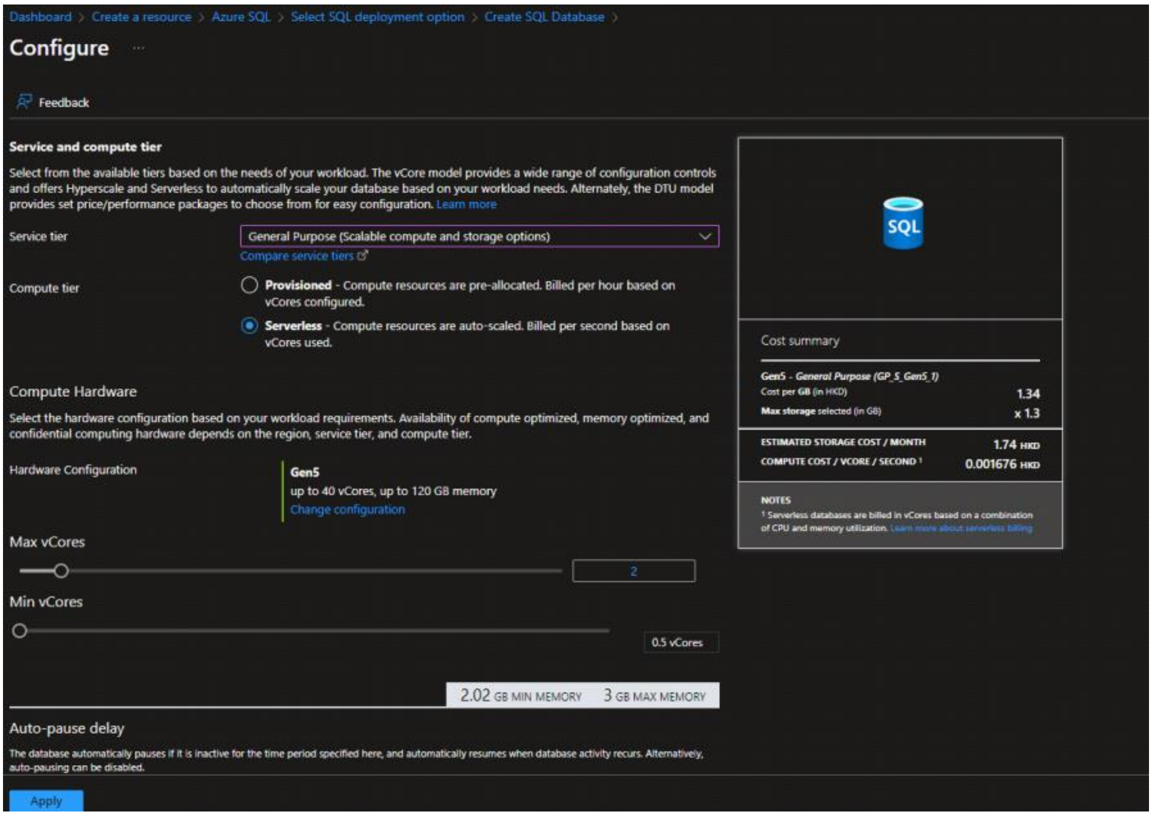
307.2 MB LOG SPACE ALLOCATED

Apply

Cost summary

Gen5 - General Purpose (GP_Gen5_2)

Cost per **vCore** (in HKD)	1851.08
vCores selected	x 2
Cost per **GB** (in HKD)	1.34
Max storage selected (in GB)	x 1.3
ESTIMATED COST / MONTH	3703.90 HKD



Dashboard > Create a resource > Azure SQL > Select SQL deployment option > Create SQL Database >

Configure

Feedback

Service and compute tier

Select from the available tiers based on the needs of your workload. The vCore model provides a wide range of configuration controls and offers Hyperscale and Serverless to automatically scale your database based on your workload needs. Alternately, the DTU model provides set price/performance packages to choose from for easy configuration. Learn more

Service tier: General Purpose (Scalable compute and storage options)

Compare service tiers

Compute tier:

○ **Provisioned** - Compute resources are pre-allocated. Billed per hour based on vCores configured.

● **Serverless** - Compute resources are auto-scaled. Billed per second based on vCores used.

Compute Hardware

Select the hardware configuration based on your workload requirements. Availability of compute optimized, memory optimized, and confidential computing hardware depends on the region, service tier, and compute tier.

Hardware Configuration: **Gen5**
up to 40 vCores, up to 120 GB memory
Change configuration

Max vCores

2

Min vCores

0.5 vCores

2.02 GB MIN MEMORY 3 GB MAX MEMORY

Auto-pause delay

The database automatically pauses if it is inactive for the time period specified here, and automatically resumes when database activity recurs. Alternatively, auto-pausing can be disabled.

Apply

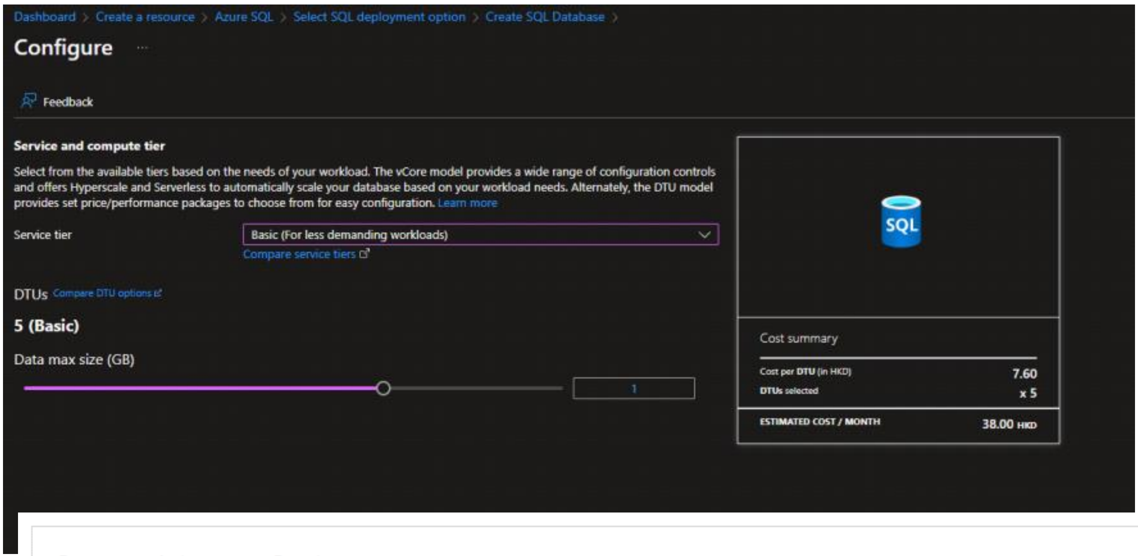
Cost summary

Gen5 - General Purpose (GP_S_Gen5_1)

Cost per **GB** (in HKD)	1.34
Max storage selected (in GB)	x 1.3
ESTIMATED STORAGE COST / MONTH	1.74 HKD
COMPUTE COST / VCORE / SECOND [1]	0.001676 HKD

NOTES

[1] Serverless databases are billed in vCores based on a combination of CPU and memory utilization. Learn more about serverless billing



Dashboard > Create a resource > Azure SQL > Select SQL deployment option > Create SQL Database >

Configure ...

Feedback

Service and compute tier

Select from the available tiers based on the needs of your workload. The vCore model provides a wide range of configuration controls and offers Hyperscale and Serverless to automatically scale your database based on your workload needs. Alternately, the DTU model provides set price/performance packages to choose from for easy configuration. Learn more

Service tier: Basic (For less demanding workloads)

Compare service tiers

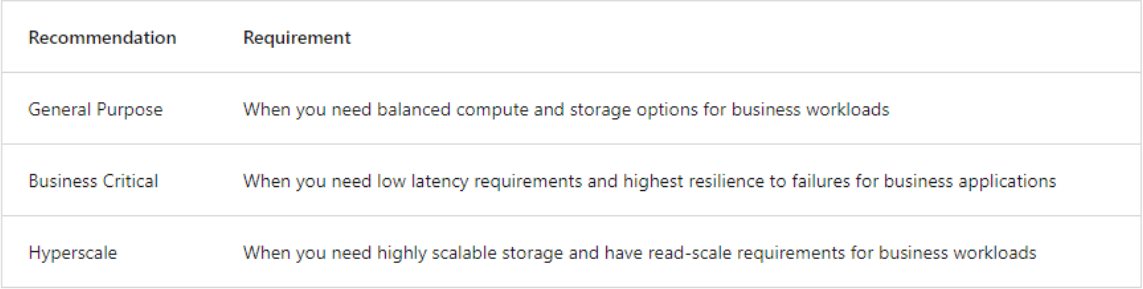
DTUs Compare DTU options

5 (Basic)

Data max size (GB): 1

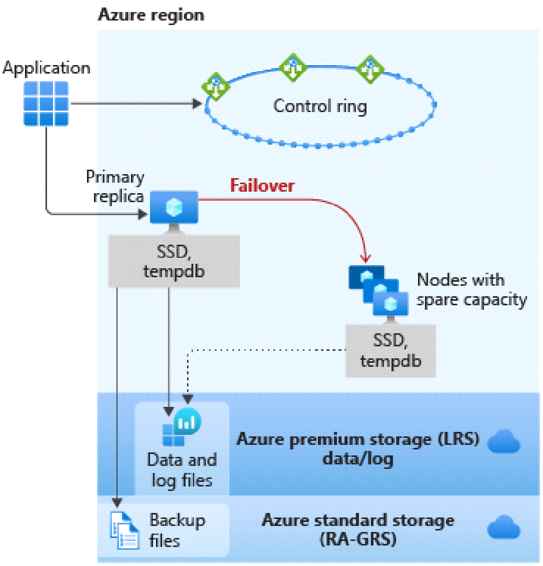
Cost summary

Cost per DTU (in HKD)	7.60
DTUs selected	x 5
ESTIMATED COST / MONTH	38.00 HKD



Recommendation	Requirement
General Purpose	When you need balanced compute and storage options for business workloads
Business Critical	When you need low latency requirements and highest resilience to failures for business applications
Hyperscale	When you need highly scalable storage and have read-scale requirements for business workloads

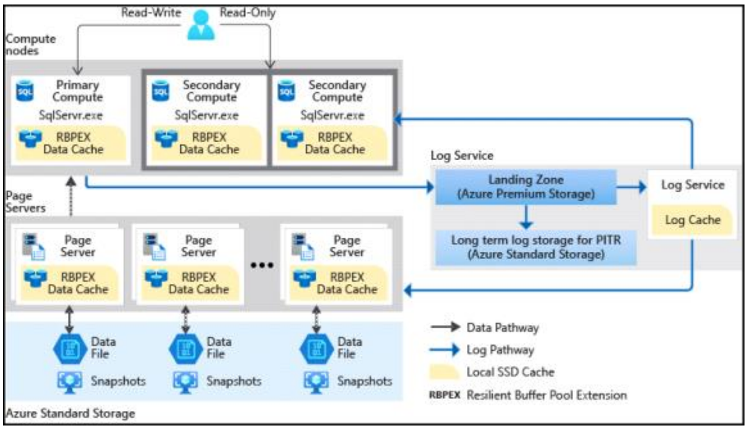
General Purpose



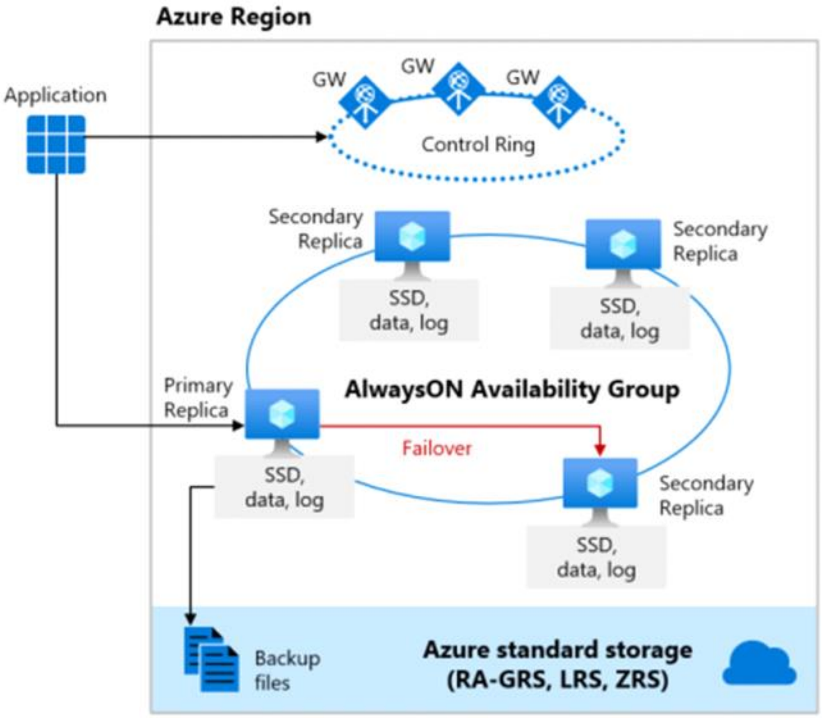
Hyperscale

https://docs.microsoft.com/en-us/azure/azure-sql/database/hyperscale-architecture?view=azuresql

- Azure SQL DB only
- Up to 100TB
- Compute Node + Page Server + Log Services
- 2nd Compute node are hot standby, can read
- Page server serve 128GB or 1 TB page data. Also have replica
- Log from primary node send to Log services
- Log services broadcast to all 2nd Compute and Page server. Data will be sync
- Restores in minutes rather than hours and days



Business Critical


Azure Region
Application
GW
GW
GW
Control Ring
Secondary Replica
SSD, data, log
Secondary Replica
SSD, data, log
Primary Replica
AlwaysON Availability Group
Failover
SSD, data, log
Secondary Replica
SSD, data, log
Backup files
Azure standard storage (RA-GRS, LRS, ZRS)

SQL Managed Instance

Sunday, June 12, 2022 10:27 PM

Features

- Have Instance-scope features, but no need to manage OS
- Azure manage something for you
  - ○ Automatic patching and version updates
  - ○ Automated backups
  - ○ High availability
  - ○ Reduced management overhead
- Only support vCore mode

Instance Scope Features

- SQL Server Agent
- Service Broker
- Common language runtime (CLR)
- Database Mail
- Linked servers
- Distributed transactions (preview)
- Machine Learning Services

Features comparison: Azure SQL Database and Azure SQL Managed Instance
https://docs.microsoft.com/en-us/azure/azure-sql/database/features-comparison?view=azuresql

Major differences that may asked in exam

- BACKUP command
- Azure Active Directory (Azure AD) authentication
- Common language runtime - CLR
- Cross-database/three-part name queries
- Linked servers
- Windows authentication

SQL Server on Azure VM

Sunday, June 12, 2022 10:34 PM

- All your SQL Server skills should directly transfer, though Azure can help automate backups and security patches.
- You have access to the full capabilities of SQL Server
- You're responsible for updating and patching the OS and SQL Server

Labs

Sunday, June 12, 2022 11:38 PM

Create a database

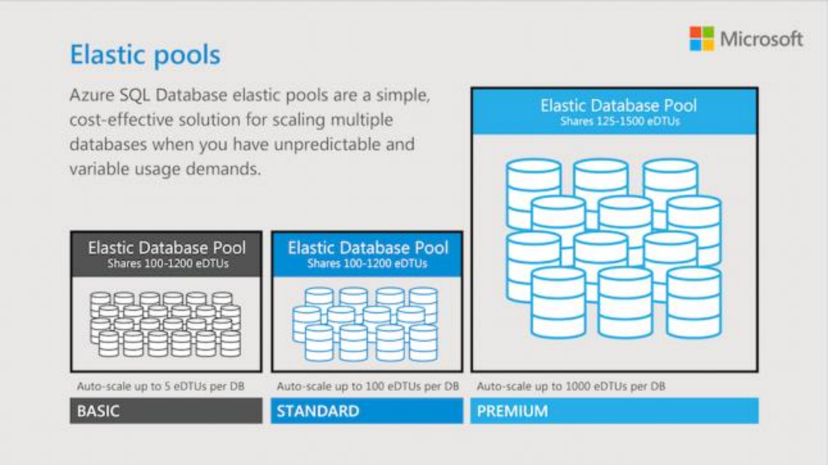
https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/exercise-create-sql-database

Scalability

Monday, June 13, 2022 9:50 AM

Vertical – Scale up
Horizontal – Scale out

Scale up – Elastic Pool



Microsoft

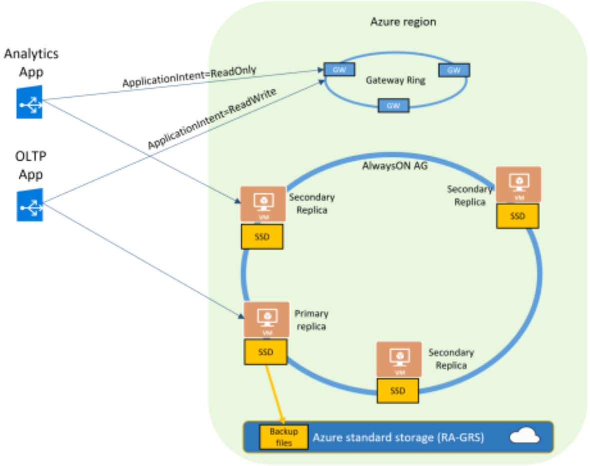
Elastic pools

Azure SQL Database elastic pools are a simple, cost-effective solution for scaling multiple databases when you have unpredictable and variable usage demands.

Scale Out

- Read only scale out (Similar to CQRS)
- Sharding (Partitioning)

Azure SQL Managed Instance	Azure SQL Database
For the basic, standard and general purpose tier, read scale-out feature is unavailable	For the basic, standard and general purpose tier, read scale-out feature is unavailable
For the Business Critical tier, read scale-out is auto-provisioned	For the Premium and Business Critical tier, read scale-out is auto-provisioned
	Read scale-put feature is available in Hyperscale tier if at least one secondary replica is created

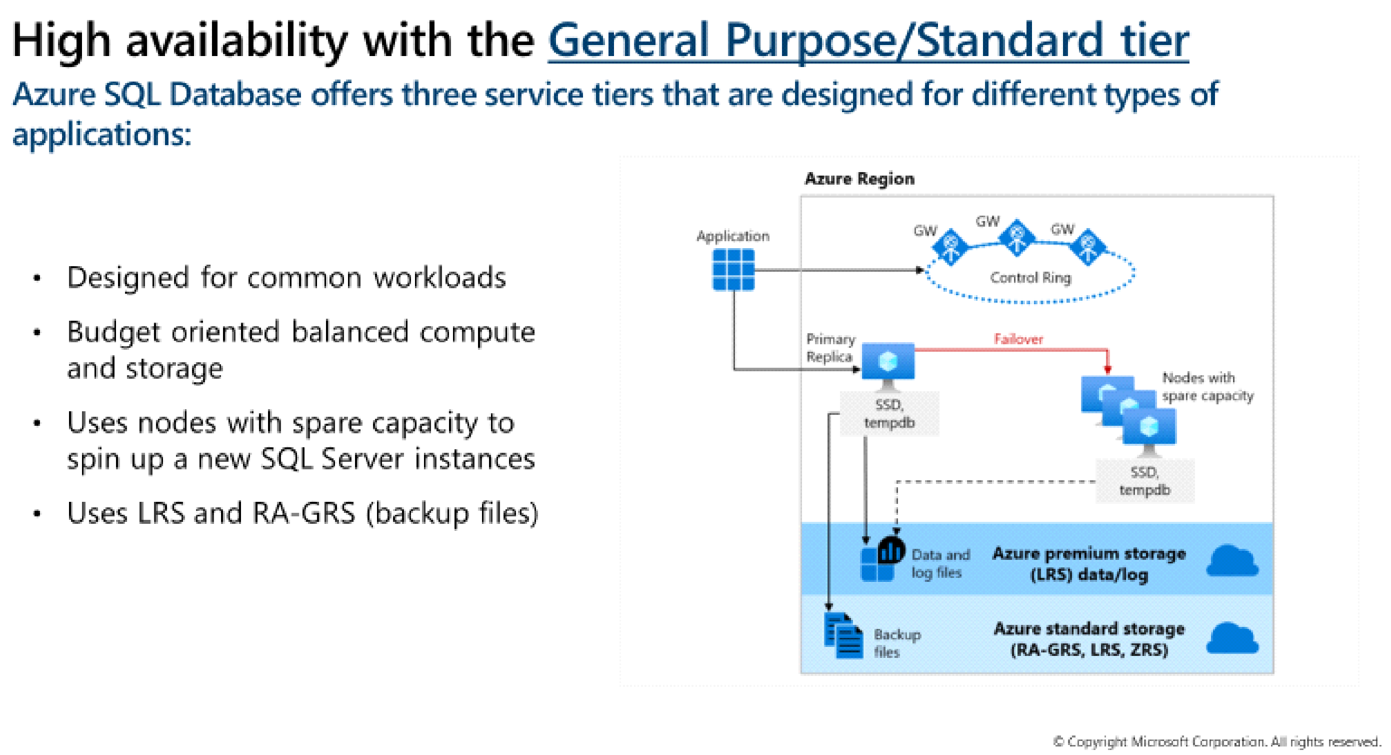


Reasons for Sharding include

- If the total amount of data is too large to fit constraints of a single database
- If the transaction throughput of the overall workload exceeds capacities of an individual database
- When different customers or tenents' data needs physical isolation from each other
- Within an organization, there is a geographical separation of data for compliance reasons

Availability

Monday, June 13, 2022 10:02 AM

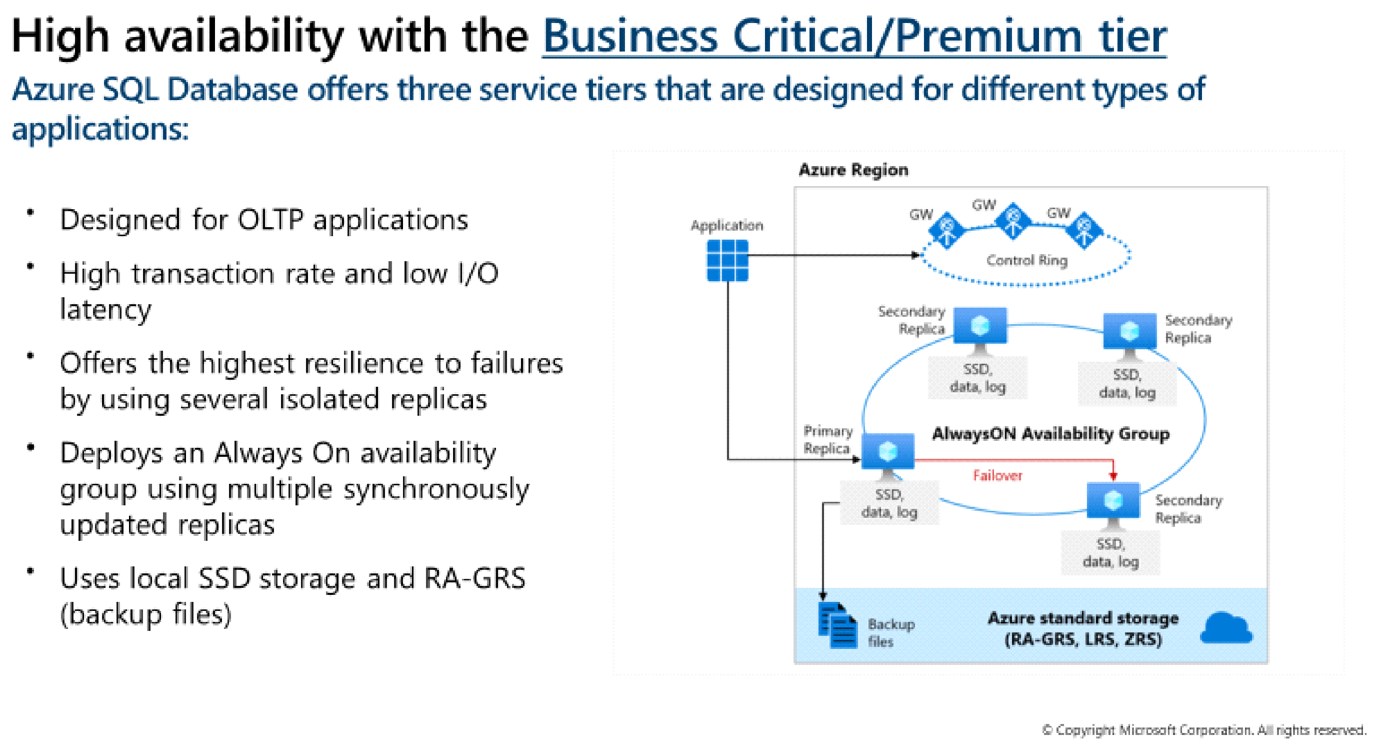


High availability with the General Purpose/Standard tier

Azure SQL Database offers three service tiers that are designed for different types of applications:

- Designed for common workloads
- Budget oriented balanced compute and storage
- Uses nodes with spare capacity to spin up a new SQL Server instances
- Uses LRS and RA-GRS (backup files)

© Copyright Microsoft Corporation. All rights reserved.



High availability with the Business Critical/Premium tier

Azure SQL Database offers three service tiers that are designed for different types of applications:

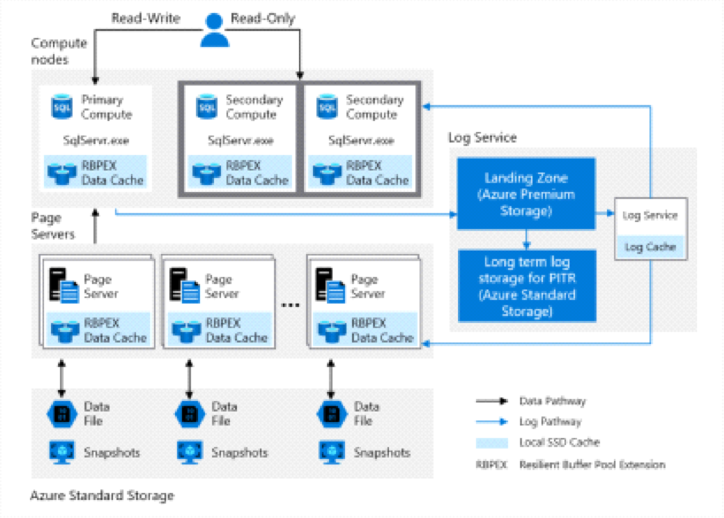
- Designed for OLTP applications
- High transaction rate and low I/O latency
- Offers the highest resilience to failures by using several isolated replicas
- Deploys an Always On availability group using multiple synchronously updated replicas
- Uses local SSD storage and RA-GRS (backup files)

© Copyright Microsoft Corporation. All rights reserved.

High availability with the Hyperscale tier

Azure SQL Database offers three service tiers that are designed for different types of applications:

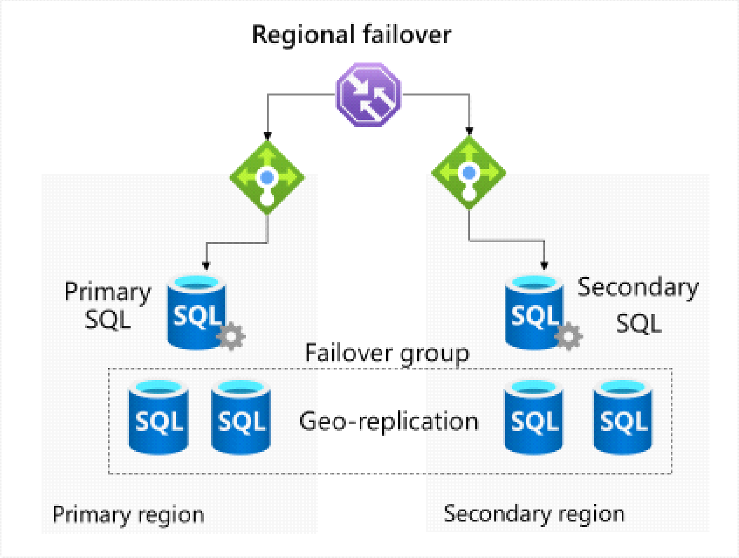
- Designed for very large OLTP databases – as large as 100 TB
- Able to autoscale storage and scale compute
- Captures instantaneous backups (using snapshots)
- Restores in minutes rather than hours and days
- Scale up or down in real time to accommodate workload changes



Select a database failover strategy

Consider datacenter and regional failover.

- In the same region -use AlwaysOn availability zones with failover to secondary replicas
- Across regions – use geo-replication and failover groups



Security

Monday, June 13, 2022 10:25 AM

DATA STATE	ENCRYPTION METHOD
Data-at-rest	Transparent data encryption (TDE), Always Encrypted
Data-in-motion	SSL/TLS, Always Encrypted
Data-in-process	Dynamic data masking

Protect data-at-rest

TDE

- TDE performs encryption and decryption of the data at the page level.
- The data is encrypted as the data is written to the data page on disk and decrypted when the data page is read into memory.
- The end result is that all data pages on disk are encrypted.
- Database backups will also be encrypted because a backup operation just copies the data pages from the database file to the backup device. No decryption is done during the backup operation.
- TDE encrypts the storage of an entire database by using a symmetric key called the Database Encryption Key (DEK).
- Service-managed TDE - where the DEK is protected by a built-in server certificate.
- Customer-managed TDE - the TDE Protector that encrypts the DEK is supplied by customer and stored in a customer-owned and managed in their key management system

Azure's Azure Key Vault ==> RBAC

Protect data-in-transit

SCENARIO	SOLUTION
Secure access from multiple workstations located on-premises to an Azure virtual network	Use site-to-site VPN
Secure access from an individual workstation located on-premises to an Azure virtual network	Use point-to-site VPN
Move large data sets over a dedicated high-speed wide-area network (WAN) link	Use Azure ExpressRoute
Interact with Azure Storage through the Azure portal	All transactions occur via HTTPS. You can also use Storage REST API over HTTPS to interact with Azure Storage and Azure SQL Database.

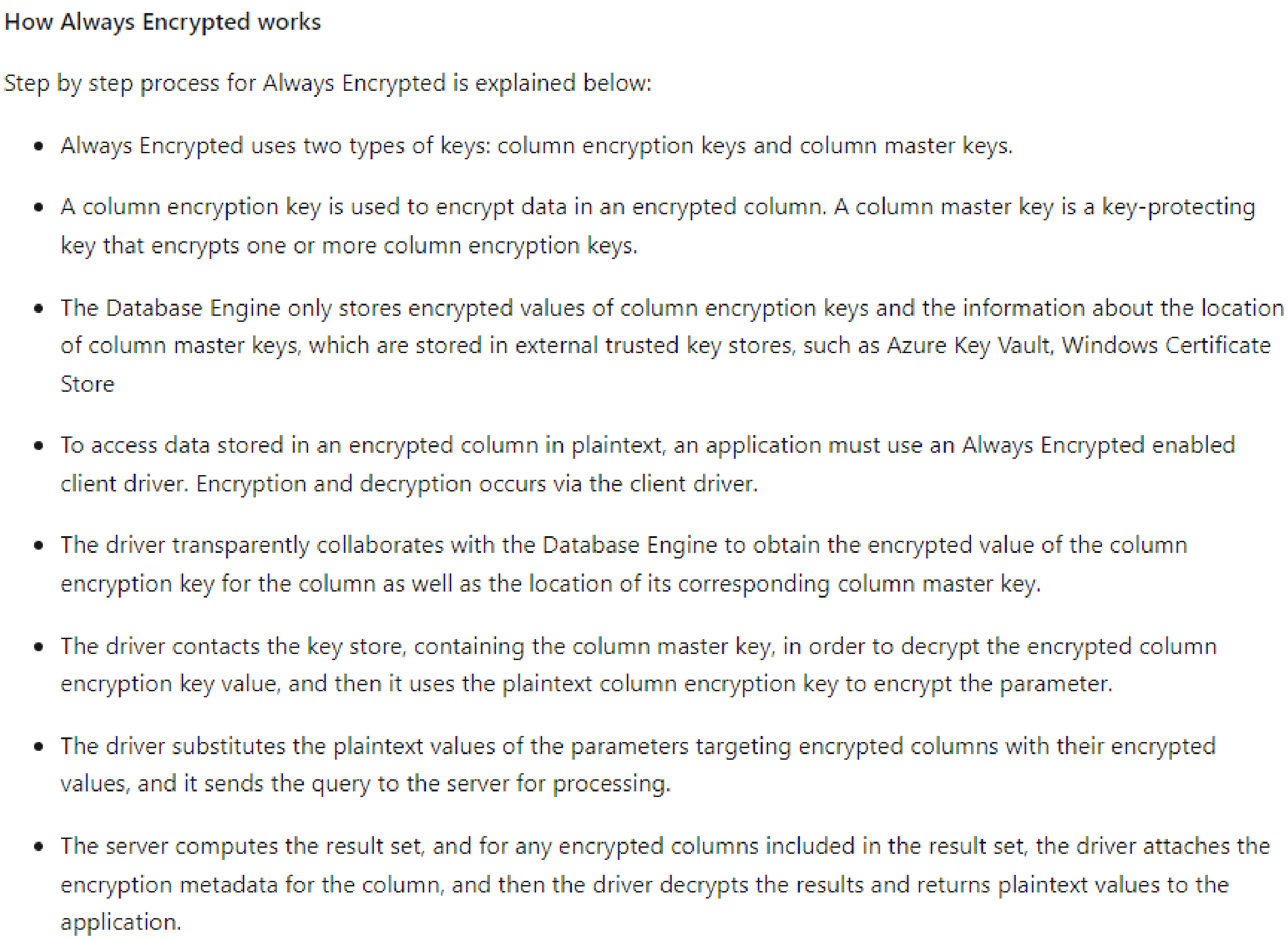
Protect data-in-use

Dynamic Data Masking

- Data masking policy can be set up in Azure portal only for Azure SQL Database
- Dynamic data masking can be set up using PowerShell cmdlets and REST API
- On Presentation Layer only. Data at storage in fact no masking

Always Encrypted feature for data-at-rest and data-in-transit

- Suggest and encrypt sensitive data in DB
- Real encrypt in storage
- Even DB admin cannot retrieve
- Use key – Bring Your Own Key
- Key can be stored in Windows Certificate Store or in Azure Key Vault



How Always Encrypted works

Step by step process for Always Encrypted is explained below:

- Always Encrypted uses two types of keys: column encryption keys and column master keys.
- A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
- The Database Engine only stores encrypted values of column encryption keys and the information about the location of column master keys, which are stored in external trusted key stores, such as Azure Key Vault, Windows Certificate Store
- To access data stored in an encrypted column in plaintext, an application must use an Always Encrypted enabled client driver. Encryption and decryption occurs via the client driver.
- The driver transparently collaborates with the Database Engine to obtain the encrypted value of the column encryption key for the column as well as the location of its corresponding column master key.
- The driver contacts the key store, containing the column master key, in order to decrypt the encrypted column encryption key value, and then it uses the plaintext column encryption key to encrypt the parameter.
- The driver substitutes the plaintext values of the parameters targeting encrypted columns with their encrypted values, and it sends the query to the server for processing.
- The server computes the result set, and for any encrypted columns included in the result set, the driver attaches the encryption metadata for the column, and then the driver decrypts the results and returns plaintext values to the application.

CosmosDB

Monday, June 13, 2022 10:41 AM

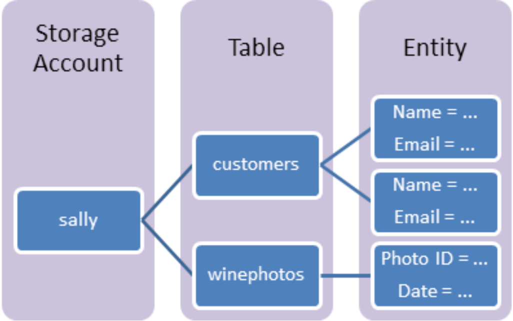
What is CosmosDB?

- NoSQL database
- Aggregate API for
  - Tables
  - Core(SQL for JSON)
  - MongoDB
  - Cassandra
  - Gremlin

Image from Google serach https://www.property.hk/article_content.php?author=PHK_TML&id=57760

Azure Storage Table

- Key value pair
- Cannot have complex joining
- But can have primary cluster index – fast

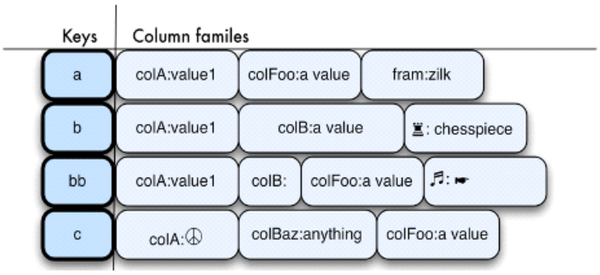

Storage Account
Table
Entity
sally
customers
winephotos
Name = ...
Email = ...
Name = ...
Email = ...
Photo ID = ...
Date = ...

CosmosDB Table API limitation

- Not sorted in order of partition key and row key
- Row key limited to 255 bytes
- Support Cross-Origin Resource Sharing (CORS)
- Table name case-sensitive, while Storage Acct Table is case-insensitive
- Charge on provision created, while Tabla charge when capacity are start using.
- CosmosDB faster, 10ms. While Storage Acct Table may up to 10 seconds

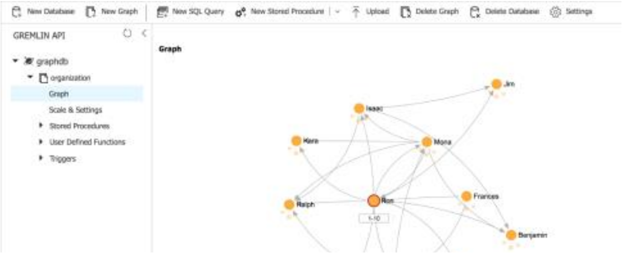
MongoDB, Core (SQL) ==> JSON
Cassandra ==> Wide Columnar No SQL database
Table ==> Key value pair tabular
Gremlin ==> Graph

Cassandra

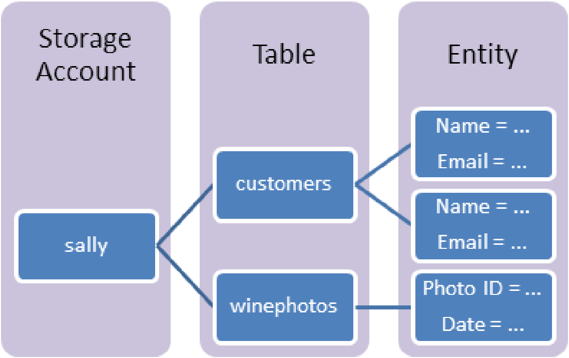


Keys	Column familes			
a	colA:value1	colFoo:a value	fram:zilk	
b	colA:value1	colB:a value	♜: chesspiece	
bb	colA:value1	colB:	colFoo:a value	♬: ☛
c	colA:☮	colBaz:anything	colFoo:a value	

Germlin

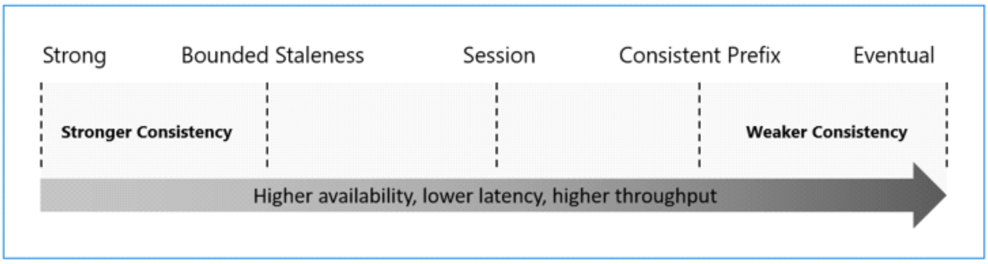


Table



Explore consistency levels (1 / 2)

Azure Cosmos DB approaches data consistency as a spectrum of choices instead of two extremes.



Explore consistency levels (2 /2)

Consistency Level	Description
Strong	When a write operation is performed on your primary database, the write operation is replicated to the replica instances. The write operation is committed (and visible) on the primary only after it has been committed and confirmed by all replicas.
Bounded Staleness	This level is similar to the Strong level with the major difference that you can configure how stale documents can be within replicas. Staleness refers to the quantity of time (or the version count) a replica document can be behind the primary document.
Session	This level guarantees that all read and write operations are consistent within a user session. Within the user session, all reads and writes are monotonic and guaranteed to be consistent across primary and replica instances.
Consistent Prefix	This level has loose consistency but guarantees that when updates show up in replicas, they will show up in the correct order (that is, as prefixes of other updates) without any gaps.
Eventual	This level has the loosest consistency and essentially commits any write operation against the primary immediately. Replica transactions are asynchronously handled and will eventually (over time) be consistent with the primary. This tier has the best performance, because the primary database does not need to wait for replicas to commit to finalize its transactions.

Azure SQL Edge

Monday, June 13, 2022 10:36 AM

Suitable for IoT and IoT Hub

- **Streaming**
- **Time series storage engine to process time-indexed data**

Azure SQL Edge is ideal for

Requirement	**SQL Edge capability**
Connectivity limitations	Azure SQL Edge supports solutions that work with, or without, network connectivity.
Slow or intermittent broadband connection	Azure SQL Edge provides a powerful, local database. It negates needing to forward all data to a cloud-based database, which eliminates latency.
Data security and privacy concerns	Azure SQL Edge implements RBAC and ABAC, encryption, and data classification. This helps you secure and control access to your IoT apps' data.
Synchronization and connectivity to back-end systems	Azure SQL Edge provides ease of exchanging data with other systems like Azure SQL Database, SQL Server, and Azure Cosmos DB.
Familiarity	Azure SQL Edge shares the same codebase as SQL Server. Developers with skills in SQL Server or SQL Database can reuse their code and skills

2 deployment mode

1) In Azure

2) Containerization : Docker image in Docker Hub

Overall

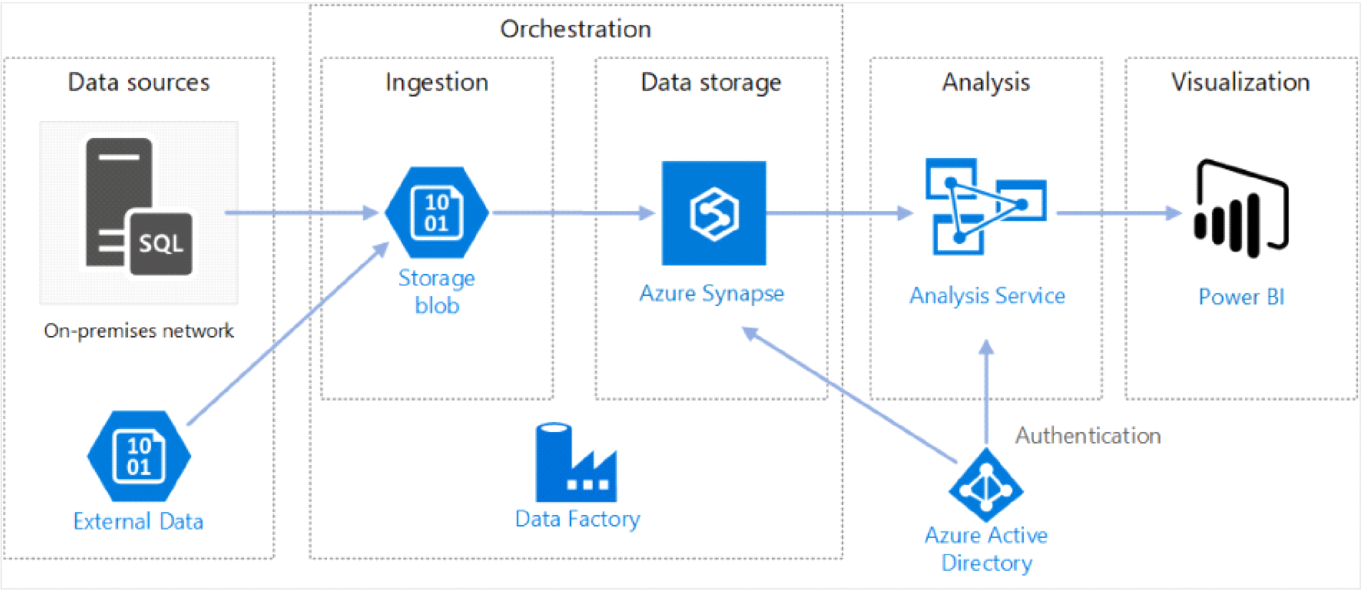
Monday, June 13, 2022 5:10 PM

Data Factory ==> ETL and data integration service (like workflow engine)
Data Lake ==> Repository of data
Databrick ==> BigData & Machine Learning engine. Can query process and analysis, and then feed Azure ML
Synapse Analytics ==> no code ELT to feed BI and ML

Azure Data Factory

Monday, June 13, 2022 5:37 PM

- ELT Tools
- Create and schedule data-driven workflows
- Main functions
  - Orchestrate data movement
  - Transform data at scale

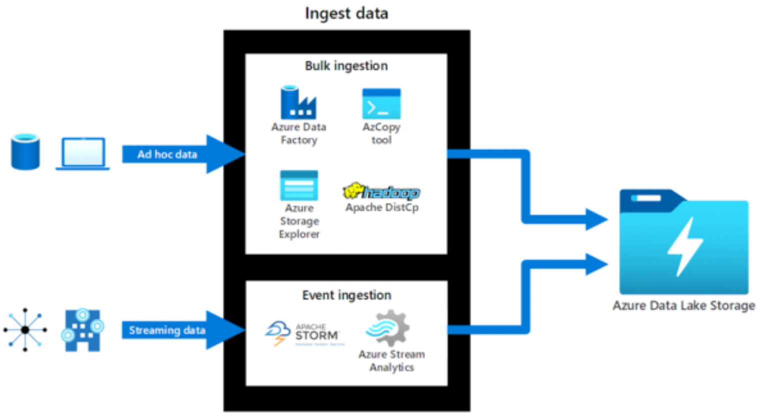


Components of Azure Data Factory

- Linked services
  - Ingest of different data source
- Activities
  - data movement
  - data transformation
  - control activities
- Pipelines
  - Group of activities
- Datasets
  - Source data
- Data Flows
  - develop data transformation logic without writing code
- Integration Runtimes
  - Bridge between the activity and linked Services objects
  - Azure, Self-hosted, and Azure-SSIS

Azure Data Lake Storage

Monday, June 13, 2022 7:27 PM



Use Azure Data Lake when you need

- a data repository on the cloud for managing large volumes of data
- Data types: JSON files, CSV, log files, and other formats in real time
- Real-time data ingestion and storage (e.g. Azure Data Factory)

Ingesting data

- Ad hoc data
  - AzCopy, CLI, PowerShell, Storage Explorer
- Relational data
  - Azure Data Factory sources => Cosmos DB, SQL Database, Managed instances
- For streaming data
  - Apache Storm on Azure HDInsight, Azure Stream Analytics.

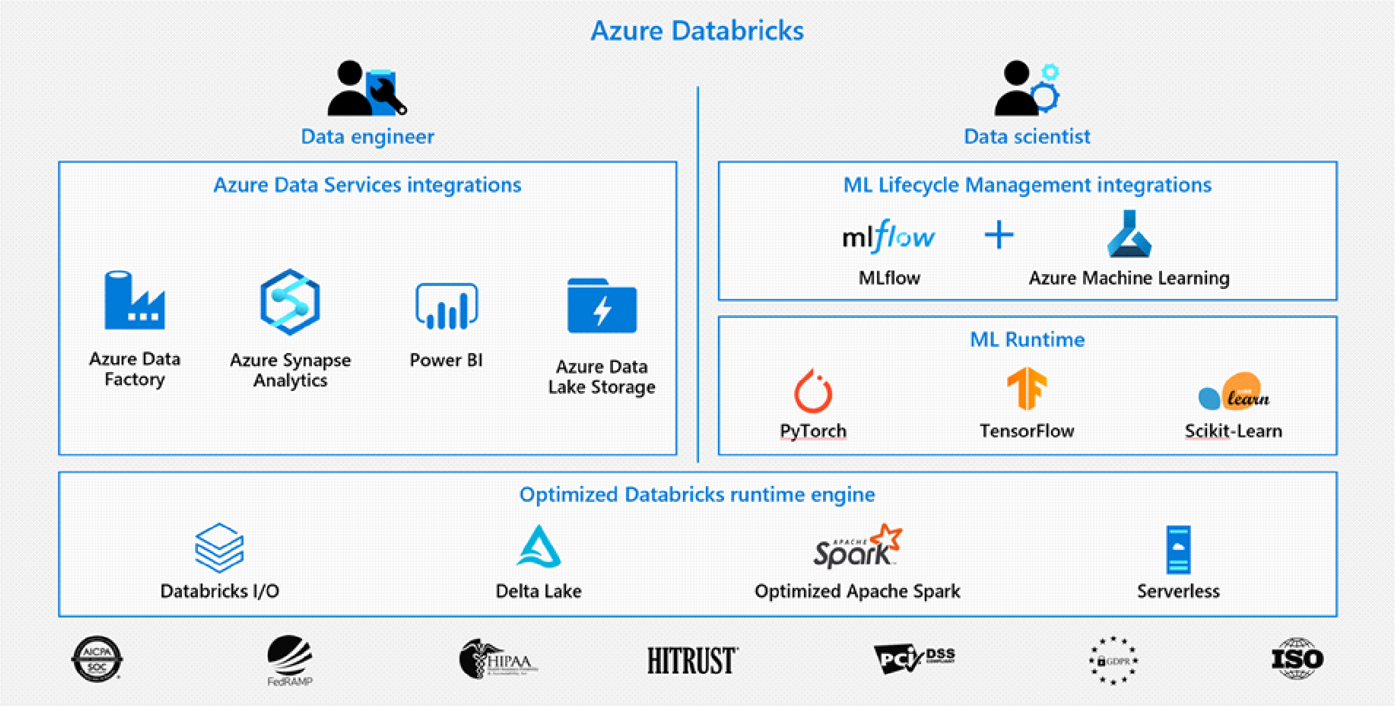
Criteria	**Azure Data Lake**	**Azure Blob Storage**
Data type	Good for storing large volumes of text data	Good for storing unstructured non-text based data such as photos, videos, backup etc.
Geographic redundancy	Need to set up replication of data	By default, provides geo redundant storage
Namespaces support	Supports hierarchical namespaces	Supports flat namespaces
Hadoop compatibility	Hadoop services can use data stored in Data Lake	Is not Hadoop compatible
Security	Allows for more granular access	Granular access not supported

Azure Databricks

Monday, June 13, 2022 11:31 PM

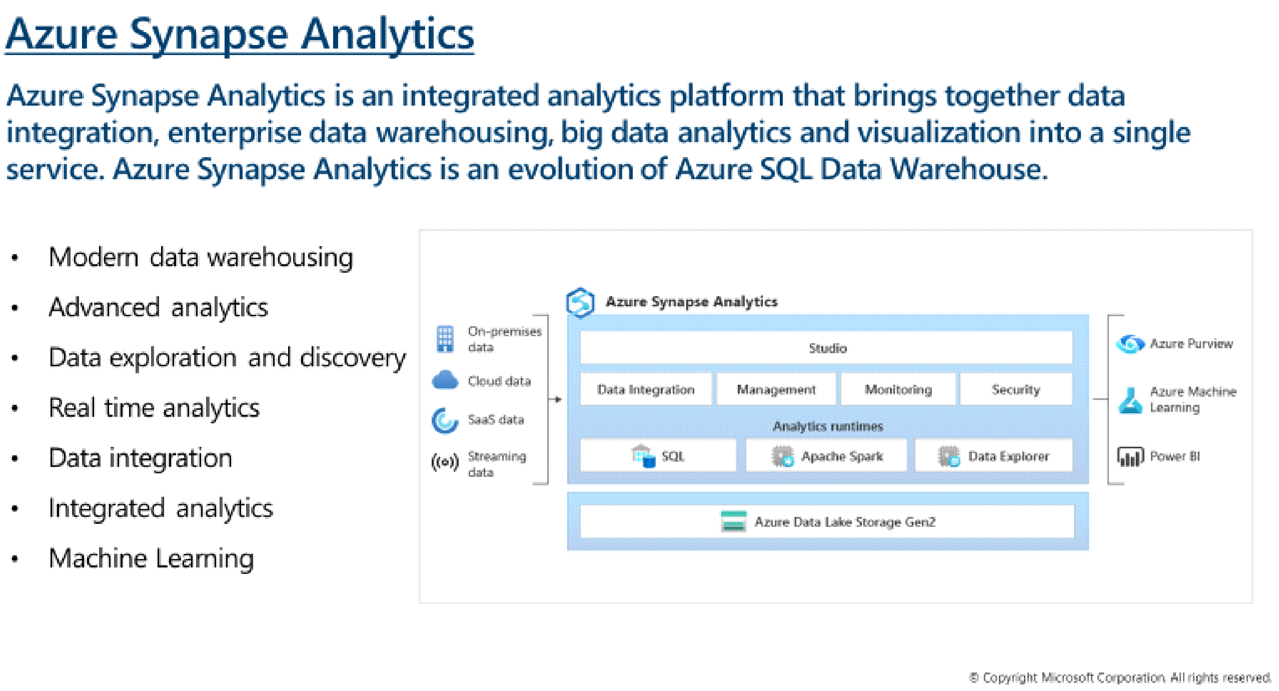
Provides data science and engineering teams with a single platform for Big Data processing and Machine Learning. Offers three environments for developing data intensive applications

Environment	Description
Databricks SQL	Provides an easy-to-use platform for analysts who want to run SQL queries on their data lake, create multiple visualization types to explore query results from different perspectives, and build and share dashboards.
Databricks Data Science & Engineering	Provides an interactive workspace that enables collaboration between data engineers, data scientists, and machine learning engineers. For a big data pipeline, the data (raw or structured) is ingested into Azure through Azure Data Factory in batches, or streamed near real-time using Apache Kafka, Event Hub, or IoT Hub. This data lands in a data lake for long term persisted storage, in Azure Blob Storage or Azure Data Lake Storage. As part of your analytics workflow, use Azure Databricks to read data from multiple data sources and turn it into breakthrough insights using ***Spark***.
Databricks Machine Learning	An integrated end-to-end machine learning environment incorporating managed services for experiment tracking, model training, feature development and management, and feature and model serving.



Azure Synapse Analytics

Monday, June 13, 2022 11:41 PM



Azure Synapse Analytics

Azure Synapse Analytics is an integrated analytics platform that brings together data integration, enterprise data warehousing, big data analytics and visualization into a single service. Azure Synapse Analytics is an evolution of Azure SQL Data Warehouse.

- Modern data warehousing
- Advanced analytics
- Data exploration and discovery
- Real time analytics
- Data integration
- Integrated analytics
- Machine Learning

Azure Synapse Analytics

On-premises data

Cloud data

SaaS data

Streaming data

Studio

Data Integration | Management | Monitoring | Security

Analytics runtimes

SQL | Apache Spark | Data Explorer

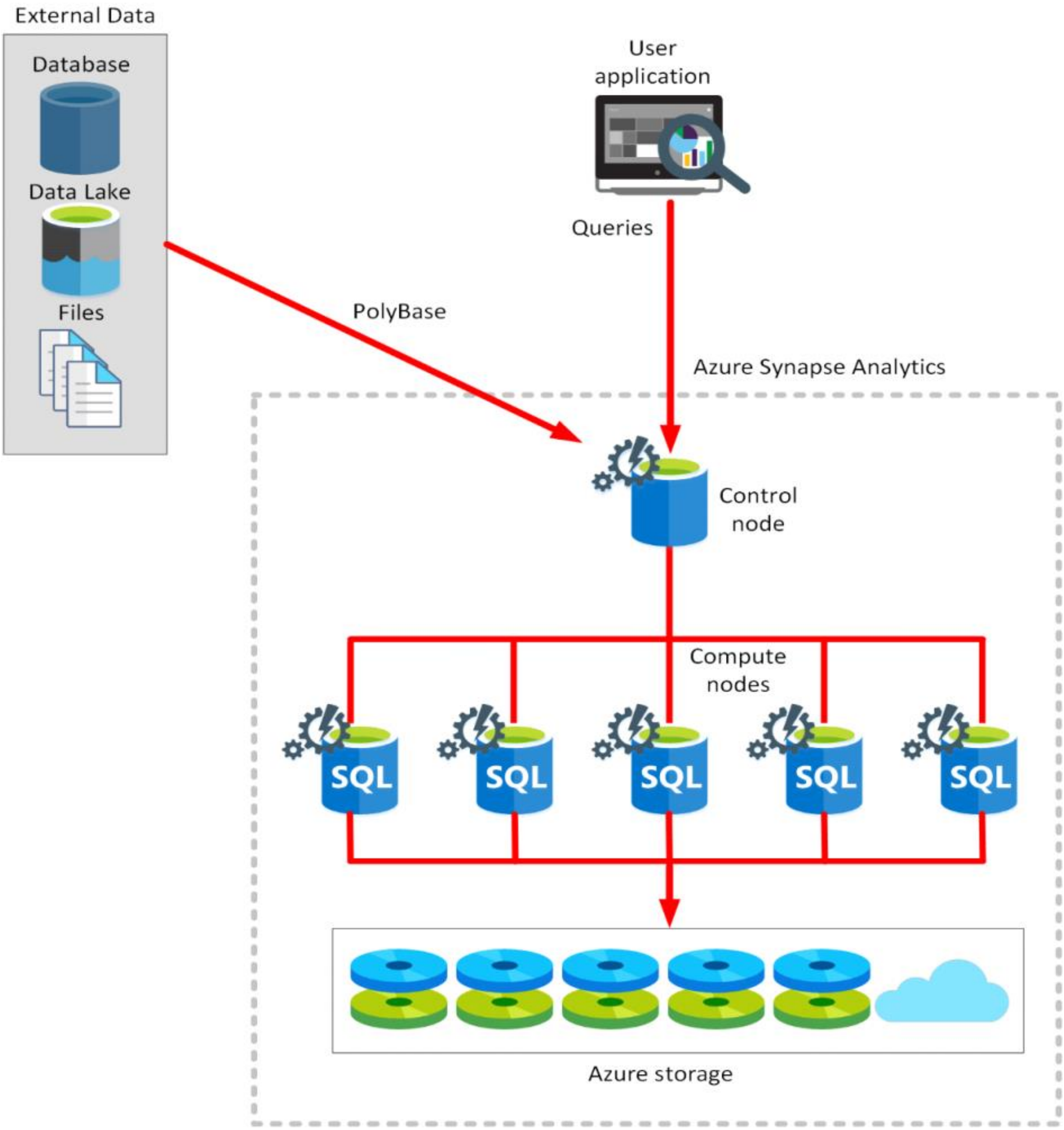
Azure Data Lake Storage Gen2

Azure Purview

Azure Machine Learning

Power BI

- Ingest from different external source
- Enable Parallel Processing
- User submit T-SQL like query statement
- Azure Synapse Analytics process it
    - Distribute by Control node
    - Compute in Compute node
- Use PolyBase to retrieve data from both relational and non-relation storage



Components

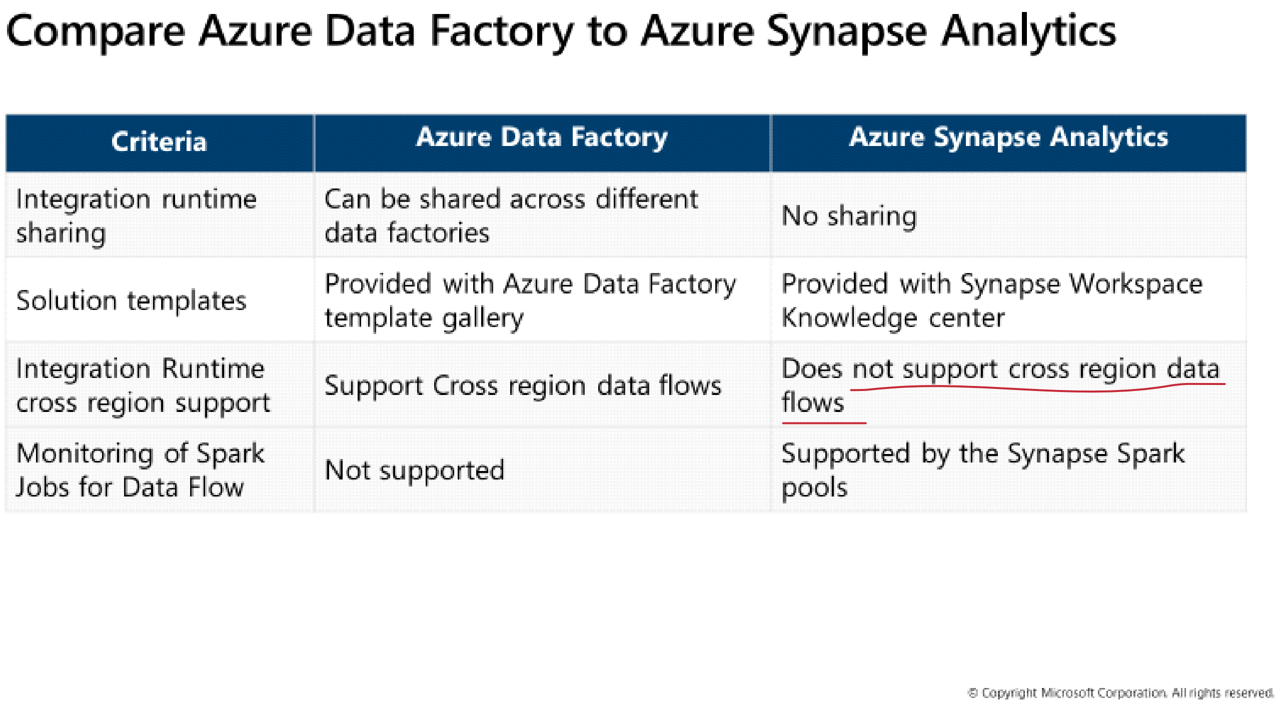
- **Synapse SQL pool**: Synapse SQL offers both serverless and dedicated resource models to work with using node-based architecture. For predictable performance and cost, you can create dedicated SQL pools, for unplanned or ad hoc workloads, you can use the always-available, serverless SQL endpoint.

- **Synapse Spark pool**: This is a cluster of servers running Apache Spark to process data. You write your data processing logic using one of the four supported languages: Python, Scala, SQL, and C# (via .NET for Apache Spark). Apache Spark for Azure Synapse integrates Apache Spark-the open source big data engine used for data preparation, data engineering, ETL, and machine learning.

- **Synapse Pipelines**: Azure Synapse Pipelines leverages the capabilities of Azure Data Factory and is the cloud-based ETL and data integration service that allows you to create data-driven workflows for orchestrating data movement and transforming data at scale. You could include activities that transform the data as it is transferred, or you might combine data from multiple sources together.

- **Synapse Link**: This component allows you to connect to Cosmos DB. You can use it to perform near real-time analytics over the operational data stored in a Cosmos DB database.

- **Synapse Studio**: This is a web-based IDE that can be used centrally to work with all capabilities of Azure Synapse Analytics. You can use Synapse Studio to create SQL and Spark pools, define and run pipelines, and configure links to external data sources.

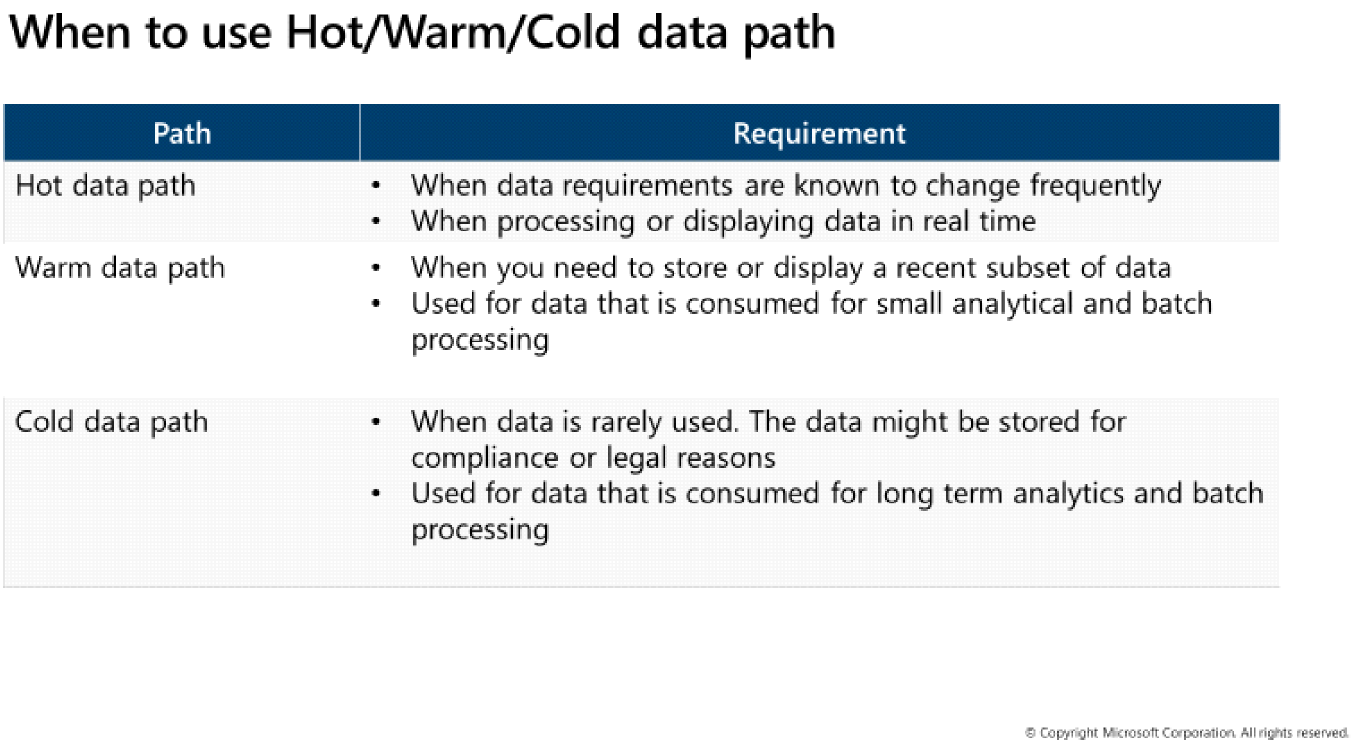


Compare Azure Data Factory to Azure Synapse Analytics

Criteria	Azure Data Factory	Azure Synapse Analytics
Integration runtime sharing	Can be shared across different data factories	No sharing
Solution templates	Provided with Azure Data Factory template gallery	Provided with Synapse Workspace Knowledge center
Integration Runtime cross region support	Support Cross region data flows	Does not support cross region data flows
Monitoring of Spark Jobs for Data Flow	Not supported	Supported by the Synapse Spark pools

Hot, warm, cold data path

Monday, June 13, 2022 11:57 PM



When to use Hot/Warm/Cold data path

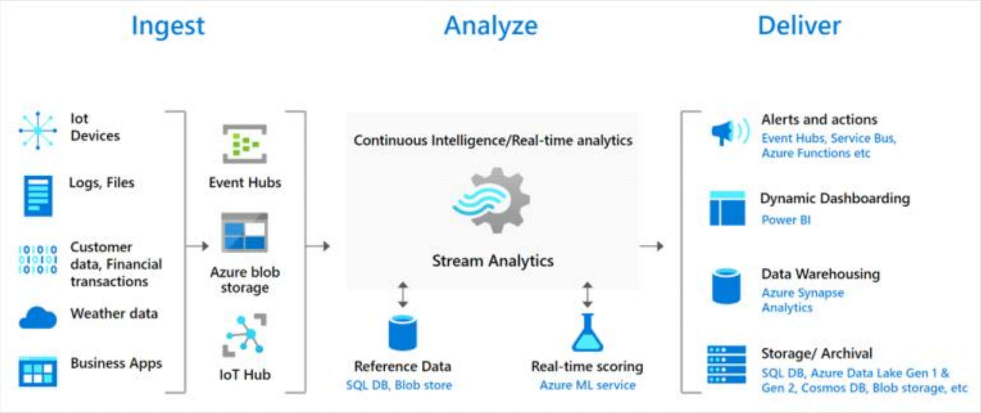
Path	Requirement
Hot data path	• When data requirements are known to change frequently • When processing or displaying data in real time
Warm data path	• When you need to store or display a recent subset of data • Used for data that is consumed for small analytical and batch processing
Cold data path	• When data is rarely used. The data might be stored for compliance or legal reasons • Used for data that is consumed for long term analytics and batch processing

Path	Suitable storage on Azure	Processing
Warm	Azure SQL CosmosDB	Stream Analytics
Cold	Azure Blobs (objects) Azure Data Lake Storage Gen2 Azure Files Azure Queues Azure Tables	Azure Data Factory generate and put to Azure Data Lake or direct ingest by Databrick

Azure Stream Analytics

Tuesday, June 14, 2022 12:15 AM

- fully managed (PaaS offering)
- real-time analytics
- complex event-processing engine
- real-time analytics on multiple streams of data
  - IoT
  - Sensor
  - Clickstreams
  - Social media feeds
- Ingest source
  - Azure Event Hubs
  - Azure IoT Hub
  - Azure Blob Storage
- Analyze by
  - SQL like query to filter/sort/aggregate
  - Extends by JS & C#
- Deliver to
  - Downstream by Azure Event Hubs/ Service Bus/Functions
  - Visualize in Power BI in real-time
  - Train ML by placing output to Azure Synapse Analytics
  - Store ==> SQL/ Cosmos/Blob.....



Design a messaging solution

Monday, June 20, 2022 9:57 PM

https://forms.office.com/r/XHgm9kDCiS

Services	Scenario
Azure Queue storage	• A simple queue to organize messages. • An audit trail of all messages that pass through the queue. • Queue to exceed 80 GB in size. • To track progress for processing a message inside of the queue.
Azure Service Bus queues	• An At-Most-Once delivery guarantee. • At-Least-Once message processing (PeekLock receive mode) • At-Most-Once message processing (ReceiveAndDelete receive mode) • To group messages into transactions. • To receive messages without polling the queue. • To handle messages larger than 64 KB but less than 256 KB. • Queue size will not grow larger than 80 GB. • To publish and consume batches of messages.
Azure Service Bus topics	• Multiple receivers to handle each message. • Multiple destinations for a single message but need queue-like behavior.

Labs : Work with Azure Queue Storage queues in .NET
https://docs.microsoft.com/en-us/azure/storage/queues/storage-tutorial-queues?toc=%2Fazure%2Fstorage%2Fqueues%2Ftoc.json&tabs=dotnet%2Cenvironment-variable-windows

Labs : Create a Service Bus queue and topic

https://docs.microsoft.com/en-us/learn/modules/implement-message-workflows-with-service-bus/3-exercise-implement-a-service-bus-topic-and-queue

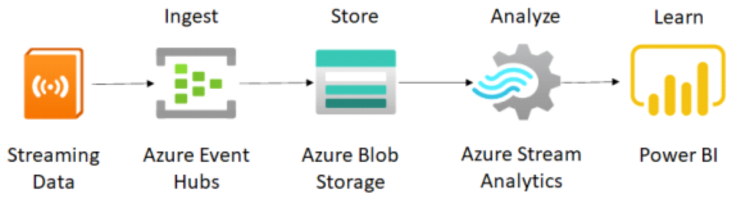
Labs : Send and receive messages by using a queue

https://docs.microsoft.com/en-us/learn/modules/implement-message-workflows-with-service-bus/5-exercise-write-code-that-uses-service-bus-queues

Azure Event Hubs

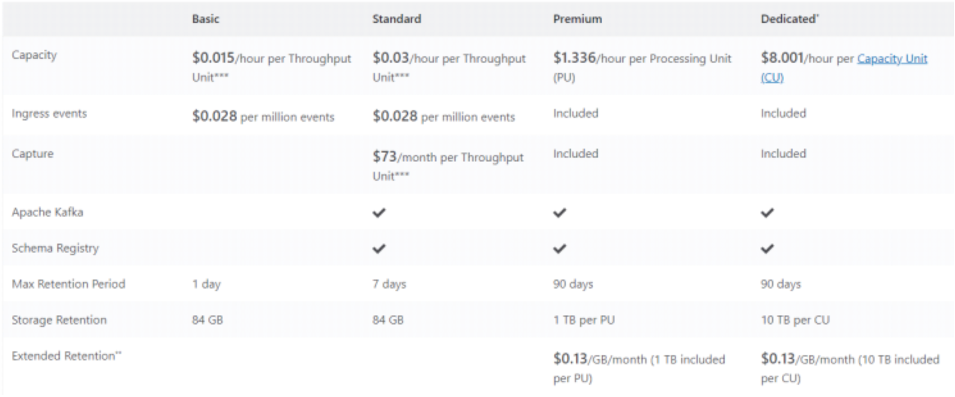
Monday, June 20, 2022 10:00 PM

- Endpoint for an event source to inject the event into Azure environment
- Just a storage of these event and WAIT for other consumers to PULL data/event from it
- Store the data in storage account



A single throughput unit equates to

- Ingress: Up to 1 MB per second or 1000 events per second (whichever comes first).
- Egress: Up to 2 MB per second or 4096 events per second.



	Basic	Standard	Premium	Dedicated*
Capacity	$0.015/hour per Throughput Unit***	$0.03/hour per Throughput Unit***	$1.336/hour per Processing Unit (PU)	$8.001/hour per Capacity Unit (CU)
Ingress events	$0.028 per million events	$0.028 per million events	Included	Included
Capture		$73/month per Throughput Unit***	Included	Included
Apache Kafka		✓	✓	✓
Schema Registry		✓	✓	✓
Max Retention Period	1 day	7 days	90 days	90 days
Storage Retention	84 GB	84 GB	1 TB per PU	10 TB per CU
Extended Retention**			$0.13/GB/month (1 TB included per PU)	$0.13/GB/month (10 TB included per CU)

Labs : Create an event hub using Azure CLI

https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-quickstart-cli#code-try-0

Labs : Use Java to send events to or receive events from Azure Event Hubs (azure-messaging-eventhubs)

https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-java-get-started-send

Labs : Build real time Power BI dashboards with Stream Analytics no code editor

https://docs.microsoft.com/en-us/azure/stream-analytics/no-code-power-bi-tutorial?toc=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fevent-hubs%2Ftoc.json&bc=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fbread%2Ftoc.json

Exam

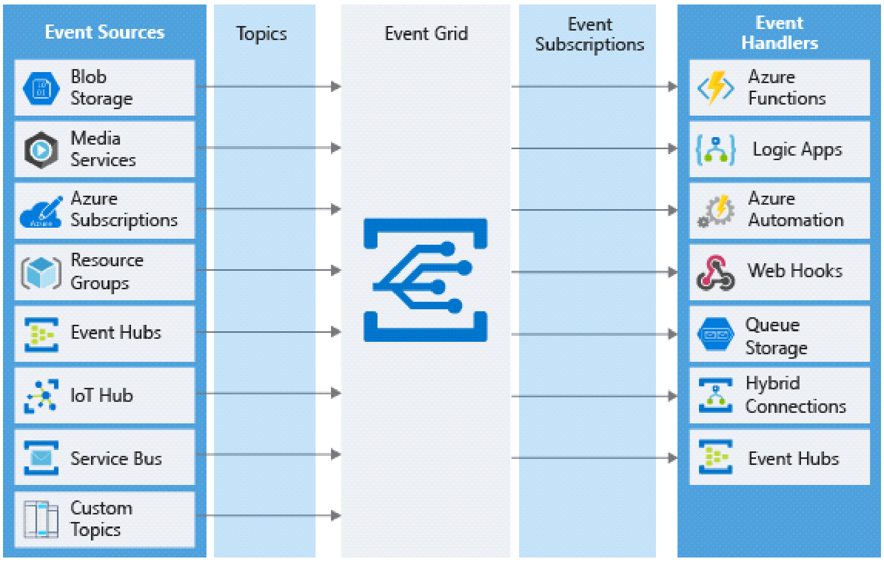
What is the differences between

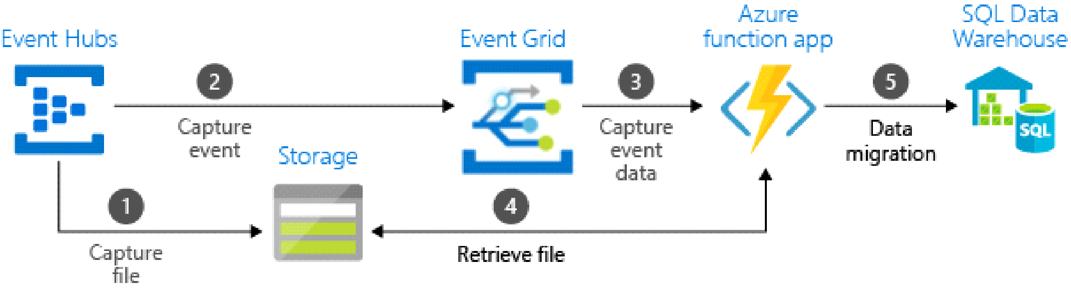
- Event hubs ==> ingest of data, endpoint for event source, storage
- Event grid ==> Route the azure event/custom event in topics, to source that subscribe an event
- Data factory ==> ETL of Data and generate transformed output to Data Lake for later use

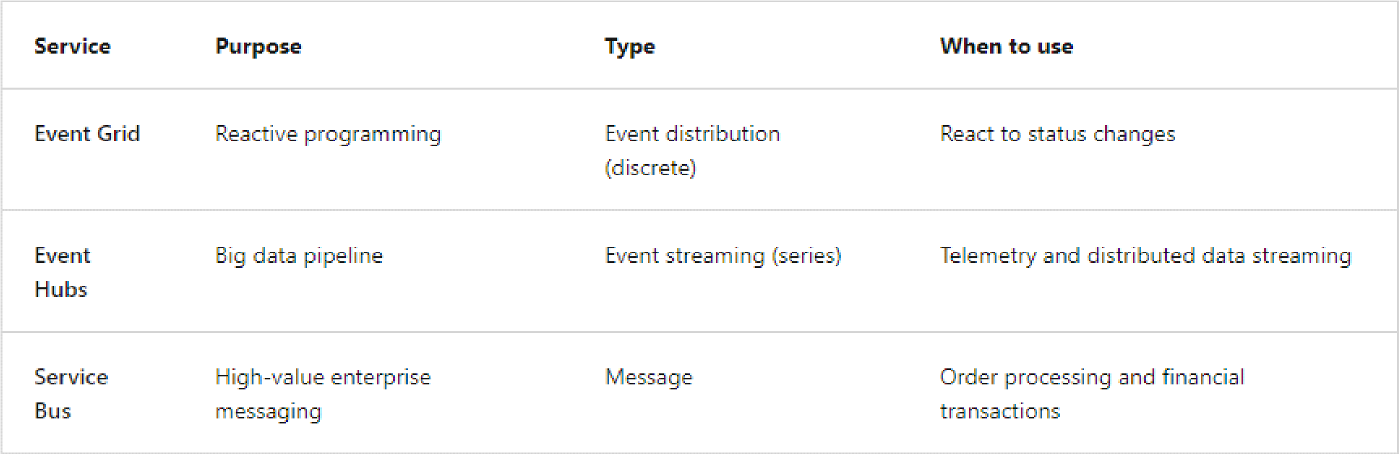
Azure Event Grid

Monday, June 20, 2022 10:23 PM

- Routing of event
- No need to pull (But Azure event hubs need pull)







Service	Purpose	Type	When to use
Event Grid	Reactive programming	Event distribution (discrete)	React to status changes
Event Hubs	Big data pipeline	Event streaming (series)	Telemetry and distributed data streaming
Service Bus	High-value enterprise messaging	Message	Order processing and financial transactions

Azure IoT Hub

Monday, June 20, 2022 10:31 PM

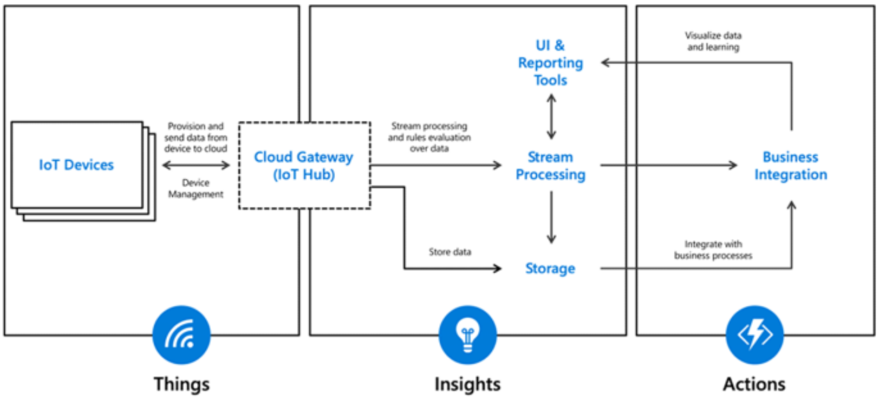
Central message hub for IoT applications and its attached devices.

When to use IoT Hub?

- Application complexity
- Data throughput
- Securing solution end to end allowing for per-device authentication
- Bi-directional communication

Capabilities over Event Hub:

- Per-device identity
- File upload from devices
- Device provisioning service

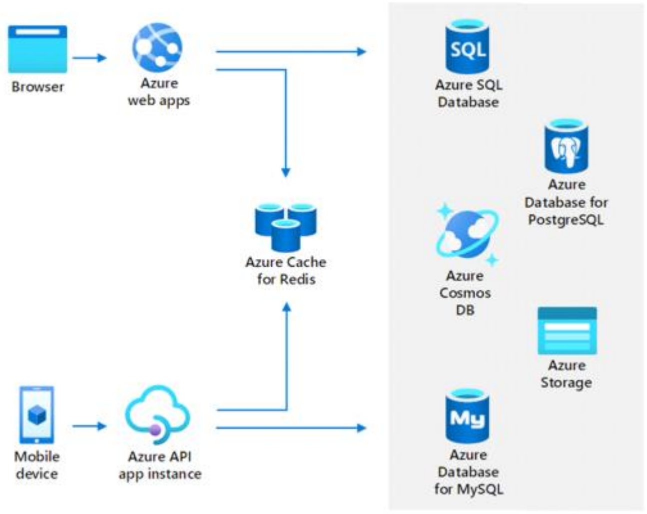

IoT Devices
Provision and send data from device to cloud
Device Management
Cloud Gateway (IoT Hub)
Stream processing and rules evaluation over data
Store data
UI & Reporting Tools
Stream Processing
Storage
Visualize data and learning
Business Integration
Integrate with business processes
Things
Insights
Actions

Azure Cache for Redis

Monday, June 20, 2022 10:29 PM

Store frequently accessed data so that applications can be responsive to users.

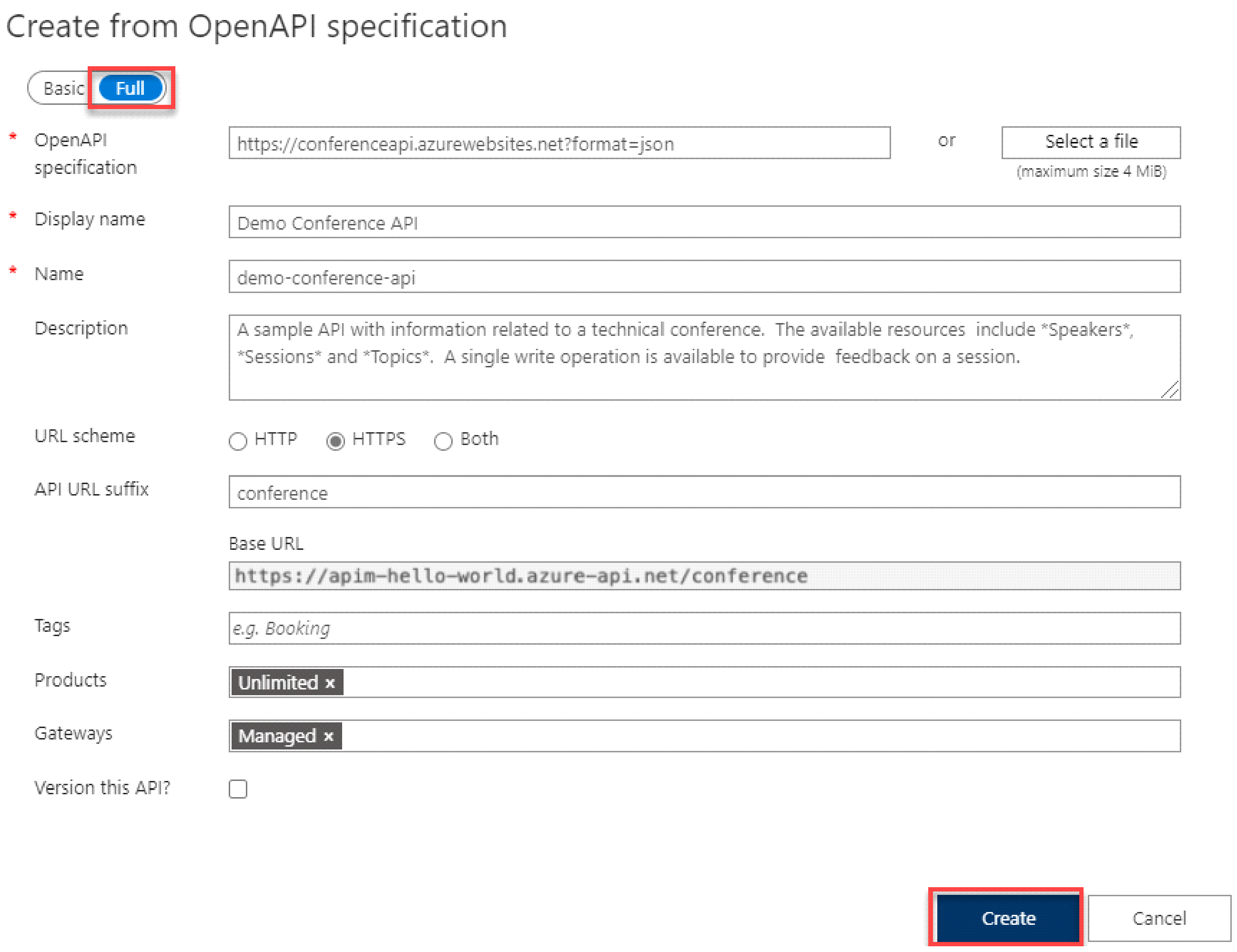
Audience	**Azure Cache for Redis**
Data cache	Databases are often too large to load directly into a cache. It's common to use the cache-aside pattern to load data into the cache only as needed. When the system makes changes to the data, the system can also update the cache, which is then distributed to other clients. Additionally, the system can set an expiration on data, or use an eviction policy to trigger data updates into the cache.
Content cache	Many web pages are generated from templates that use static content such as headers, footers, banners. These static items shouldn't change often. Using an in-memory cache provides quick access to static content compared to backend datastores. This pattern reduces processing time and server load, allowing web servers to be more responsive. It can allow you to reduce the number of servers needed to handle loads. Azure Cache for Redis provides the Redis Output Cache Provider to support this pattern with ASP.NET.
Session store	This pattern is commonly used with shopping carts and other user history data that a web application might associate with user cookies. Storing too much in a cookie can have a negative effect on performance as the cookie size grows and is passed and validated with every request. A typical solution uses the cookie as a key to query the data in a database. Using an in-memory cache, like Azure Cache for Redis, to associate information with a user, is much faster than interacting with a full relational database.
Job and message queuing	Applications often add tasks to a queue when the operations associated with the request take time to execute. Longer running operations are queued to be processed in sequence, often by another server. This method of deferring work is called task queuing. Azure Cache for Redis provides a distributed queue to enable this pattern in your application.
Distributed transactions	Applications sometimes require a series of commands against a backend data-store to execute as a single atomic operation. All commands must succeed, or all must be rolled back to the initial state. Azure Cache for Redis supports executing a batch of commands as a single transaction.



Azure APIM

Monday, June 20, 2022 10:38 PM

Labs : Create a new Azure API Management service instance by using the Azure CLI
https://docs.microsoft.com/en-us/azure/api-management/get-started-create-service-instance-cli



Create from OpenAPI specification

Basic [✓ Full]

* OpenAPI specification: https://conferenceapi.azurewebsites.net?format=json or Select a file (maximum size 4 MiB)

* Display name: Demo Conference API

* Name: demo-conference-api

Description: A sample API with information related to a technical conference. The available resources include *Speakers*, *Sessions* and *Topics*. A single write operation is available to provide feedback on a session.

URL scheme: ○ HTTP ● HTTPS ○ Both

API URL suffix: conference

Base URL: https://apim-hello-world.azure-api.net/conference

Tags: e.g. Booking

Products: Unlimited ×

Gateways: Managed ×

Version this API? □

Product

Product include:

- one or more APIs
- a usage quota
- the terms of use

After a product is published, developers can subscribe to the product and begin to use the product's APIs.

Policy that APIM provide

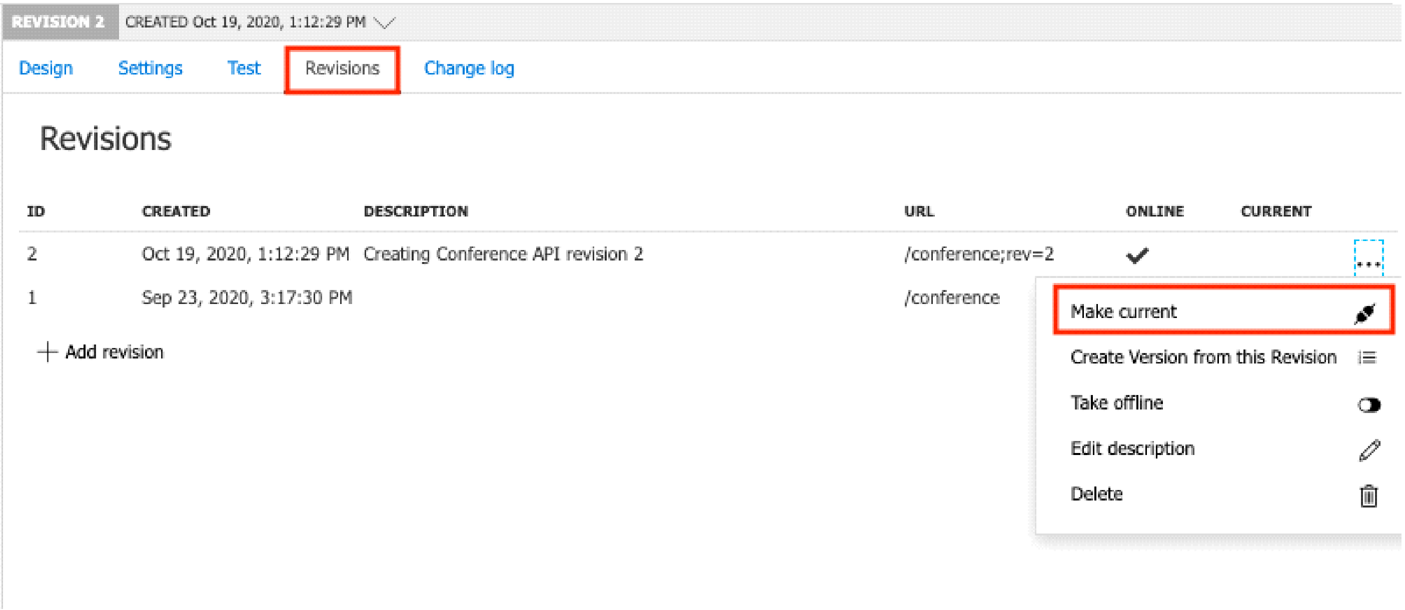
https://docs.microsoft.com/en-us/azure/api-management/policies/

Common policy:

- Authorize access based on JWT claims
- Add a Forwarded header to allow the backend API to construct proper URLs
- Add a header containing a correlation id
- Filter response content
- Rate limit policy
- Replace original URLs in the body of the API response with API Management gateway URLs

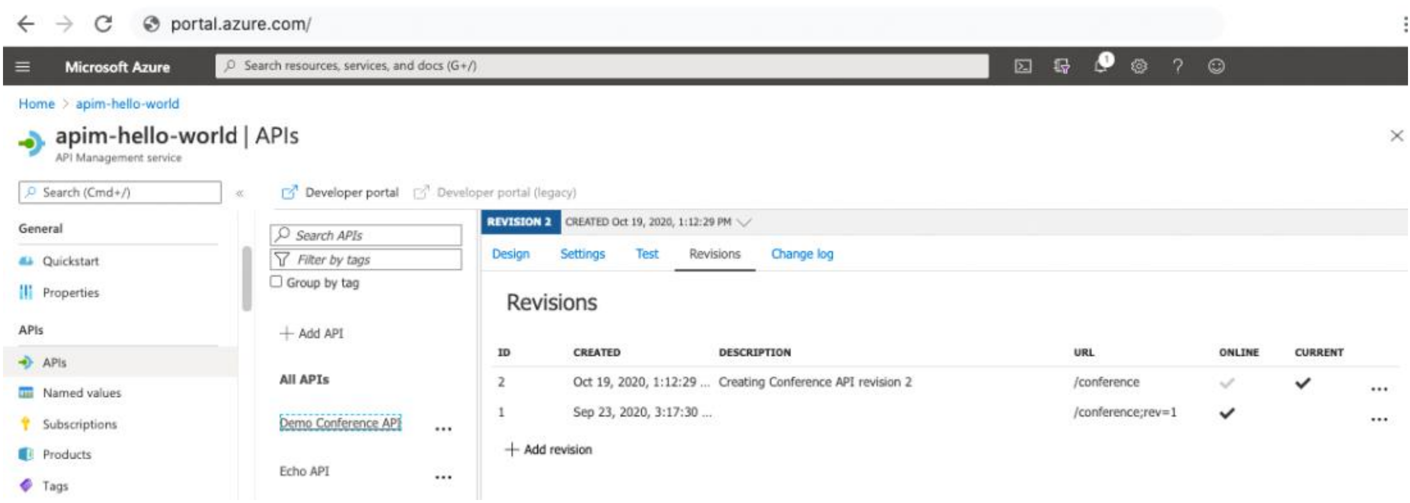
Version

https://docs.microsoft.com/en-us/azure/api-management/api-management-get-started-revise-api?tabs=azure-portal



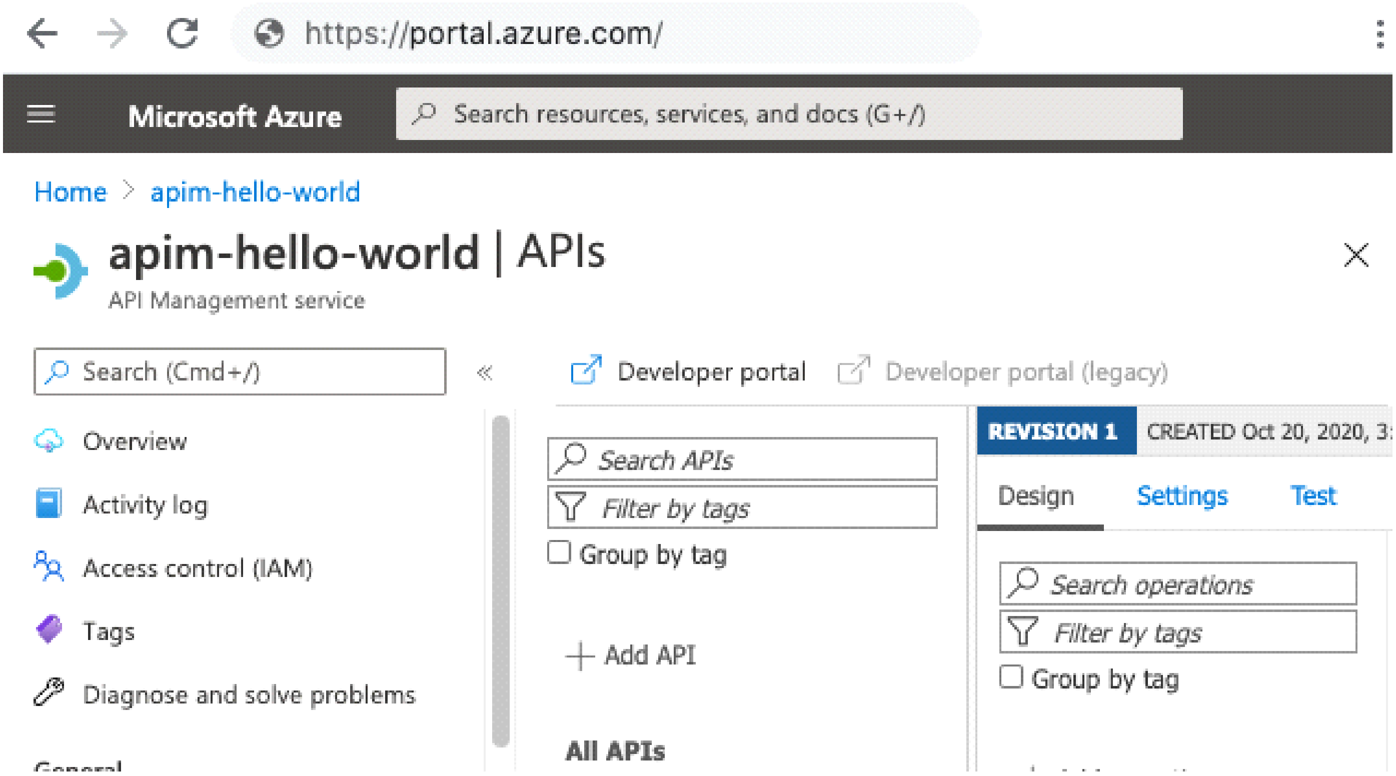
Revisions

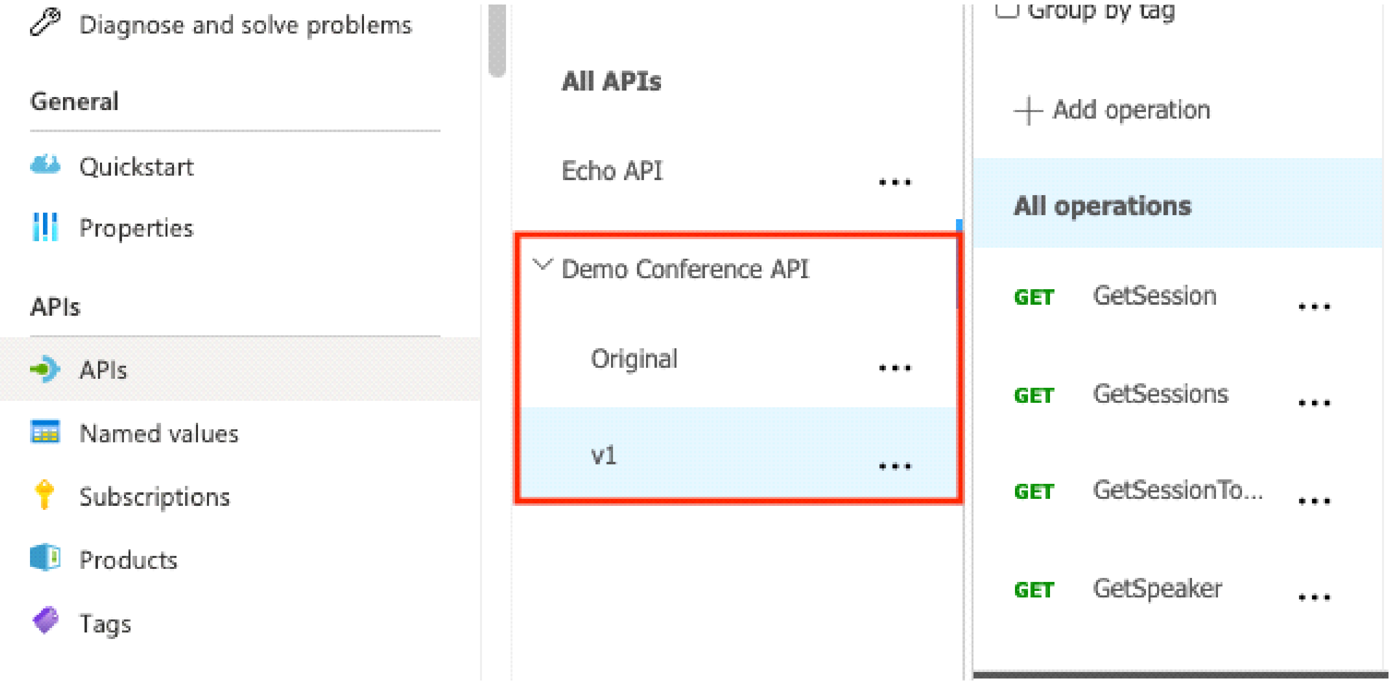
ID	CREATED	DESCRIPTION	URL	ONLINE	CURRENT
2	Oct 19, 2020, 1:12:29 PM	Creating Conference API revision 2	/conference;rev=2	✓	...
1	Sep 23, 2020, 3:17:30 PM		/conference		

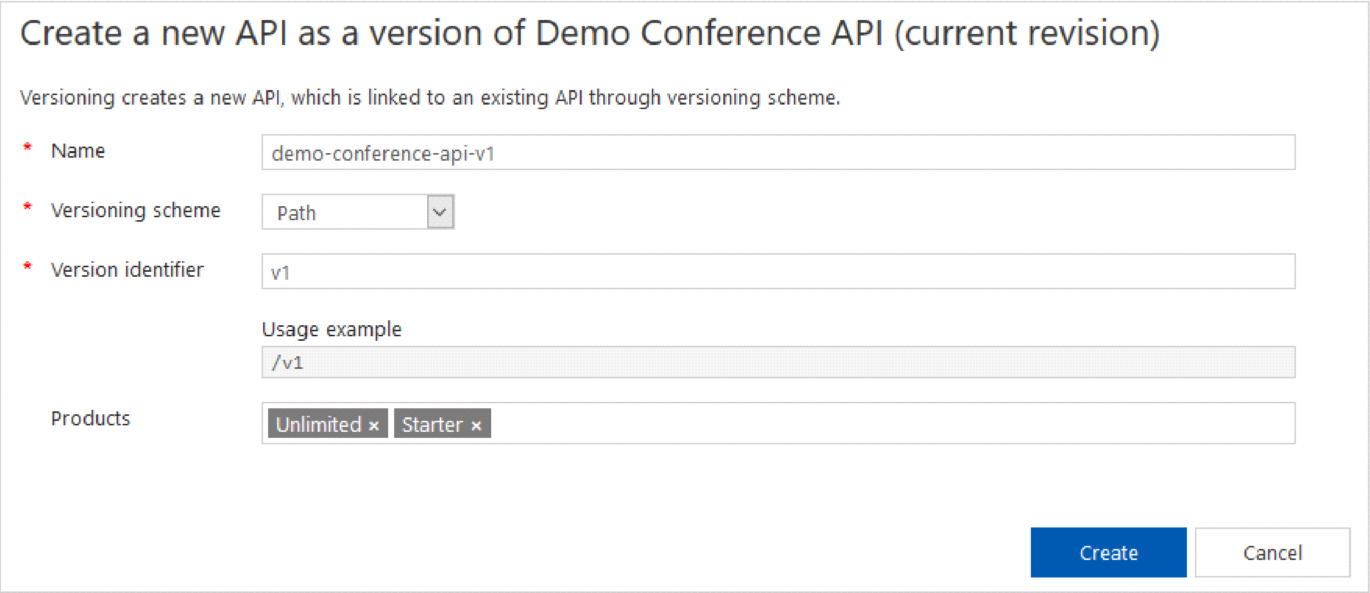


Revisions

ID	CREATED	DESCRIPTION	URL	ONLINE	CURRENT
2	Oct 19, 2020, 1:12:29 ...	Creating Conference API revision 2	/conference	✓	✓
1	Sep 23, 2020, 3:17:30 ...		/conference;rev=1	✓	







Create a new API as a version of Demo Conference API (current revision)

Versioning creates a new API, which is linked to an existing API through versioning scheme.

* Name	demo-conference-api-v1
* Versioning scheme	Path
* Version identifier	v1
	Usage example /v1
Products	Unlimited × Starter ×

Azure Automation

Monday, June 20, 2022 10:56 PM

ARM Template
- JSON
- Bicep

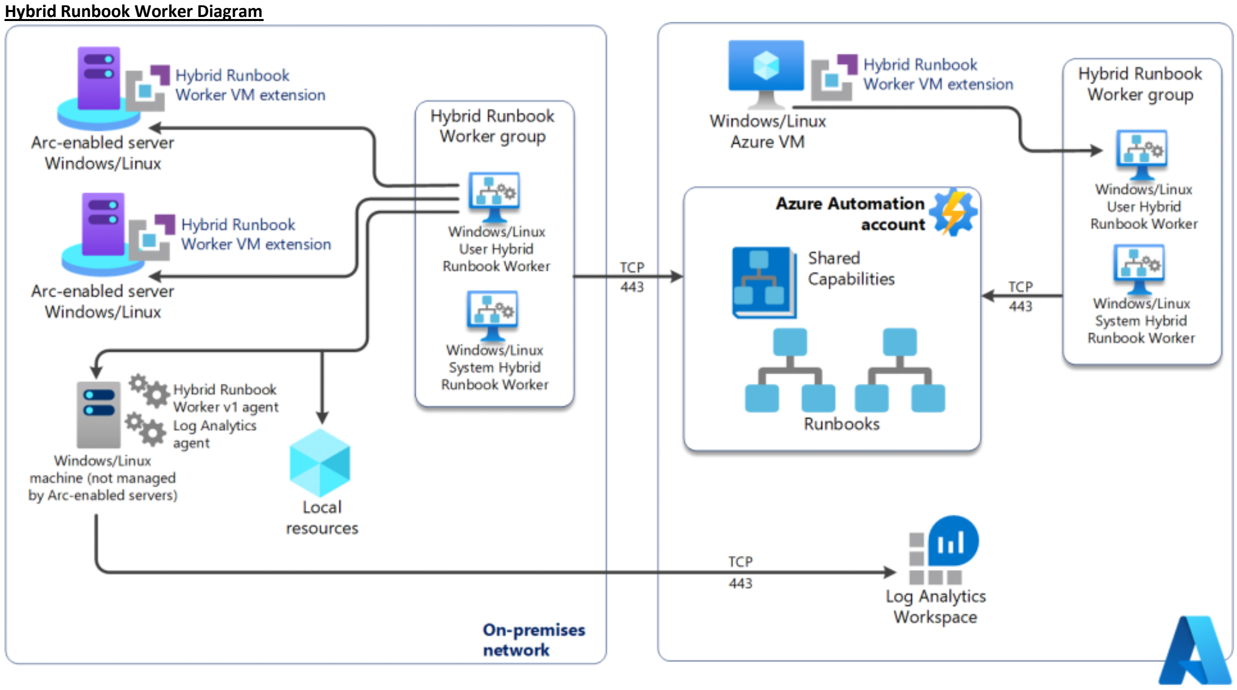
Labs : Automation DSC - Add LAMP to a Windows Server using automation
https://docs.microsoft.com/en-us/azure/automation/quickstarts/dsc-configuration

Azure Automation

Automation is needed in three broad areas of cloud operations:
- Deploy and manage - Deliver repeatable and consistent infrastructure as code.
- Response - Create event-based automation to diagnose and resolve issues.
- Orchestrate - Orchestrate and integrate your automation with other Azure or third party services and products.

Process Automation
- Runbook
- Hybrid Runbook Worker
  https://docs.microsoft.com/en-us/azure/automation/automation-hybrid-runbook-worker
- Webhooks
  - Azure Logic Apps
  - Azure Power Apps
  - Azure Event Grid
  - Azure Power Automate
- Configuration Management
  - https://docs.microsoft.com/en-us/azure/automation/automation-dsc-overview
  - Lab => https://docs.microsoft.com/en-us/azure/automation/quickstarts/dsc-configuration
- Update Management

Hybrid Runbook Worker Diagram


Hybrid Runbook Worker VM extension
Arc-enabled server Windows/Linux
Hybrid Runbook Worker VM extension
Arc-enabled server Windows/Linux
Hybrid Runbook Worker v1 agent
Log Analytics agent
Windows/Linux machine (not managed by Arc-enabled servers)
Local resources
Hybrid Runbook Worker group
Windows/Linux User Hybrid Runbook Worker
Windows/Linux System Hybrid Runbook Worker
TCP 443
On-premises network
Windows/Linux Azure VM
Hybrid Runbook Worker VM extension
Azure Automation account
Shared Capabilities
Runbooks
Hybrid Runbook Worker group
Windows/Linux User Hybrid Runbook Worker
Windows/Linux System Hybrid Runbook Worker
TCP 443
TCP 443
Log Analytics Workspace

Common scenarios

Azure Automation supports management throughout the lifecycle of your infrastructure and applications. Common scenarios include:

- **Schedule tasks** - stop VMs or services at night and turn on during the day, weekly or monthly recurring maintenance workflows.
- **Build and deploy resources** - Deploy virtual machines across a hybrid environment using runbooks and Azure Resource Manager templates. Integrate into development tools, such as Jenkins and Azure DevOps.
- **Periodic maintenance** - to execute tasks that need to be performed at set timed intervals like purging stale or old data, or reindex a SQL database.
- **Respond to alerts** - Orchestrate a response when cost-based, system-based, service-based, and/or resource utilization alerts are generated.
- **Hybrid automation** - Manage or automate on-premises servers and services like SQL Server, Active Directory, SharePoint Server, etc.
- **Azure resource lifecycle management** - for IaaS and PaaS services.
  - Resource provisioning and deprovisioning.
  - Add correct tags, locks, NSGs, UDRs per business rules.
  - Resource group creation, deletion & update.
  - Start container group.
  - Register DNS record.
  - Encrypt Virtual machines.
  - Configure disk (disk snapshot, delete old snapshots).
  - Subscription management.

    - Start-stop resources to save cost.
- **Monitoring & integrate** with 1st party (through Azure Monitor) or 3rd party external systems.
    - Ensure resource creation\deletion operations is captured to SQL.
    - Send resource usage data to web API.
    - Send monitoring data to ServiceNow, Event Hub, New Relic and so on.
    - Collect and store information about Azure resources.
    - Perform SQL monitoring checks & reporting.
    - Check website availability.
- **Dev/test automation scenarios** - Start and start resources, scale resources, etc.
- **Governance related automation** - Automatically apply or update tags, locks, etc.
- **Azure Site Recovery** - orchestrate pre/post scripts defined in a Site Recovery DR workflow.
- **Azure Virtual Desktop** - orchestrate scaling of VMs or start/stop VMs based on utilization.
- **Configure VMs** - Assess and configure Windows and Linux machines with configurations for the infrastructure and application.
- **Retrieve inventory** - Get a complete inventory of deployed resources for targeting, reporting, and compliance.
- **Find changes** - Identify and isolate machine changes that can cause misconfiguration and improve operational compliance. Remediate or escalate them to management systems.

Case Study

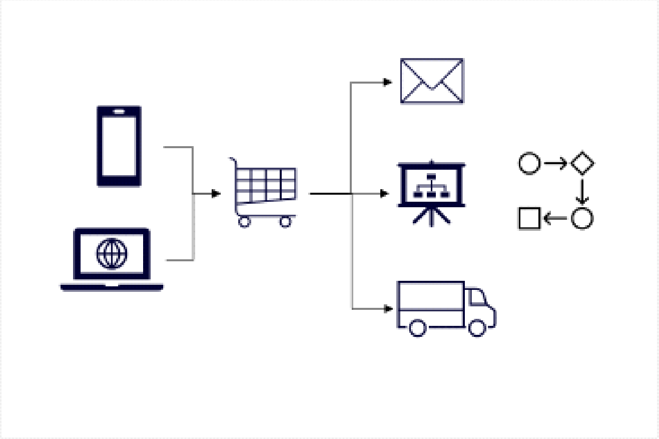
Monday, June 20, 2022 11:14 PM

https://forms.office.com/r/XHgm9kDCiS

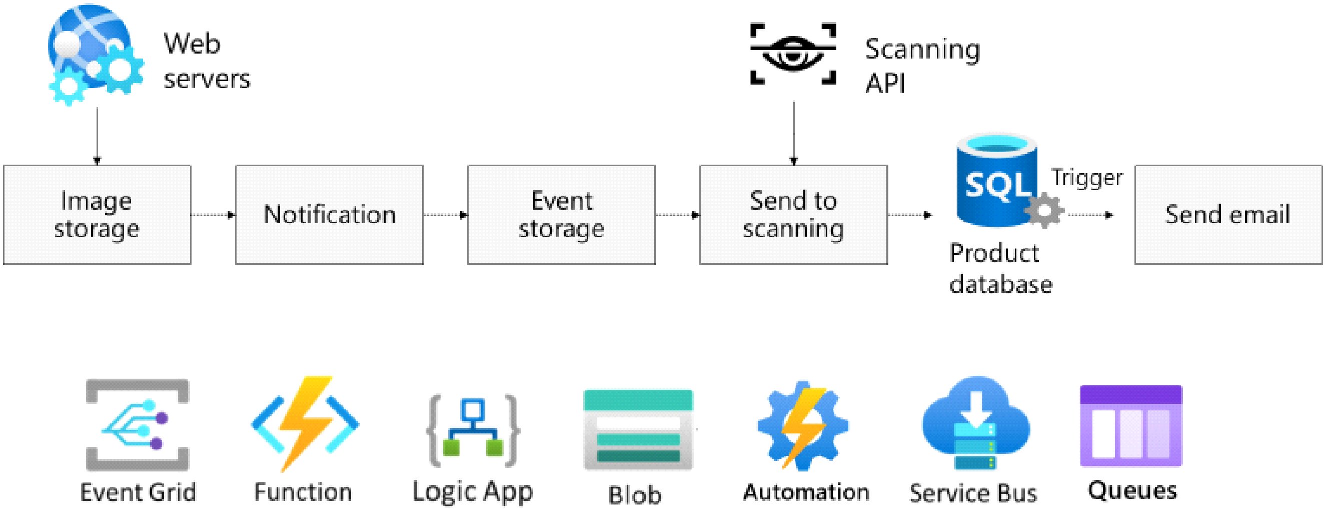
Case Study – Application architecture

A new product catalog design

- New product catalog, ordering process, and shopping cart
- Services will rely on a combination of relational and non-relational data
- It is critical that the service hosting the application supports rapid autoscaling and high availability



Instructor case study discussion



Web servers

Scanning API

Image storage

Notification

Event storage

Send to scanning

Trigger

Product database

Send email

Event Grid

Function

Logic App

Blob

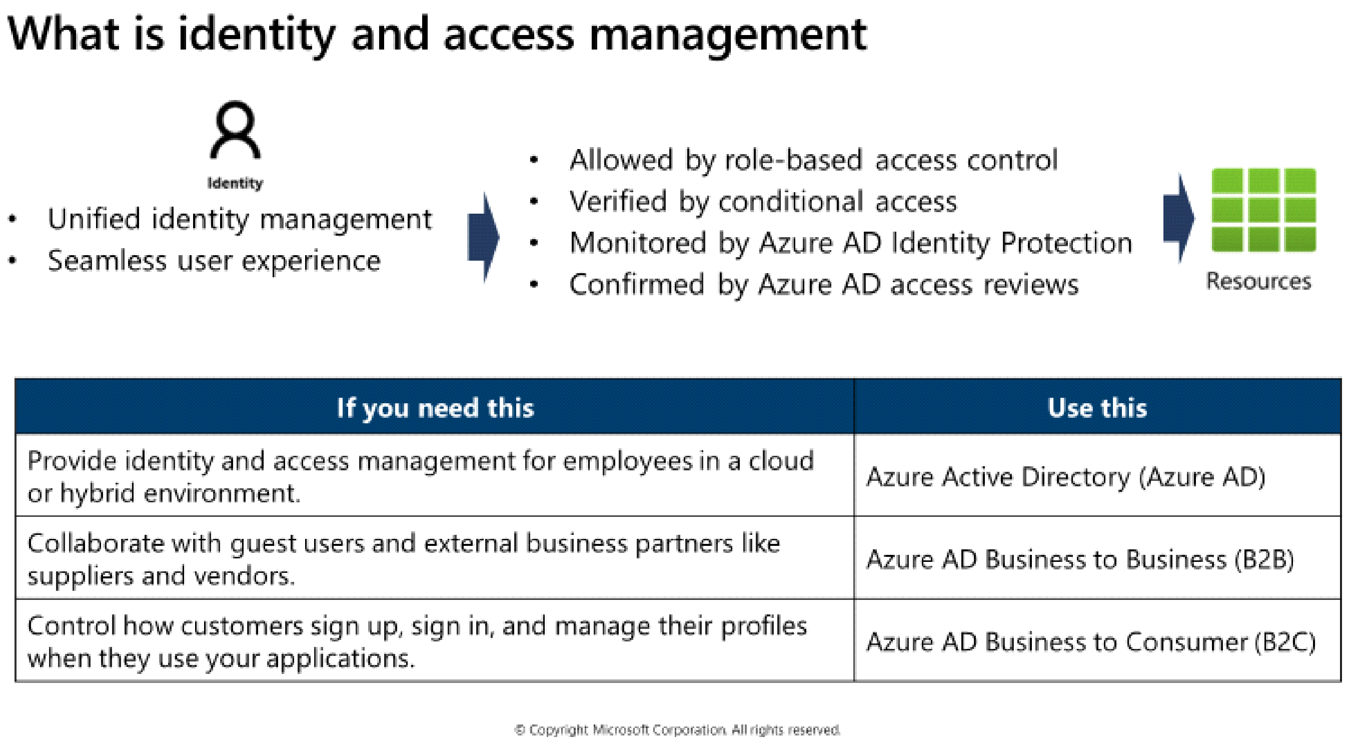
Automation

Service Bus

Queues

Identity and Access Management (IAM)

Monday, June 20, 2022 11:27 PM



What is identity and access management

Identity

- Unified identity management
- Seamless user experience

- Allowed by role-based access control
- Verified by conditional access
- Monitored by Azure AD Identity Protection
- Confirmed by Azure AD access reviews

Resources

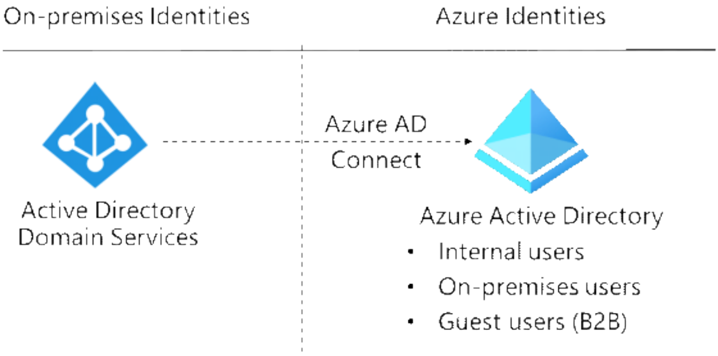
If you need this	Use this
Provide identity and access management for employees in a cloud or hybrid environment.	Azure Active Directory (Azure AD)
Collaborate with guest users and external business partners like suppliers and vendors.	Azure AD Business to Business (B2B)
Control how customers sign up, sign in, and manage their profiles when they use your applications.	Azure AD Business to Consumer (B2C)

Azure Active Directory

Monday, June 20, 2022 11:27 PM

Azure AD is the Azure solution for identity and access management. Azure AD is a multitenant, cloud-based directory, and identity management service.

- Centralize identity management
- Establish a single Azure AD instance
- Use **Azure AD Connect**, or AD Connect cloud sync for hybrid identity sync



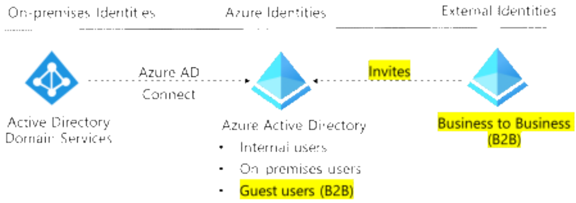
Best practices

- Centralize identity management
- Establish a single Azure AD instance
- Don’t synchronize local high privileges accounts to Azure AD
- Turn on password hash synchronization
- Enable single sign-on (SSO)

Azure AD (B2B)

Monday, June 20, 2022 11:30 PM

Azure AD B2B enables you to securely collaborate with external partners



- Integrate with identity providers
- Use conditional access policies to intelligently grant or deny access
- Require MFA for guest users
- Guest users sign in to your apps and services with their own work, school, or social identities
- Their identities are managed by the partner themselves

Best practices

- Designate an application owner to manage guest users
- Use conditional access policies to intelligently grant or deny access
- Enable MFA
- Integrate with identity providers
- Create a self-service sign-up user flow

Labs : Set up sign in for an ASP.NET application using Azure Active Directory B2C
https://docs.microsoft.com/en-us/azure/active-directory-b2c/quickstart-web-app-dotnet

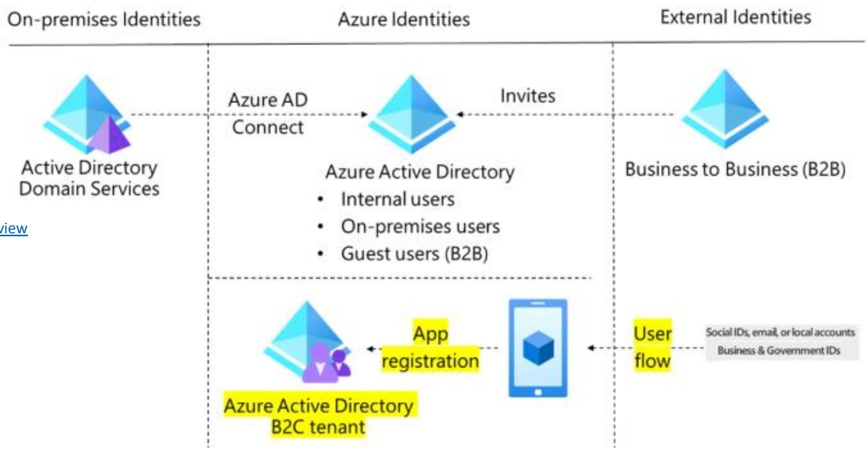
Azure AD (B2C)

Monday, June 20, 2022 11:44 PM

Azure AD B2C is a type of Azure AD tenant that you use to manage customer identities and their access to your applications

- Integrate with external user stores
- Provide single sign-on access with a user-provided identity
- Create a custom-branded identity solution
- Use policies to configure user journeys
- Use progressive profiling to gradual collect user information
- Pass user data to a 3rd party for validation

Labs : Create an Azure Active Directory B2C tenant
https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-create-tenant

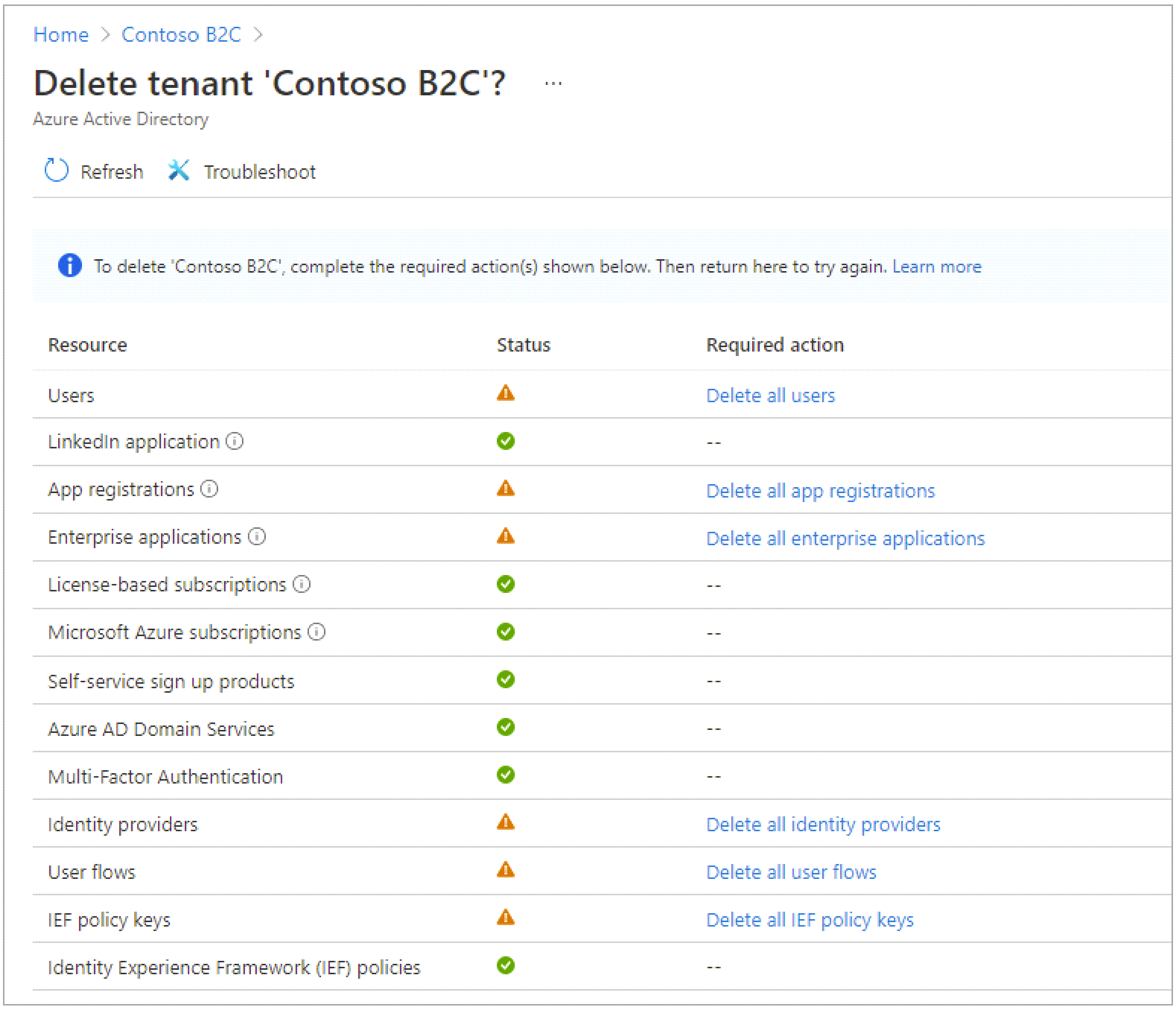


Best practices

- Configure user journeys by using policies
  - User flows
  - Custom policies
  - https://docs.microsoft.com/en-us/azure/active-directory-b2c/user-flow-overview
  - Reuse the same user flows across different applications
  - Consistent user journey across all applications
- Use identity providers to let users sign in using their social identities
- Customize your user interface

With some basic knowledge on identity solutions, let's review our design choices.

Feature	Azure AD B2B	Azure AD B2C
Purpose	Collaborating with business partners from external organizations like suppliers, partners, vendors. Users appear as guest users in your directory. These users may or may not have managed IT.	Customers of your product. These users are managed in a separate Azure AD directory / tenant.
Users	Partner users acting on behalf of their company or employees of the company	Customers acting as themselves.
Profiles	Managed through access reviews, email verification, or access/deny lists.	Users manage their own profiles.
Discoverability	Partner users are discoverable and can find other users from their organization.	Customers are invisible to other users. Privacy and content are enforced.
Identity providers supported	External users can collaborate using work accounts, school accounts, any email address, SAML and WS-Fed based identity providers, Gmail, and Facebook.	Consumer users with local application accounts (any email address or user name), various supported social identities, and users with corporate and government-issued identities via SAML/WS-Fed based identity provider federation.
External user management	External users are managed in the same directory as employees but are typically annotated as guest users. Guest users can be managed the same way as employees, added to the same groups, and so on.	External users are managed in the Azure AD B2C directory. They're managed separately from the organization's employee and partner directory (if any).
Branding	Host/inviting organization's brand is used.	Fully customizable branding per application or organization.



Delete tenant 'Contoso B2C'? ...

Azure Active Directory

To delete 'Contoso B2C', complete the required action(s) shown below. Then return here to try again. Learn more

Resource	Status	Required action
Users	⚠	Delete all users
LinkedIn application ⓘ	✓	--
App registrations ⓘ	⚠	Delete all app registrations
Enterprise applications ⓘ	⚠	Delete all enterprise applications
License-based subscriptions ⓘ	✓	--
Microsoft Azure subscriptions ⓘ	✓	--
Self-service sign up products	✓	--
Azure AD Domain Services	✓	--
Multi-Factor Authentication	✓	--
Identity providers	⚠	Delete all identity providers
User flows	⚠	Delete all user flows
IEF policy keys	⚠	Delete all IEF policy keys
Identity Experience Framework (IEF) policies	✓	--

Conditional Access

Monday, June 20, 2022 11:55 PM

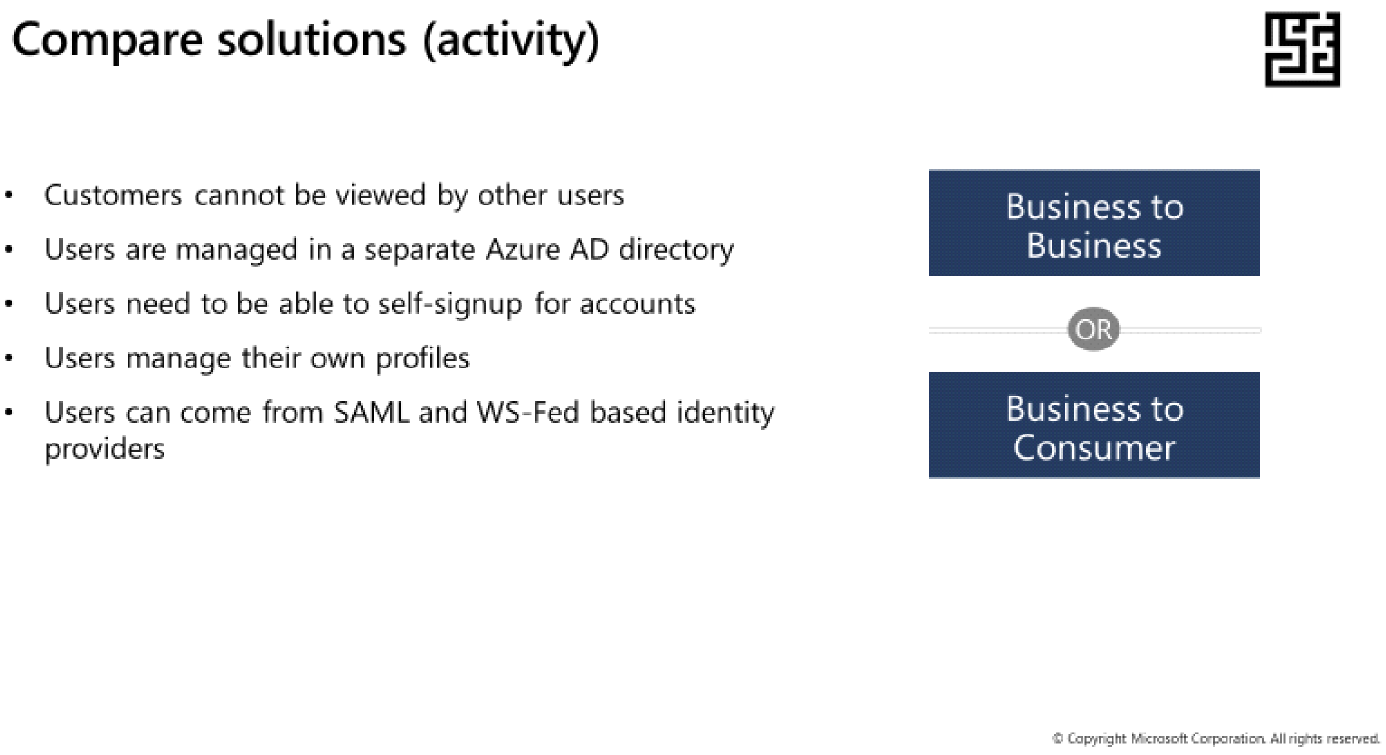
Conditional Access is an Azure AD tool that allows (or denies) access to resources.

- Use to enable multifactor authentication
- Require managed devices
- Access only approved client applications
- Exclude countries from which you never expect a sign in
- Respond to potentially compromised accounts.
- Completely block access
- Block legacy authentication protocols.
- Test using the report-only mode

Labs : Using the location condition in a Conditional Access policy
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Discussion

Monday, June 20, 2022 11:53 PM



Compare solutions (activity)

- Customers cannot be viewed by other users
- Users are managed in a separate Azure AD directory
- Users need to be able to self-signup for accounts
- Users manage their own profiles
- Users can come from SAML and WS-Fed based identity providers

Business to Business
OR
Business to Consumer

Access Review

Tuesday, June 21, 2022 1:38 PM

Tutorial: Manage access to resources in Azure AD entitlement management

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-first

Recommend a network architecture solution based on workload requirements

Sunday, June 26, 2022 9:32 PM

Connectivity services	How to connect to Azure Resource, either within Azure, between Azure and on-perm, or on-perm to on-perm via Azure Virtual Network (VNet), Virtual WAN, ExpressRoute, VPN Gateway, Virtual network NAT Gateway, Azure DNS, Peering service, and Azure Bastion
Application protection services	Services that protect your Azure Services Load Balancer, Private Link, DDoS protection, Firewall, Network Security Groups, Web Application Firewall, and Virtual Network Endpoints
Application delivery services	Azure Services that control the traffic of request/response Content Delivery Network (CDN), Azure Front Door Service, Traffic Manager, Application Gateway, Internet Analyzer, and Load Balancer

Requirements:

- Naming
- Regions
- Subscriptions
- Segmentation
- Security
  - Traffic filtering
  - Traffic routing
- Connectivity
- Permissions
- Policy

Hub and spoke network topology
Subnet vs VNet
Plan IP addressing : Private vs Public vs Private IP in Subnet

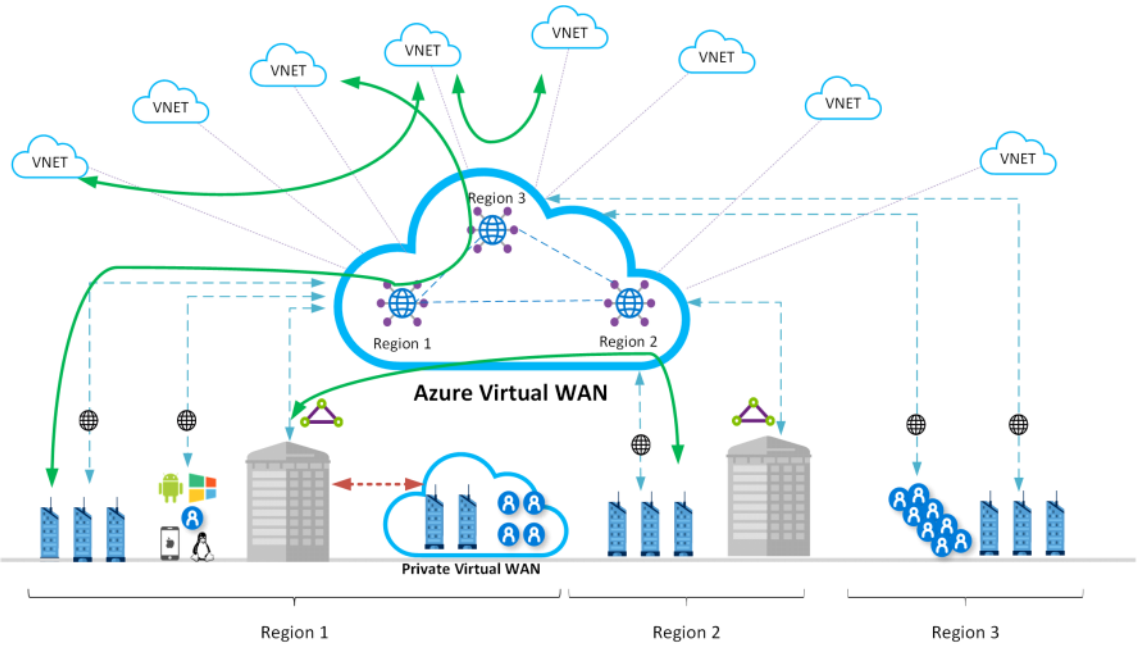
Lab: Filter network traffic with a network security group using the Azure portal
https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic

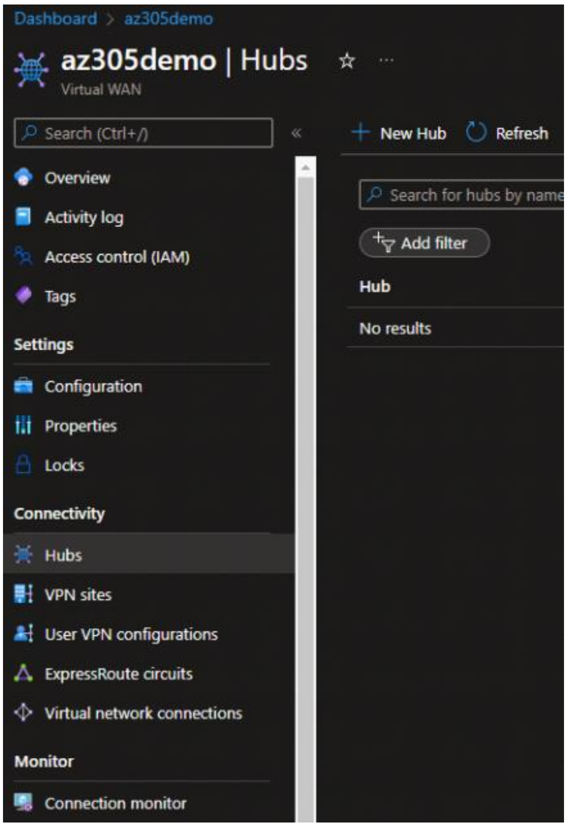
Lab: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources

Design for on-premises connectivity to Azure Virtual Networks

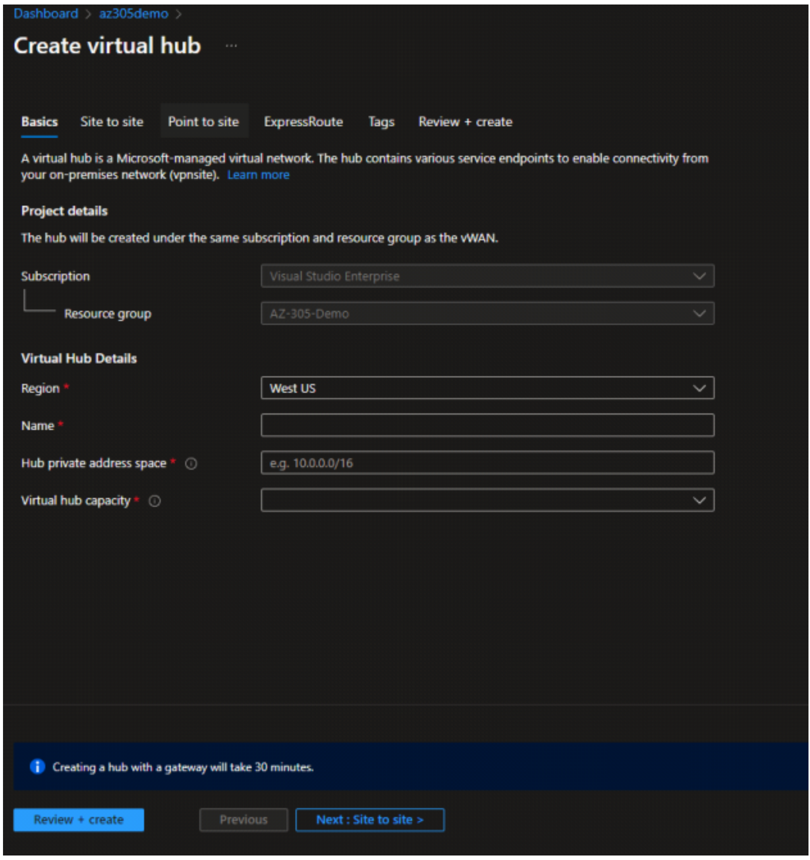
Sunday, June 26, 2022 9:40 PM

- VNet
- ExpressRoute
- ExpressRoute + VPN
- Azure Virtual WAN (Hub-Spoke)
    - Reduce many-to-many mesh network setup





No results



Create virtual hub

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). Learn more

Project details

The hub will be created under the same subscription and resource group as the vWAN.

Subscription: Visual Studio Enterprise

Resource group: AZ-305-Demo

Virtual Hub Details

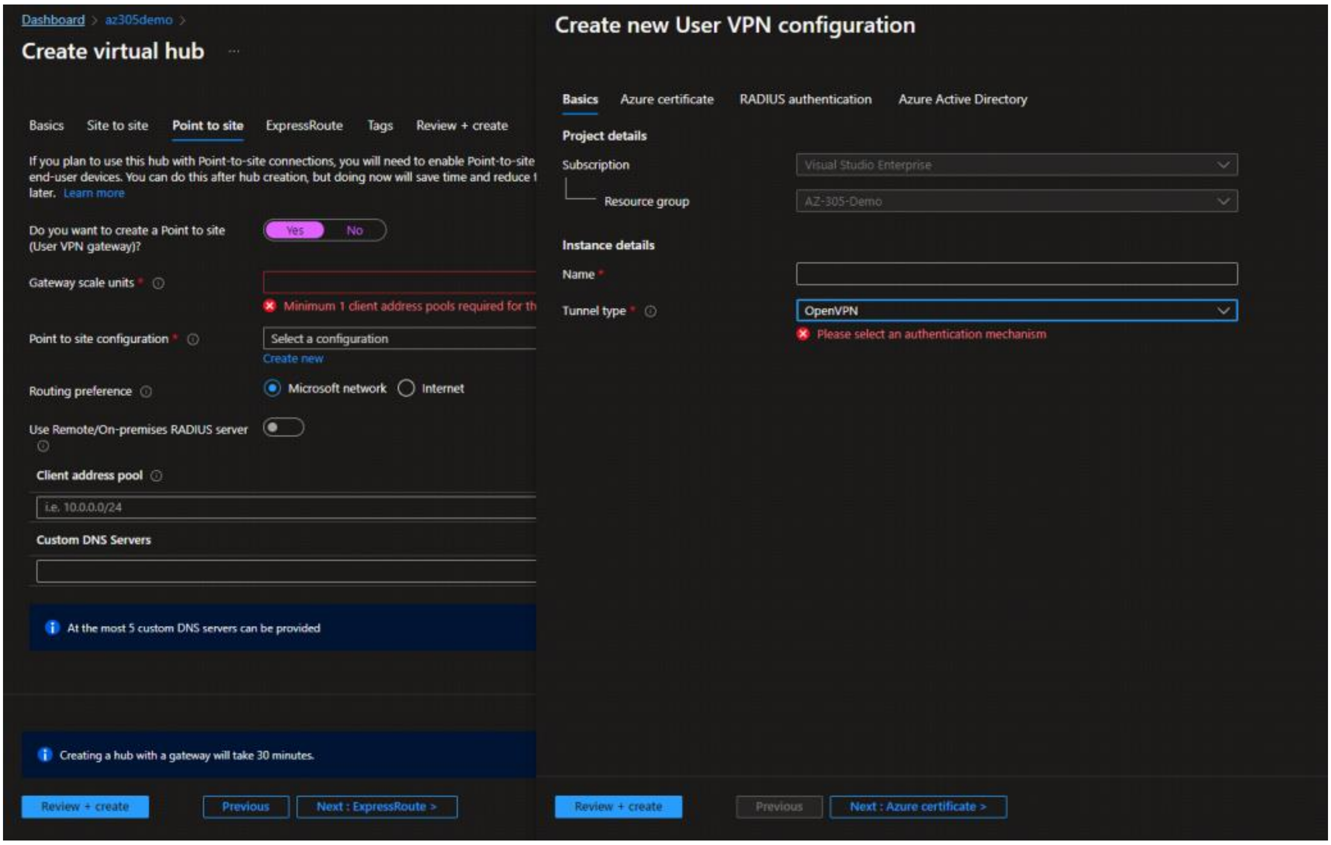
Region *: West US

Name *:

Hub private address space *: e.g. 10.0.0.0/16

Virtual hub capacity *:

Creating a hub with a gateway will take 30 minutes.



Create virtual hub

If you plan to use this hub with Point-to-site connections, you will need to enable Point-to-site end-user devices. You can do this after hub creation, but doing now will save time and reduce t later. Learn more

Do you want to create a Point to site (User VPN gateway)? [✓ Yes] No

Gateway scale units *

Minimum 1 client address pools required for th

Point to site configuration * Select a configuration

Create new

Routing preference ● Microsoft network ○ Internet

Use Remote/On-premises RADIUS server

Client address pool

i.e. 10.0.0.0/24

Custom DNS Servers

At the most 5 custom DNS servers can be provided

Creating a hub with a gateway will take 30 minutes.

Create new User VPN configuration

Project details

Subscription: Visual Studio Enterprise

Resource group: AZ-305-Demo

Instance details

Name *

Tunnel type * OpenVPN

Please select an authentication mechanism

Design for Azure network connectivity services

Sunday, June 26, 2022 9:46 PM

- **Communicate between Azure resources**: You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets.

- **Communicate between each other**: You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions.

- **Communicate to the internet**: All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use Public IP addresses or public Load Balancer to manage your outbound connections.

- **Communicate with on-premises networks**: You can connect your on-premises computers and networks to a virtual network using VPN Gateway or ExpressRoute.

Design network segmentation

- Subscription
- Virtual Network
- Network Security Groups (NSG)
- Application Security Groups (ASGs)
  - An ASG allows you to group a set of VMs under an application tag. Once an ASG is created and VMs are assigned to it, the ASG can be used as a source or target in the NSG to simplify management.
- Azure Firewall

Design network topology

Pattern 1: Single Virtual Network
Pattern 2: Multiple Virtual Networks with peering in between them
Pattern 3: Multiple Virtual Networks in a hub & spoke model

Network capabilities	**Pattern 1**	**Pattern 2**	**Pattern 3**
Connectivity/Routing: how each segment communicates to each other	System routing provides default connectivity to any workload in any subnet	Same as a pattern 1	No default connectivity between spoke virtual networks. A layer 3 router, such as the Azure Firewall, in the hub virtual network is required to enable connectivity.
Network level traffic filtering	Traffic is allowed by default. NSG can be used for filtering this pattern.	Same as a pattern 1	Traffic between spoke virtual networks is denied by default. Azure Firewall configuration can enable selected traffic, such as windowsupdate.com.
Centralized logging	NSG logs for the virtual network	Aggregate NSG logs	Azure Firewall logs to Azure Monitor all accepted/denied traffic that is

		across all virtual networks	sent via a hub
Unintended open public endpoints	DevOps can accidentally open a public endpoint via incorrect NSG rules.	Same as a pattern 1	Accidentally opened public endpoint in a spoke virtual network won't enable access. The return packet will be dropped via stateful firewall (asymmetric routing).
Application level protection	NSG provides network layer support only.	Same as a pattern 1	Azure Firewall supports FQDN filtering for HTTP/S and MSSQL for outbound traffic and across virtual networks.
Connectivity/Routing: how each segment communicates to each other	System routing provides default connectivity to any workload in any subnet	Same as a pattern 1	No default connectivity between spoke virtual networks. A layer 3 router such as the Azure Firewall in the hub virtual network is required to enable connectivity.

Virtual network NAT gateway

Outbound only connectivity

Outbound connectivity is possible without load balancer or public IP addresses directly attached to virtual machines

Choose Virtual Network NAT gateway when

- You need on-demand outbound to internet connectivity without pre-allocation
- You need one or more static public IP addresses for scale
- You need configurable idle timeout
- You need TCP reset for unrecognized connections

Priority of routes

1. User Defined Routes (UDR)
2. BGP (Border Gateway Protocol) routes
3. System routes

Routing

When creating a virtual network peering between two virtual networks, a route is added for each address range within the address space of each virtual network for which a peering is created.

Lab: Connect virtual networks with virtual network peering using the Azure portal
https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal

Lab: Route network traffic with a route table using the Azure portal
https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal

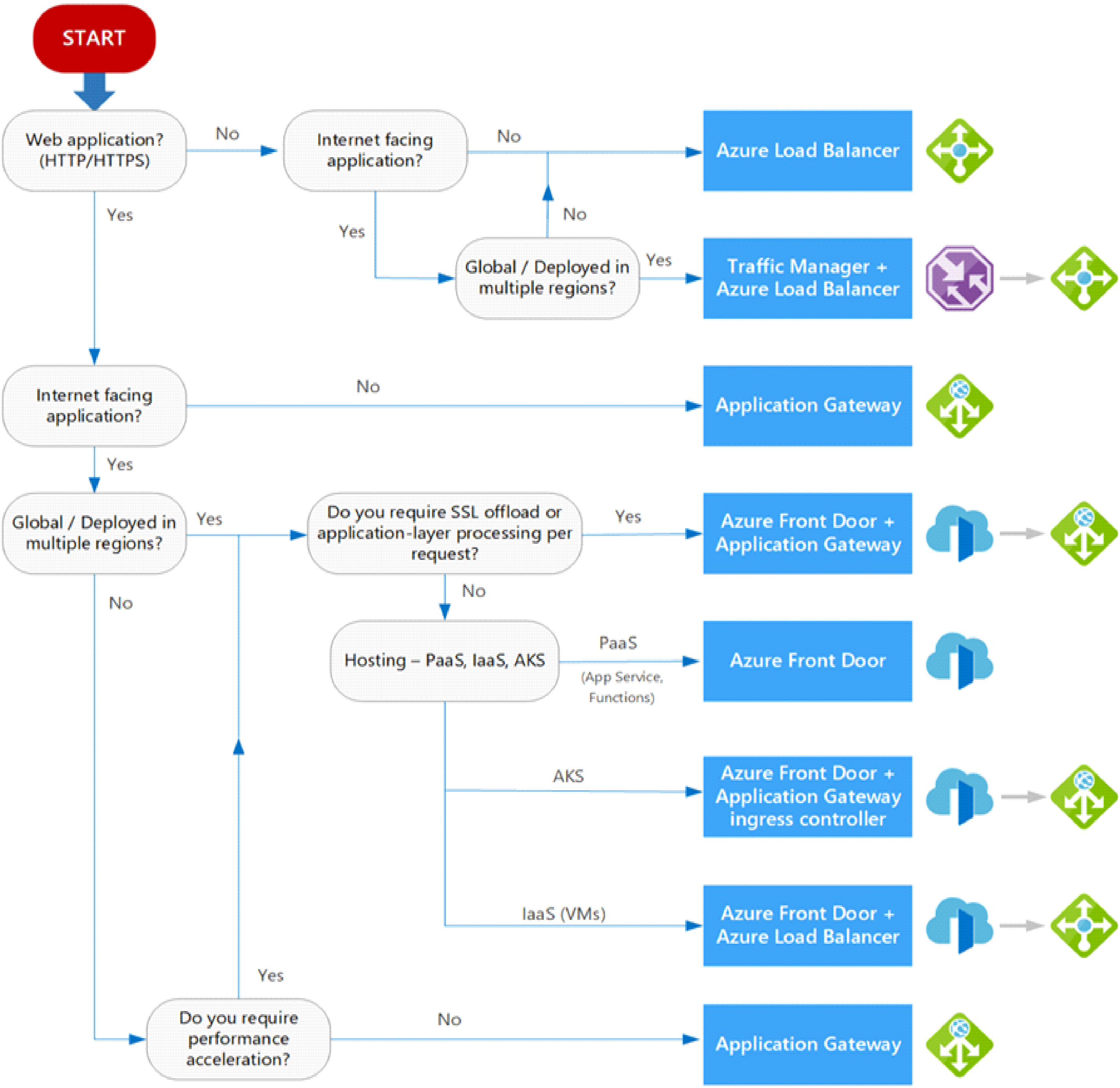
Design for application delivery services

Sunday, June 26, 2022 10:12 PM

Choosing a load balancer solution

Decision criteria

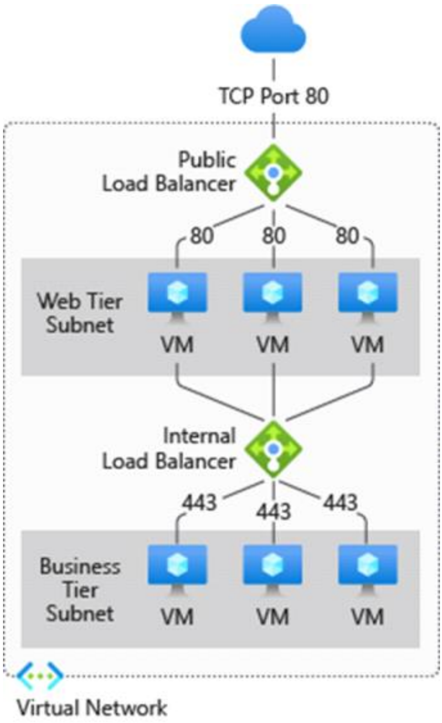
- Traffic type
- Global versus. regional
- Availability
- Cost
- Features and limits


START
Web application? (HTTP/HTTPS)
No
Internet facing application?
No
Azure Load Balancer
Yes
Yes
No
Global / Deployed in multiple regions?
Yes
Traffic Manager + Azure Load Balancer
Internet facing application?
No
Application Gateway
Yes
Global / Deployed in multiple regions?
Yes
Do you require SSL offload or application-layer processing per request?
Yes
Azure Front Door + Application Gateway
No
No
Hosting – PaaS, IaaS, AKS
PaaS
(App Service, Functions)
Azure Front Door
AKS
Azure Front Door + Application Gateway ingress controller
IaaS (VMs)
Azure Front Door + Azure Load Balancer
Yes
Do you require performance acceleration?
No
Application Gateway

Load Balancer

Sunday, June 26, 2022 10:15 PM

- Layer 4 load-balancing for all UDP and TCP protocols
- Manages inbound and outbound connections
- Provides public and internal load-balanced endpoints
- Uses rules to map inbound connections to backend destinations
- Health probes manage service availability
- Single Region
  - This is not the same as Cross-region load balancer (Preview) https://docs.microsoft.com/en-us/azure/load-balancer/cross-region-overview

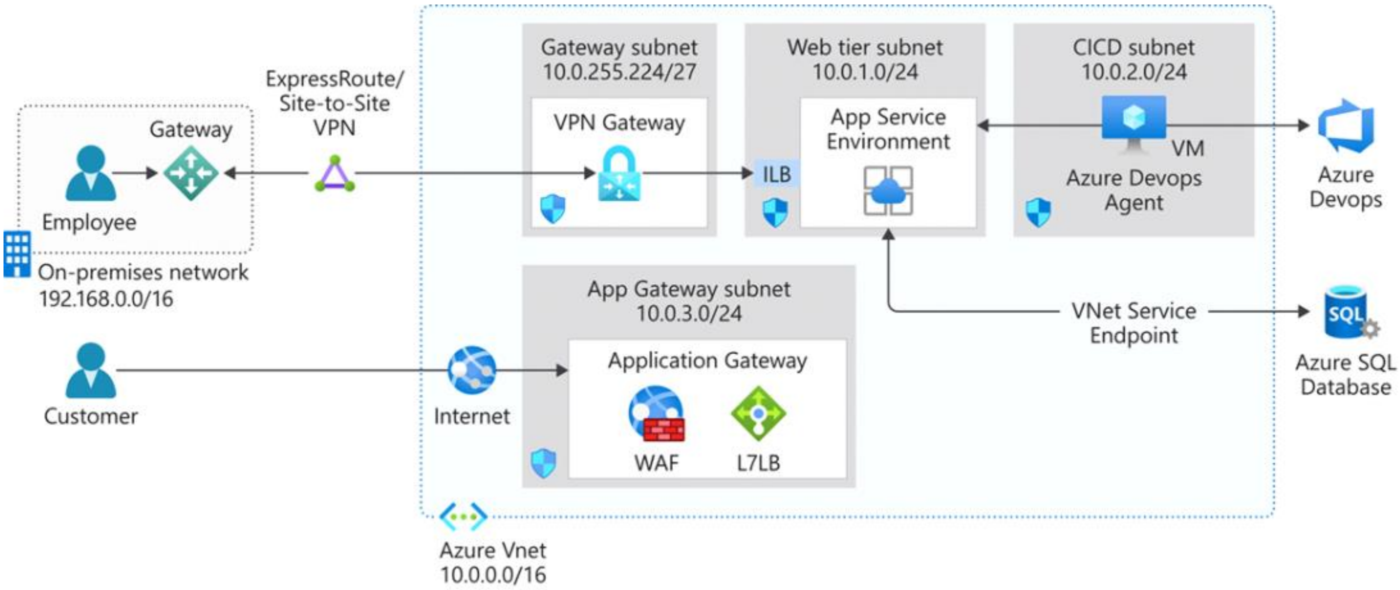


Application Gateway

Sunday, June 26, 2022 10:20 PM

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. It is an Application Delivery Controller (ADC) as a service, offering various layer 7 load-balancing capabilities for your applications.

- Layer 7 - HTTP(s) only
- Supports WAF -stateful inspection
- Traffic routing
- SSL/TLS termination
- Supports PaaS (Ignore this one, PaaS should use FrontDoor) and Ips
- Regional service

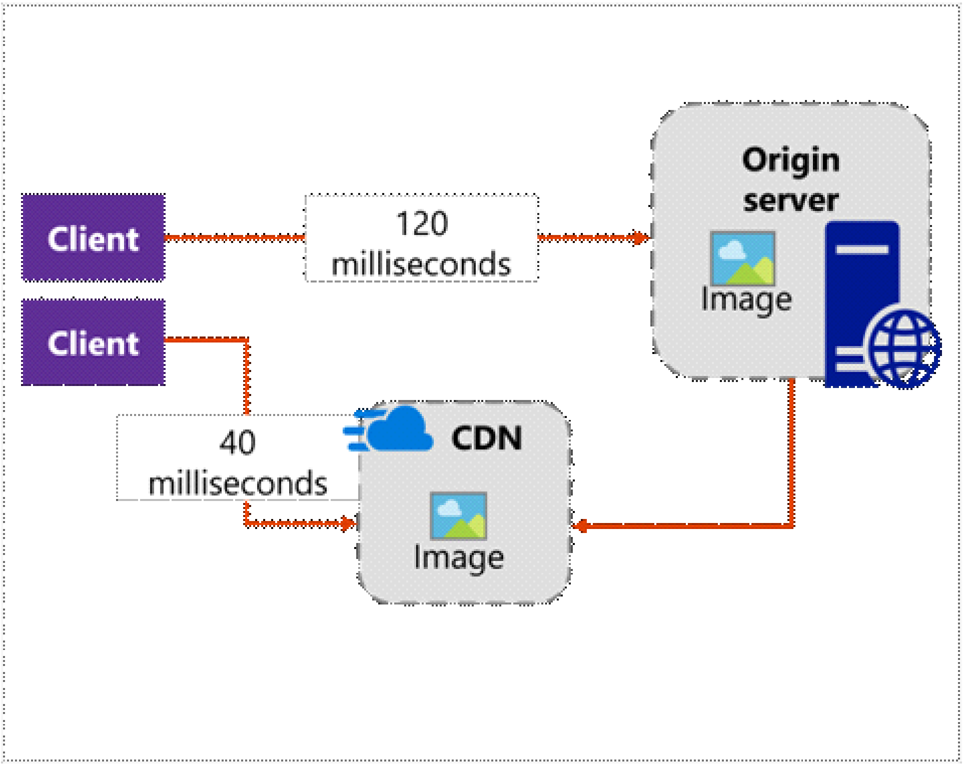


Content Delivery Network

Sunday, June 26, 2022 10:23 PM

Azure CDN offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world.

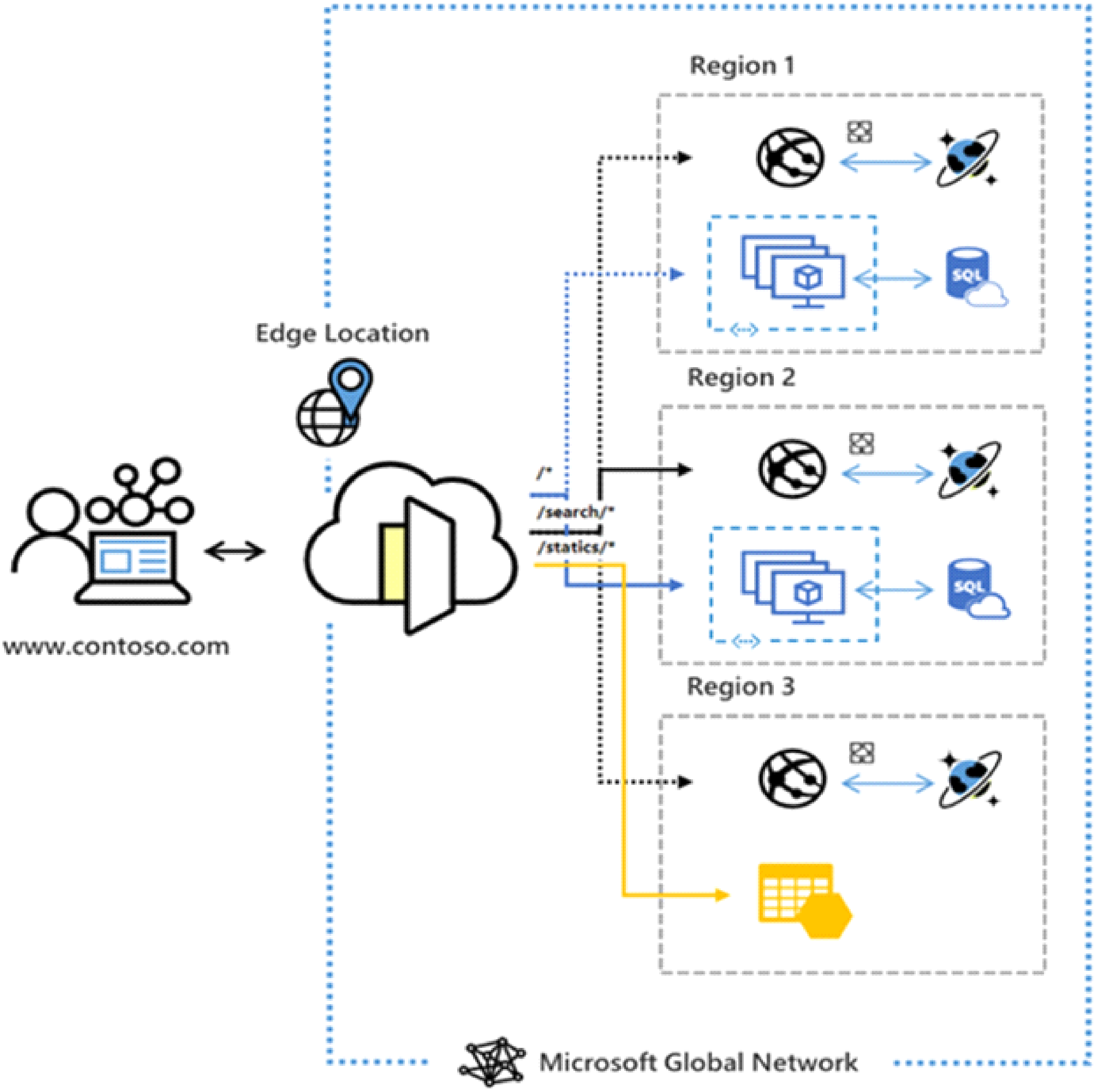
- You want point-of-presence locations that are close to large clusters of users.
- You want to reduce latency - both the transmission delay and the number of router hops.
- You want custom domains, file compression, caching, and geo-filtering.



Azure Front Door

Sunday, June 26, 2022 10:24 PM

- You need to ensure that requests are sent to the lowest latency backends (low latency)
- You have primary and secondary backends (priority)
- You want to distribute traffic using weight coefficients (weighted)
- You want to ensure requests from the same end user gets sent to the same backend (affinity)
- Your traffic is HTTP(s) based and you need WAF and/or CDN integration
- ***Path base routing***

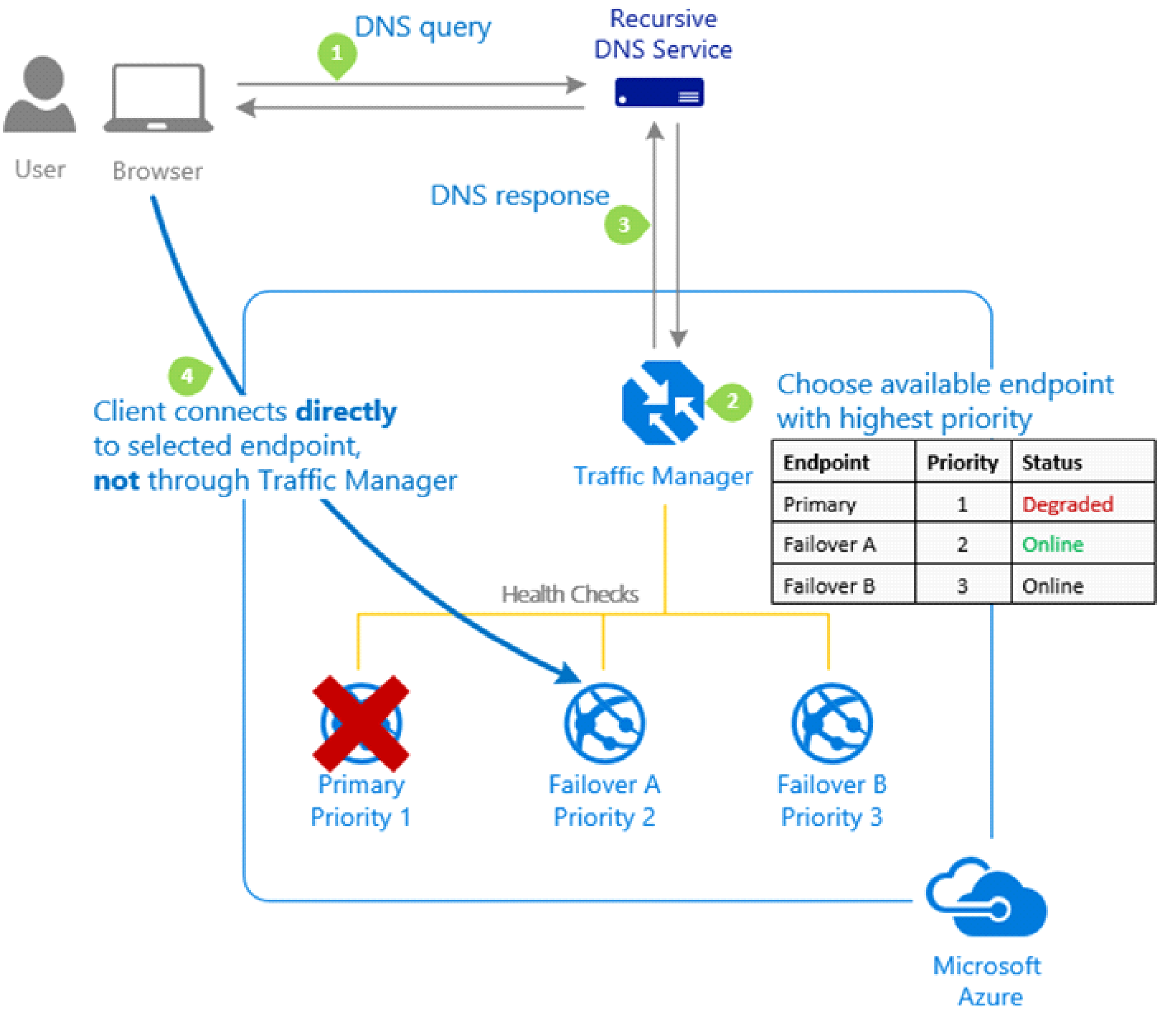


Traffic Manager

Sunday, June 26, 2022 10:27 PM

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions. Traffic Manager provides a range of traffic-routing methods to distribute traffic such as priority, weighted, performance, geographic, multi-value, or subnet.

- To increase application availability
- Improve application performance
- Combine hybrid applications
- Distribute traffic for complex deployments



Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

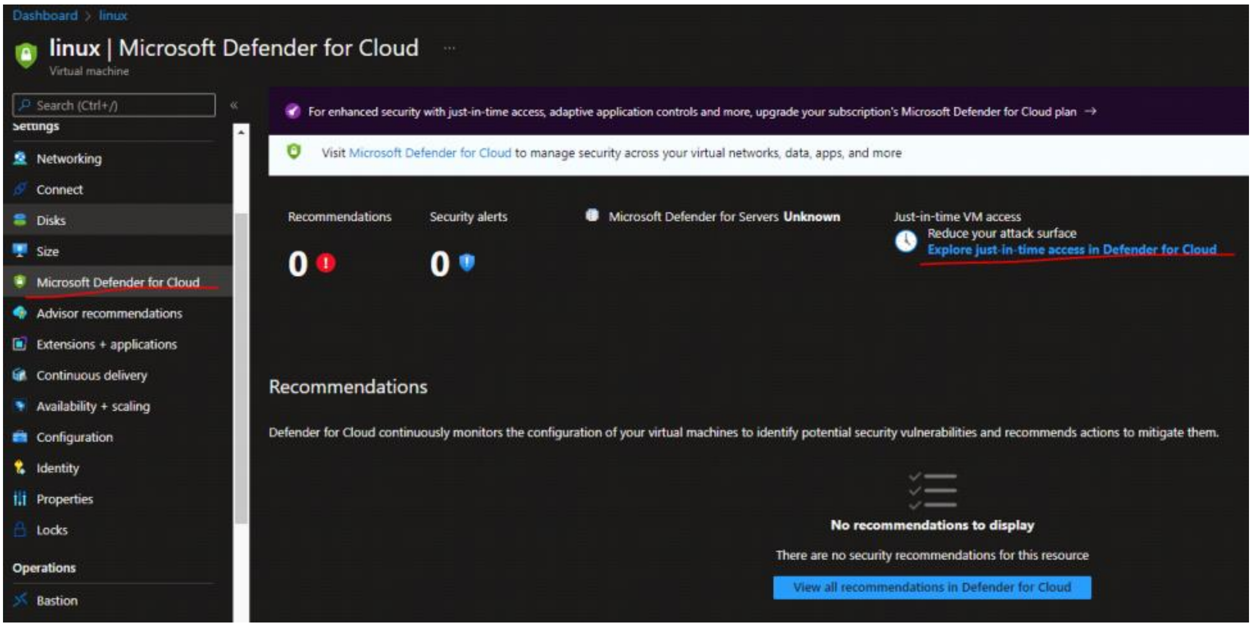
Design for application protection services

Sunday, June 26, 2022 10:29 PM

Please refer to PowerPoint. There are already points that help you to make the decision

- Service endpoints
- Azure Private Link
- Network security groups (NSG)
- Azure Firewall
  - Premium Feature https://docs.microsoft.com/en-us/azure/firewall/premium-features?WT.mc_id=Portal-Microsoft_Azure_HybridNetworking
  - TLS inspection - decrypts outbound traffic, processes the data, then encrypts the data and sends it to the destination.
  - IDPS - A network intrusion detection and prevention system (IDPS) allows you to monitor network activities for malicious activity, log information about this activity, report it, and optionally attempt to block it.
  - URL filtering - extends Azure Firewall's FQDN filtering capability to consider an entire URL. For example, www.contoso.com/a/c instead of www.contoso.com.
  - Web categories - administrators can allow or deny user access to website categories such as gambling websites, social media websites, and others.
- Web Application Firewall
- DDoS Protection
- Azure Bastion
- Just in Time (JIT) Network Access
  - Requires Azure Defender licensing for Azure Defender

- **Azure Firewall alone**
  - when there are no web applications in the virtual network.
- **Application Gateway alone**
  - when there are only web applications in the virtual network, and network security groups (NSGs) provide sufficient output filtering.
- **Azure Firewall** and **Application Gateway** in parallel
  - the most common design, when you want Azure Application Gateway to protect HTTP(S) applications from web attacks, and Azure Firewall to protect all other workloads and filter outbound traffic.
- **Application Gateway** in front of **Azure Firewall**
  - when you want Azure Firewall to inspect all traffic and WAF to protect web traffic, and the application needs to know the client's source IP address.
- **Azure Firewall** in front of **Application Gateway**
  - when you want Azure Firewall to inspect and filter traffic before it reaches the Application Gateway.



For enhanced security with just-in-time access, adaptive application controls and more, upgrade your subscription's Microsoft Defender for Cloud plan →

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations 0

Security alerts 0

Microsoft Defender for Servers **Unknown**

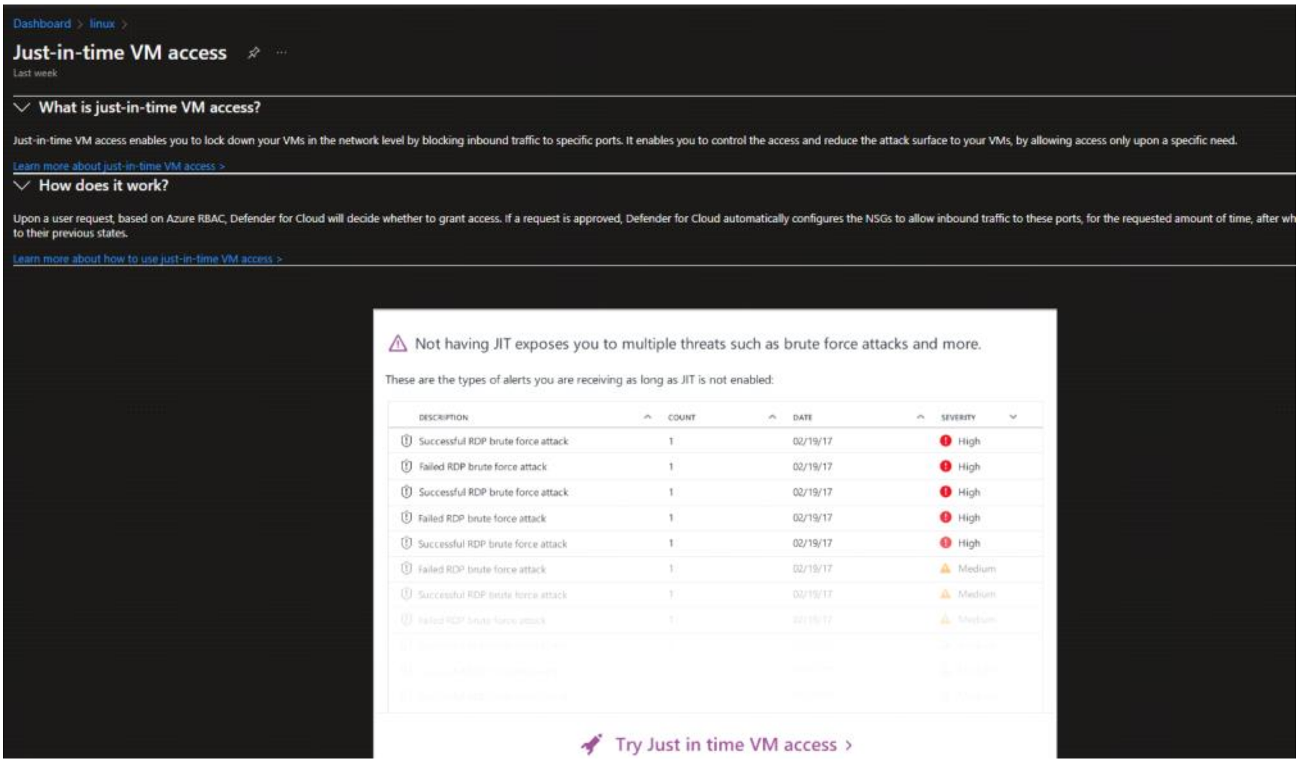
Just-in-time VM access
Reduce your attack surface
Explore just-in-time access in Defender for Cloud

Recommendations

Defender for Cloud continuously monitors the configuration of your virtual machines to identify potential security vulnerabilities and recommends actions to mitigate them.

No recommendations to display

There are no security recommendations for this resource



What is just-in-time VM access?

Just-in-time VM access enables you to lock down your VMs in the network level by blocking inbound traffic to specific ports. It enables you to control the access and reduce the attack surface to your VMs, by allowing access only upon a specific need.

Learn more about just-in-time VM access >

How does it work?

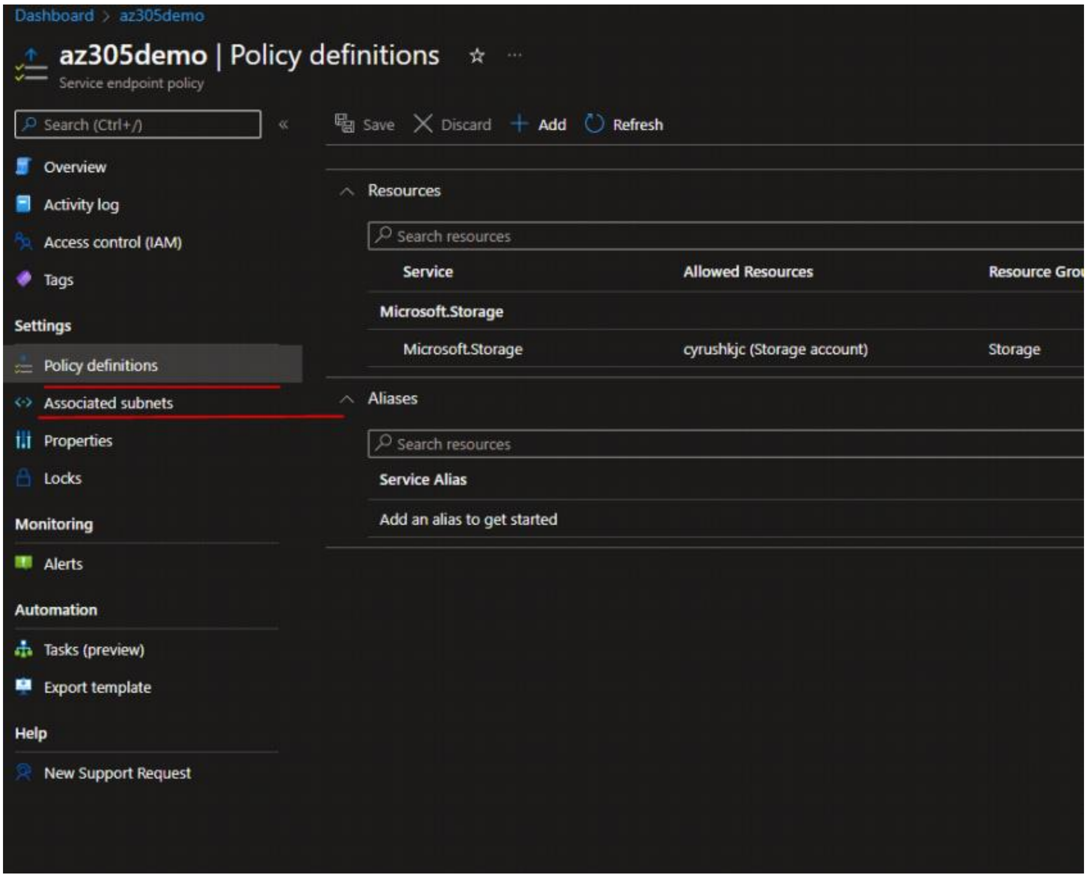
Upon a user request, based on Azure RBAC, Defender for Cloud will decide whether to grant access. If a request is approved, Defender for Cloud automatically configures the NSGs to allow inbound traffic to these ports, for the requested amount of time, after wh
to their previous states.

Learn more about how to use just-in-time VM access >

Not having JIT exposes you to multiple threats such as brute force attacks and more.

These are the types of alerts you are receiving as long as JIT is not enabled:

DESCRIPTION	COUNT	DATE	SEVERITY
Successful RDP brute force attack	1	02/19/17	High
Failed RDP brute force attack	1	02/19/17	High
Successful RDP brute force attack	1	02/19/17	High
Failed RDP brute force attack	1	02/19/17	High
Successful RDP brute force attack	1	02/19/17	High
Failed RDP brute force attack	1	02/19/17	Medium
Successful RDP brute force attack	1	02/19/17	Medium
Failed RDP brute force attack	1	02/19/17	Medium



Service	Allowed Resources	Resource Grou
Microsoft.Storage		
Microsoft.Storage	cyrushkjc (Storage account)	Storage