## Infrastructure as a Service (laaS)c

### Virtual Machines

### **Availability Set**

- 2 fault domains for classic
- 3 fault domains for Resource Manager deployments

### • 5 update domains Scale Set

- Max 100 VMs
- Max 1000 VMs with placement groups (auto scale) Managed disks needed for large scale sets

### VM Series

- Compute optimised
- D,E,G Memory optimised Storage optimised
- Graphic GPU optimised High performance computing
- Join VMs to domain
- Enable Azure AD Domain Services

## Hybrid Applications

## **Relay Service**

- Hybrid Connections • Establish a rendezvous point in the cloud On-prem app connects using HTTP/ Sockets to cloud
- WCF Relays (Service Bus Relays)
- On-prem app uses WCG bindings to connect to Srv Bus

## App Service Hybrid Connections

## Connects Azure and on-prem applications using TCP

Part of App Service and is a separate Azure feature

## **AD Application Proxy**

### Access on-prem web apps from the cloud

- Provides single sign on (SSO) + secure remote access
- Connector lightweight agent on on-prem server External endpoint – direct URL or access via MyApps

- Connect to ML, HDInsight, Data Lake Analytics Data sent over HTTP using certificates
- No firewall ports need to be opened

- Access services within same VNet (VMs. DBs. ...)

- Uses Service Bus
- Azure -> Analytics, Logic Apps, Flow, Power Apps,

### Provides central repository

### One catalog per tenant

• Sources – Blob Storage, Data Lake, QL Server, Oracle, .

## **SQL** Data Warehouse

## Massive Parallel Processing (MPP)

 Uses Hadoop/Spark and Machine Learning for insights Uses Data Movement Service (DMS) between nodes

## **Analysis Services**

Same architecture as SQL Server Analysis • Enterprise grade data modelling in the cloud

## SQL Database

### Relational database

- Elastic Database Pools (eDTUs) Individual databases (DTUs)
- High availability, geo-replication, failover groups
- Backup and Recovery Basic – 7 days retention Standard and Premium – 35 days
  Restore - Point-in-time, deleted DB, Geo, and Az
- Recovery Vault
- **SQL Server Stretch Database** • Move or archive cold data from on-premises SQL Server to

## **High Performance Compute**

## **HPC Workload Series**

- Graphic GPU optimised High performance computing **HPC Pack**

### • Windows Server 2012, 2016, and Linux Create HPC clusters on-prem

- Cloud-native HPC solution
- HPC head node and compute nodes Virtual Machine Scale Sets (VMSS)
- VMs using RDMA are placed in same VMSS
- Virtual Network Azure Blob Storage for node disks
- lybrid HPC solution
- + ExpressRoute to connect cloud with on-prem + VPN Gateway endpoint between cloud and on-prem

## **Data Management Gateway**

- Create workflows to automate data move + transform

## App Service VNet Integration

### nables access from app to other services

- Deploy app inside a VNet

## On-Premise Data Gateway

## Bridge between on-prem data sources and Azure

## Scalable Data Implementations

## Data Catalog

## Cloud Service for big data processing and analytics

### Data pipelines, activities, datasets, linked services, triggers,

pipeline ru, parameters, control flow Available in - East US, East US2, West Europe

Data Factory

### Big data storage and analytics service

 Based on Hadoop Yes Another Resource Negotiator (YARN • Solutions - Store, Analytics, and HDInsights

Data Lake

• Storage repository for big data workloads • Unlimited structured, semi-, and unstructured data

- Uses serverless approach • Pas-as-you-go, monthly commitment
- Uses U-SQL to analyse the data

- Deploys Hadoop components in form of clusters in cloud
- Opensource service for analysing and processing data Apache Hadoop, Spark, HBase, Storm, Kafka, Interac Microsoft R Server

## MySQL

- Open source relational database
- Used by PHP developers, CMS WordPress ACID, replication, Performance, security, extensibility,
- concurrency, JSON support
- Basic 1TB, 4 CPUs, locally redundancy
- General Purpose 1TB, 4 CPUs, local+geo redundancy Memory Optimised – 1TB, 5 CPUs, local+geo red.

## **PostgresSQL**

### pen source relational database

 Open Source, ACID, Replication, Performance, Security, Concurrency, JSON, JSON Indexing, EXtensibility

## Web Apps

## **App Service Plans**

### Free and Shared

## Up to 3 instances (manual)

### Standard Up to 10 instances (auto scale)

- 5 Slots Daily backups
- Azure Traffic Manage
- Premium
- Up to 20 instances (auto scale)
- 20 Slots
- Daily backups Azure Traffic Manage

## solated

 App Service Environment (ASE) – scalable, secure • Up to 100 instances/plan or 100 plans with one instance

## Scalability

- Select different (better) Service Plan
- Scale out Web App manually or automatically

Cache static content to multiple regions

## Content Delivery Network (CDN)

Ideal for development, testing, and non-critical work

### Standard

- No SLA
- Ideal for production and cost effective

- High availability SLA
- Redis persistence

## Traffic Manager

 Performance, Weighted, Priority, Geographic Handle load & locate closest geo region at DNS level

## Multiple programming languages ASP.NET, Core, Angular, React.js Securing Web API

- Active Directory Federated Services (ADFS)

- Create workloads > 53GB

## Web APIs

## Redis Cache

- Data replication between two nodes

## · Ability to isolate

- Azure AD B2C with Facebook and Google providers
- API Management policies, API keys, throttlin

## Functions

### Serverless compute service

Event-driven actions and triggersHTTP-based API endpoints (HTTP triggers)

### Timer triggers

Programming LanguagesC#, F#, Node.js, Java, PHP, PowerShell, Batch, JavaScript,

## Python, Typescript

### Consumption App Service Plan (cost effective) Other App Service Plans

## API Management

### Service that exposes different apps as APIs API Gateway

### Bridge between app and outside world

### Enhanced security, policies, authentication Caching, throttling

**API Management Portal** 

### Package APIs into open or protected products **Developer Portal** Developers can access APIs and documentation

## Logic Apps

**Workflow Driven** Integration with cloud and on-prem services

## • Role Based Access Control (RBAC)

Orchestration

## **Cloud DevOps Ready**

### Use containers to develop and deploy Decouple application from infrastructure

Orchestration Platform

### Cloud and on-prem Container orchestration

- Application developer (creates applications) Application administrator (creates config & packages) · Operator (deploys, monitors, maintain

# **Architecting Microsoft Azure Solutions** 1/3

# Storage Solutions

Access tiers

Classic, does not support latest features.

Replication (X redundant storage)

Locally – 3 copies within data center

Storage and Replication General-purpose v1

Blob storage

General-purpose v2 Newest, that combines v1 and blob storage Latest features at a reduction in costs

Same features as storage v2 acc, but only block blobs.

• Zone – US East 2 and US Central, 3 datacenter copies

## File Storage

Create file shares in the cloud Access with Server Massage Block (SMB) protocol

Cached fast access on Win Server using Azure File Sync

## StorSimple

ntegrated storage spanning on-rem an cloud StorSimple Virtual Array

Leased physical device

 Hyper-V 2000 R2 and VMWare 5.5 iSCSI server (AN) or File Server (NAS). StorSimple 8000 Series

## Cosmos DB Storage

**Premium Azure Table Storage**  Multi-model and globally distributed database • Low latency, high availability, high performance

• SQL, MongoDB, Gremlin (Graph), Table, Cassandra

Virtual Appliance Manager replicates data to cloud

## Blob Storage

Jnstructured data – VHDs, images, audio, etc.

• Hot – optimised for frequently accessed data

Max 1TB page blob, 200GB block blob

### • Cool – Suitable for backups and not often viewed data Archive – set at blob level, cannot be read or modified

- Table Storage

### Queue Storage

nchronous processing of mess;

Semi-structured, non-relational data

Access via OData and LINA queries

Max 500TB data

### REST.API supports GET, PUT, and PEEK Messages max 64KB and max 7days lifetime

## Disk Storage Used for VMs stored in Az Blob storage as page blobs. Standard – unmanaged HDD disk drives. LRS and GRS

• Premium – SDD, high-performance disk support

## Search

### Text search, analysis, and linguistic analysis Free, Basic, Standard S1/S2/S3/HD

Rich search experience over Azure storage

SQL Database, CosmosDB, Blob Storage

## Virtual Network

### Subnets • Max 1000 subnets per VNet • Max 10 VNet connections (peering) per subscription

Max 50 VNets per subscription

### Max 20 public static addresses per subscription Private Address Max 4096 private addresses per VNet

• Max 60 public dynamic addresses per subscription

• DNS for multiple VNets requires own DNS server

Traffic Manager

Pubic Address

**VNets** 

Traffic management DNS level

### oad balancing Use with load balancer for high-avail and high-per

VMs, Cloud Service, Web Apps, and external endpoints

**Network Security** 

 Network Security Groups (NSG) User Defined Routes (UDR) Firewalls

**User Defined Rules** 

**Network Security Groups**  Inbound and outbound rules Checked between VMs, VNets, and other services Applied to one or more subnets or network interfaces

Low order numbers are higher priority

### • Create UDRs & IP forwarding by creating a routing table Virtual Network Service Tunneling • Force external traffic through a site-to-site VPN tunnel **Web Application Firewall**

- Part of Application Gateway and based on OWASP 3.0 Can protect max 20 applications behind an App G/W • Examples: SQL Injection, Cross-Site Scripting, Bots,

### Containers

- Azure Container Instances (ACI) • One ACI = one Docker conainer
- Short-running workloads

### Azure Container Services (AKS)

Serverless and Microservices

- Load balancing
- Long running workloads

## Deployments vs Migrations

## Cloud Infrastructure Ready

## Host on VMs as-is

### **Cloud Optimised** Modernise mission critical application

### Service Fabric

- Lifecycle Management Service developer (creates microservices)

## Networking

oad Balancing Transport Layer 4 Any protocol

### Azure VMs and Cloud service endpoints VNet: Internet and internal facing Endpoint monitoring: Supported via probes

DNS level

 Application level 7 HTTP and HTTPS

### **Azure VPN** VpnGw1 – max 30 site-site, 128 point-site, avg 650Mbps

### Internet Key Exchange (IKE) management protocol Point-to-site

### ExpressRoute Any-to-Ant (IPVPN) – provider sets up secure connection

- AJATO Transformations Limited | 2018.09 | github.com/wpschaub/Quick-Reference-Posters

## **Load Balancer**

## • Standard ... up to 1000 VMs, HA ports, and NSG.

## Application Gateway

• VNet: Any public or internal IP address • Endpoint monitoring: Supported via probes SSL off loading to avoid costly decryption

## **External Connectivity**

### • VpnGw2 – max 30 site-site, 128 point-site, avg 1Gbps • VpnGw3 – max 30 site-site, 128 point-site, avg 1.25Gbps Site-to-site

### VNet-to-Vnet Max 10 VNet connections (peering) per subscription

## Securing Resources

## **Active Directory**

- Directory and identity management
  Plans Free (no SLA, 500k objects), Basic, Premium P1/P2
  Protocols OAuth 2.0, OpenID Connect
- Work and school accounts
- Azure Active Directory Library (ADAL)
- Endpoint V2
- Work, school, and personal accounts
  Microsoft Authentication Library (MSAL)
- Microsoft Graph

## Connects multi services and provides single endpoint AAD is integrated in Microsoft Graph

## AD Federation Services

### Authentication provider for external users to on-prem

- WEB SSO for federated users accessing on-prem apps, using Azure AD Connect
- Web Services (WS) WS-Federation compatible
   No external user account management own credentials
- using Security Assertion Markup Language (SAML) • Install on-prem of Azure VM and use MS Graph.

## Multi-Factor Authentication

### Two step verification (MFA)

- Have phone, verification app, 3<sup>rd</sup> party OAuth tokens

## **AD Connect**

### Synchronise on-prem AD identities with Azure

- AAD password hash synchronisation
- User passwords hashes synched between AD and AAD Hash synched with any change

- Provides single sign-on (SSO)
  AAD pass-through authentication
  Passwords are not synchronised, but validated on-prem
  Provides single sign-on (SSO)

## AD Business to Consumer B2C

## Cloud identity management for mobile and web apps • Leveraged using MSAL

- Social Accounts Facebook, Google, LinkedInn
- Enterprise Accounts OpenID Connect, SAM
- Local accounts email/user and password App must be registered inside Azure B2C tenant

## AD Business to Business B2B

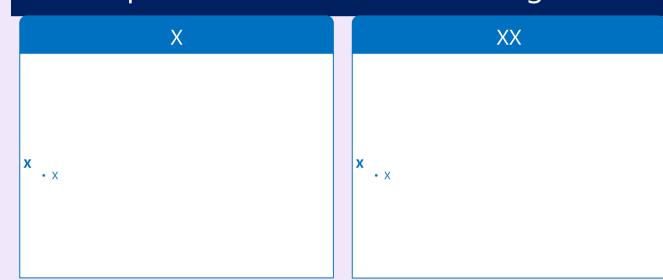
- Enables organizations to work safely with others

   Enabled by default for all AAD tenants

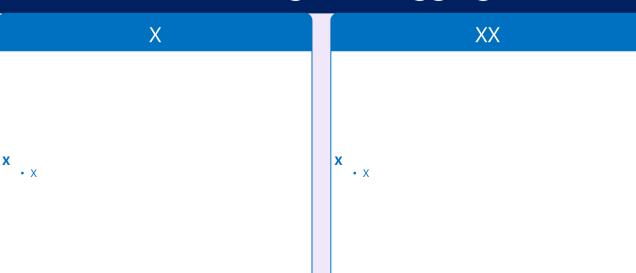
   Integrated with Office 365

   AD Premium Features requires license ration of 5:1
- Every AS Premium licence = five external users Set conditions for users, for example, enforce MFA
- Use policies to delegate permissions

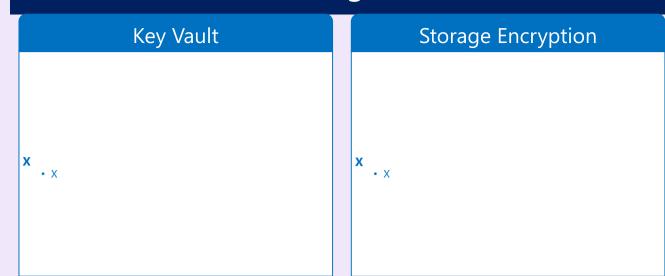
## **Operations Automation Strategies**

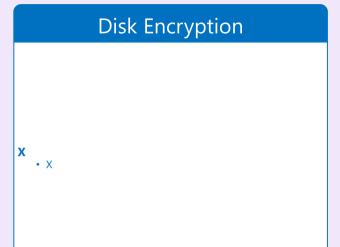


# Monitoring and Logging

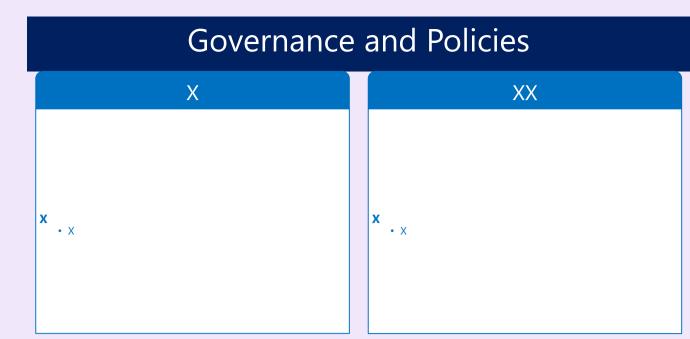


## Securing Data

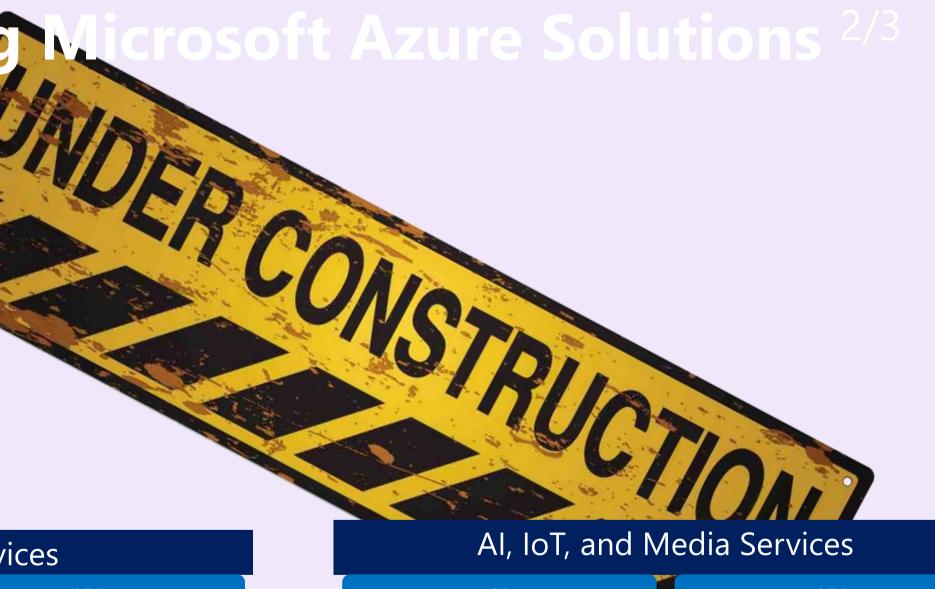




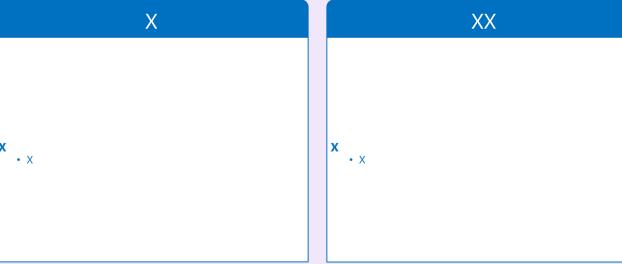


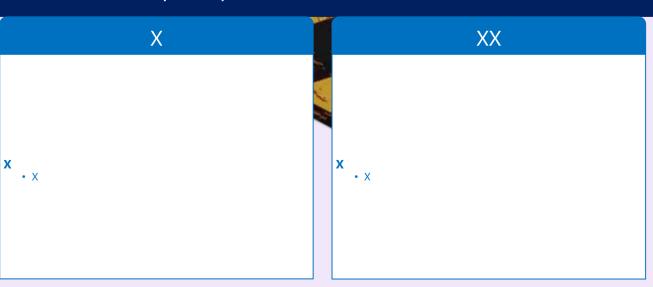


**AD Managed Service Identity** 

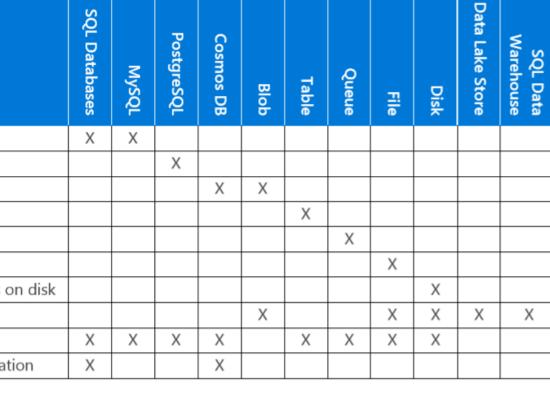


# Messaging Services





Storage Options	SQL Databases	MySQL	PostgreSQL	Cosmos DB	Blob	Table	Queue	File	Disk	Data Lake Store	SQL Data Warehouse
Relational data	Х	Χ									
Object-relational data			Χ								
Unstructured data				Χ	Χ						
Semi-structured data						Х					
Queue messages							Х				
Files on disk								Х			
High-performance files on disk									Х		
Store large data					Χ			Х	Х	Х	Х
Store small data	Х	Х	Χ	Χ		Х	Χ	Х	Х		
Geographic data replication	Х			Х							





Azure Service Bus Queues	Azure Storage Queues			
Message lifetime >7 days	Message lifetime <7days			
Guaranteed (first in–first out) ordered	Queue size >80 GB			
Duplicate detection	Transaction logs			
Message size ≤1 MB	Message size ≤64 KB			



	Event Grid	Event Hubs	IoT Hub	Topics	Service Bus Queues	Storage Queues
Event ingestion	Χ	X	Х			
Device management			Х			
Messaging	Х	Х	Х	Х	X	Х
Multiple consumers	X	Х	Х	Х		
Multiple senders	Х	Х	Х	Х	X	Х
Use for decoupling		Х	Х	Х	X	Х
Use for publish/subscribe	X					
Max message size	64 KB	256 KB	256 KB	1 MB	1 MB	64 KB

	Azure Container Services	Azure Container Instances	Azure Service Fabric
For production deployments of complex systems (with a container orchestrator)	X		
For running simple configurations (possibly without orchestrator)		X	
For long-running workloads on containers	X		
For short-running workloads on containers		X	
For orchestrating a system based on containers	X		X
Orchestrating with open-source orchestrators ( <u>DC/OS</u> , <u>Docker Swarm</u> , <u>Kubernetes</u> )	×		
Orchestrating with built-in orchestrator			X

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport level (Layer 4)	Application level (Layer 7)	DNS level
Application protocols supported	Any	HTTP and HTTPS	Any (An HTTP endpoint is required for endpoint monitoring)
Endpoints	Azure VMs and Cloud Services role instances	Any Azure Internal IP address or public internet IP address	Azure VMs, Cloud Services, Azure Web Apps, and external endpoints
Vnet support	Can be used for both Internet facing and internal (Vnet) applications	Can be used for both Internet facing and internal (Vnet) applications	Only supports Internet-facing applications
Endpoint Monitoring	Supported via probes	Supported via probes	Supported via HTTP/HTTPS GET

