Architecting Microsoft Azure Solutions 1/3

Infrastructure as a Service (IaaS)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
- A General purpose
- F Compute optimised
- D,E,G Memory optimised
- L Storage optimised
- N Graphic GPU optimised
- H High performance computing

Join VMs to domain
- Enable Azure AD Domain Services

High Performance Compute

HPC Workload Series
- A General purpose
- N Graphic GPU optimised
- H 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

Hybrid HPC solution
+ ExpressRoute to connect cloud with on-prem
+ VPN Gateway endpoint between cloud and on-prem

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

Data Management Gateway

Data-integration service
- Create workflows to automate data move + transform
- Connect to ML, HDInsight, Data Lake Analytics
- Data sent over HTTP using certificates
- No firewall ports need to be opened

App Service Hybrid Connections

Connects Azure and on-prem applications using TCP
- Uses Azure Relay Service
- Part of App Service and is a separate Azure feature

App Service VNet Integration

Enables access from app to other services
- Deploy app inside a VNet
- Access services within same VNet (VMs, DBs, ...)
- TCP or UDP

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

On-Premise Data Gateway

Bridge between on-prem data sources and Azure
- Uses Service Bus
- Azure -> Analytics, Logic Apps, Flow, Power Apps, ...
- On-Prem -> SQL Server, SQL Analytics, SharePoint, ...

Web Apps

App Service Plans

Free and Shared
Basic
- Up to 3 instances (manual)

Standard
- Up to 10 instances (auto scale)
- 5 Slots
- Daily backups
- Azure Traffic Manager

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

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

Scalability

Up
- Select different (better) Service Plan

Out
- Scale out Web App manually or automatically

Content Delivery Network (CDN)

Cache static content to multiple regions

Redis Cache

Basic
- Ideal for development, testing, and non-critical work
- No SLA

Standard
- Ideal for production and cost effective
- Data replication between two nodes
- High availability SLA

Premium
- Redis persistence
- Create workloads > 53GB
- Ability to isolate

Traffic Manager

Routing methods
- Performance, Weighted, Priority, Geographic

Handle load & locate closest geo region at DNS level

Web APIs

Multiple programming languages
- ASP.NET, Core, Angular, React.js

Securing Web API
- Azure AD
- Azure AD B2C – with Facebook and Google providers
- Active Directory Federated Services (ADFS)
- API Management – policies, API keys, throttling, ...

Serverless and Microservices

Functions

Serverless compute service
Event-driven actions and triggers
- HTTP-based API endpoints (HTTP triggers)
- Timer triggers

Programming Languages
- C#, F#, Node.js, Java, PHP, PowerShell, Batch, JavaScript, Python, Typescript

Plans
- 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
- Define custom APIs
- 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
- BizTalk, ...

Containers

Azure Container Instances (ACS)
- One ACI = one Docker conainer
- Role Based Access Control (RBAC)
- Short-running workloads

Azure Container Services (AKS)
- Load balancing
- Orchestration
- Long running workloads

Deployments vs Migrations

Cloud Infrastructure Ready
- Host on VMs as-is

Cloud DevOps Ready
- Use containers to develop and deploy
- Decouple application from infrastructure

Cloud Optimised
- Modernise mission critical application

Service Fabric

Orchestration Platform
- Cloud and on-prem
- Container orchestration

Lifecycle Management
- Service developer (creates microservices)
- Application developer (creates applications)
- Application administrator (creates config & packages)
- Operator (deploys, monitors, maintains)

Scalable Data Implementations

Data Catalog

Provides central repository
- One catalog per tenant
- Sources – Blob Storage, Data Lake, QL Server, Oracle, ...

Data Factory

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

SQL Data Warehouse

Massive Parallel Processing (MPP)
- Uses Hadoop/Spark and Machine Learning for insights
- Uses Data Movement Service (DMS) between nodes

Data Lake

Big data storage and analytics service
- Based on Hadoop Yes Another Resource Negotiator (YARN)
- Solutions - Store, Analytics, and HDInsights

Data Lake Store
- Storage repository for big data workloads
- Unlimited structured, semi-, and unstructured data

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

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

Analysis Services

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

MySQL

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

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 Azure SQL

PostgresSQL

Open source relational database
- Open Source, ACID, Replication, Performance, Security, Concurrency, JSON, JSON Indexing, EXtensibility

Storage Solutions

Storage and Replication

General-purpose v1
- Classic, does not support latest features.

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

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

Replication (X redundant storage)
- Locally – 3 copies within data center
- Zone – US East 2 and US Central, 3 datacenter copies
- Geo – three regional 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

Integrated storage spanning on-rem an cloud
- iSCSI and SMB support

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

StorSimple 8000 Series
- Leased physical device
- Virtual Appliance Manager replicates data to cloud

Cosmos DB Storage

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

APIs
- SQL, MongoDB, Gremlin (Graph), Table, Cassandra

Blob Storage

Unstructured data – VHDs, images, audio, etc.
- Max 1TB page blob, 200GB block blob

Access tiers
- Hot – optimised for frequently accessed data
- Cool – Suitable for backups and not often viewed data
- Archive – set at blob level, cannot be read or modified

Table Storage

Semi-structured, non-relational data
- Suitable for datasets without complex joins
- Access via OData and LINA queries
- Max 500TB data

Queue Storage

Asynchronous processing of messages
- 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 redundancy only.
- Premium – SDD, high-performance disk support

Search

Rich search experience over Azure storage
- SQL Database, CosmosDB, Blob Storage
- Text search, analysis, and linguistic analysis

Tiers
- Free, Basic, Standard S1/S2/S3/HD

Networking

Virtual Network

VNets
- Max 50 VNets per subscription

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

Pubic Address
- Max 60 public dynamic addresses per subscription
- Max 20 public static addresses per subscription

Private Address
- Max 4096 private addresses per VNet

DNS
- DNS for multiple VNets requires own DNS server

Traffic Manager

Traffic management
- DNS level
- Any protocol
- VMs, Cloud Service, Web Apps, and external endpoints
- VNet: Internet facing
- Endpoint monitoring: HTTP/HTTPS GET

Load balancing
- Use with load balancer for high-avail and high-per

Network Security

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

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

User Defined Rules
- 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, ...

Load Balancer

Load Balancing
- Transport Layer 4
- Any protocol
- Azure VMs and Cloud service endpoints
- VNet: Internet and internal facing
- Endpoint monitoring: Supported via probes

Types
- Basic
- Standard ... up to 1000 VMs, HA ports, and NSG.

Application Gateway

Gateway
- DNS level
- Application level 7
- HTTP and HTTPS
- VNet: Any public or internal IP address
- Endpoint monitoring: Supported via probes

SSL
- SSL off loading to avoid costly decryption

Firewall
- Web Application Firewall (WAF)

External Connectivity

Azure VPN
- Basic – max 10 site-site, 128 point-site, avg 100Mbps
- VpnGw1 – max 30 site-site, 128 point-site, avg 650Mbps
- VpnGw2 – max 30 site-site, 128 point-site, avg 1Gbps
- VpnGw3 – max 30 site-site, 128 point-site, avg 1.25Gbps

Site-to-site
- Requires Routing and Remote Access Service (RRAS)
- Internet Protocol Security (IPSec) connection
- Internet Key Exchange (IKE) management protocol

Point-to-site
- Connect IKE2 or Secure Socket Tunneling Protocol (SSTP)
- No RRAS device required

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

ExpressRoute
- Any-to-Ant (IPVPN) – provider sets up secure connection
- Point-to-Point Ethernet –two provider connections
- Co-Located at Cloud Exchange – two cross connections

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

X

X

X

X

High Performance Compute

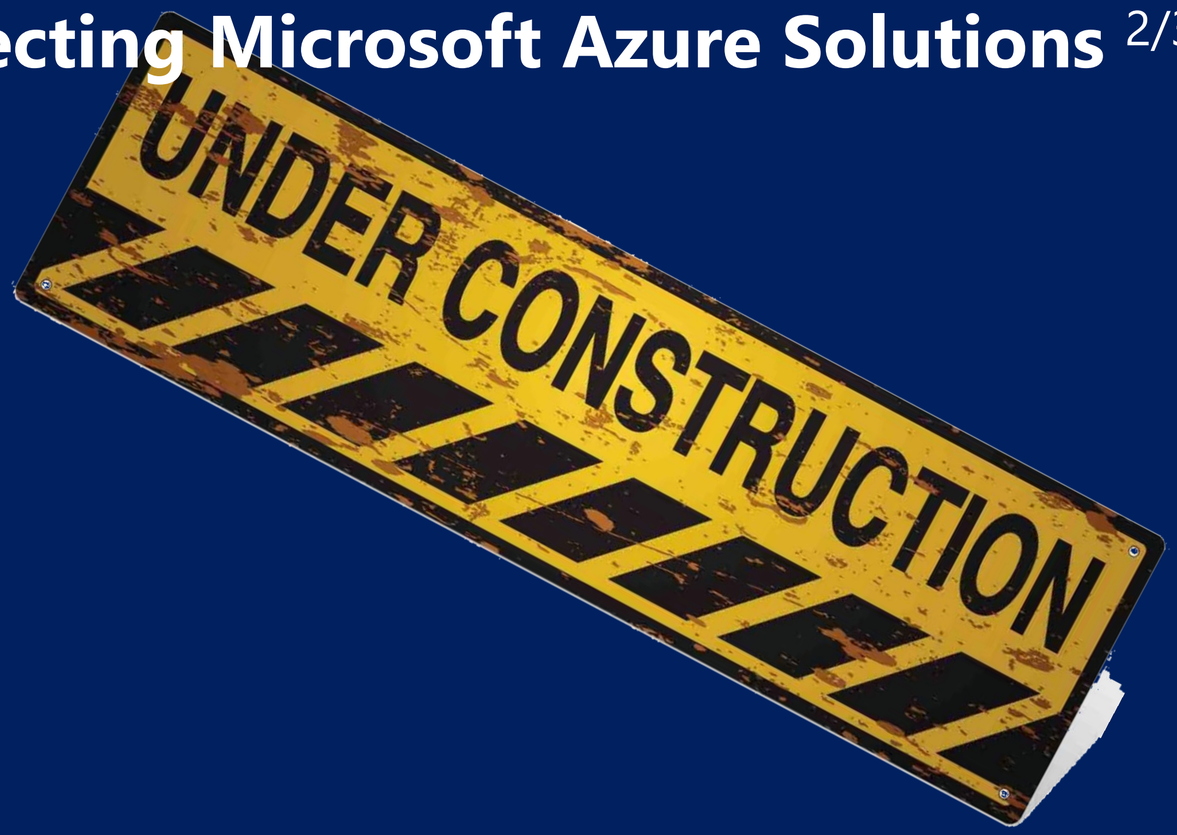
X

High Performance Compute

X

High Performance Compute

Architecting Microsoft Azure Solutions 2/3



Architecting Microsoft Azure Solutions 3/3

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

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	X	X	X			
Device management			X			
Messaging	X	X	X	X	X	X
Multiple consumers	X	X	X	X		
Multiple senders	X	X	X	X	X	X
Use for decoupling		X	X	X	X	X
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 (DC/OS, Docker Swarm, Kubernetes)	X		
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