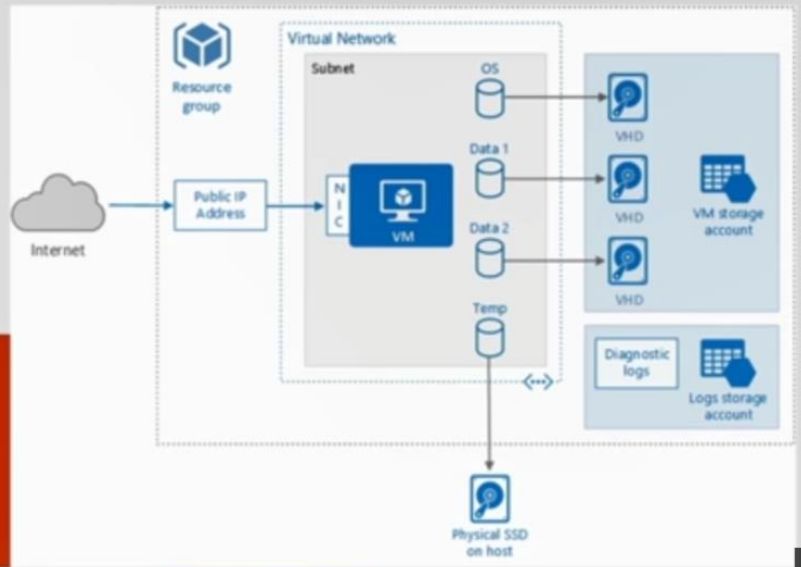
Overview



Management options
- Portal
- PowerShell
- CLI
- REST API

VM Best Practices

Microsoft Ignite

Virtual Machines

ARM Templates Portal

Edit template

Edit your Azure Resource Manager template

Add resource | Quickstart tem... | Download

Parameters (0)

Variables (0)

Resources (0)

```
1 {
2     "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3     "contentVersion": "1.0.0.0",
4     "parameters": {},
5     "resources": []
6 }
```

ARM Template Walkthrough

ARM Templates Portal

Edit template

Edit your Azure Resource Manager template

Add resource | Quickstart tem... | Download

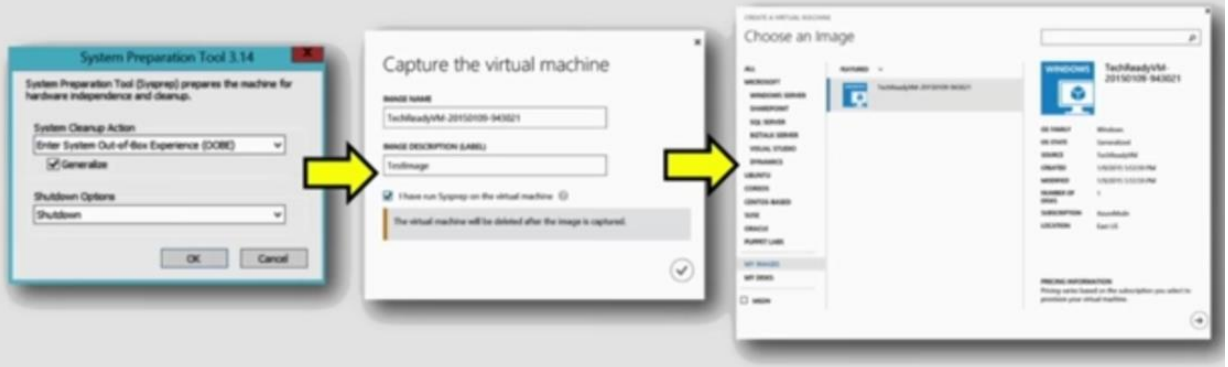
Load a quickstart template

Select a template (disclaimer)

- 201-vm-sql-full-autopatching
- 201-vm-sql-full-keyvault
- 201-vm-win-iis-app-ssl
- 201-vm-winrm-keyvault-windows
- 201-vm-winrm-lb-windows
- 201-vm-winrm-windows
- 201-vmaccess-on-ubuntu

ARM Template Walkthrough

Uploading Images



Generalize a Windows VM

Availability sets

Planned vs unplanned maintenance

Configure multiple virtual machines in an availability set for redundancy
Configure each application tier into separate availability sets
Combine a Load Balancer with availability sets Azure Load Balancer overview
Use multiple storage accounts for each availability set

Upgrade domains

Five (non-user configurable) domains by default
Groups of VMs and hardware that can be rebooted at the same time

Fault domains

Three domains by default
Group of virtual machines that share a common power source and network switch
Separate hardware & network

Manage the availability of VMs
How to create an availability set

Storage replication options

Locally redundant

- Default
- Up to three nodes in the same data center

Zone redundant storage

- Up to three data centers in the same region

Geo-redundant storage

- Data center in a different region

Read-access geo-redundant storage

- Data center in a different region
- Secondary data can be read

Azure Storage replication

ARM VM Storage

Azure Disk Encryption

Azure Disk Encryption for Windows and Linux IaaS VMs

Configure disk caching

Input/output operations per second (IOPS)
Throughput (Mbps)
Read/write vs Read and striping

Storage capacity

Scalability and Performance Targets

Sizing and egress traffic limits

Azure File service

SMB file shares
File system I/O APIs
Provisioning (Portal, PowerShell, Storage client libraries, Storage REST API – cannot use ARM)

Premium vs Standard

Storage Accounts

Premium: high-performance, low-latency disk support for I/O intensive workloads

Premium Storage

Virtual Machine Scale Sets

Identical set of VMs

- PaaS-like autoscale
- Focus is load and elastic in and out
- Foundation of Azure Service Fabric

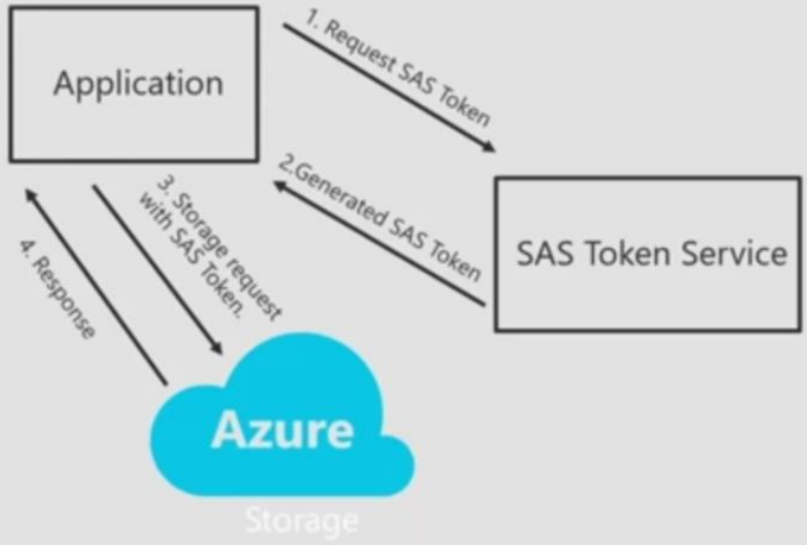
Scaling

- PaaS-like autoscale using autoScaleSettings in ARM template
  - Rules using metricTriggers
- Can combine Desired State Configuration (DSC) extension
- Initial scale setting using ARM template:

```
"sku": {
  "name": "Standard_A0",
  "tier": "Standard",
  "capacity": 3
},
```

Virtual Machine Scale Sets Overview

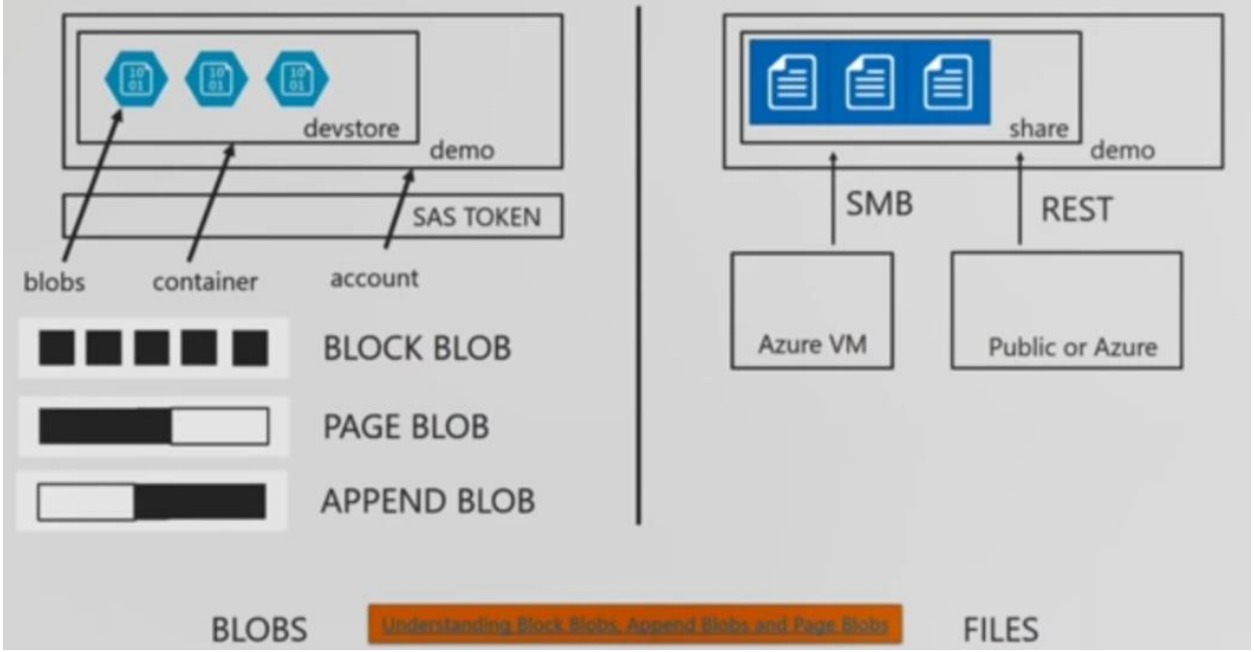
Access control with Shared Access Signature (SAS)



Tools to Generate SAS

- Azure Portal
- Storage Explorer
- PowerShell
  `New-AzureStorageBlobSASToken`, …
- Cross-Platform CLI
  `storage blob sas create`, …
- Custom Code
  - Protocol fully documented on MSDN

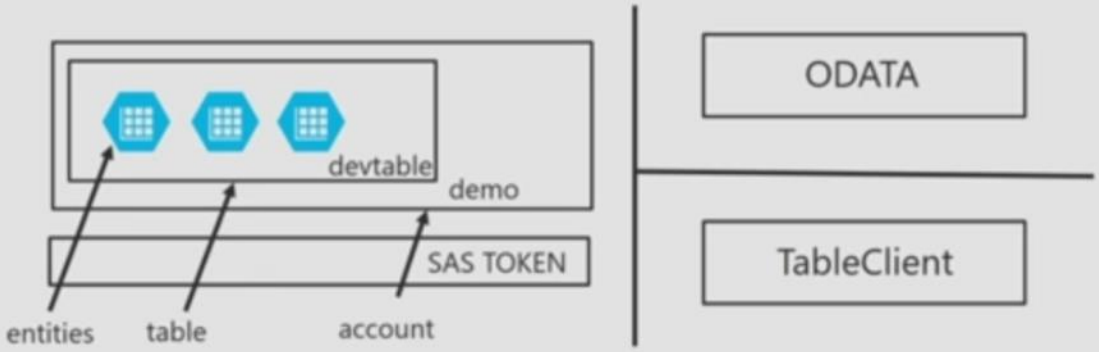
Blobs / Files



Storage

Description	Azure Blobs	Azure Files
Durability Options	LRS, ZRS, GRS (and RA-GRS for higher availability)	LRS, GRS
Accessibility	REST APIs	**SMB 2.1 (standard file system APIs)** REST APIs
Connectivity	REST – Worldwide	SMB 2.1 - Within region REST – Worldwide
Endpoints	http://myaccount.blob.core.windows.net/mycontainer/myblob	\\myaccount.**file**.core.windows.net\myshare\myfile.txt http://myaccount.**file**.core.windows.net/myshare/myfile.txt
Directories	Flat namespace however prefix listing can simulate virtual directories	True directory objects
Case Sensitivity of Names	Case sensitive	Case **insensitive**, but case **preserving**
Capacity	Up to 500TB containers	5TB file shares
Throughput	Up to 60 MB/s per blob	Up to 60 MB/s per **share**
Object size	Up to 1 TB/blob	Up to 1 TB/file
Billed capacity	Based on bytes written	Based on file size

Tables



Storage access

Blobs

//[account].blob.core.windows.net/[container]/[blob]

Files

//[account].file.core.windows.net/[file]

Tables

//[account].table.core.windows.net/[table]([paritition key],[row key])

Queues

//[account].queue.core.windows.net/[queue]

SQL Database

SQL Database Service Tiers

BASIC

- Small databases
- Single active operation
- Dev/Test
- Small scale apps
- 5 DTU

STANDARD

- Great option for cloud apps
- Multiple operations
- Workgroup or web apps
- 10 – 100 DTU

PREMIUM

- High transaction volumes
- Large number of users
- Multiple operations
- Mission critical apps
- 100 – 800 DTU

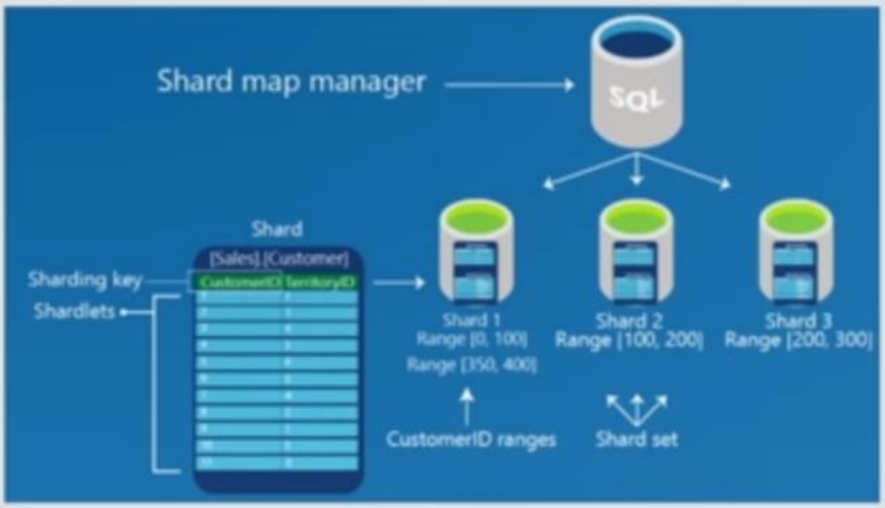
Migration between tiers is possible (Portal, PowerShell or REST API)

SQL Database

SQL Database Scaling

Maintains global mapping information about all shards (databases) in a shard set

Metadata used to route based on sharding key



Azure Storage Service Encryption (SSE)

- Features
  - 256 BIT AES Encryption
  - Block, Page and Append Blobs
  - General purpose and Blob Storage Accounts
  - All redundancy levels and all Regions
  - ARM, no ASM

- Limitations
  - No Classic storage and Classic migrated
  - No Existing Data before turned on
  - No Tables, Queues, and Files data

Azure Storage Service Encryption for Data at Rest

Search

Index

Create an index

Persistent store of documents

Operations and analyzers

Custom analyzers in Azure Search

Add data

Upload data to search

Push JSON data with .NET SDK or REST API

Pull with *indexers* supporting Azure storage and .NET SDK or REST API

Handle Results

Search pagination and layout

Total hits and page counts

Layout results

Sorting and filtering

Redis Cache

- Tiers Caching tiers
  Basic, Standard & Premium
- Concurrency
  Optimistic vs pessimistic Managing concurrency in a cache
- Distributed app caching
  Shared vs Private
  Data persistence Data persistence
  Clustering Clustering

Redis Pub/Sub
How to Use Azure Redis Cache
Caching guidance

Cosmos DB

Cosmos DB APIs

DocumentDB, Table, Graph, MobgoDB Introduction to Azure Cosmos DB: Table API

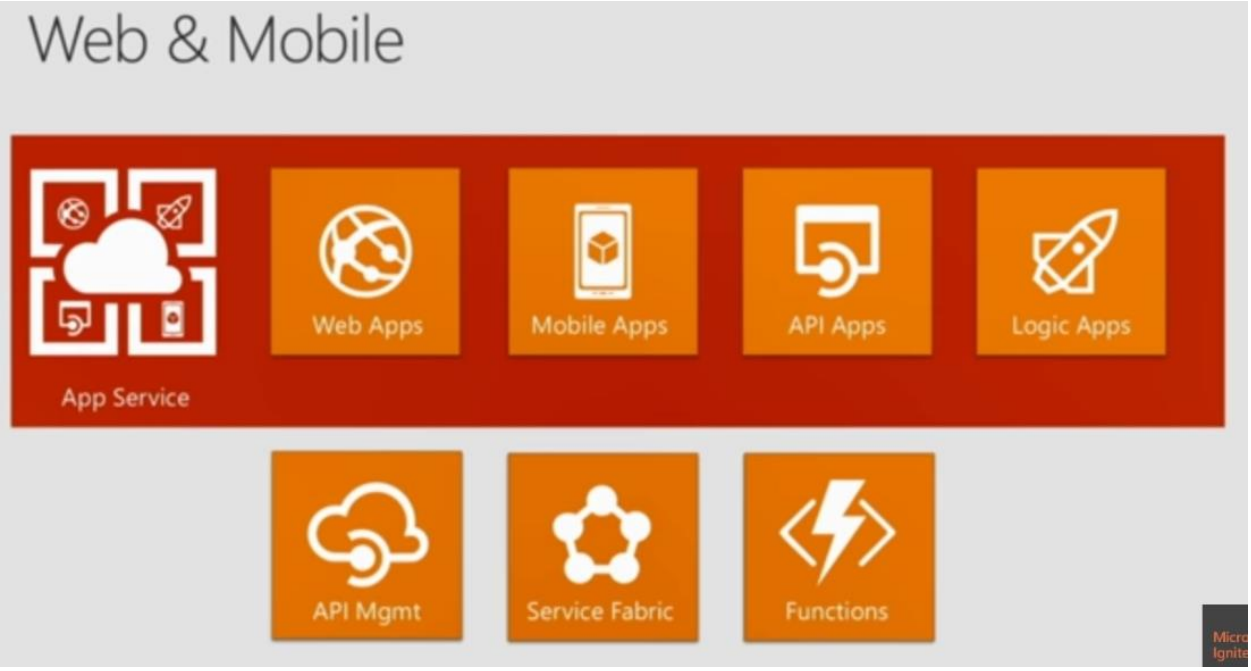
Create & Query Azure Cosmos DB DocumentDB API: SQL syntax

DocumentDB, Table, Graph (Vertex, Edge)
Expire data & TTL behavior Expire data in Azure Cosmos DB collections automatically...

Scale & Distribute Globally

Portal, PowerShell, CLI Automatic regional failover for business continuity in Azure Cosmos DB

Cosmos DB Documentation



Azure App Service

Build and scale great web and mobile apps

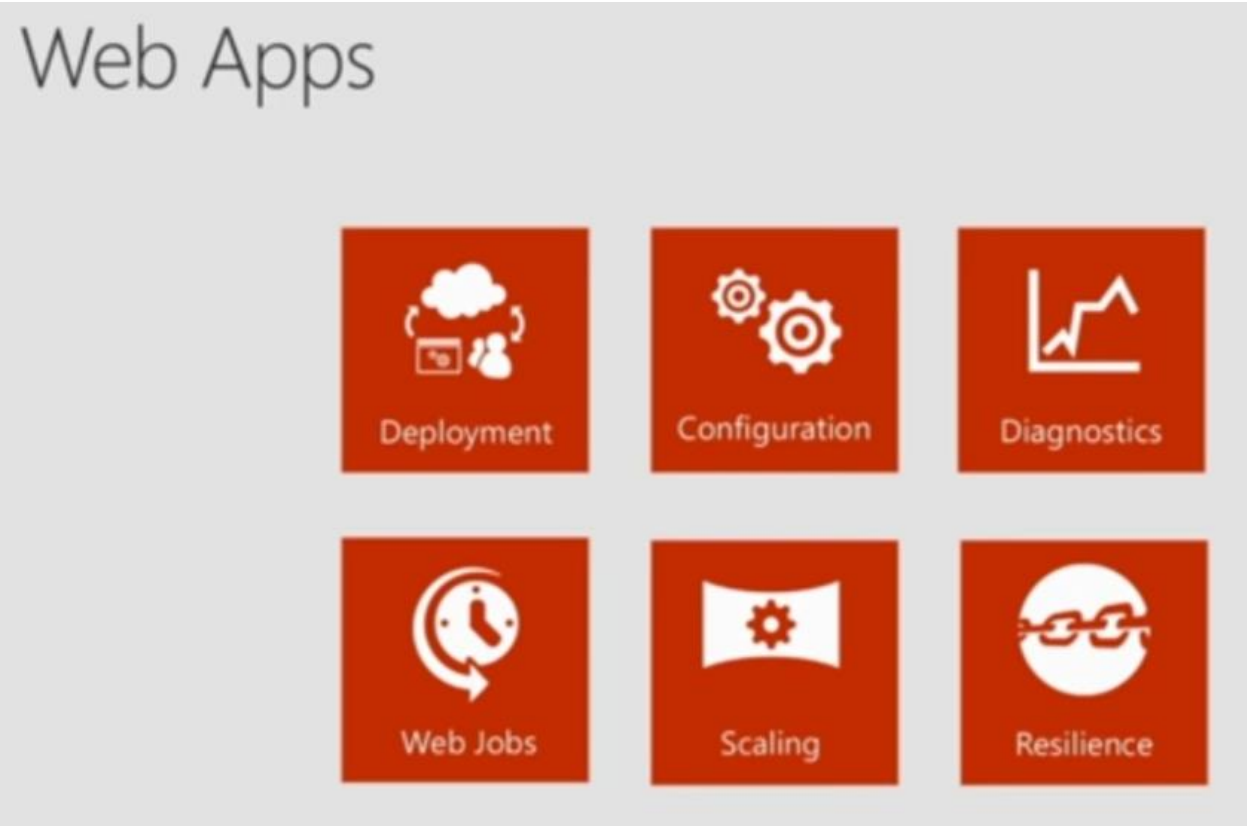
- Web apps
- Mobile apps
- Logic apps
- API apps

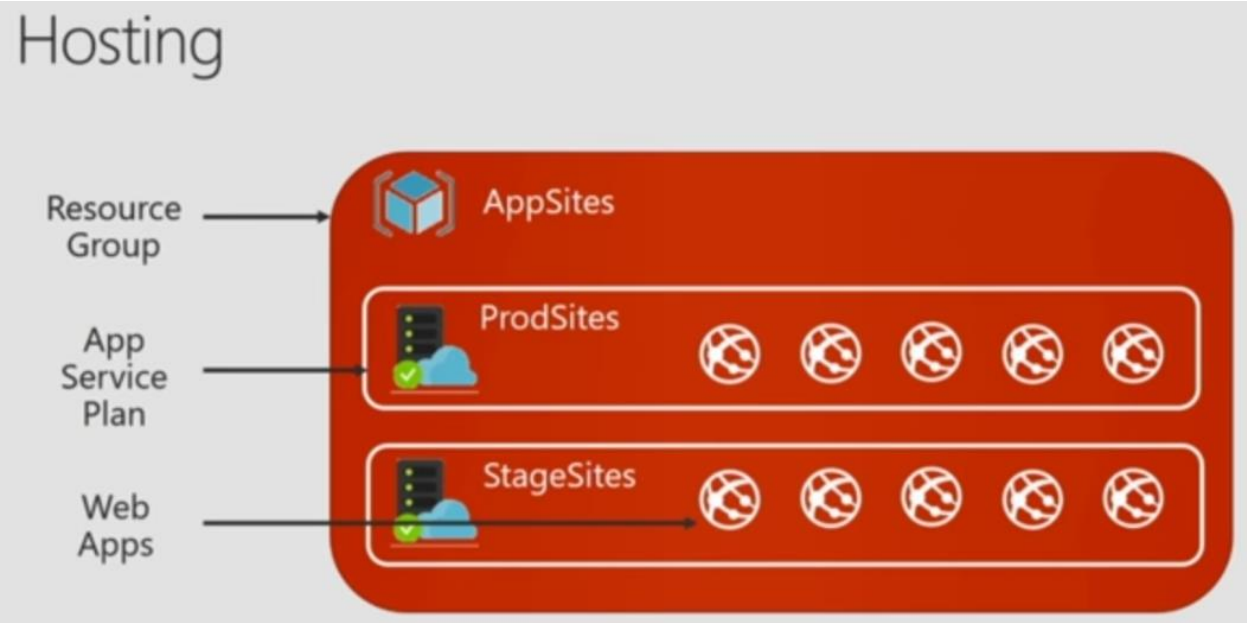
Auto-patching and auto-scale

.NET, Java, Node.js, PHP, Python

Integrate with SaaS and on-premises

Continuous integration with VSTS, Github, BitBucket, and more


Web Apps
Deployment
Configuration
Diagnostics
Web Jobs
Scaling
Resilience

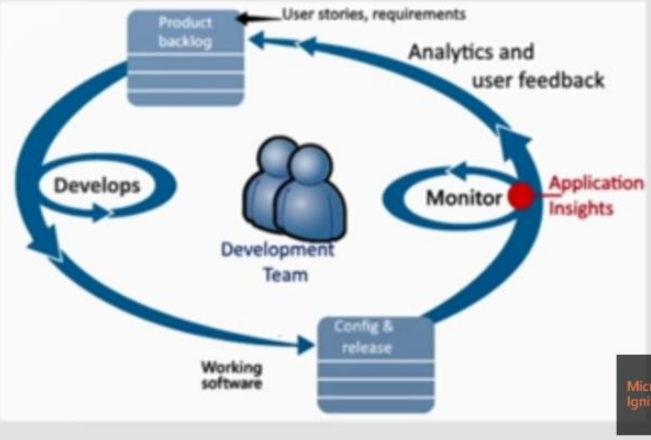

Hosting
Resource Group
App Service Plan
Web Apps
AppSites
ProdSites
StageSites

Azure Application Insights

Monitor

- WebApps, ASP.NET, Java Apps
- Windows Services
- Docker apps, JavaScript
- SharePoint Sites
- Node.js, Objective-C,
- PHP, Python, Ruby

Azure Application Insights



DevOps Cycle

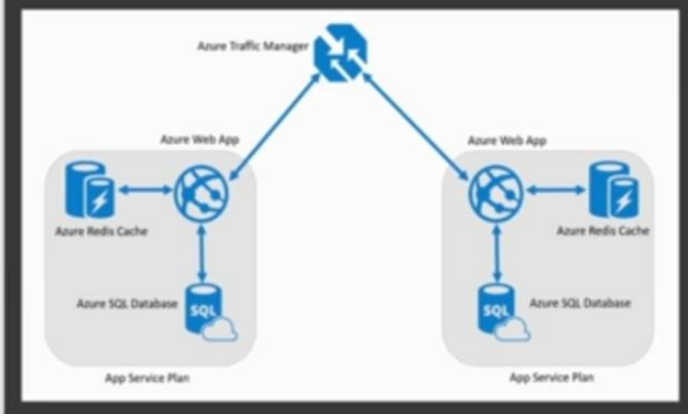
- Detect, Triage, Diagnose
- Monitor Perf, Failures, Usage
- aka.ms/azure/AppInsights

Microsoft Ignite

Scaling a web app

Scalable and global web app and database

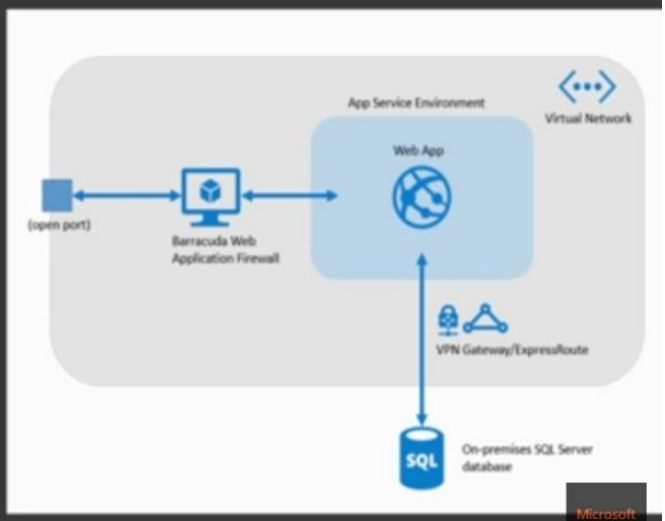
- Scale quickly with a slider bar, from a schedule, or based on CPU load
- Route users globally to copies of Web Apps and SQL Databases
- Improve performance by using a distributed cache layer



Isolating a web app

Web app with Personally Identifiable Information (PII) and database

- Host resources isolated and securely
- Block malicious requests through active defense firewalls
- Access on-premises resources from a cloud environment with a secure connection



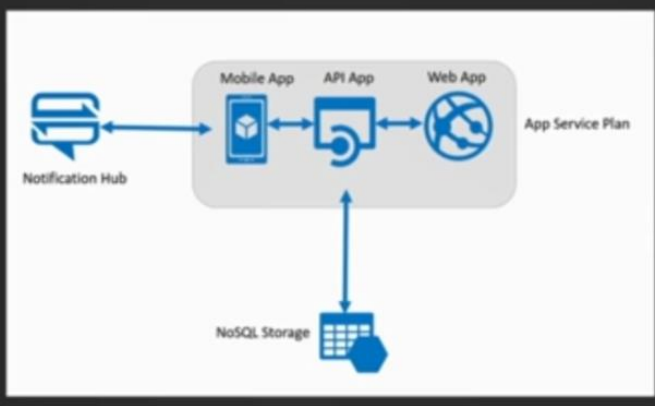
Adding mobile features to a web app

Native or Xamarin-native mobile client app that connects to an Azure Mobile App back end and shares data and APIs with an Azure Web App

- Create cross-platform mobile clients easily and consistently
- Share data and APIs as-is across mobile and web
- Enable mobile back-end features for push notifications, offline data sync, and auto-scaling

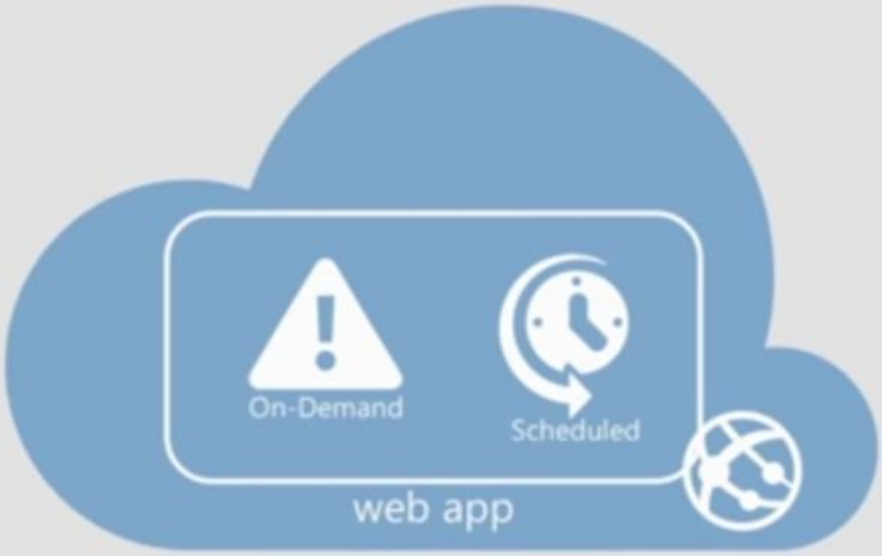
Add push notifications

Offline Data Sync in Azure Mobile Apps



Microsoft Ignite

WebJobs



Creating WebJobs

Uploaded in a zip file

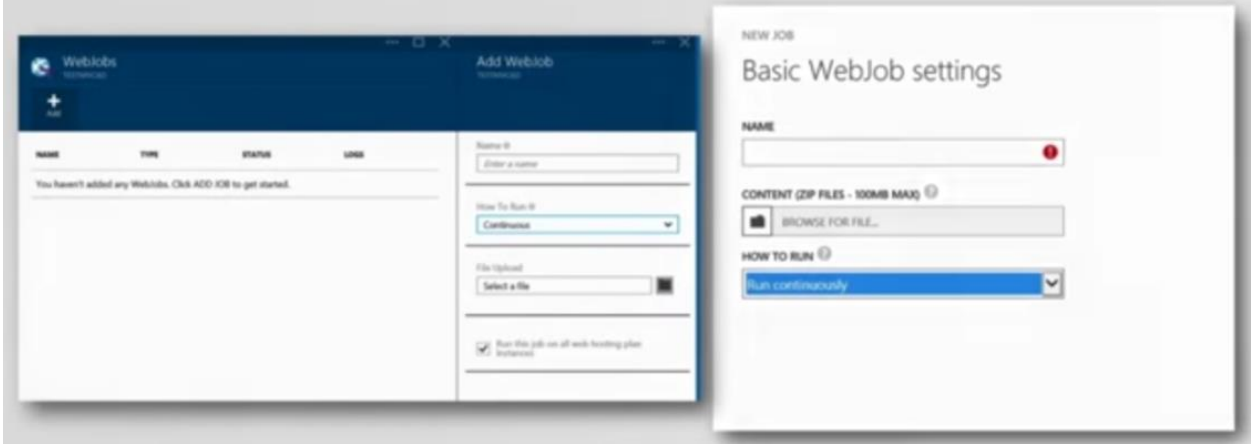
Types

- Python
- Batch
- PowerShell
- Java
- .NET

Scheduling

- settings.job file at root of zip file
  - { "schedule": "*second minute hour day month dayofweek*" }
- Or, just use the Azure UI

Configuring WebJobs



Azure Functions

Asynchronous, event-driven, serverless experience

Respond to events occurring in other Azure services, SaaS products (e.g., Office365, Salesforce), on-premises systems

Only pay while function is executing

Fully open source

Integrations with Logic Apps

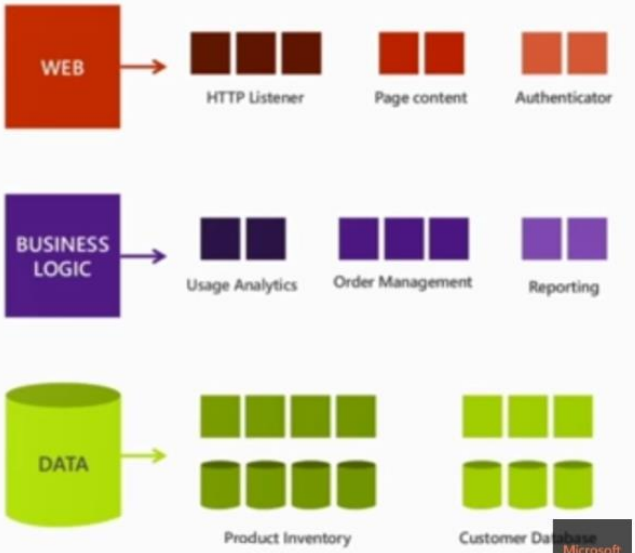
Azure Functions triggers and bindings concepts

AZURE FUNCTIONS

Microsoft Ignite

Modernization with microservices

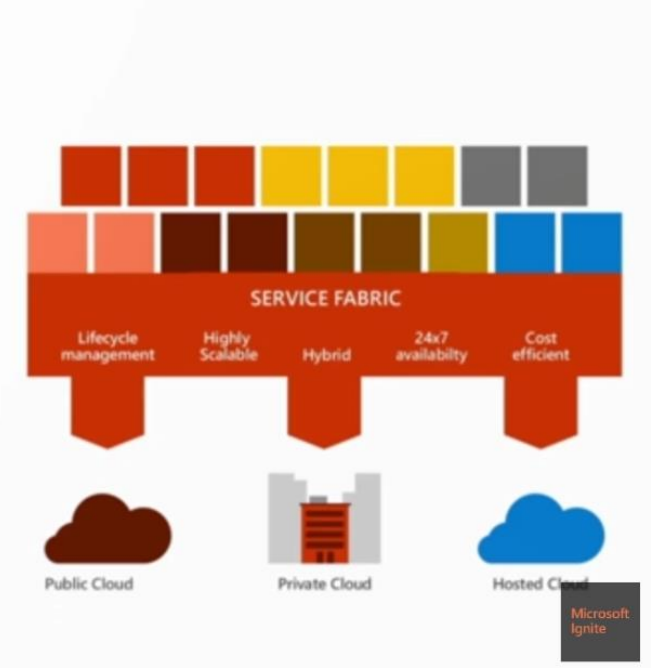
- Individually built and deployed
- Small, independently executing services
- Integrate using published API calls for overall application's functionality



Microsoft Ignite

Azure Service Fabric

- Manage microservices at scale
- CI/CD pipeline endpoint
- 24x7 service availability
- Stateful services
- Containers and Docker
- Multi-cloud



Service Fabric

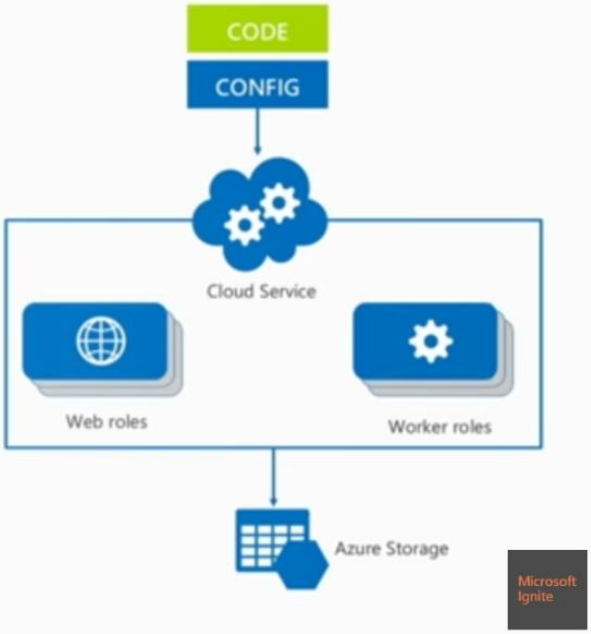
- Build & Deploy services
  - Actors-based service Reliable Actors state management Reentrancy Partitioning
  - Container service Service Fabric and containers Add a web front end
  - Guest Executable service
- Monitor & diagnose services
- Scale, Upgrade & Secure

Service Fabric Overview

Cloud services

PaaS with VM control

- Simple .NET runtime
- Health, discovery, updates
- OS Patching
- The original PaaS offering from 2010. Best used when low-level OS access is required, but consider the newer PaaS models first.



API Management

- Create Managed APIs Key Concepts
  - API Gateway + Developer Portal + Publisher Portal

Rate Limits

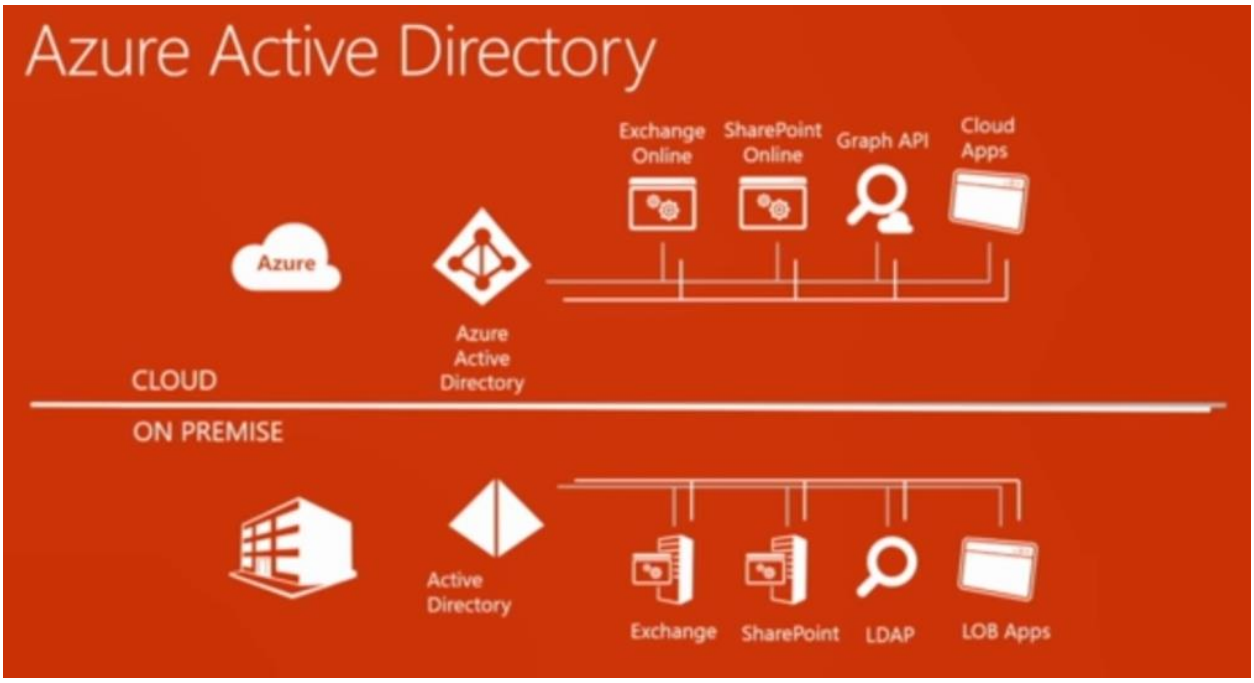
Policies

Customize the Developer Portal

Add Caching

API Inspector to trace calls


Identity and Networks
Azure AD
AD B2B/B2C
Communicate
Messaging


Azure Active Directory
Exchange Online
SharePoint Online
Graph API
Cloud Apps
Azure
Azure Active Directory
CLOUD
ON PREMISE
Active Directory
Exchange
SharePoint
LDAP
LOB Apps

Secure Resources using Managed Identities

Graph API

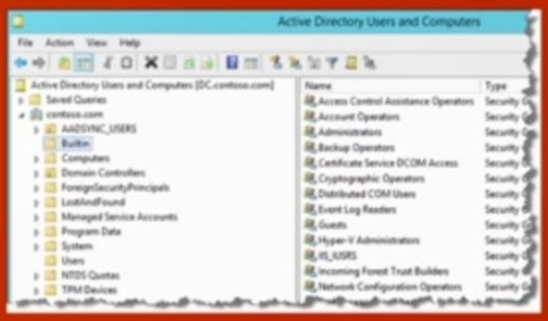
Programmatic Access to Azure AD | RESTful
CRUD | Application must be registered and configured
Requests use standard HTTP Methods

OAuth

AuthZ web apps and web APIs in Azure AD Tenant
Access authorization, role-based assignment
for app and user authorization

OpenID Connect

AuthZ protocol for SSO
Extends Oauth 2.0 for use as AuthN protocol



AD on-premises vs Azure AD

Microsoft Ignite

Azure Business to Consumer (B2C)

Sign up, Sign in, Password reset & other policies

Social & Local Accounts

Seamless User Experience

Multi-Factor Authentication

Protocol support (OIDC, OAuth2)

Azure AD Graph API

Azure B2C Overview

Microsoft Ignite

B2C vs B2B

Compare B2B collaboration and B2C in Azure Active Directory

Azure AD B2B Collaboration	Azure AD B2C
What is it for?	
IT Pros providing access to their organization's data and applications to **partner organizations and collaborators.**	Developers working on **Consumer- & citizen-facing** mobile & web apps that reach out to the customer, and citizens directly.
Who is it for?	
Partner users that are acting ***on behalf of***, i.e. as representatives or employees of their organization.	Consumers and citizens that are **acting as themselves.**
Manageability	
Access reviews, **email verification**, **allowlist/denylist, etc...** govern access to host application and resources.	**Self-Serve**. Users manage their own profiles.
Discoverability	
Partner users are **discoverable** and can see other users from their own organization (subject to policy).	Consumers and citizens are **invisible** to other consumers and citizens. Privacy and consent are paramount.

Microsoft Ignite

Service Bus

- FIFO Queues
- Simple Client

QUEUES

- Targeting Messages
- Work with Queues

TOPICS

- Expose OnPrem service to public
- Leverage WCF

RELAY

- Push notification infrastructure
- Support for non-MSFT targets

NOTIFICATION HUBS

Microsoft Ignite

Service Bus Queue vs Storage Queue

Service bus queues

- FIFO guaranteed
- Delivery once and only once
- 60 second default locks can be renewed
- Messages are finalized once consumed
- Native integration with WCF and WF

Storage queues

- Order not guaranteed
- Delivery at least once, maybe multiple times
- 30 second default locks, extendable to 7 days
- In-place updates of content
- Can integrate with WF through custom activity

Azure Key Vault

- Store access keys and SAS tokens in Key Vault
- Use Azure Automation job to periodically rotate keys, generate SAS Tokens, Update Key Vault Key Rotation and Auditing
- Give applications permission in Key Vault to read secrets
- Applications read keys and tokens from Key Vault Use Azure Key Vault From A Web App
  - Cache secrets in app for time less than rotation period
- Hardware Security Modules (HSMs)
  - Bring Your Own Key (BYOK) scenario HSM-protected keys