AZ-900 Microsoft Azure Fundamentals

Scott Duffy, Instructor

© 2021 Scott Duffy, softwarearchitect.ca... get the course for these slides at: http://sjd.ca/az900
Nov 2020 update
Microsoft Azure Fundamentals

“foundational level knowledge of cloud services and how those services are provided with Microsoft Azure”
Microsoft Azure Fundamentals

- Candidates with non-technical backgrounds
- Candidates with a technical background who have a need to validate their foundational level knowledge around cloud services
Microsoft Azure Fundamentals

- Describe cloud concepts
- Describe core Azure services
  - Describe core solutions and management tools
  - Describe general and network security features
- Describe identity, governance, privacy and Compliance features
  - Describe cost management and SLA
You’ll be prepared to take and pass the AZ-900 exam
But you don’t have to, if you just want to learn cloud concepts
What is the Cloud?
There is no cloud
it's just someone else's computer
The ability to rent computing resources - on demand
What Computing Resources?

Windows and Linux Servers
Unlimited Storage
Databases
Queues
Content Delivery Network
Batch Processing Jobs
What Computing Resources?

Big Data - Hadoop
Media Services
Machine Learning
Chat Bots
Cognitive Services
1000+

Azure Service options
Exam AZ-900: Microsoft Azure Fundamentals

In response to the coronavirus (COVID-19) situation, Microsoft is implementing several temporary changes to our training and certification program. Learn more.

The content of this exam was updated on November 9, 2020. Please download the skills measured document below to see what changed.

Candidates for this exam should have foundational knowledge of cloud services and how those services are provided with Microsoft Azure. The exam is intended for candidates who are just beginning to work with cloud-based solutions and services or are new to Azure.

Azure Fundamentals exam is an opportunity to prove knowledge of cloud concepts, Azure services, Azure workloads, security and privacy in Azure, as well as Azure pricing and support. Candidates should be familiar with the general technology concepts, including concepts of networking, storage, compute, application support, and application development.

Azure Fundamentals can be used to prepare for other Azure role-based or specialty certifications, but it is not a prerequisite for any of them.

Part of the requirements for: Microsoft Certified: Azure Fundamentals
Related exams: none
Important: See details
Go to Certification Dashboard
AZ-900 Microsoft Azure Fundamentals

Scott Duffy, Instructor

© 2021 Scott Duffy, softwarearchitect.ca... get the course for these slides at: http://sjd.ca/az900
Describe Cloud Concepts (20-25%)
Describe Cloud Concepts (20-25%)

Identify the benefits and considerations of using cloud services

- identify the benefits of cloud computing, such as High Availability, Scalability, Elasticity, Agility, and Disaster Recovery
- identify the differences between Capital Expenditure (CapEx) and Operational Expenditure (OpEx)
- describe the consumption-based model

Describe the differences between categories of cloud services

- describe the shared responsibility model
- describe Infrastructure-as-a-Service (IaaS),
- describe Platform-as-a-Service (PaaS)
- describe serverless computing
- describe Software-as-a-Service (SaaS)
- identify a service type based on a use case

Describe the differences between types of cloud computing

- define cloud computing
- describe Public cloud
- describe Private cloud
- describe Hybrid cloud
- compare and contrast the three types of cloud computing
Benefits of Cloud Computing
Benefits

Cost savings - both real and accounting
Agility
Availability
Security
Global reach
Range of ready on-demand services
Range of tools
Cost Savings
Cost Savings - Real

Economies of scale

Total cost of ownership (TCO) - electricity, Internet, cooling, employees

Microsoft can run a server cheaper than anyone else with few exceptions

4 vCPU server - as low as $187/mo
You can take actions to reduce your cost - i.e. autoscaling
Global Reach
It’s not possible for most businesses to run data centers in multiple countries.
High Availability
Expressed as a percentage, it’s the ability of a system to respond to users.
99.99%  

Four nines, 4 minutes per month
Scalability
The ability of a system to handle growth of users or work
Elasticity
The ability of a system to automatically grow and shrink based on application demand
capacity

User demand
The ability to change rapidly based on changes to market or environment
Disaster Recovery
The ability of a system to recover from failure within a period of time, and how much data is lost
Capital Expenditure (CapEx) and Operational Expenditure (OpEx)
CapEx is money invested in assets (like computers) that return investment over time.
OpEx is money spent every day on operating expenses
Consumption-Based Model
Pay per minute
Pay per hour
Pay per execution
Infrastructure-as-a-Service (IaaS)
Virtual machines, networking, load balancers, firewalls
Platform-as-a-Service (PaaS)
Upload code packages and have them run, without access to the hardware
Software-as-a-Service (SaaS)
Access to configuration only
Shared Responsibility Model
Shared responsibility model

Responsibility

- Information and data
- Devices (Mobile and PCs)
- Accounts and identities
- Identity and directory infrastructure
- Applications
- Network controls
- Operating system
- Physical hosts
- Physical network
- Physical datacenter

SaaS | PaaS | IaaS | On-prem

Responsibility always retained by customer

Responsibility varies by service type

Responsibility transfers to cloud provider
Serverless
There are still servers... you just don’t ever have to deal with them
Even less access to the server than PaaS
Even with PaaS, you have to choose an App Service Plan
With PaaS, scaling is your responsibility
Serverless means not worrying about choosing the right plan.
Serverless means not worrying about scaling
Serverless means you might pay $0 if you don’t use the service
Azure Serverless Offers

Compute - Azure Functions

Compute - Serverless Kubernetes (Virtual Nodes w/ ACI)

Database - Azure SQL Database Serverless

Database - Cosmos DB Serverless (preview)
Public cloud
Azure owns the hardware, on their network and infrastructure
Private cloud
Looks and acts like a cloud, except customer owns or leases or has exclusive access to the hardware
Hybrid cloud
Combination of public and private clouds; scale private infrastructure to the cloud
Compare and Contrast
Public vs private vs hybrid
AZ-900 Microsoft Azure Fundamentals

Scott Duffy, Instructor

© 2021 Scott Duffy, softwarearchitect.ca... get the course for these slides at: http://sjd.ca/az900
Describe Core Azure Services (15-20%)
Describe Core Azure Services (15-20%)

Describe the core Azure architectural components

- describe the benefits and usage of Regions and Region Pairs
- describe the benefits and usage of Availability Zones
- describe the benefits and usage of Resource Groups
- describe the benefits and usage of Subscriptions
- describe the benefits and usage of Management Groups
- describe the benefits and usage of Azure Resource Manager
- explain Azure resources

Describe core resources available in Azure

- describe the benefits and usage of Virtual Machines, Azure App Services, Azure Container Instances (ACI), Azure Kubernetes Service (AKS), and Windows Virtual Desktop
- describe the benefits and usage of Virtual Networks, VPN Gateway, Virtual Network peering, and ExpressRoute
- describe the benefits and usage of Container (Blob) Storage, Disk Storage, File Storage, and storage tiers
- describe the benefits and usage of Cosmos DB, Azure SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, and SQL Managed Instance
- describe the benefits and usage of Azure Marketplace
Core Azure architectural components
Regions
60+

Regions - not all accessible by everyone
Region Pairs
What are Paired Regions?

Each region has one other region which is treated as it’s “pair”

Almost always in the same geography - data storage laws

The data connection between region pairs is the highest speed available

Software rollouts are deployed to one region of a pair and the other is not touched

If multiple regions go down, one region of each pair is treated as a priority
<table>
<thead>
<tr>
<th>Region</th>
<th>Example Pair</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>Canada Central - Canada East</td>
</tr>
<tr>
<td>Europe</td>
<td>North Europe - West Europe</td>
</tr>
<tr>
<td>USA</td>
<td>East US - West US</td>
</tr>
<tr>
<td>USA</td>
<td>East US 2 - Central US</td>
</tr>
<tr>
<td>USA</td>
<td>North Central US - South Central US</td>
</tr>
<tr>
<td>Brazil</td>
<td>Brazil South - South Central US</td>
</tr>
</tbody>
</table>
Availability Zones
Resource Groups
Azure Subscription
Subscription is a billing unit
Users have access to one or more subscriptions, with different roles.
All resources consumed by a subscription will be billed to the owner.
Can be used to organize resources into completely distinct accounts
Management groups
Azure Resource Manager (ARM)
Instance of services that you create, that are yours to use
AZ-900 Microsoft Azure Fundamentals

Scott Duffy, Instructor

© 2021 Scott Duffy, softwarearchitect.ca... get the course for these slides at: http://sjd.ca/az900
Core resources in Azure
Getting Deep into the Technical

- Compute services
- Networking services
- Storage services
- Database services
- Azure Marketplace
Compute services covered

- Virtual Machines (VM)
- App services (Web apps)
- Azure Container Instances (ACI)
- Azure Kubernetes Service (AKS)
- Windows Virtual Desktop
Compute - “Executing code” in the cloud
Virtual Machines

Infrastructure as a service - IaaS

Take an existing machine from your environment into the cloud - a copy

Windows or Linux operating systems - several of each

A “slice” of a physical machine shared with other customers

Full control over it, as if it was your machine
Virtual Machine Types

Over 200 to choose from

Number of CPU cores, CPU speed, RAM size, temporary disk size, IOPS, etc
App Services

A new paradigm for running code in the cloud

Give your code and configuration to Azure, and they will run it

Promise of performance but no access to hardware

Platform as a Service (PaaS)
Containers

Another paradigm for running code in the cloud

Containers contain everything the app needs to run in a “container image”

Fastest and easiest to deploy

**Azure Container Instance (ACI)** - single instance, quickest way to deploy a container

**Azure Kubernetes Service (AKS)** - runs on a cluster of servers, enterprise-grade
Windows Virtual Desktop

Desktop version of Windows that runs in the cloud

You software installed, your files - available from anywhere

Can even see your desktop on iOS and Android, or from any web browser

Runs on Azure
Networking Services Covered

Virtual Networks
VPN Gateway
VNet Peering
ExpressRoute
Types of Networking Services

- Connectivity Services
- Protection Services
- Delivery Services
- Monitoring Services
Connectivity

**Virtual Network** - emulating a physical network

Microsoft Global Network already exists, so a virtual network is just software configuration

**Virtual Private Network (VPN)** - connecting two networks as if they were on the same network, uses a Network Gateway

**ExpressRoute** - high-speed private connection to Azure
Protection - Security Section of the Course

DDos Protection - Distributed Denial of Service attack protection

Azure Firewall

Network Security Groups

Private Link
Delivery - Not on the Exam

**Load Balancer** - distribute traffic evenly between multiple backend servers

**Application Gateway** - a higher-level of load balancer with an optional firewall

**Content Delivery Network (CDN)** - stores common static files on the edge, closer to the users for (perceived) improved performance

**Azure Front Door Service** - a load balancer, CDN and firewall all-in-one
Monitoring - Management Tools Section of the Course

Network Watcher

ExpressRoute Monitor

Azure Monitor
Storage Services Covered

Container (Blob) Storage
Disk Storage
File Storage
Storage Tiers
Storage - one of the foundational technologies on which much is built
Container (Blob) and File Storage

The Azure Storage account

General Purpose v2 (gpv2) is the most common type

Blobs, Tables *, Queues *, Files

Azure Data Lake Storage Gen2

Cheapest type of storage

Pay Per GB (~1.8 cents per GB)
Many, Many Options

Access tiers - Hot, Cool, Archive

Performance tiers - Standard or Premium

Location

Redundancy / Replication

Failover options
Disk Storage

Azure Virtual Machine Disks

Managed Disks

Reserve capacity in advance

Optimized to virtual hard disks
Database Services Covered

Cosmos DB
Azure SQL Database
Azure Database for MySQL
Azure Database for PostgreSQL
SQL Managed Instance
Most sophisticated applications have some type of database
Cosmos DB

Extremely fast storage

Designed for modern applications such as mobile video games, social networks, and things requiring thousands of global replication

NoSQL Storage

Multi-modal

Supports many open-source APIs and protocols
Azure SQL Database

Runs on the SQL Server engine underneath

Relational DB

Database as a service

Easy to replicate

Easy to scale

Easy to migrate from SQL Server on-prem
Azure Database for MySQL

Managed MySQL database

Common open-source DB

Makes migration to the cloud easier if you rely on this one

Wordpress uses it
Azure Database for PostgreSQL

 Managed PostgreSQL database

 Open-source DB

 Has better support for clusters and more complex server setups

 Makes migration to the cloud easier if you rely on this one
SQL Managed Instance

Most compatible with existing SQL Server

Minimal code changes

Fully managed by Azure

Always up-to-date
Azure Marketplace
Describe Core Solutions and Management Tools (10-15%)
Describe core solutions and management tools on Azure (10-15%)

Describe core solutions available in Azure

- describe the benefits and usage of Internet of Things (IoT) Hub, IoT Central, and Azure Sphere
- describe the benefits and usage of Azure Synapse Analytics, HDInsight, and Azure Databricks
- describe the benefits and usage of Azure Machine Learning, Cognitive Services and Azure Bot Service
- describe the benefits and usage of serverless computing solutions that include Azure Functions and Logic Apps
- describe the benefits and usage of Azure DevOps, GitHub, GitHub Actions, and Azure DevTest Labs

Describe Azure management tools

- describe the functionality and usage of the Azure Portal, Azure PowerShell, Azure CLI, Cloud Shell, and Azure Mobile App
- describe the functionality and usage of Azure Advisor
- describe the functionality and usage of Azure Resource Manager (ARM) templates
- describe the functionality and usage of Azure Monitor
- describe the functionality and usage of Azure Service Health
Internet of Things (IoT)

IoT Hub

IoT Central

Azure Sphere

Created by Flatart from Noun Project
Azure Sphere

A platform designed to work with connected devices

Includes:

- a secure, silicon chip
- Sphere OS
- Cloud-based security services
Big Data and Analytics

Azure Synapse Analytics
(formerly SQL Data Warehouse)

HDInsight

Azure Databricks
Artificial Intelligence (AI)

Azure Machine Learning

Cognitive Services

Azure Bot Service
Azure Bot Service

A natural language chatbot service

A database of frequently-asked questions

A front-end that allows people to ask questions
And get answers
Serverless

Azure Functions

Logic Apps

Event grid
DevOps Solutions

Azure DevOps
GitHub
GitHub Actions
Azure DevTest Labs
GitHub

Microsoft purchased GitHub in 2018

The most popular place to store your company’s source code

Has private and public options

Integrates with tools such as Visual Studio

Based on the “git” source control language invented by Linus Torvalds of Linux fame
GitHub Actions

Automate software workflows

What happens once someone “checks in” changes to code?
Possibly includes Continuous Integration (CI)
Possibly includes automatic compilation of code to check for errors
Possibly includes running a suite of tests against code
Having a Web App automatically update when new code is checked in.
Azure Tools

Azure CLI
PowerShell
Azure Portal
Azure Cloud Shell
Azure Mobile App
Azure Mobile App
Monitor the health and status of resources from your phone.
Run commands; start, stop and restart servers
Azure Advisor
**Microsoft Azure**  Advisor recommendations

**Overview**

- High Availability: 8 Recommendations, 25 impacted resources
  - 1 High impact, 7 Medium impact, 0 Low impact

- Security: 21 Recommendations, 63 impacted resources
  - 21 High impact, 0 Medium impact, 0 Low impact

- Performance: 1 Recommendation, 1 impacted resource
  - 1 High impact, 0 Medium impact, 0 Low impact

- Cost: 2 Recommendations, 11 impacted resources
  - 2 High impact, 0 Medium impact, 0 Low impact

**Tips & tricks**

- You can customize Advisor to process recommendations for resources that matter to you the most.
- You can optimize underutilized virtual machines to reduce your monthly Azure spend.
- You can improve the performance of your SQL Azure databases.
- You can enable virtual machine backup to protect your data from corruption or accidental deletion.
ARM Templates
Azure Resource Manager (ARM)

The deployment and management service for Azure

Management layer that allows you to create, update, and delete resources called “deployments”

All actions that you take to manage your Azure resources goes through the ARM layer
"resources": [
{
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2019-06-01",
    "name": "[parameters('storageAccountName')]",
    "location": "[parameters('location')]",
    "sku": {
        "name": "Standard_LRS",
        "tier": "Standard"
    },
    "kind": "StorageV2",
    "properties": {
        "accessTier": "Hot"
    },
    "resources": [
        
    ]
}
"type": "Microsoft.Storage/storageAccounts",
"apiVersion": "2019-06-01",
"name": "[parameters('storageAccountName')]",
"location": "[parameters('location')]",
"sku": {
    "name": "Standard_LRS",
    "tier": "Standard"
},
"kind": "StorageV2",
"properties": {
    "accessTier": "Hot"
},
"resources": [
{
    "type": "blobServices/containers",
    "apiVersion": "2019-06-01",
    "name": "[concat('default/', parameters('containerName'))]",
    "dependsOn": [
        "[parameters('storageAccountName')]"
    ]
}]}
Azure Monitor
Azure Service Health
No service issues found

See 1 resolved service issues in the last 24 hours, or see all past issues in the health history.

Launch guided tour
**Summary**

**Summary of impact:** Between 07:50 and 08:36 UTC on 22 May 2019, a subset of customers may have experienced connectivity issues when accessing Azure services in North Europe.

**Root Cause:** During this incident, approximately 12% of the network flows in or out of a single row of servers in a data center in North Europe would have failed.

Each row of servers in an Azure data center (DC) is connected to the DC network spine by eight routers. During this incident, one of the eight routers in a single row of a DC in North Europe began dropping all packets that it was expected to forward. Flows are spread over the eight routers, so flows sent to this one router would have been dropped. The other seven routers would have been forwarding the same flows to the target destinations in the network spine.
Describe General and Network Security Features (10-15%)
Describe general security and network security features (10-15%)

Describe Azure security features

- describe basic features of Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
- describe the functionality and usage of Key Vault
- describe the functionality and usage of Azure Sentinel
- describe the functionality and usage of Azure Dedicated Hosts

Describe Azure network security

- describe the concept of defense in depth
- describe the functionality and usage of Network Security Groups (NSG)
- describe the functionality and usage of Azure Firewall
- describe the functionality and usage of Azure DDoS protection
Azure Security Center

Unified infrastructure security management system that monitors and protects your systems inside and outside of Azure

- Strengthen security
- Protect against threats
- Get secure faster
**Security Center | Overview**

Showing subscription ‘Pay-As-You-Go (Azure Courses)’

- **Policy & compliance**
  - **Overall Secure Score**
    - **22%** (~5 of 23 points)
  - **Regulatory compliance**
    - View and monitor your compliance posture relative to industry standards and regulations
    - **Enable Regulatory Compliance →**
  - **Subscription coverage**
    - 1 TOTAL
    - Fully covered: 0
    - Partially covered: 1
    - Not covered: 0
    - 9 Covered resources

- **Resource security hygiene**
  - **Recommendations**
    - High Severity: 12
  - **Resource health by severity**
    - 2 Compute & apps resources
  - **Networking**
    - 3 Unhealthy resources
Security Center | Overview
Showing subscription ‘Pay-As-You-Go (Azure Courses)’

Resource security hygiene

Recommendations
- High Severity: 12
- Medium Severity: 1
- Low Severity: 1
- TOTAL: 14

Resource health by severity
- 2: Compute & apps resources
- 4: Data & storage resources
- 3: Identity & access resources

Networking
- Unhealthy resources: 3
- Monitored resources: 4

There are 1 high severity recommendations to resolve.

Secure your network resources

Review and improve your Secure Score

Review and resolve security vulnerabilities to improve your Secure Score and secure your workload

Learn more >
Key Vault
Central, secure repository for your secrets, certificates and keys
<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A37CA50C-C519-4605-8A73-5F67</td>
<td>Wrapped BEK</td>
</tr>
<tr>
<td>weather-service-api</td>
<td></td>
</tr>
</tbody>
</table>
Create a key

Options

Generate

* Name

Key Type

RSA EC

RSA Key Size

2048 3072 4096

Set activation date? □

Set expiration date? □

Enabled? Yes No
<table>
<thead>
<tr>
<th>NAME</th>
<th>THUMBPRINT</th>
<th>STATUS</th>
<th>EXPIRATION DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMPLETED</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>azsjdscf-cert</td>
<td>61D304B7D8692F0CDF120C2C940...</td>
<td>✔ Enabled</td>
<td>2/25/2020</td>
</tr>
<tr>
<td>newsfckey</td>
<td>395F068B7972B75D5F09C7C82D6...</td>
<td>✔ Enabled</td>
<td>2/25/2020</td>
</tr>
<tr>
<td><strong>IN PROGRESS, FAILED OR CANCELLED</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>There are no certificates available.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Administrator with Azure subscription creates and manages vault and keys.

Azure Key Vault

[Diagram showing flow of URIs for keys to Azure developer and usage logging for keys to security administrator.]
Azure Sentinel
What is Sentinel?

Centralizes all the log files from various resources

Analyzes them to detect threats

Allows you to run queries on those logs yourself

Investigate an incident

Orchestration and automation to fix the issues
Azure Dedicated Hosts
Hardware that is dedicated to you and only you
You can reserve a machine and run multiple virtual machines on it (to the machine limit)
Defense in Depth
Security Layers

- Data - i.e. virtual network endpoint
- Application - i.e. API Management
- Compute - i.e. Limit Remote Desktop access, Windows Update
- Network - i.e. NSG, use of subnets, deny by default
- Perimeter - i.e. DDoS, firewalls
- Identity & access - i.e. Azure AD
- Physical - i.e. Door locks and key cards
## Defense in Depth

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-based access</td>
<td>Encryption</td>
<td>DDOS Protection</td>
<td>Antimalware</td>
<td>Log Management</td>
</tr>
<tr>
<td>Multifactor Authentication</td>
<td>Confidential Computing</td>
<td>NG Firewall</td>
<td>AI-Based Detection and Response</td>
<td>Security Posture Assessment</td>
</tr>
<tr>
<td>Central Identity Management</td>
<td>Key Management</td>
<td>Web App Firewall</td>
<td>Cloud Workload Protection</td>
<td>Policy and Governance</td>
</tr>
<tr>
<td>Identity Protection</td>
<td>Certificate Management</td>
<td>Private Connections</td>
<td>SQL Threat Protection</td>
<td>Regulatory Compliance</td>
</tr>
<tr>
<td>Privileged Identity Management</td>
<td>Information Protection</td>
<td>Network Segmentation</td>
<td>IoT Security</td>
<td>SIEM</td>
</tr>
</tbody>
</table>
Network Security Group (NSG)
Azure Firewall
Azure DDoS Protection
<table>
<thead>
<tr>
<th>Feature</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Always on monitoring</td>
<td></td>
</tr>
<tr>
<td>Automatic mitigation for L3/L4 attacks</td>
<td></td>
</tr>
<tr>
<td>L7 Protection with Application Gateway Web application firewall</td>
<td></td>
</tr>
<tr>
<td>Globally deployed</td>
<td></td>
</tr>
<tr>
<td>Protection policies tuned to your VNet</td>
<td></td>
</tr>
<tr>
<td>Logging, alerting, and telemetry</td>
<td></td>
</tr>
<tr>
<td>Resource cost scale protection</td>
<td></td>
</tr>
</tbody>
</table>
AZ-900 Microsoft Azure Fundamentals

Scott Duffy, Instructor

© 2021 Scott Duffy, softwarearchitect.ca... get the course for these slides at: http://sjd.ca/az900
Describe Identity, Governance, Privacy, and Compliance Features (20-25%)
Describe identity, governance, privacy, and compliance features (20-25%)

Describe core Azure identity services

- explain the difference between authentication and authorization
- define Azure Active Directory
- describe the functionality and usage of Azure Active Directory
- describe the functionality and usage of Conditional Access, Multi-Factor Authentication (MFA), and Single Sign-On (SSO)

Describe Azure governance features

- describe the functionality and usage of Role-Based Access Control (RBAC)
- describe the functionality and usage of resource locks
- describe the functionality and usage of tags
- describe the functionality and usage of Azure Policy
- describe the functionality and usage of Azure Blueprints
- describe the Cloud Adoption Framework for Azure

Describe privacy and compliance resources

- describe the Microsoft core tenets of Security, Privacy, and Compliance
- describe the purpose of the Microsoft Privacy Statement, Online Services Terms (OST) and Data Protection Amendment (DPA)
- describe the purpose of the Trust Center
- describe the purpose of the Azure compliance documentation
- describe the purpose of Azure Sovereign Regions (Azure Government cloud services and Azure China cloud services)
What is “Identity”?
In computing, “identity” is a representation of a person, application or device.
Examples of Identity

John Henry Doe

johndoe@example.com

Monthly Payroll Application

The laser printer at 6th Floor West
Usually requires a password, a secret key or a certificate to prove
Many applications require you to log in to use some of its functionality
How It’s Traditionally Handled
Client-Server Model

Client App
Web Browser
Mobile App

User ID, Password

Server
Web Site

DB
Traditionally, companies have written their own code to handle this
Some of the more famous “hacks” have been on custom created identity systems.
Hacks

Some companies were storing the password in “plain text”

Some companies were using a simple, reversible hash algorithm (MD5)

Some companies were storing the “salt” along with the data

Not enforcing password change policies

Not enforcing password complexity policies
Azure provides an identity management system based on their popular "Active Directory"
Azure Active Directory
(Azure AD or AAD)
Azure Active Directory is not the same as Active Directory
Traditional AD does not work with Internet protocols
Azure AD provides “identity as a service”
Instead of having to write code to handle users, passwords, password reset
The AAD Model

Identity Provider

User ID, Password

Client App
Browser
Mobile App

signed token

Server
Web Server

signed token

trust, key
Benefits of Azure AD
Security

Created by Peter van Driel from Noun Project
Reduced development time, easier support
More features
Centralized administration
Only one user ID and password - Single Sign-On
Integration with other Azure services
The difference between Authentication and Authorization
Authentication is a user proving who they are - user id and password
Authorization is ensuring that a user is permitted to perform an action.
Move away from all authenticated users having admin access
Azure Active Directory
Microsoft’s preferred solution for identity management
Azure AD Powers Other Microsoft Services

Azure
Skype
Outlook
OneDrive
Xbox
Office 365 - Teams, SharePoint, PowerBI, etc
Complete solution for managing users, groups, roles
Single-sign on
Synchronize with your corporate AD
Conditional Access
User A attempts to log in to the app from within the company office, as she does every day.
User B attempts to log in to the app for the first time in 4 months
Administrator C attempts to log in to the app from their phone
Administrator D attempts to log in to the app from a location 1200 miles from the office
You can treat some access attempts as “routine”, and some as “not normal”
Azure Multi-Factor Authentication
Require 2 or more pieces of evidence (factors) in order to log in
Three Factors

Something you **know** - i.e password

Something you **have** - i.e mobile phone, access to email account

Something you **are** - i.e fingerprint
Your unique password could be 1 piece of evidence
But a second piece of evidence is required - a unique, time-limited code sent to you.
SMS, email, authenticator app, phone call
Role-Based Access Control (RBAC)
Microsoft’s’s preferred solution for access control
Create roles that represent the common tasks of the job
Accountant
Developer
Business Lead
Assign granular permissions to that role
Assign users to that role
Do not assign granular permissions to an individual
Locks
Read Only
Can Not Delete
Add lock

Lock name: dontdelete

Lock type: Delete

Notes:
This is needed for production processes

[OK] [Cancel]
Using RBAC, you can restrict who has access to locks.
Resource Tags
Can add metadata to Azure resources
Helps with billing and support issues
Azure Policy
Governance
Create rules across all of your Azure resources
Evaluate compliance to those rules
Examples of Built-In Policies

- Require SQL Server 12.0
- Allowed Storage Account SKUs
- Allowed Locations
- Allowed Virtual Machine SKUs
- Apply tag and its default value
- Not allowed resource types
Can create custom policies using JSON definition
Azure Blueprints
Azure Subscription templates with Roles and Policies already defined
Cloud Adoption Framework for Azure
Microsoft Cloud Adoption Framework for Azure

The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey.

Cloud Adoption Framework guidance

This guidance aligns to the phases of the cloud adoption lifecycle, ensuring easy access to the right guidance at the right time.
Set of documentation, guidance, tools
Best practices for succeeding in the cloud
Microsoft Cloud Adoption Framework for Azure

**Define Strategy**
- Understand motivations
- Business outcomes
- Business justification
- Prioritize project

**Plan**
- Digital estate
- Initial organization alignment
- Skills readiness plan
- Cloud adoption plan

**Ready**
- Azure setup guide
- First landing zone
- Expand the landing zone
- Best practices

**Adopt**
- Migrate
  - Azure migration guide
  - Migration scenarios
  - Best practices
  - Process improvements
- Innovate
  - Azure innovation guide
  - Innovation scenarios
  - Best practices
  - Process improvements

**Govern**
- Methodology • Benchmark
- Initial best practice • Governance maturity

**Manage**
- Business commitments • Operations baseline
- Operations maturity
Get started with the Cloud Adoption Framework

05/04/2020 • 2 minutes to read • 🏆🏆🏆

These common scenarios provide a roadmap through the Microsoft Cloud Adoption Framework for Azure. They can help you balance speed, innovation, and control by using an agile approach to start with a minimally viable solution. You can iterate on and improve that solution over time.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>We need to understand the fundamental concepts around cloud adoption</td>
<td>If your journey involves the cloud, there are a few initial concepts to understand and decisions to make.</td>
</tr>
<tr>
<td>We want to migrate existing workloads to the cloud</td>
<td>This guide is a great starting point if your primary focus is migrating on-premises workloads to the cloud.</td>
</tr>
<tr>
<td>We want to build new products and services in the cloud</td>
<td>This guide can help you prepare to deploy innovative solutions to the cloud.</td>
</tr>
<tr>
<td>We're blocked by environment design and configuration</td>
<td>This guide provides a quick approach to designing and configuring your environment.</td>
</tr>
<tr>
<td>We need to ensure operational excellence during cloud transformation</td>
<td>The steps in this guide help the strategy team lead the organizational change management that's required to consistently deliver on the cloud vision.</td>
</tr>
</tbody>
</table>
Core Tenets of Security, Privacy and Compliance
Azure: Trusted Cloud

- Security
- Privacy
- Compliance
- Resiliency
- Intellectual Property (IP) protection
Security

- Azure is built with security in mind
- Azure delivers tools and technologies to help organizations protect applications and data
- Azure uses encryption
- Azure offers advanced tools to detect and defend against security threats
Privacy

- You own all your data in Azure
- Microsoft will not mine your data or use it for marketing
- You control where the data is located and who has access
- You can access your own data at any time for any reason
- Microsoft follows a specific policy for government and law enforcement requests
- Microsoft follows a specific policy to remove data if you discontinue using their service
Compliance

Microsoft follows international standards and helps customers to follow those standards too if they wish.

Azure has more than 90 compliance certifications.

Azure follows more than 50 regional standards.

Azure can help with standards in more than 35 industries like health care, government, finance, etc.
Reliability and Resiliency

- High availability
- Disaster recovery
- Backup
Protecting IP

You can build your solutions on top of Azure’s products and services

Azure offers specific protections against frivolous infringement claims

See: Azure IP Advantage and Shared Innovation Initiative
Microsoft Privacy Statement
privacy.microsoft.com
Microsoft Privacy Statement

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what’s next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products. You provide some of this data directly, and we get some of it by collecting data about your interactions, use and experiences with our products. The data we collect depends on the context of your interactions with Microsoft and the choices that you make, including your privacy settings and the products and features that you use. We also obtain data about you from third parties.

If you represent an organisation, such as a business or educational institution, that utilises Enterprise and Developer Products from Microsoft, please see the Enterprise and developer products section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organisation, please see the Products provided by your organisation and the Microsoft account sections for more information.

You have choices when it comes to the technology you use and the data you share. When we ask you to provide personal data, you can decline. Many of our products require some personal data to provide you with a service. If you choose not to provide data necessary to provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this
Online Service Terms (OST)
For all Online Services

Introduction

The parties agree that these Online Services Terms govern Customer’s use of the Online Services and that the DPA (defined in the Glossary) sets forth their obligations with respect to the processing and security of Customer Data and Personal Data by the Online Services. The parties also agree that, unless a separate Professional Services agreement exists, these Online Services Terms govern the provision of Professional Services, including but not limited to the terms in the Professional Services section and terms in the DPA for the processing and security of Professional Services Data and Personal Data in connection with that provision. Separate terms, including different privacy and security terms, govern Customer’s use of Non-Microsoft Products (as defined below). In the event of any conflict or inconsistency between the DPA and any other terms in Customer’s volume licensing agreement (including these terms), the DPA shall prevail.

Service Level Agreements

Most Online Services offer a Service Level Agreement (SLA). For more information regarding the Online Services SLAs, please refer to http://microsoft.com/licensing/contracts.

Applicable Online Services Terms and Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current Online Services Terms will apply and will not change during Customer’s subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the Online Services Terms that apply to Customer’s use of those new features, supplements or related software.
Data Protection Addendum (DPA)
Microsoft Online Services Data Protection Addendum
Last updated July 21, 2020

Published in English on July 21, 2020. Translations will be published by Microsoft when available. Those commitments are binding on Microsoft as of July 19, 2020.
Trust center
Microsoft Azure

Now you can take advantage of the latest security, privacy, and compliance features of Microsoft Azure. In this site, you’ll learn about the trusted cloud, how your data is stored and accessed, and our comprehensive approach to securing your IT environment.

About Microsoft Azure

Microsoft Azure is a cloud computing platform that features a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and web. Azure includes integrated tools, pre-built templates, and managed services that make it easier to build and manage enterprise, mobile, web, and Internet of Things (IoT) apps faster, using skills you have and technologies you already know.

We understand that some organizations are still wary about cloud computing; keeping data confidential is essential for any organization. That’s why Microsoft has made an industry-leading commitment to the protection and privacy of your data. We were the first cloud provider recognized by the European Union’s data protection authorities for our commitment to rigorous EU privacy laws. Microsoft was also the first major cloud provider to adopt the new international cloud privacy standard, ISO 27018.

Azure safeguards customer data in the cloud and provides support for companies that are bound by extensive regulations regarding the use, transmission, and storage of customer data.

Azure Security Documentation
Get the information you need
Compliance terms such as GDPR, ISO and NIST
Many different standards for technology across the world.
Microsoft claims to be in compliance with many of them.
And has tools to help you be in compliance with others
General Data Protection Regulation (GDPR)

GDPR is a new set of rules designed to give EU citizens more control over their personal data.

- Affects companies outside of the EU that handle EU citizen’s data.
- Data has to be collected legally under strict conditions.
- Data has to be protected from misuse.
- Reporting obligations if data is mishandled.
<table>
<thead>
<tr>
<th>Certification</th>
<th>Azure</th>
<th>Azure Government</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSA STAR Certification</td>
<td>✓</td>
<td>✓ (new)</td>
</tr>
<tr>
<td>ISO 27001:2013</td>
<td>✓</td>
<td>✓ (new)</td>
</tr>
<tr>
<td>ISO 27017:2015</td>
<td>✓</td>
<td>✓ (new)</td>
</tr>
<tr>
<td>ISO 27018:2014</td>
<td>✓</td>
<td>✓ (new)</td>
</tr>
<tr>
<td>ISO 20000-1:2011</td>
<td>✓ (new)</td>
<td>✓ (new)</td>
</tr>
<tr>
<td>ISO 22301:2012</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ISO 9001:2015</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
ISO 9001:2015 is for Quality Management Systems (QMS)
ISO/IEC 20000-1:2011 is for Service Management Systems (SMS)
NIST Cybersecurity Framework (CSF)

National Institute of Standards and Technology (NIST)

Audited for compliance to security and privacy processes
NIST Cybersecurity Framework (CSF)

Microsoft and the NIST CSF

NIST Cybersecurity Framework (CSF) is a voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Microsoft Cloud services have undergone independent, third-party FedRAMP Moderate and High Baseline audits and are certified according to the FedRAMP standards. Additionally, through a validated assessment performed by HITRUST, security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

Learn how to accelerate your NIST Cybersecurity Framework deployment with Compliance Manager and our Azure Security and Compliance Blueprint:

Download the Azure Security and Compliance Blueprint - NIST CSF Risk Assessment Checklist ▶ Learn more about the NIST CSF assessment for Office 365 in Compliance Manager ▶
Azure Sovereign Regions
Separate account
For US government agencies - federal, state and local
Department of Defense (DoD) has its own too
Isolated data centers separate from the Azure public cloud
Meets standards specific to government
FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS
portal.azure.us
Different URLs for connecting to storage, functions, etc.
Azure China
Separate account
Data remains in China
Describe Azure cost management and Service Level Agreements (10-15%)
Describe Azure cost management and Service Level Agreements (10-15%)

Describe methods for planning and managing costs

- identify factors that can affect costs (resource types, services, locations, ingress and egress traffic)
- identify factors that can reduce costs (reserved instances, reserved capacity, hybrid use benefit, spot pricing) Describe the functionality and usage of the Pricing calculator and the Total Cost of Ownership (TCO) calculator
- describe the functionality and usage of Azure Cost Management

Describe Azure Service Level Agreements (SLAs) and service lifecycles

- describe the purpose of an Azure Service Level Agreement (SLA)
- identify actions that can impact an SLA (i.e. Availability Zones)
- describe the service lifecycle in Azure (Public Preview and General Availability)
Factors affecting costs
Different services are billed based on different factors
Free services
Free services

Resource groups
Virtual network (up to 50)
Load balancer (basic)
Azure Active Directory (basic)
Network security groups
Free-tier web apps (up to 10)
Pay per usage (consumption model)
Opportunity for cost savings

Azure Functions:

- 1 million executions free per month
- $0.20 per million executions
- Cheapest virtual machine is $20 per month
Pay per usage services

Functions

Logic Apps

Storage (pay per GB)

Outbound bandwidth

Cognitive Services API
Pay for time (per second)
Per second billing means billing stops when the VM is stopped *
Stability in pricing

Pay a fixed price per month for computing power or storage capacity

Whether you use it or not

Discounts for 1-year or 3-year commitment in VM (Reserved Instances)

Multi-tenant or isolated environment
Pay for bandwidth
First 5 GB is free
Inbound data is free
Bandwidth costs

Outbound data, $0.05 to $0.087 / GB for Zone 1 (NA and EU w/o Germany)
Outbound data, $0.057 to $0.10 / GB for DE Zone 1 (Germany)
Outbound data, $0.08 to $0.12 / GB for Zone 2 (Asia, Africa and Oceania)
Outbound data, $0.16 to $0.181 / GB for Zone 3 (Brazil)

(Availability zone pricing is different)
1 PB of data transfer = $52,000
Best practices for minimizing Azure costs
Azure Advisor cost tab
Auto shutdown on dev/qa resources
Utilize cool/archive storage where possible
Reserved instances
Configure alerts when billing exceeds an expected level
Use Policy to restrict access to certain expensive resources
Auto scaling resources
Downsize when resources over-provisioned
Ensure every resource has an owner (tags)
Spot Pricing
Ability to use virtual machine when nobody is using it for a discounted price
But when someone needs to use it, you get kicked off
Like a “last minute” travel website
Or the “same day tickets” window at a Broadway show
Pricing calculator
https://azure.microsoft.com/en-ca/pricing/calculator/
Estimates are hard to make 100% accurate
Configurable Options

Region

Tier

Subscription Type

Support Options

Dev/Test Pricing
Export and share the estimate
Total Cost of Ownership (TCO) calculator
The cost of a server is more than just the cost of the hardware
Other costs

- Electricity
- Cooling
- Internet connectivity
- Rack space
- Setup labor
- Maintenance labor
- Backup
Azure Cost Management
Another free tool inside Azure to analyze spending
Analyze spending over time
Tracking against budgets
Schedule reports
Service Level Agreement (SLA)
The Service Level Agreement (SLA) describes Microsoft’s commitments for uptime and connectivity. The SLA for individual Azure services are listed below.

AI + Machine Learning
Create the next generation of applications using artificial intelligence capabilities for any developer and any scenario

- **Azure Bot Service**
  Intelligent, serverless bot service that scales on demand

- **Machine Learning Studio**
  Easily build, deploy, and manage predictive analytics solutions

- **Cognitive Services**
  Add smart API capabilities to enable contextual interactions

Microsoft Genomics
Power genome sequencing & research insights

Azure Machine Learning service
Bring AI to everyone with an end-to-end, scalable, trusted platform with experimentation and model management
SLA for Virtual Machines

Last updated: March 2018

- For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.

- For all Virtual Machines that have two or more instances deployed in the same Availability Set, we guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.

- For any Single Instance Virtual Machine using premium storage for all Operating System Disks and Data Disks, we guarantee you will have Virtual Machine Connectivity of at least 99.9%.

Introduction

General Terms

SLA details

Additional Definitions

"Availability Set" refers to two or more Virtual Machines deployed across different Fault Domains to avoid a single point of failure.

"Availability Zone" is a fault-isolated area within an Azure region, providing redundant power, cooling, and networking.
Preview features
Preview features are for “testing” and not production use.
Could change significantly before it goes live
May not go live
Public and Private Preview
Public preview available to everyone
Private Preview requires registration
Announcing private preview of Azure VM Image Builder

Posted on 26 September, 2018

Daniel Sol, Program Manager, Azure Compute

Today I am excited to announce the private preview of Azure VM Image Builder, a service which allows users to have an image building pipeline in Azure. Creating standardized virtual machine (VM) images allow organizations to migrate to the cloud and ensure consistency in the deployments. Users commonly want VMs to include predefined security and configuration settings as well as application software they own. However, setting up your own image build pipeline would require infrastructure and setup. With Azure VM Image Builder, you can take an ISO or Azure Marketplace image and start creating your own golden images in a few steps.

How it works

Azure VM Image Builder lets you start with either a Linux-based Azure Marketplace VM or Red Hat Enterprise Linux (RHEL) ISO and begin to add your own customizations. Your customizations can be added in the form of a shell script, and because the VM Image Builder is built on HashiCorp Packer, you can also import your existing Packer shell provisioner scripts. As the last step, you specify where you would like your images hosted, either in the Azure Shared Image Gallery or as an Azure Managed Image. See below for a quick video on how to create a custom image using the VM Image Builder.
Azure VM Image Builder – Private Preview Signup

Thank you for your interest in the Azure VM Image Builder. Please sign up for the private preview and we will get back to you.
General Availability (GA)
Web Application Firewall (WAF) for Azure Front Door service is now generally available.

Web Application Firewall (WAF) for Azure Front Door service is now generally available. Customers can use WAF to define security policies that allow, block, forward or rate limit access to their web applications delivered through Azure Front Door.

- A WAF security policy may consist of an ordered list of custom rules and Azure managed pre-configured rulesets.
- Custom rules are based on a combination of client IP addresses, geolocation, http parameters, request methods and size constraints.
- The pre-configured default rule set can be enabled to protect your applications from OWASP top 10 threats.
- New or updated WAF configurations are deployed globally within minutes, letting you respond quickly to changing attack patterns.
- WAF for Azure Front Door is integrated with Azure Monitor and the logs can be accessed through an Azure storage account, Azure Event Hub or Azure Log Analytics.

Along with the general availability of the service, we are also adding in preview a new Azure managed pre-configured ruleset, Bot Protection Ruleset, that can be enabled to block requests coming from malicious IPs based on Microsoft's threats intelligence data feeds.

For more details, see WAF overview. To get started, follow WAF configuration guide.
Thank you and best of luck!
Grab Your Free Resources

Located at the end of the course:

- Free PDF Study Guide
- Download the slides and MP3 audio if you like to study offline
- 50 question practice test