

Describe Cloud Concepts - AZURE FUNDAMENTALS

**Introduction to Cloud technologies
& AZ-900 certification preparation**

Describe Azure identity, access, and security

Identity, authentication, authorization & access management

Identity

The fact of being something or someone

Authentication

The process of verification / assertion of identity

Authorization

The process of ensuring that only authenticated identities get access to the resources for which they have been granted access

Access management

The process of controlling, verifying, tracking and managing access to authorized users and applications

Authentication method

Process of authentication

Knowledge factor - Something you know

Ex: password, pin

Possession factor - Something you have

Ex: phone, token, card, key

Physical characteristic factor - Something you are

Ex: fingerprint, voice, face

Location Factor - Somewhere you are

Ex: gps, country

Types of Authentication

Passwords + 2 Factor Authentication

+ Security - Convenience

Passwords

- Security + Convenience

Passwordless authentication

+ Security + Convenience

Multi-factor authentication (MFA)

Single Sign On (SSO)

FIDO2 security keys (Fast IDentity Online)

Azure Active Directory



Azure Active
Directory

Azure Active Directory (Azure AD) is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop (+on-premises Active Directory deployment)

Identities management

Users, groups, applications

Access management

Subscriptions, resource groups, role, role assignments,
authentication & authorization settings

Cross-platform



Azure



Microsoft 365



Office 365

Sync services

Syncs with on-premises active directory

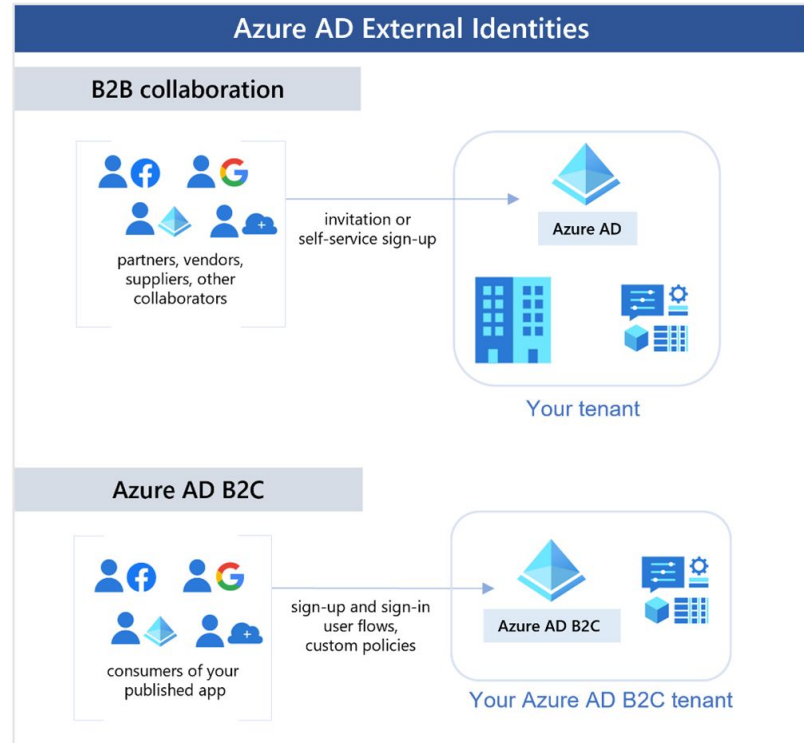
Azure AD External identities

Azure AD External Identities refers to all the ways you can securely interact with users outside of your organization (Identity and access management)

Ex: Collaborate with partners or manage customers' identity experiences

Azure AD business to customer (B2C) - Publish custom-developed apps to customers, while using Azure AD B2C for identity and access management.

Business to business (B2B) collaboration - Collaborate with external users using their preferred identity to sign-in to your Microsoft / enterprise applications



Conditional access



Azure AD
Conditional...

Tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.



Role, Security principal & Scopes

Role (role definition) is a collection of actions that the assigned identity will be able to perform

What can be done?



Security principal is an Azure object (identity) that can be assigned to a role (users, groups, applications)

Who can do it?







Scope one or more Azure resources that the access applies to

Where can it be done?



Role assignment is a combination of the role definition, security principal and scope

	Role				
	Reader	Resource-specific	Custom	Contributor	Owner
Scope	 Management group	Users managing resources			Admins
	 Subscription				
	 Resource group				
	 Resource	Automated processes			

Role-based Access Control (RBAC) is an authorization system built on Azure Resource Manager and is designed for fine-grained access management of azure resources

Defense in depth

Defense in depth removes reliance on any single layer of protection and uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data. It provides alert information that security teams can act upon, either automatically or manually.

Physical security layer

is the first line of defense to protect computing hardware in the datacenter.

Identity & access layer

controls access to infrastructure and change control.

Perimeter layer

uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.

Network layer

limits communication between resources through segmentation and access controls.

Compute layer

secures access to virtual machines.

Application layer

helps ensure that applications are secure and free of security vulnerabilities.

Data layer

controls access to business and customer data that you need to protect.

Microsoft defender for cloud & Zero Trust policy



Microsoft
Defender for...

Defender for Cloud is natively integrated and is a monitoring tool for security posture management and threat protection (Through a secure score).

Continuously Assess

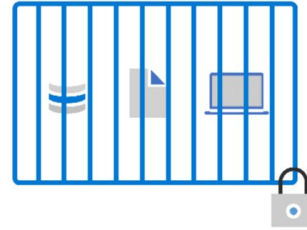
Know your security posture. Identify & track vulnerabilities

Secure

Harden resources and services with Azure Security Benchmark

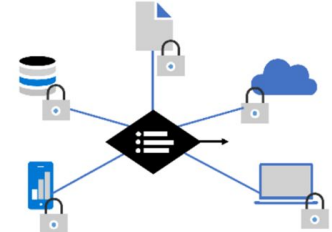
Defend

Detect & resolve threats to resources, workloads, and services



Classic Approach

Restrict everything to a 'secure' network



Zero Trust

Protect assets anywhere with central policy

Zero Trust is a security framework requiring all users to be authenticated, authorized, and continuously validated for security configuration and posture before being granted access to data/app.

Describe Azure management and governance

Chapter study guide

Describe Azure management and governance (30–35%)

Describe cost management in Azure

- Describe factors that can affect costs in Azure
- Compare the Pricing calculator and the Total Cost of Ownership (TCO) calculator
- Describe the Azure Cost Management and Billing tool
- Describe the purpose of tags

Describe features and tools in Azure for governance and compliance

- Describe the purpose of Azure Blueprints
- Describe the purpose of Azure Policy
- Describe the purpose of resource locks
- Describe the purpose of the Service Trust Portal

Describe features and tools for managing and deploying Azure resources

- Describe the Azure portal
- Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell
- Describe the purpose of Azure Arc
- Describe Azure Resource Manager and Azure Resource Manager templates (ARM templates)

Describe monitoring tools in Azure

- Describe the purpose of Azure Advisor
- Describe Azure Service Health
- Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights

Describe cost management in Azure

Factor affecting cost

Resource type

Azure creates metered instances for provisioning resource to track the resources' usage and generate a usage record that is used to calculate your bill.

Consumption

Pay-as-you-go is a straight forward pricing mechanism that allows for maximum flexibility. If you use more compute this cycle, you pay more and vice versa.

Maintenance

To control costs, it's important to maintain your cloud environment and through a resource needs assessment.

Geography

Depends of the billing zones (Intra- or extra-europe transfert). The cost of power, labor, taxes, and fees vary depending on the location. Azure resources can differ in costs to deploy depending on the region.

Bandwidth

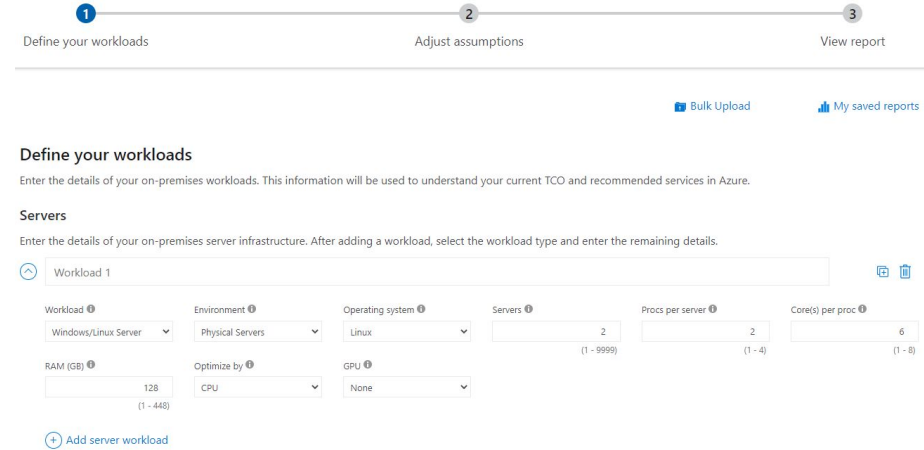
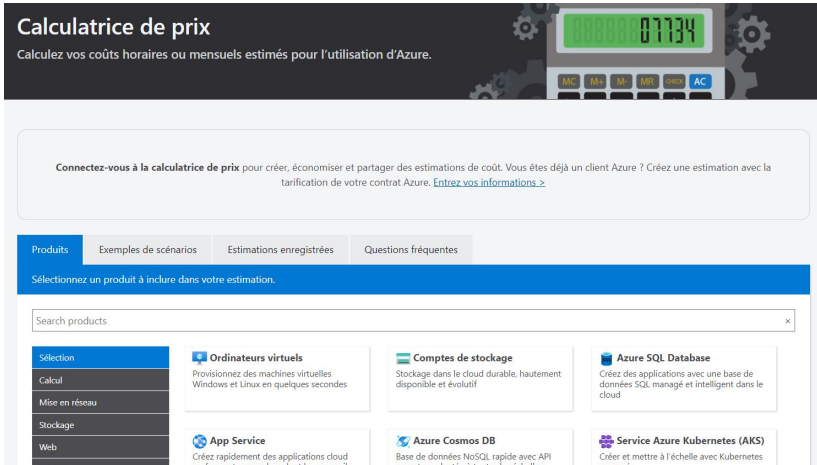
Network traffic when uploading (inbound/egress) data to Azure or downloading (outbound/egress) from Azure

Azure Marketplace

Lets you purchase Azure-based services from third-party vendors. You may pay for not only the Azure services that you're using, but also the services of the third-party vendor. Billing structures are set by the vendor.

Pricing and Total Cost of Ownership calculators

The pricing calculator and the total cost of ownership (TCO) calculator are two calculators that help you understand potential Azure expenses. Both calculators are accessible from the internet, and both calculators allow you to build out a configuration. However, the two calculators have very different purposes



Tags



Tags

Simple Name (Key) - Value pairs, applicable for resources, resource groups and subscriptions to organize Azure resources, and used for resource governance, security, operations management, cost management, and automation.

Functional - mark by function
(env, prod)

Classification - mark by policies used
(restricted, open)

Finance/accounting - mark for billing purposes
(finance, marketing)

Partnership - mark by association of users/groups
(BSB, DSOB)

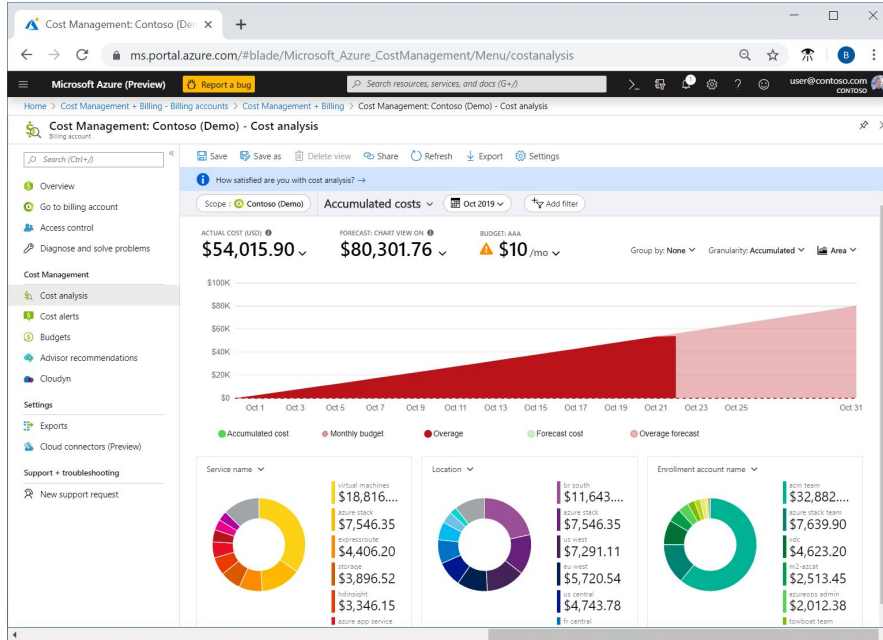
An example tagging structure

A resource tag consists of a name and a value. You can assign one or more tags to each Azure resource.

Name	Value
AppName	The name of the application that the resource is part of.
CostCenter	The internal cost center code.
Owner	The name of the business owner who's responsible for the resource.
Environment	An environment name, such as "Prod," "Dev," or "Test."
Impact	How important the resource is to business operations, such as "Mission-critical," "High-impact," or "Low-impact."

Keep in mind that you don't need to enforce that a specific tag is present on all of your resources. For example, you might decide that only mission-critical resources have the Impact tag. All non-tagged resources would then not be considered as mission-critical.

Azure cost management



Cost
Management ...

Centralized service for reporting usage and billing of Azure environment

Self-service cost exploration capabilities

Budgets & alerts

Cost recommendations

Automated exports

Describe features and tools in Azure for governance and compliance

Blueprint and Azure policy



Blueprints

A **Blueprint** is a guide, pattern or design for making something and is for Azure a centralized storage for organizationally approved design patterns

Blueprint definition : describing what should happen (reusable package)

Blueprint assignment : describing where it should happen (package deployment)

Package of various Azure components (artifacts) :

Resource groups

ARM templates

Policy assignments

Role assignments



Policy

Designed to help with resource governance, security, compliance, cost management, and focus on resource properties (Vs RBAC focused on user actions)

Policy definition - Defines what should happen

- Define the condition (if/else) and the effect (deny, audit, append, modify)
- Built-in and custom policies are supported

Policy initiative - a group of policy definitions

Policy assignment - assignment of a policy definition/initiative to a scope

- Scopes can be assigned to management groups, subscriptions, resource groups and resources
- Policies allow for exclusions of scopes

Resource locks & Service Trust center

Resource Locks

Designed to prevent accidental deletion and/or modification

Used in conjunction with RBAC

Two types of locks

- Read-only - only read actions are allowed
- Delete - all actions except delete are allowed

Scopes are hierarchical (inherited)

- Subscriptions > Resource Groups > Resources

Management Groups can't be locked

Only owner and user access administrator roles can manage locks (built-in roles)

Service Trust Portal

is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices. It is Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.

- Security
- Compliance
- Privacy
- Policies
- Practices

[Service Trust Portal](#)

Describe features and tools for managing and deploying Azure resources

Tools interacting with azure

Azure Portal

A public web-based interface for management of Azure platform, designed for self-service and simple tasks and customizable

Azure Powershell (Powershell)

A Powershell / module designed for automation, Multi-platform, and simple to use:

Connect-AzAccount : *log into azure*

Get-AzResourceGroup : *list resource groups*

New-AzResourceGroup : *create new resource group*

New-AzVm : *create virtual machine*

Azure CLI (Bash)

A Powershell / module designed for automation, Native OS terminal scripting, Multi-platform, and simple to use:

Az login : log into Azure

Az group list : list resource groups

Az group create : create new resource group

Az vm create : create virtual machine

Describe Azure Resource Manager and Azure ARM templates

Azure Resource Manager (ARM)

is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

- *Manage your infrastructure through declarative templates rather than scripts. A Resource Manager template is a JSON file that defines what you want to deploy to Azure.*
- *Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.*

ARM templates

Infrastructure as code is a concept where you manage your infrastructure as lines of code. ARM templates are another example of infrastructure as code at work.

- *Leveraging Azure Cloud Shell, Azure PowerShell, or the Azure CLI are some examples of using code to deploy cloud infrastructure*
- *By using ARM templates, you can describe the resources you want to use in a declarative JSON format. With an ARM template, the deployment code is verified before any code is run.*

Azure arc



Azure Arc

In utilizing Azure Resource Manager (ARM), Arc lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations. Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

Azure Arc provides a centralized, unified way to:

Manage your entire environment together by projecting your existing non-Azure resources into ARM.

Manage multi-cloud and hybrid virtual machines, Kubernetes clusters, and databases as if they are running in Azure.

Use familiar Azure services and management capabilities, regardless of where they live.

Continue using traditional ITOps while introducing DevOps practices to support cloud and native patterns in your environment.

Configure custom locations as an abstraction layer on top of Azure Arc-enabled Kubernetes clusters and cluster extensions.

Describe monitoring tools in Azure

Azure advisor & Azure service health & Azure Monitor



Advisor

Personalized recommendations for all your subscriptions, resource groups, and services.

Reliability

is used to ensure and improve the continuity of business-critical applications.

Security

is used to detect threats and vulnerabilities.

Performance

is used to improve the speed of applications.

Operational Excellence

is to achieve process and workflow efficiency, resource manageability, and deployment best practices.

Cost

is used to optimize & reduce overall spending.



Service Health

Keep track of resource, both your specifically deployed resources and the overall status of Azure

Azure Status

is a broad picture of the status of Azure globally

Service Health

provides a narrower view of Azure services and regions.

Resource Health

is a tailored view of your actual Azure resources.



Monitor

A platform for collecting data on your resources, analyzing that data, visualizing the information, and even acting on the results (On-premises & multi-cloud)

Azure Log Analytics

Azure Monitor Alerts

Application Insights

To go further

- [AZ 900 practice assessment](#)
- [Microsoft Certified: Azure Fundamentals - Certifications](#)
 - Exam page
 - [Training](#)