AZ-900 Azure fundamentals

0. General concepts

A recommended region represents a set of datacenters or availability zones deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Alternate regions (designated in the Azure portal as other), are not designed to support availability zones.

Outbound data transfer (leaving Azure cloud or an Azure region) is charged at the normal rate and inbound data transfer is free.

Subscriptions can include multiple resource groups, and a resource gropu can't include another resource group. A resource group can include services from multiple regions.

To minimize capex and opex, hybrid cloud. A complete migration to public cloud involves high opex.

For products governed by the Modern Lifecycle Policy, Microsoft will provide a minimum of 12 months' notification prior to ending.

1. Compute services

1.1. Virtual machines

Software emulations of physical computers. They include a virtual processor, memory, storage and networking resources and they host an OS. They give total control over the OS, the ability to run custom software. They are of type IaaS. When a VM is stopped, there are no more costs associated to the VM but there are storage costs, for example disks attached to the VM.

Azure Site recovery: native disaster recovery as a service (DRaaS).

> Virtual machine scale sets

This can be used to deploy and manage a set of identical VMs, to perform autoscale

> Batch

Another option for autoscaling, this enables large-scale parallel and high-performance computing (HPC) batch jobs with the ability to scale to tens, hundreds or thousands of VMs.

1.2. Container instances

These are Azure compute resources that can be used to deploy and manage containers, which are lightweight, virtualized application environments.

- Container instance: fastest and simplest way to run a container. PaaS
- Kubernetes service: complete orchestration for containers with distributed architectures and large volumes of containers.

1.3. App service

This can be used to build, deploy and scale web, mobile, WebJobs and API apps running on any platform. It supports Windows, Linux, iOS and Android and enables automated deployments from Github, Azure DevOps or any Git repository. This is of type PaaS.

App service provides deployment and management, securing endpoints, autoscaling of sites, load balancing and traffig manager: thus providing high availability.

1.4. Functions

Serverless, event-driven compute option. Commonly used when performing work in response to an event (often a REST request) timer, or message from another Azure service, and when that work can be completed quickly, within seconds. Functions can run locally or in the cloud.

- Stateless (default): they behave as if they are restarted every time they respond to an event
- Stateful (durable functions): a context is passed through the function to track prior activity

1.5. Logic apps

Functions execute code, logic apps execute workflows. It starts with a trigger, the logic app creates a logic app instance that runs the actions in the workflow. These can include data conversions and flow controls, conditional statements, rules, switch statements, loops and branching. Workflows are persisted as a json file with a known workflow schema.

Functions execute code to complete each step. Logic apps, the actions and the relationships between them are defined using a GUI. Logic apps are stateful, and then can be run only on the cloud.

1.6. Windows virtual desktop

This is a desktop and application virtualization service that runs on the cloud. It enables users to use a cloud-hosted version of Windows from any location. It works across devices using Windows, Mac, iOS, Android and Linux.

WVD allows to load balance users on the VM host pools. Host pools are collections of VMs with the same configuration assigned to multiple users. For best performance, load balancing can be set up to occur as users sign in (breadth mode). In this way, users are sequentially allocated across the host pool for the workload. To

save costs, the VMS can be configured for depth mode load balancing where users are fully allocated on one VM before moving to the next.

WVD is free if you have an eligible Microsoft 365 license. To save up costs, buy 1-year or 3-year reserved VM instances.

2. Networking resources

Virtual networking provides:

- Isolation and segmentation: when setting up a virtual network, you define a private IP address space by using either public or private IP address ranges. That IP address space can be divided into subnets and you can allocate part of the defined address space to each named subnet.
- Internet communications
- Communication between Azure resources
    - Virtual networks: they connect to compute resources: VMs, App service, Kubernetes
    - Service endpoints: they connect to other resource types, SQL databases and storage accounts
- Communication with on-premises resources
    - Point-to-site VPN: connection from a computer outside the organization, back into the corporate network. The client computer initiates an encrypted VPN connection to connect that computer to the Azure virtual network
    - Site-to-site VPN: links the on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. The devices in Azure appear as being on the local network. The connection is encrypted and works over the internet
    - Azure ExpressRoute: for higher bandwidth and even higher levels of security, ExpressRoute provides dedicated private connectivity to Azure that doesn't travel over the Internet. All inbound data transfer is free of charge
- Route network traffic: by default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the Internet. To control routing and override the default settings:
    - Route tables: you can define rules about how traffic should be directed, or how packets should be routed between subnets
    - Border gateway protocol (BGP) works with Azure VPN gateways or ExpressRoute to propagate on-premises BGP routes to Azure virtual networks
- Filter network traffic between subnets
    - Network security groups: this contains multiple inbound and outbound security rules. These can allow or block traffic, based on factors such as source and destination IP address, port, and protocol
    - Network virtual appliances: this is a specialized VM that can be compared to a hardened network appliance. This carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization

Virtual networks (even in different regions) can be linked by using virtual network peering. This enables resources in each virtual network to communicate with each other. With user-defined routing (UDR), network admins can control the routing tables between subnets within a VNet, as well as between VNets, allowing greater control over network traffic flow.

2.1. VPN Gateway

VPNs are encrypted tunnels within another network. They are usually deployed to connect 2+ trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network.

A VPN gateway is a type of virtual network gateway. They enable the following connectivity:

- Connect on-premises datacenters to virtual networks through a site-to-site connection
- Connect individual devices to virtual networks through a point-to-site connection
- Connect virtual networks to other virtual networks through a network-to-network connection

A VPN gateway can be of 2 types:

> Policy-based VPNs

They statically specify the IP address of packages that should be encrypted through each tunnel. Static rougint: address prefixes from both networks control how traffic is encrypted/decrypted through the VPN tunnel. The source and destination of the tunneled network are declared in the policy and don't need to be declared in routing tables.

> Route-based VPNs

When defining which IP addresses are behind each tunnel is too cumbersome, route-based gateways can be used. IP routing (can be static or dynamic) decides which of the tunnel interfaces (network interface or virtual tunnel interface) to use when sending each packet. These VPNs are preferred for on-premises devices, since they are more resilient to topology changes such as the creation of new subnets.

2.2. ExpressRoute

It connects on-premises networks into Azure or Microsoft 365 over a private connection with a connectivity provider. By not bringing the connection over the public Internet, the connection is faster, more reliable, has consistent latencies and higher security.

ExpressRoute allows layer 3 (address-level) connectivity, built-in redundancy, dynamic routing.

Even if you have an ExpressRoute connection, DNS queries, certificate revocation list checking and azure CDN requests are still sent over the Internet.

3. Storage services

To use Azure Storage, you need a Storage account (IaaS). This provides a unique namespace for your data.

3.1. Disk storage

Provides disks for VMs. Data is persistently stored and accessed from an attached virtual hard disk. Disks can be SSD, HDD.

3.2. Blob storage

Object storage solution.

- Hot access tier: frequently accessed data (e.g., images for the website)

- Cool access tier: infrequently accessed data and stored for 30+ days (invoices for customers). It has lower availability but still high durability, retrieval latency and throughput
- Archive access tier: rarely accessed data and stored for 180+ days, with flexible latency requirements. Data is stored offline and has the lowest cost, but also the highest cost to rehydrate and access data. This tier can't be selected at account level.

3.3. Files

Fully-managed file shares that can be accessed via Server Message Block and Network File System protocols, fileshares can be accessed from anywhere via a customized URL pointing to the file. File shares can be mounted by cloud or on-premises deployments of Windows, Linux and macOS. Fileshares can be accessed form multiple VMs. Azure Files ensures that data is encrypted at rest, and SMB protocol ensures that data is encrypted in transit.

4. Databases and analytics services

The Azure database migration service helps migrate existing databases with minimal downtime.

4.1. CosmosDB

PaaS service, support schema-less data, allows for highly responsive and always on apps to support constantly changing data. The data is stored in atom-record-sequence (ARS) format, and then abstracted and projected as an API. The choices are SQL, MongoDB, Cassandra, Tables and Gremlin.

4.2. SQL database

Relational PaaS database based on Microsoft SQL server database engine.

4.3. Database for MySQL

Azure Database for MySQL is the logical choice for existing LAMP stack applications.

4.4. Synapse analytics

Limitless analytics service that brings together enterprise data warehousing and big data analytics. Unified experience to ingest, prepare, manage and serve data for immediate BI and ML needs.

4.5. HDInsight

Fully managed, open-source analytics service for enterprises to process massive amounts of data. Spark, Hadoop, Kafka, HBase, Storm and ML services can be run here. It also supports ETL (extraction, transformation and loading), data warehousing, ML and IoT.

4.6. Databricks

Data analytics platform for **big data analysis**. It offers three environments for developing data intensive applications: Databricks SQL, Databricks Data Science & Engineering, and Databricks Machine Learning.

Databricks Data Science & Engineering (sometimes called simply "Workspace") is an analytics platform based on Apache Spark.

4.7. Data lake analytics

On-demand analytic job service that simplifies big data. With queries, data can be transformed and valuable insights can be extracted.

5. Core solutions and management tools

5.1. IoT services

5.1.1. IoT Hub

Managed service, hosted in the cloud, acting as a central message hub for bidirectional communication between IoT devices and a cloud-hosted solution backend. It also supports device-to-cloud telemetry, file upload from devices, request-reply methods. IoT Hub allows for **command and control**. It can track events such as device creation, device failures, device connections.

5.1.2. IoT Central

Pre-built customizable user interface, built upon IoT Hub, to view and control and monitor devices remotely. Offers performance monitoring, alerts and notifications, pushing firmware updates to the device.

It offers templates that construct dashboards, alerts and so on, to connect a device without any coding. Device developers still need to create code to run on the devices, and that code must match the device template specification.

5.1.3. Sphere

Creates an end-to-end, highly secure IoT solution that encompasses everything from the hardware and OS to sending messages from the device to the message hub. Azure Sphere has built-in communication and security features for internet-connected devices. Best used for security-critical solutions.

- Sphere micro-controller unit (MCU), which processes the OS and signals from sensors
- Customized linux OS that handles communication with the security service
- Sphere security service (AS3), makes sure that the device is not maliciously compromised. It offers certificate-based authentication. After authenticating, AS3 pushes any OS or approved customer-developed software updates to the device

5.2. AI services

5.2.1. Machine learning service

Requires own data.

- Create a data processing pipeline
- Build models
- Deploy models as an API to an endpoint

5.2.2. Cognitive services

Prebuild ML models for computer vision, NLP, speech, recommendation (Cognitive Services Personalizer). Used to get predictions on existing models.

5.2.3. Bot service

Virtual agents that interacts with humans, with a specific use case. It can rely on other AI services.

5.3. Serverless

5.3.1. Functions

Hosts a single method or function that runs in response to an event. Scale automatically, and charges accrue only when a function is triggered. It is a stateless environment, a function behaves as if it's restarted every time it responds to an event. Pricing depends on the number of executions and the running time of each.

Orchestration can be performed using Durable Functions, by chaining functions together while maintaining state.

5.3.2. Logic apps

Code/no-code orchestration platform hosted as a cloud service. it is designed in a web-based designer and can execute logic triggered by Azure services, without writing any code. It is priced based on the number of executions and the type of connectors that it uses.

5.4. DevOps

- Repos: source-code repository
- Boards: agile project management suite
- Pipelines: CI/CD pipeline automation tool
- Artifacts: repository for hosting artifacts: compiled source code, which can be fed into testing or deployment pipeline steps
- Test plans: automated test tool that can be used in a CI/CD pipeline to ensure quality before a software release
- DevTest labs: automated way to manage building, setup, and experiments, which involve tearing down VMs.

Github vs. Azure DevOps: the second one allows a much more granular set of permissions.

5.5. Portals

- Azure Portal
    - During Private Preview phase, Microsoft invites a few customers to take part in early access to new concepts and features. After the public preview is completed, the feature is open for any licensed customer to use and is supported via all Microsoft support channels
    - Any new service that is in the Public Preview state is marked in Azure portal with a (Preview) label, which makes it easy to distinguish the service from a service that is in GA phase
- Azure mobile app
- Azure PowerShell, to run cmdlets. Windows-friendly
- Azure CLI, to run commands in bash. Linux-friendly

- In Azure Cloud shell (interactive, authenticated, browser-accessible shell), you can run bash and powershell
- Local PowerShell or CommandPrompt, needs installation of Azure CLI module
- ARM templates: write resources you want in a JSON format, and the template orchestrates the creation of these resources

5.6. Monitoring

5.6.1 Advisor

Evaluates Azure resources and makes recommendations to improve cloud optimization. The recommendation service includes suggested actions that you can take, postpone or dismiss. For example points out unused or underutilized resources. Makes recommendations on:

- Reliability
- Security
- Performance
- Cost
- Operational excellence

For example, it can provide recommendations on VMs that aren't backed up and enables you to back up these VMs.

5.6.2. Monitor

Platform for collecting, analyzing, visualizing and potentially taking action based on the metric and logging data from the entire Azure and on-premises environment.

Additionally, you can use the data to help you react to critical events in real time, through alerts delivered to teams via SMS, email, and so on. Or you can use thresholds to trigger autoscaling functionality to scale up or down to meet the demand.

Some popular products such as Azure Application Insights, a service for sending telemetry information from application source code to Azure, uses Azure Monitor under the hood. With Application Insights, your application developers can take advantage of the powerful data-analysis platform in Azure Monitor to gain deep insights into an application's operations and diagnose errors without having to wait for users to report them.

5.6.3. Service health

Personalized view of the health of Azure services, regions and resources you manage. You can set up alerts to help triage outages and planned maintenance. After an outage, Service health provides official incident reports, called root cause analyses (RCAs). It helps deal with

- Service issues
- Planned maintenance
- Health advisories, issues that require you to act to avoid service interruption. Health advisories are announced in advance to allow you to plan

It doesn't help with network setings for VMs, for example.

Azure Service Health include 3 services:

- Status: informs you of service outages
- Service health: personalized view of the health of services and regions. It can create notifications or alerts when there are status changes
- Resource health: information about the health of individual resources, such as a specific VM instance

6. Security

6.1. Security center

Provides visibility of your security posture across all your services, on Azure and on-prem.

Monitoring service to see security posture across all services, Azure and on-prem. Security posture: cybersecurity policies and controls, as well as how well you can predict, prevent and respond to security threats. It can:

- Monitor security settings across on-premises and cloud workloads
- Automatically apply required security settings to new resources as they come online
- Provide security recommendations that are based on your current configurations, resources, and networks
- Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited
- Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources. You can also use adaptive application controls to define rules that list allowed applications to ensure that only applications you allow can run
- Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred
- Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to

The overall secure score measures how good an organization's security posture is You can see how many compliance controls you have passed.

Also resource security hygiene with 3 tiers (low, medium and high severity).

6.2. Sentinel

SIEM system (security information and event management). Such a system aggregates security data from many different sources, and provides capabilities for threat detection and response.

- Collect cloud data at scale
- Detect threats
    - Built-in analytics: known threat templates
    - Custom analytics: you can create rules to search for specific criteria
- Investigate threats with AI
- Respond rapidly to incidents with the investigation graph
    - With Monitor workbooks, you can set an alert that looks for malicious IP addresses and create a workbook that: opens a ticket, sends a message to the channel in teams/slack, send all the info to the admins in an email with 2 options: block or ignore

- Connect data sources: Microsoft solutions, other services and industry-standard data sources

6.3. Key vault

Centralized cloud service to store secrets in a single, central location.

- Manage secrets: tokens, passwords, certificates, API keys
- Manage encryption keys
- Manage SSL/TLS certificates
- Store secrets backed by hardware security modules (HSMs)

Benefits:

- Centralized application secrets
- Securely stored secrets and keys
- Access monitoring and access control
- Simplified administration of application secrets
- Integration with other Azure services

6.4. Dedicated host

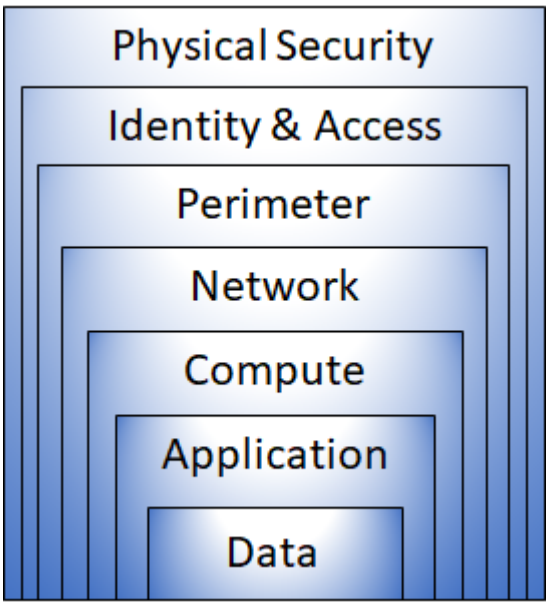
For applications that must follow regulatory compliance that requires them to be the only customer using the physical machine hosting their VMs, dedicated hosts provides dedicated physical servers.

- Allows visibility and control over the server infrastructure
- Helps address compliance requirements
- Lets you choose the number of processors, server capabilities, VM series and VM sizes

The charge is per dedicated hosts, independent of how many VMs you deploy to it. The host price is based on the VM family, type (hardware size) and region.

7. Network security

Defense in depth protects information and prevents it from being stolen. It's a set of layers, with the data to be secured at the center.



Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert telemetry that security teams can act upon, either automatically or manually.

1. Physical security: access to buildings and hardware
2. Identity & access: control access, single sign-on (SSO) and MFA
3. Perimeter: DDoS protection, perimeter firewalls
4. Network: limits communication between resources through segmentation and access controls. deny by default
5. Compute: secures access to VMs, endpoint protection, keep systems patched and current
6. Application: ensure that apps are free of vulnerabilities, store secrets securely
7. Data: most data is stored in databases, disks, on SaaS apps

> Security posture

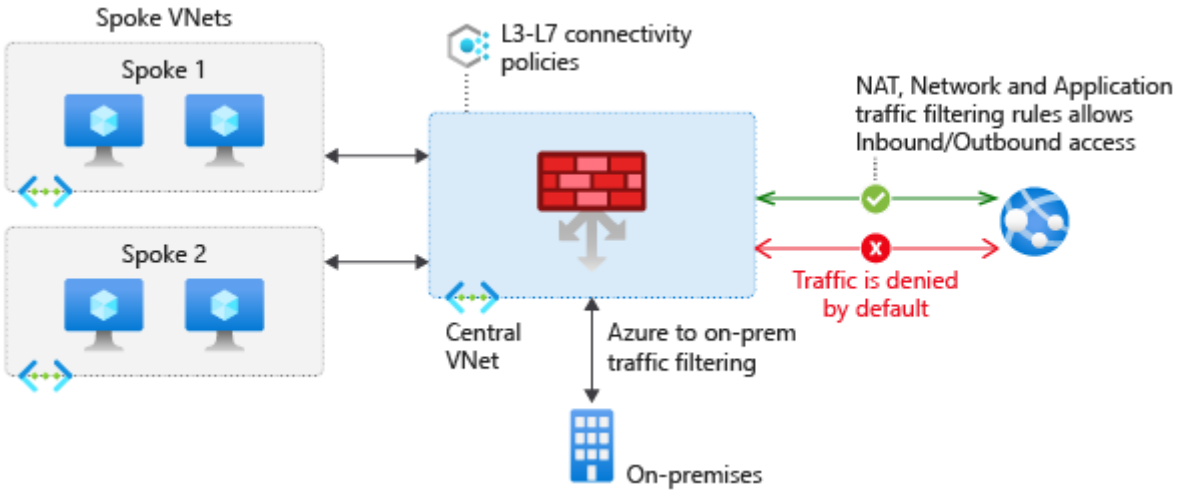
It's the ability to protect from and respond to security threats.

- Confidentiality: the principle of least privilege, restrict access to information only to individuals explicitly granted access, at only the level that they need to perform their work
- Integrity: prevent unauthorized changes to information: at rest, and in transit
- Availability: ensures that services are functioning and can be accessed only by authorized users. DDoS attacs are designed to degrade the availability of a system

7.1. Azure Firewall

Azure Firewall is a stateful firewall. A stateful firewall analyzes the complete context of a network connection, not just an individual packet of network traffic. Azure Firewall features high availability and unrestricted cloud scalability.

Here's a diagram that shows a basic Azure Firewall implementation:



- Built-in high availability
- Unrestricted cloud scalability
- Inbound and outbound filtering rules
- Inbound Destination Network Address Translation (DNAT) support
- Azure Monitor logging

7.2. DDoS protection

A DDoS attack attemps to overwhelm and exhaust an app's resources, making the app slow and unresponsive to legitimate users. 3 service tiers:

- Basic: automatically enabled for free. This ensures that Azure infrastructure itself is not affected during a large-scale DDoS attack. The Azure global network is used to distribute and mitigate attack traffic across regions
- Standard: provides always-on traffic monitoring and real-time mitigation of common network-level attacks. The Azure global network is used to distribute and mitigate attack traffic across Azure regions

DDoS proteciton can help prevent:

- Volumetric attacks: flood the network layer with seemingly legitimate traffic
- Protocol attacks: exploit weaknesses in layer 3 and 4 protocol stack
- Resource layer (app-layer) attacks: layer 7, to prevent it you need a web application firewall (WAF)

7.3. Network security group (NSG)

Internal firewall that enables the filtering of network traffic to and from Azure resources within an Azure VPC. It can contain several inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol (UDP/TCP).

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

> How to secure specific layers

- Perimeter layer
  - DDoS protection
  - Azure Firewall with perimeter firewall
- Network layer: allow only the network connectivity that is required
  - Limit communication between resources by segmenting your network and configuring access controls
  - Deny by default
  - Restrict inbound internet access and limit outbound where appropriate
  - Implement secure connectivity to on-premises networks

> Combine services

- NSGs and Azure Firewall
  - NSGs provide distributed network-layer traffic filtering to limit traffic to resources within virtual networks in each subscription
  - Azure Firewall provides network-level and application-level protection across different subscriptions and virtual networks
  - together they provide better defense-in-depth network security
- Azure WAF and Azure Firewall
  - WAF is part of Azure application gateway, it provides the web apps with centralized, inbound protection

    - Azure Firewall provides
        - Inbound protection for non-HTTP/S protocols (RDP, SSH, FTP)
        - Outbound network-level protection for all ports and protocols
        - Application-level protection for outbound HTTP/S

8. Identity, governance, privacy and compliance

- Authentication: process of establishing the identity of a person/service that wants to access a resource. It establishes whether the user is who they say they are
- Authorization: process of establishing what level of access an authenticated person/service has. It specifies what data they're allowed to access and what they can do with it

8.1. Active Directory

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your own organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally, and also detects suspicious sign-in attempts from unexpected locations or unknown devices. Azure AD services:

- Authentication
- Single sign-on
- Application management
- Device management

An Azure AD tenant can have multiple subscriptions (and this data can be changed) but an Azure subscription can only be associated with one Azure AD tenant. If your subscription expires, you lose access to all the other resources associated with the subscription. However, the Azure AD directory remains in Azure. You can associate and manage the directory using a different Azure subscription.

AD allows to join Windows devices, not Android devices.

8.2. Multifactor authentication

Additional security for your identities by requiring 2+ elements to fully authenticate. These can be:

- Something the user knows (email address, password)
- Something the user has (a code on the phone)
- Something a user is (biometric, fingerprint, face scan)

8.3. Conditional access

A tool that Azure AD uses to allow/deny access to resources based on *identity signals*: who the user is, where, and what device the user is requesting access from. It's a more granular MFA.

8.4. IAM

With role-based access control (RBAC), you can create roles that define access permissions.

Resource locking: a warning system that reminds you that a resource should not be deleted/changed. When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you

add later inherit the lock from the parent.

- CanNotDelete: can't delete the resource until the authorized person removes the lock
- Read-only: authorized people can read a resource, but can't delete/change it. If this lock exists, the CanNotDelete lock can be applied as well

To modify a locked resource, first remove the lock. Then apply the action that you have permission to perform.

Azure Policy enables you to create, assign, and manage policies that control or audit your resources.

> For example, you create a policy in a resource group saying that virtual networks aren't allowed in your resource group. All the VNs until then will continue to work normally, but you won't be able to add new VNs.

With Azure Blueprints, you can set standard resources that you require. For example, you can create a blueprint that specifies that a certain resource lock must exist. If the lock is removed, the blueprint replaces it.

8.5. Governance and compliance

- Microsoft privacy statement: provides trust in how Microsoft collects, protects and uses customer data
- Trust center: documentation about compliance standards
- Azure compliance documentation: legal and regulatory standards and compliance

9. Costs

9.1. TCO calculator

Total cost of ownership, estimates the cost savings of using Azure.

1. Enter the details of your on-premises workload (servers, databases, storage, networking)
2. Review the suggested industry average corsts for related operational costs (electricity, network maintenance, IT labor)
3. View side-by-side report

9.2. Pricing calculator

Estimate the accurate cost based on region, tier, billing options, support options, programs and offers. You can access pricing details, product details, and documentation for each product from within the Pricing calculator.

9.3. Service level agreement (SLA)

A SLA is a formal agreement between a service company and the customer, which defines the performance standards that Microsoft commits to the customer. Each Azure service defines its own SLA.

The primary performance commitment typically focuses on uptime, or the percentage of time that a service is successfully operational. Other SLAs focus on latency, how fast the service must respond to a request.

A *service credit* is the percentage of the fees the customer paid that are credited back according to the claim approval process. Credits typically increase as uptime decreases.