Microsoft Azure - Advanced Concepts

# Azure SLAs & Benefits

Service Level Agreements (SLAs) in Azure define Microsoft’s commitment to uptime and connectivity for services.   
- SLAs guarantee availability (e.g., 99.9%, 99.95%, or 99.99%) depending on the service.   
- They provide financial credits if availability commitments are not met.   
Benefits: High availability, business continuity, fault tolerance, and trust in cloud reliability.

**What is an SLA?**

A **Service Level Agreement (SLA)** is a formal contract provided by Microsoft that defines the **availability, uptime, and performance** guarantees of Azure services. It assures customers that Azure services will be operational and accessible for a defined percentage of time.

**Key Points about Azure SLAs:**

1. **Availability Guarantee:**
   * Example: 99.9%, 99.95%, 99.99% uptime.
   * This ensures services are accessible most of the time in a given month.
2. **Service-specific SLAs:**
   * Each Azure service (e.g., Virtual Machines, SQL Database, Storage, etc.) has its own SLA.
   * Example:
     + Azure VMs (with Premium SSDs in Availability Zones) → 99.99% uptime.
     + Azure Cosmos DB → 99.999% (five-nines) availability.
3. **Financial Backing:**
   * If Microsoft fails to meet SLA commitments, customers receive **service credits**.
4. **Composite SLAs:**
   * When combining multiple services (e.g., App Service + SQL Database), the overall SLA is calculated by multiplying individual SLAs.

**Benefits of Azure SLAs**

1. **High Availability:** Ensures critical applications remain online and accessible.
2. **Business Continuity:** Reduces downtime, protecting revenue and reputation.
3. **Trust & Reliability:** Organizations can confidently run mission-critical workloads.
4. **Cost Justification:** Financial credits compensate for downtime.
5. **Compliance & Risk Management:** Helps businesses meet SLAs required in contracts with their own customers.

**Example SLA Numbers**

* **99.9% availability** → ~43 minutes downtime per month.
* **99.95% availability** → ~22 minutes downtime per month.
* **99.99% availability** → ~4 minutes downtime per month.
* **99.999% availability** → ~26 seconds downtime per month.

**User Story – E-commerce Company on Azure**

**Scenario:**

An **e-commerce company (ShopX)** runs its online shopping portal on **Azure App Services** with a backend **Azure SQL Database**. During holiday sales, even a few minutes of downtime could mean losing **millions in revenue** and customers.

**Implementation:**

* ShopX deploys its web app in **multiple Availability Zones**.
* It chooses Azure SQL Database with **99.99% SLA** and App Service with **99.95% SLA**.
* The composite SLA is calculated as:
  + 0.9999 × 0.9995 = **99.94% availability**.
* This means ShopX’s portal can be down for only ~26 minutes per month.

**Benefit in Action:**

* During a major sale, ShopX experiences an **Azure VM outage** in one zone.
* Because of **multi-zone deployment**, the application automatically fails over to another zone, minimizing downtime.
* The customers experience uninterrupted shopping, and ShopX avoids losing revenue.
* If downtime exceeds SLA, Microsoft provides **financial credits** which ShopX can use against future billing.

Note: In this way, Azure SLAs provide **confidence, resilience, and cost protection** for businesses relying on the cloud.

# Azure Networking Services

**Azure Virtual Network (VNet)**

* Equivalent to a traditional on-premises network but hosted in the cloud.
* Allows Azure resources (VMs, Databases, App Services, etc.) to securely communicate with each other.
* Supports **subnets, routing, firewalls, and IP addressing**.
* You can connect VNets to each other (VNet Peering) or to on-premises networks (VPN/ExpressRoute).

# Azure AD & RBAC

\*\*Azure Active Directory (Azure AD)\*\*: A cloud-based identity and access management service.   
- Provides single sign-on (SSO), multi-factor authentication (MFA), and secure access to apps.   
- Enables integration with Microsoft 365, SaaS apps, and on-premises Active Directory.   
  
\*\*Role-Based Access Control (RBAC):\*\*   
- Enables fine-grained access management to Azure resources.   
- Roles (Owner, Contributor, Reader, Custom Roles) define what actions users can perform.   
- Helps enforce least privilege security model.

# Azure Blueprints & Policies

\*\*Azure Blueprints:\*\*   
- Allow organizations to define and deploy a set of governance artifacts (ARM templates, policies, role assignments, resource groups).   
- Used for compliance, security, and consistency in environments.   
  
\*\*Azure Policies:\*\*   
- Define rules to enforce organizational standards.   
- Examples: Restricting VM sizes, enforcing tag usage, requiring encryption.   
- Provides compliance monitoring and remediation.

**1. Introduction**

In cloud environments, **governance and compliance** are critical. Organizations must ensure that resources are deployed in a **controlled, secure, and compliant** way.  
Azure provides two powerful tools for this:

* **Azure Blueprints** → For standardized, repeatable environment deployments.
* **Azure Policies** → For enforcing rules and compliance after deployment.

**2. Azure Blueprints**

**What are Azure Blueprints?**

Azure Blueprints allow you to **orchestrate the deployment of multiple governance artifacts** such as:

* **Role Assignments** (who can access resources)
* **Policy Assignments** (what rules to enforce)
* **ARM Templates** (infrastructure as code)
* **Resource Groups** (logical containers for resources)

It’s like creating a **blueprint/template** for an environment that can be repeatedly applied to multiple subscriptions or tenants.

**Key Features of Azure Blueprints**

1. **Repeatability:** Deploy environments consistently across multiple subscriptions.
2. **Compliance:** Ensure all resources follow organizational standards.
3. **Versioning:** Maintain different versions of a blueprint for updates and rollbacks.
4. **Locking:** Prevent accidental deletion or modification of critical resources.
5. **Integration with CI/CD:** Automate deployments for faster rollout.

**Use Cases of Azure Blueprints**

* Enforcing **enterprise security** standards across multiple departments.
* Automating deployment of **regulated environments** (e.g., HIPAA, ISO, GDPR).
* Quickly setting up **dev/test/prod environments** with predefined configurations.
* Ensuring every new subscription has the same **baseline policies, RBAC roles, and resources**.

**3. Azure Policies**

**What are Azure Policies?**

Azure Policies define **rules and constraints** for resources to enforce compliance.  
They ensure resources stay within **organizational or regulatory guidelines**.

**Key Features of Azure Policies**

1. **Policy Definitions:** The rule itself (e.g., “VMs must use managed disks”).
2. **Initiatives:** A group of policies bundled together for easier management.
3. **Assignments:** Applying policies to specific scopes (management group, subscription, resource group).
4. **Compliance Reporting:** View which resources are compliant/non-compliant.
5. **Remediation:** Automatically fix non-compliant resources if configured.

**Examples of Azure Policies**

* Allow only specific **VM sizes** to be deployed.
* Require resources to have **tags** (like Department=Finance).
* Enforce data to be stored only in **specific Azure regions**.
* Require **encryption** for all storage accounts.
* Deny creation of public IP addresses.

**Benefits of Azure Policies**

* Enforces **governance and security** automatically.
* Ensures compliance with **industry regulations**.
* Provides **real-time compliance checks**.
* Reduces human errors by automating enforcement.

**4. How Blueprints & Policies Work Together**

* **Azure Policies** enforce **ongoing compliance** (e.g., VMs must use managed disks).
* **Azure Blueprints** deploy the **initial setup** (e.g., create a Resource Group, assign RBAC roles, enforce encryption policy).

Think of Blueprints as **planning and deploying a city**, while Policies are **the laws that govern it**.

**5. Real-World Example – Bank Compliance**

A **banking company** must ensure:

1. All resources are deployed in **East US region**.
2. Every resource has a **CostCenter tag** for billing.
3. SQL databases must be encrypted.
4. Only authorized roles (Finance Admins) can manage the environment.

**Solution:**

* **Blueprint**:
  + Deploys a Resource Group for Finance.
  + Assigns RBAC roles (Finance Admin).
  + Assigns policies like “Allowed Location = East US.”
* **Policies**:
  + Enforce tags (CostCenter required).
  + Deny unencrypted SQL databases.
  + Deny VMs outside East US.

This ensures every finance environment is deployed consistently, and ongoing compliance is enforced.

**Summary:**

* **Azure Blueprints** = Automated deployment of environments (baseline governance).
* **Azure Policies** = Continuous enforcement of compliance rules.
* Together, they enable **secure, compliant, and standardized Azure environments**.

# Conditional Access & Zero Trust

\*\*Conditional Access:\*\*   
- A policy-based approach to enforce access control based on user, device, location, or risk.   
- Example: Require MFA when accessing from outside the corporate network.   
  
\*\*Zero Trust Security Model:\*\*   
- "Never trust, always verify" approach.   
- Assumes breaches are inevitable, and every access request is validated.   
- Uses identity verification, device compliance, least privilege, and monitoring.

Real Time Example:

# Defender for Cloud

Microsoft Defender for Cloud (formerly Azure Security Center):   
- A cloud-native security solution providing threat protection and compliance.   
- Features include:   
 - Security posture management   
 - Threat detection and alerts   
 - Recommendations for hardening resources   
 - Supports hybrid and multi-cloud environments.

**1. What is Defender for Cloud?**

* **Microsoft Defender for Cloud** is a **cloud-native security solution** that helps organizations protect workloads across **Azure, on-premises, and multi-cloud** (AWS, GCP).
* It provides:
  + **Threat protection**
  + **Security posture management (CSPM)**
  + **Compliance monitoring**
  + **Workload protection (CWPP)**

**2. Key Features**

**a) Cloud Security Posture Management (CSPM)**

* Continuously assesses resources (VMs, Storage, SQL, etc.) for misconfigurations.
* Gives **secure score** to measure security posture.
* Recommends fixes (like enabling encryption, securing ports, updating OS).

**b) Cloud Workload Protection (CWPP)**

* Protects workloads across **Azure, on-premises, AWS, GCP**.
* Includes protection for:
  + **Virtual machines (Windows/Linux)**
  + **Databases (SQL, Cosmos DB, PostgreSQL, etc.)**
  + **Storage accounts (Blob, Files, etc.)**
  + **Containers (AKS, Kubernetes, Docker)**
  + **App services & Functions**

**c) Threat Protection**

* Detects attacks using **AI & threat intelligence**.
* Examples of detected threats:
  + Brute-force attacks on VMs.
  + SQL injection attempts on databases.
  + Suspicious access patterns.
* Integrates with **Microsoft Sentinel (SIEM)** for deeper investigation.

**d) Compliance & Governance**

* Provides regulatory compliance dashboard.
* Supports standards like:
  + ISO 27001
  + NIST
  + PCI-DSS
  + GDPR
* Shows compliance score and non-compliance resources.

**e) Integration**

* Works with **Azure Policy** for enforcement.
* Can integrate with **Microsoft Defender XDR** for unified protection.

**3. Benefits**

* **Unified security** across hybrid and multi-cloud.
* **Proactive threat detection** using AI.
* **Improved compliance** with continuous assessments.
* **Faster incident response** via integration with Sentinel.
* **Cost savings** by reducing breaches and downtime.

**4. Real-World Example – FinBank**

**Scenario**

A **bank (FinBank)** migrates critical workloads (customer accounts, payment apps) to Azure. Security and compliance are top priority.

**How Defender for Cloud helps:**

1. **Security Posture (CSPM):**
   * Defender identifies open RDP ports on VMs.
   * Recommends closing ports and using Just-in-Time (JIT) VM access.
   * Secure Score improves after remediation.
2. **Workload Protection (CWPP):**
   * Protects FinBank’s SQL databases from SQL injection.
   * Monitors suspicious queries (e.g., mass data export attempts).
3. **Threat Detection:**
   * Detects brute-force login attempts on internet-facing VMs.
   * Alerts security team instantly with remediation steps.
4. **Compliance:**
   * FinBank must comply with **PCI-DSS** (payment security standard).
   * Defender maps bank’s workloads to PCI controls and highlights gaps.
5. **Integration:**
   * Alerts sent to **Microsoft Sentinel** for centralized monitoring.
   * Automated playbooks trigger MFA enforcement if anomalies are detected.

**Result:**  
FinBank runs secure workloads, complies with regulations, and proactively responds to threats using **Defender for Cloud**.

# Azure Cost Management Tools

Azure provides tools to monitor and optimize spending:   
1. \*\*Azure Cost Management + Billing\*\*: Tracks cloud expenses, sets budgets, and forecasts costs.   
2. \*\*Azure Pricing Calculator\*\*: Estimates cost of services before deployment.   
3. \*\*Azure TCO Calculator\*\*: Compares cost of on-premises infrastructure vs. Azure.   
4. \*\*Azure Advisor\*\*: Recommends cost optimization strategies (e.g., resizing VMs, shutting down idle resources).

# Azure Resource Manager (ARM)

Azure Resource Manager (ARM) is the deployment and management service for Azure.   
- Provides a consistent management layer to deploy, update, and delete resources.   
- Uses ARM templates (JSON-based) for infrastructure as code (IaC).   
- Benefits: Declarative syntax, dependency management, resource grouping, and RBAC integration.   
- ARM ensures idempotency, meaning deployments can be repeated with the same result.