**1. Azure AI Services Kavramları & Kaynak Türleri**

**1.1. Temel AI Hizmetleri**

* **Azure OpenAI**:
  + GPT serisi ve DALL·E modellerine REST/SDK yoluyla erişim.
  + **İpucu:** Sıkça “model deployment”, “prompt design”, “temperature/prompt tuning” soruları gelir.
* **Azure AI Vision**:
  + Görüntüde nesne algılama, caption generation, OCR.
  + **İpucu:** “Computer Vision Read API” vs “Analyze API” farkını bilin.
* **Azure AI Speech**:
  + Speech-to-text, text-to-speech, speaker recognition, speech translation.
  + **İpucu:** Custom Speech vs Standard Speech SKU’ları arasındaki farkı kavra.
* **Azure AI Language**:
  + Entity Recognition, Sentiment Analysis, Text Summarization, Conversational Language Understanding (LUIS).
  + **İpucu:** “Language Studio” içindeki QnA Maker ve LUIS dizayn seçeneklerini hatırla.
* **Azure AI Translator**:
  + Gerçek zamanlı veya toplu çeviri.
  + **İpucu:** Custom Translator ile “Translation glossaries” kullanımı önemli.
* **Azure AI Face / Custom Vision / Document Intelligence / Content Safety / Content Understanding / AI Search**
  + Özet: Yüz tanıma, özel görüntü sınıflandırma, belge alan çıkarımı, içerik güvenliği, çok modlu içerik analizi, arama & vektör indeksleme.
  + **İpucu:** AI Search’te “Skillset” ve “Indexer” kavramlarını ayırt edebilmelisin.

**1.2. Standalone vs Multi-Service Kaynaklar**

| **Tür** | **İçerdiği Hizmetler** | **Ne Zaman?** |
| --- | --- | --- |
| **Standalone** | Her bir servis için ayrı kaynak (ör: yalnızca Vision, yalnızca Speech). | Küçük/tekil senaryolar; ücretsiz katmanları kullan. |
| **Multi-Service** | Tek endpoint altında birden çok servis.  - **Azure AI services**  - **Azure AI Foundry** | Çoklu AI iş yükleri; yönetimi merkezileştirmek istediğinde. |

* **Azure AI services** (multi-service): Speech, Language, Translator, Vision, Face, Custom Vision, Document Intelligence
* **Azure AI Foundry** (multi-service + ek özellikler): yukarıdakiler + OpenAI, Content Safety, Content Understanding

**İpucu:** Sınavda “hangi durumda multi-service, hangi durumda standalone tercih edilir?” sorusu gelebilir—yönetim, maliyet ve erişim kilit kriterlerdir.

**2. Azure AI Foundry – Proje Tabanlı Geliştirme**

**2.1. Neden Azure AI Foundry?**

* **Proje organizasyonu**: Resource bağlantıları, veri, kod ve dağıtımlar portal üzerinde gruplanır.
* **Yönetim kolaylığı**: Erişim kontrolü, izleme, maliyet takibi merkezi.
* **Gelişmiş araçlar**:
  + **Foundry SDK** ile kod tabanlı otomasyon.
  + **Responsible AI** değerlendirme araçları (fairness, interpretability).

**2.2. Proje Türleri**

| **Proje Türü** | **Özellikler** |
| --- | --- |
| **Foundry projects** | - Azure AI Foundry kaynağına bağlanır - OpenAI modelleri, Agent Service, diğer AI servisleri merkezden yönetilir |
| **Hub-based projects** | - Azure AI Hub kaynağı (Foundry + managed compute + Prompt Flow + storage & Key Vault entegrasyonu) - ML portal ile entegrasyon desteği |

* **Foundry Project**: Genellikle sohbet uygulamaları ve ajanlar için yeterli.
* **Hub-based Project**: Çok disiplinli ekipler, Prompt Flow tasarımı, özel model ince ayarı (fine-tuning) senaryolarında tercih edilir.

**İpucu:** AI-102 sorularında “hangi proje türü hangi senaryoya uygundur?” gibi karşılaştırma soruları gelebilir.

**3. Kaynak Oluşturma & Tüketim**

1. **Provision**
   * Portal / Azure CLI (az cognitiveservices account create) / ARM / Bicep
2. **Yetkilendirme**
   * Anahtar + endpoint (connection string) <br>– ya da Managed Identity ile Key Vault’tan çekme
3. **Tüketim**
   * REST API çağrıları (doğrudan HTTP)<br>– ya da SDK’lar (Python, C#, JavaScript)
4. **Görsel Araçlar**
   * **Language Studio**, **Vision Studio**, **Document Intelligence Studio**, **Custom Vision Portal**

**İpucu:** Sınavda “CLI ile resource oluşturma” veya “Managed Identity kullanarak çağrı yapma adımları” sorulabilir.

**4. Bölgesel Kullanılabilirlik & Maliyet**

* **Region Awareness**:
  + Bazı modeller (ör. GPT-4o, DALL·E 3) her bölgede yoktur.
  + **Exam Tip:** “modelAvailability” API’si ile kontrol edilebilir.
* **Pricing**:
  + Farklı servislerde farklı fiyatlama modelleri (istek başı, karakter/saat bazlı, sayfa başı).
  + **Ücretsiz katman**: Genellikle 5K istek/ay’a kadar ücretsiz.
  + **Cost Management**: Bütçe uyarıları, harcama uyarı politikaları oluştur.

**İpucu:** “En ucuz çözüm” veya “maliyet optimizasyonu” temalı senaryolarda free-tier, minimal SKU vb. kavramları kullan.

**5. Sınavda Dikkat Etmen Gerekenler**

* **Terminoloji**: Skill, indexer, endpoint, deployment, project vs. kavramlarına hâkim ol.
* **Senaryo Soruları**: Çoğu soru gerçek dünya senaryosu üzerinden “hangi servisi, hangi kaynak türünü, hangi kimlik doğrulamayı seçersin?” biçiminde gelir.
* **Hands-on Deneyim**: Portal’da hızlıca kaynak oluşturup test etme pratiği çok işine yarar.
* **CLI & SDK**: En az bir dilde (Python veya C#) örnek kod yazabildiğinden ve CLI komutlarından haberdar olduğundan emin ol.
* **Responsible AI**: Model interpretability, bias detection, logging ve explainability araçlarından soru gelebilir.

**1. Azure AI Services Concepts & Resource Types**

**Azure OpenAI**

**Question:**  
“You need to deploy a GPT-4 model with a custom prompt design for your chatbot. Which two parameters should you tune to control response creativity and length?  
A. temperature  
B. max\_tokens  
C. batch\_size  
D. stop\_sequences”

**Answer:** A. temperature, B. max\_tokens  
**Türkçe Açıklama:** “temperature” yanıtların yaratıcılığını, “max\_tokens” ise uzunluğunu kontrol eder.

**Azure AI Vision**

**Question:**  
“Your application needs to extract printed text from images and then detect objects. Which two REST endpoints should you call?  
– Read API  
– Analyze API  
– OCR API  
– Detect API”

**Answer:** Read API, Detect API  
**Türkçe Açıklama:** “Read API” metin çıkarımı, “Detect API” nesne algılama sunar.

**Azure AI Speech**

**Question:**  
“A customer wants real-time speech translation and speaker identification. Which SKU(s) support these features?  
A. Standard Speech  
B. Custom Speech  
C. Speech Translation  
D. Speaker Recognition”

**Answer:** C. Speech Translation, D. Speaker Recognition  
**Türkçe Açıklama:** “Speech Translation” gerçek zamanlı çeviri, “Speaker Recognition” konuşmacı tespiti sağlar.

**Azure AI Language**

**Question:**  
“You need to build a QnA bot that uses FAQs and supports sentiment analysis. Which two services do you configure?  
– Language Understanding (LUIS)  
– QnA Maker  
– Text Analytics  
– Translator”

**Answer:** QnA Maker, Text Analytics  
**Türkçe Açıklama:** QnA Maker SSS botu, Text Analytics ise duygu analizini destekler.

**Azure AI Translator**

**Question:**  
“Your solution must use a custom glossary to translate domain-specific terms. Which feature and service combination do you choose?  
A. Translator service + glossaries  
B. Language service + custom entities  
C. Custom Translator + translation glossaries  
D. Translator Text API + custom model”

**Answer:** C. Custom Translator + translation glossaries  
**Türkçe Açıklama:** Custom Translator, özel sözlüklerle terimleri doğru çevirir.

**AI Search vs. Other Services**

**Question:**  
“You have a blob of PDFs and want to build a semantic search index with vector embeddings. Which two components must you configure in Azure Cognitive Search?  
– Skillset  
– Indexer  
– Data source connection  
– Content Safety policy”

**Answer:** Skillset, Indexer  
**Türkçe Açıklama:** Skillset embedding üretir, Indexer ise dizin oluşturur.

**2. Azure AI Foundry – Project-Based Development**

**Scenario Requirements → Project Type**

* Centralized model & agent deployments → **Foundry Project**
* Fine-tuning custom LLMs and Prompt Flow support → **Hub-based Project**
* Shared compute for data-science notebooks → **Hub-based Project**
* Lightweight chat app with minimal admin overhead → **Foundry Project**

**Türkçe Açıklama:** Foundry projeleri hafif uygulamalar içindir; Hub-based projeler ise ileri senaryolar ve ince ayar için uygundur.

**3. Resource Provisioning & Consumption**

**Ordered Steps:**

1. az cognitiveservices account create ...
2. az identity create ...
3. Assign **Cognitive Services User** role to the managed identity
4. Store the resource’s endpoint in Azure Key Vault
5. Access Key Vault from your SDK code using default credentials

**Türkçe Açıklama:** Kaynağı IaC ile oluştur, Managed Identity’ye rol ata, uç noktayı Key Vault’a koy ve kodda doğrudan anahtar saklamaktan kaçın.

**4. Regional Availability & Cost Management**

**Multiple-Choice**

**Question:**  
“You plan to deploy DALL·E 3 but discover it isn’t yet available in your target region. Which two actions can you take?  
A. Deploy to the next nearest supported region and replicate via Front Door  
B. Use the modelAvailability REST API to confirm support  
C. Switch to a free-tier Custom Vision instance instead  
D. Request regional expansion from Azure support”

**Answer:** A. Deploy to the next nearest supported region and replicate via Front Door, B. Use the modelAvailability REST API to confirm support  
**Türkçe Açıklama:** Yakın bölgeye deploy edip Front Door ile yönlendirebilir veya modelAvailability API’siyle kontrol edebilirsiniz.

**Cost Scenario**

**Prompt:**  
You have a proof-of-concept chat application expected to send 10,000 messages/month. You need to keep costs under $50.

* **Which pricing tier and region do you select?**
  + Choose the free-tier (S0) or the lowest Standard tier (S1) in a low-cost region (e.g., *West US*).
* **How do you monitor and alert if spending exceeds $40?**
  + Create a budget alert in Azure Cost Management to notify via email when spend > $40.

**Türkçe Açıklama:** Free-tier veya düşük SKU, West US gibi uygun bölge; bütçe uyarısıyla harcamayı izleyin.

**5. What to Watch for on Exam Day**

**Case Study: Contoso Retail Document Pipeline**

1. **Provision:**
   * Blob Storage (ingest)
   * Azure AI Document Intelligence (Form Recognizer)
   * Azure Cognitive Search
   * Azure OpenAI (GPT deployment)
2. **Secure:**
   * **At Rest:** Storage Service Encryption
   * **In Transit:** HTTPS/TLS
   * **Access Control:** Managed Identity + RBAC, keys in Key Vault
3. **High-Level Steps (IaC or Portal):**
   * **IaC:** Define resources in ARM/Bicep (storageAccounts, cognitiveServices/accounts, searchServices, openai/deployments).
   * **Indexer:** Configure data source → skillset with Form Recognizer → index.
   * **Generative AI:** Query search index → feed results as prompt to GPT → summarize.

**Türkçe Açıklama:** Katmanlı bir mimari: veri ingest, alan çıkarımı, indeksleme, ardından GPT ile özet üretim.

**Türkçe Özet: Developer Tools ve SDK’lar**

Azure AI Foundry portalı üzerinden pek çok işi yapabilseniz de, gerçek dünyada kod yazmak, test etmek ve deploy etmek için uygun araçlar ve SDK’lar kullanmanız gerekir.

1. **Geliştirme Araçları & Ortamlar**
   * **Visual Studio**: .NET Framework odaklı, Windows uygulamaları geliştirenler için tam teşekküllü IDE.
   * **Visual Studio Code (VS Code)**: Çoklu dil ve kütüphane desteğiyle hafif, geniş eklenti desteği sunan kod editörü.
2. **Azure AI Foundry for VS Code Uzantısı**
   * Proje oluşturma
   * Model seçme ve deploy etme
   * Playground’da test etme
   * Ajan (agent) oluşturma
3. **GitHub & GitHub Copilot**
   * Kaynak kontrol ve DevOps için GitHub entegrasyonu
   * Copilot: Kod tamamlama ve örnek önerileriyle verimliliği artırır
4. **Yaygın Diller & SDK’lar**
   * **Diller**: C#, Python, Node.js/TypeScript, Java, vb.
   * **Azure AI Foundry SDK**: Foundry projelerine bağlanma, kaynak bağlantılarını yönetme
   * **Foundry Models API**: Generative AI modelleriyle etkileşim
   * **Azure OpenAI in Foundry Models API**: OpenAI tabanlı chat uygulamaları
   * **Azure AI Services SDKs**: Vision, Speech, Language, Translator, Search gibi servisler için kütüphaneler
   * **Foundry Agent Service**: Semantic Kernel gibi çerçevelerle ajan çözümleri geliştirme

**Olası Soru Tipleri ve Sınava Hazırlık**

**1. Multiple-Choice Soruları**

**Q1.** “You need to scaffold a new Azure AI Foundry project and deploy a GPT model from VS Code. Which two actions do you perform using the Azure AI Foundry extension?  
A. Create a project  
B. Configure Cost Management alerts  
C. Deploy a model  
D. Write IaC templates”

**İpucu:** A, C. (Uzantı proje oluşturma ve model deploy’a odaklıdır.)

**Q2.** “A developer wants to call the Text Analytics service from a Python application without storing keys in code. Which two steps are required?  
A. Install azure-ai-textanalytics SDK  
B. Store the API key in environment variables  
C. Assign a Managed Identity to the app  
D. Use DefaultAzureCredential to authenticate”

**İpucu:** A, D. (SDK + DefaultAzureCredential ile kimlik doğrulama.)

**2. Drag-and-Drop / Hot-Area Senaryoları**

**Scenario:**  
Your team uses GitHub for source control and wants AI-assisted code suggestions. You develop in VS Code on Windows.

**Task:** Drag each requirement to the tool/service:

| **Requirement** | **Tool/Service** |
| --- | --- |
| Integrated debugging for .NET code | Visual Studio |
| AI-assisted code completion | GitHub Copilot |
| Quick edits in JS/Python projects | VS Code |
| Repository & CI/CD pipelines | GitHub |

**3. Case Study Excerpt**

**You need to add AI functionality to an existing Java application:**

* Use Azure AI Vision SDK to detect objects in images at runtime.
* Automate deployment via pipeline.
* Secure credentials.

**Questions:**

1. Which SDK package do you include in your Maven project?
2. Outline the CLI or pipeline steps to deploy the Vision resource and grant permissions.
3. How do you store and retrieve the endpoint key securely in code?

**Çalışma:**

1. com.azure:azure-ai-vision
2. az cognitiveservices account create … + Managed Identity rol atama
3. Key Vault + DefaultAzureCredential

**4. Terminoloji ve Kavram Eşleştirme**

* **Azure AI Foundry SDK** → Kodla proje yönetimi
* **Playground** → Model testi
* **Semantic Kernel** → Ajan entegrasyonu
* **AZ CLI** → Kaynak oluşturma IaC senaryoları

**Responsible AI – Kapsamlı ve Detaylı Özeti**

Yapay zekâ tabanlı sistemler, insan benzeri kararlar alabilme yeteneği sayesinde güçlü çözümler sunar. Ancak bu gücü doğru ve etik bir şekilde kullanmak için sorumluluk çerçevesi oluşturmak gerekir. Aşağıda Microsoft’un benimsediği “Responsible AI” ilkeleri eksiksiz olarak ele alınmıştır.

**1. Adalet (Fairness)**

* **Tanım:** AI sistemlerinin tüm kişiler ve gruplar için ayrımcılık yapmadan, eşit muamele göstermesi.
* **Risk:** Eğitim verisindeki dengesizlikler (ör. belirli etnik grupların aşırı veya eksik temsil edilmesi) modelin önyargılı (biased) kararlar vermesine neden olabilir.
* **Uygulama Adımları:**
  1. **Veri İncelemesi ve Temizliği**
     + Demografik, sosyo-ekonomik, coğrafi vb. farklılıklara göre eğitim verisini analiz edin.
     + Aşırı temsil edilen veya ihmal edilen grupları dengeleyin (re-sampling, weighting).
  2. **Adil Metri̇kler Kullanımı**
     + Statistical Parity Difference, Equal Opportunity Difference, Disparate Impact gibi metri̇klerle modelin çıktısını ölçün.
  3. **Bias Mitigasyonu Teknikleri**
     + Pre-processing: Veriyi dönüştürerek önyargıyı azaltma.
     + In-processing: Model eğitimi sırasında fairness kısıtları ekleme.
     + Post-processing: Tahminleri adil hale getirmek için çıktı düzeltmeleri.
  4. **Sürekli İzleme**
     + Model yayına alındıktan sonra, yeni veriler ve alt grup performanslarını periyodik olarak değerlendirin.

**2. Güvenilirlik ve Emniyet (Reliability & Safety)**

* **Tanım:** AI sistemlerinin öngörülebilir, tutarlı ve güvenli sonuçlar üretmesi; kritik senaryolarda insan hayatını tehlikeye atmayacak şekilde çalışması.
* **Risk:** Otonom araçlar, tıbbi teşhis veya finansal kararlar gibi kritik uygulamalarda küçük hata bile ciddi sonuçlar doğurabilir.
* **Uygulama Adımları:**
  1. **Geniş Kapsamlı Testler**
     + **Birim Testi:** Her fonksiyonun beklenen girdi/çıktı davranışını doğrulayın.
     + **Entegrasyon Testi:** Modüller arası etkileşimleri test edin.
     + **Edge-Case Senaryoları:** Olağan dışı veya uç durum girdileriyle model davranışını inceleyin.
     + **Stres ve Yük Testi:** Aynı anda çok sayıda istek altında servis performansını değerlendirin.
  2. **Güven Skoru (Confidence Score) Eşiği**
     + Modelin verdiği olasılıksal çıktıya eşik uygulayın (örn. ≥%90 güven).
     + Eşik altı durumlar için insansal inceleme veya “fallback” mekanizması oluşturun.
  3. **Hata ve Anomali Yönetimi**
     + Uygulama içi hataları yakalayarak, kullanıcıya güvenli hata mesajları gösterin.
     + Anomali algılama ile beklenmeyen model davranışlarını tespit edin ve gerekli alarm/uyarı akışını tetikleyin.
  4. **Kararlılık Testleri**
     + Model güncellemeleri sonrası önceki sürümle çıktı karşılaştırması (A/B testi, shadow deployment) yapın.

**3. Gizlilik ve Güvenlik (Privacy & Security)**

* **Tanım:** Kullanıcı verilerinin ve modelin eğitildiği hassas bilgilerin yetkisiz erişimden korunması.
* **Risk:** Kişisel veri sızıntısı, modeli tersine mühendislik yaparak gizli bilgileri açığa çıkarma, GDPR/KVKK gibi düzenlemelere uymama.
* **Uygulama Adımları:**
  1. **Veri Şifreleme**
     + **At Rest:** Azure Storage Service Encryption (AES-256)
     + **In Transit:** HTTPS/TLS 1.2+ protokolleri
  2. **Erişim Kontrolü**
     + **RBAC (Role-Based Access Control):** En az ayrıcalık ilkesi (least-privilege)
     + **Managed Identity:** Uygulamaların Key Vault’tan secret çekmesini sağlar
     + **Azure Key Vault:** API anahtarları, connection string’ler, sertifikalar burada saklanır ve otomatik olarak döndürülür.
  3. **Veri Maskeleme & Anonimleştirme**
     + PII (Personally Identifiable Information) içeren alanları maskelenmiş şekilde saklayın veya kullanıcı verilerini anonimleştirin.
  4. **Denetim ve Loglama**
     + Erişim log’larını, hata log’larını ve veri erişim denetim izlerini tutun.
     + SIEM (Security Information and Event Management) sistemine entegre ederek gerçek zamanlı izleme yapın.

**4. Kapsayıcılık (Inclusiveness)**

* **Tanım:** AI sistemlerinin fiziksel, kültürel, demografik tüm kullanıcı profillerine hitap etmesi; engelli bireyler de dahil olmak üzere herkesin erişebileceği şekilde tasarlanması.
* **Risk:** Erişilebilirlik eksikliği, tek tip kullanıcı grubu düşünülerek tasarlanmış arayüzler ve modeller.
* **Uygulama Adımları:**
  1. **Erişilebilirlik Standartları**
     + WCAG 2.1 AA (Web Content Accessibility Guidelines) uyumlu UI geliştirin.
     + Ekran okuyucular, klavye navigasyonu ve renk kontrastı destekleyin.
  2. **Çok Dilli ve Kültürel Duyarlılık**
     + NLP modellerinde birden fazla dili ve lehçeyi destekleyin.
     + Kültürel farklılıklara göre eğitim verisini çeşitlendirin.
  3. **Kullanıcı Testleri ve Geri Bildirim**
     + Farklı yetenek ve demografik özelliklere sahip kişilerle prototip testleri yapın.
     + Geri bildirim döngülerini sık tutarak uygulamayı sürekli iyileştirin.

**5. Şeffaflık (Transparency)**

* **Tanım:** AI sisteminin nasıl çalıştığını, hangi verilerle eğitildiğini ve ne kadar güvenilir sonuçlar verdiğini kullanıcıya açıklama.
* **Risk:** “Black box” modeller, kullanıcıların sistemin neden belirli kararı verdiğini anlayamaması.
* **Uygulama Adımları:**
  1. **Model Belgeleri ve Metaveri**
     + Model mimarisi, eğitim veri kaynakları, eğitim miktarı (ör. 10.000 örnek), hiperparametre ayarları dokümante edin.
  2. **Açıklanabilir AI (Explainable AI)**
     + SHAP veya LIME gibi araçlarla her tahminin hangi girdilerin etkisiyle yapıldığını gösterin.
     + Arayüzde, önemli özellikleri ve etkilerini gösteren görselleştirmeler kullanın.
  3. **Güven Skoru ve Sınırlar**
     + Her tahmin için güven skorunu yanıt içinde sunun (örn. %78 güven).
     + Kullanıcılara modelin kısıtlarını ve hata oranlarını bildirin.

**6. Hesap Verebilirlik (Accountability)**

* **Tanım:** AI sisteminin tüm aşamalarından (veri toplama, model eğitimi, dağıtım) sorumlu gerçek kişilerin ve süreçlerin belirlenmesi.
* **Risk:** Belirsiz sorumluluk, hatalı sonuçlarda kimsenin hesap vermemesi.
* **Uygulama Adımları:**
  1. **Yönetişim ve Organizasyonel İlkeler**
     + AI Etik Kurulu veya Sorumluluk Birimi oluşturun.
     + Geliştirme süreçlerini yöneten politika ve prosedürler tanımlayın.
  2. **Denetim İzleri (Audit Trails)**
     + Model eğitim, versiyonlama, dağıtım ve tahmin log’larını kaydedin.
     + Değişiklik yönetimi ve sürüm kontrolü (Git, Azure DevOps) kullanın.
  3. **Sorumlu Roller**
     + Veri Sorumlusu (Data Steward), Etik Sorumlusu (Ethics Officer), Güvenlik Uzmanı (Security Officer) gibi roller belirleyin.

**Sınavda Karşınıza Çıkabilecek Örnek Sorular**

**A. Çoktan Seçmeli (Multiple Choice)**

**Soru:** “A loan approval model should ensure fairness. Which action best reduces bias?”  
A. Increase model depth  
B. Balance training data across demographics  
C. Lower confidence thresholds  
D. Disable data augmentation

**Cevap:** B  
*Türkçe Açıklama:* Eğitim verisini demografik gruplar arasında dengelemek, önyargıyı azaltır.

**B. Çoklu Yanıt (Multiple Response)**

**Soru:** “You’re building an autonomous vehicle AI. Which two practices improve reliability and safety?”

* Perform edge-case simulations
* Use HTTP for faster data transfer
* Set confidence score thresholds
* Disable exception handling

**Cevap:**

* Perform edge-case simulations
* Set confidence score thresholds  
  *Türkçe Açıklama:* Kenar durum testleri ve güven skoru eşiği, kritik sistemlerde hata riskini azaltır.

**C. Vaka İncelemesi (Case Study)**

**Scenario:** A medical diagnosis model uses patient data.  
**Soru:**

1. Nasıl veri gizliliği sağlarsınız?
2. Model karar sürecini kullanıcıya nasıl açıklarsınız?

**Cevap:**

1. Data şifreleme (at rest ve in transit), Key Vault, anonimleştirme.
2. Explainable AI ile önemli özellikleri ve güven skorunu gösteren arayüz.

**D. Sürükle-Bırak (Drag-and1. Multiple Choice**

**Q: “Which technique helps ensure fairness during model training?”  
A. Data augmentation  
B. Oversampling underrepresented groups  
C. Increasing learning rate  
D. Early stopping**

**Cevap: B  
Açıklama: Az temsil edilen grupları aşırı örnekleme ile dengelemek önyargıyı azaltır.**

**2. Multiple Response**

**Q: “You need to protect sensitive user data in an AI app. Which two practices do you implement?”**

* **Encrypt data at rest**
* **Store secrets in code**
* **Use HTTPS/TLS**
* **Disable authentication**

**Cevap:**

* **Encrypt data at rest**
* **Use HTTPS/TLS  
  Açıklama: Hem disk üzerinde hem iletişimde şifreleme veri güvenliğini sağlar.**

**3. Case Study Excerpt**

**Scenario: A recruitment chatbot evaluates resumes with an NLP model.  
Q1: How do you reduce gender bias in recommendations?  
Q2: How do you inform users about model limitations?**

**Cevap:**

1. **Eğitim verisinden cinsiyet etiketlerini kaldırıp dengeli veri kullanmak.**
2. **Arayüzde “Bu öneri modelin %80 güven skoru ile yapılmıştır” ibaresi eklemek.  
   Açıklama: Etiket temizleme bias’ı azaltır; güven skoru kullanıcıyı bilgilendirir.**

**4. Drag-and-Drop**

**Match each principle with its enforcement action:**

| **Principle** | **Action** |
| --- | --- |
| **Privacy** | **Use Azure Key Vault for secret management** |
| **Reliability** | **Define confidence score thresholds** |
| **Inclusiveness** | **Conduct user tests with diverse demographics** |

**5. Hot-Area**

**Q: “Select all practices that support transparency in an AI system:”**

* **Publish model training dataset size**
* **Hide model version information**
* **Display prediction confidence**
* **Remove feature importance graphs**

**Cevap:**

* **Publish model training dataset size**
* **Display prediction confidence  
  Açıklama: Eğitim verisi büyüklüğü ve güven skoru şeffaflığı artırır.**

**6. True/False**

**Q: “Using managed identities and Azure Key Vault eliminates hard-coded credentials in your application.”**

**Cevap: True  
Açıklama: Managed Identity ile kodda düz metin anahtar tutulmaz.**

**7. Sequencing**

**Order the steps for bias mitigation:**

1. **Measure bias metrics**
2. **Apply preprocessing techniques**
3. **Train model**
4. **Evaluate subgroup performance**

**Doğru Sıra: 2 → 3 → 1 → 4  
Açıklama: Önce veri dönüştürülür, model eğitilir, bias ölçülür, alt grup performansı değerlendirilir.**

**8. Multiple Choice**

**Q: “Which tool helps explain individual predictions of a black-box model?”  
A. Azure Monitor  
B. SHAP  
C. Azure DevOps  
D. Metricbeat**

**Cevap: B  
Açıklama: SHAP, her tahminin hangi özelliklerden etkilendiğini gösterir.**

**9. Multiple Response**

**Q: “To ensure accountability, an AI project should include:”**

* **Audit logs of model training**
* **No version control**
* **Defined governance policies**
* **Disabling error reporting**

**Cevap:**

* **Audit logs of model training**
* **Defined governance policies  
  Açıklama: Kayıt tutma ve net politika tanımı sorumluluk bilinci oluşturur.**

**10. Case Study Prompt**

**Scenario: Your AI system misclassifies images of darker-skinned individuals more often.  
Q: Which two actions help address this issue?**

**Cevap:**

1. **Eğitim veri setine daha fazla örnek ekleyerek cilt tonları dengesini sağlamak.**
2. **Modeli yeniden eğitirken fairness kısıtı (constraint) uygulamak.  
   Açıklama: Veri dengeleme ve fairness constraint bias’ı azaltır.**

**-Drop)**

**Eşleştirme:**

| **İlke** | **Uygulama Adımı** |
| --- | --- |
| Fairness | Re-sampling veya weighting ile veri dengesi sağlama |
| Transparency | Tahmin güven skorunu UI’da gösterme |
| Accountability | Denetim izleri ve sürüm kontrolü |

**E. Sıralama (Ordering)**

**Adımları doğru sırada seçin:**

1. Veri anonimleştirme
2. Model eğitimi
3. Bias metri̇kleri ile ölçüm
4. Bias azaltma yöntemi uygulama

**Doğru Sıra:** 1 → 2 → 3 → 4  
*Türkçe Açıklama:* Önce veriyi hazırla, modeli eğit, bias’ı ölç, sonra azaltma uygulamalarını yap.

**1. Azure AI Foundry ile Neler Yapabilirsiniz?**

1. **Model Yönetimi & Dağıtımı**
   * OpenAI GPT-4, GPT-4o, DALL·E ve diğer generative modelleri tek bir portal üzerinden listeleyebilir, konfigüre edip, tıklamayla dağıtabilirsiniz.
   * Version kontrol, A/B test ve canary deployment senaryolarını destekler.
2. **Chat Uygulamaları ve Ajanlar**
   * Hazır “agent” şablonları (sanal asistan, müşteri destek botu vb.) ile yapı taşları üzerinden hızlıca tamamlanmış çözüm oluşturabilirsiniz.
   * Prompt Flow ile kullanıcı girdisini farklı adımlarda işleyen iş akışları tasarlayabilirsiniz.
3. **Veri Entegrasyonu**
   * Azure Blob, Azure SQL, Azure Cosmos DB gibi veri kaynaklarını bağlayıp (Add your data) modelleri bu veriler üzerinde çalıştırabilirsiniz.
   * Vector Store (semantic search) ve bilgiyi “grounding” için kullanabilirsiniz.
4. **İzleme ve Güvenlik**
   * Görev performansı (Tracing, Monitoring) araçlarıyla latency, hata oranı, token kullanımı gibi metrikleri takip edersiniz.
   * Guardrails + Controls ile içerik güvenliği, Responsible AI politikaları ekleyebilirsiniz.
5. **SDK & API Erişimi**
   * REST API veya SDK’lar (Python, C#, JavaScript) üzerinden “End­point” ve “API key” kullanarak uygulamanızı kodla entegre edersiniz.
   * Managed Identity ile anahtar yönetimi ve Key Vault entegrasyonu mümkündür.

**2. Bu Model (gpt-4o) ile Neler Yapabilirsiniz?**

* **Doğal Dil Sorgulama:** Sohbet botları, soru-cevap sistemleri, sanal asistanlar.
* **İçerik Üretimi:** Makale, özet, açıklama, ürün tanıtımı, yaratıcı metinler.
* **Kod Desteği:** Kod tamamlama, örnek kod üretme, hata açıklamaları.
* **Çeviri & Dil Analizi:** Çok dilli sohbet, dil tespiti, dil değiştirme.
* **Eğitim & Öğretim:** Ders materyalleri, quiz soruları, interaktif rehber.

**3. API Key ve Endpoint Nasıl Kullanılır?**

1. **Endpoint**:
   * Her proje/provisioned resource için benzersiz bir URL (örn. https://<your-resource>.cognitiveservices.azure.com/)
   * REST çağrılarını bu adrese yaparsınız.
2. **API Key (Authorization)**:
   * Azure Portal’da **Keys and Endpoint** bölümünde bulursunuz.
   * HTTP header’da Ocp-Apim-Subscription-Key: <API\_KEY> olarak gönderilir.
   * SDK’larda AzureKeyCredential("<API\_KEY>") ile tanımlanır.
3. **Örnek REST Çağrısı (curl)**:

bash

KopyalaDüzenle

curl -X POST "https://<resource>.cognitiveservices.azure.com/openai/deployments/gpt-4o/chat/completions?api-version=2023-03-15-preview" \

-H "Content-Type: application/json" \

-H "api-key: <YOUR\_API\_KEY>" \

-d '{

"messages":[{"role":"user","content":"Hello, world!"}],

"max\_tokens":100

}'

1. **SDK (Python) Örneği**:

python

KopyalaDüzenle

from azure.core.credentials import AzureKeyCredential

from azure.ai.openai import OpenAIClient

client = OpenAIClient(endpoint="https://<resource>.cognitiveservices.azure.com/",

credential=AzureKeyCredential("<YOUR\_API\_KEY>"))

response = client.chat.completions.create(

deployment\_id="gpt-4o",

messages=[{"role":"user","content":"What is Azure AI Foundry?"}],

max\_tokens=150

)

print(response.choices[0].message.content)

**4. Gerçek Dünya ve Sınav Perspektifi**

* **Gerçek Dünya:**
  + Ürün uygulamalarınıza entegre ederek müşteri memnuniyetini artırabilir;
  + İçerik üretim süreçlerini otomatikleştirip hız kazanabilirsiniz;
  + Analiz ve raporlama asistanları oluşturabilirsiniz.
* **AI-102 Sınavı:**
  + “How do you secure your endpoint key?” gibi IAM ve Key Vault entegre soruları;
  + “Which HTTP header is required?” şeklinde REST API soruları;
  + “What SDK class sets authorization credentials?” gibi kod bilgisi soruları gelir.

**5. Sınava Yönelik 5 Örnek Soru**

1. **Multiple Choice:**  
   “You need to call your Azure AI Foundry gpt-4o deployment from a Python app without embedding the key in code. Which approach is best?  
   A. Store key in environment variable and use AzureKeyCredential  
   B. Hard-code key in source file  
   C. Use DefaultAzureCredential with Managed Identity  
   D. Pass key as query string parameter”

**Answer:** C

1. **True/False:**  
   “When invoking the REST endpoint, you must include the API key in the Authorization header with value Bearer <key>.”

**Answer:** False (Use api-key or Ocp-Apim-Subscription-Key, not Bearer.)

1. **Case Study Excerpt:**

**Scenario:** You’ve deployed gpt-4o and need to restrict access to your corporate network only.  
**Question:** Which two Azure AI Foundry resource settings do you configure?

* + A. Public network access = Disabled
  + B. Add your office IP to Firewall rules
  + C. Enable system-assigned Managed Identity
  + D. Set endpoint to private endpoint

**Answer:** A, B

1. **Sequence:**  
   “Order the steps to integrate the endpoint into your .NET application using Key Vault and Managed Identity.”
   * Assign Managed Identity to your App Service
   * Store API key as secret in Key Vault
   * Grant identity access to Key Vault (Key Vault Access Policy)
   * In code, use DefaultAzureCredential to retrieve secret and call endpoint

**Correct Order:** 1 → 2 → 3 → 4

1. **Drag-and-Drop / Matching:**

**Match each component with its description:**  
| Component | Description |  
|------------------------|---------------------------------------------|  
| Endpoint | Model deployment URL |  
| API Key | Shared secret for authentication |  
| Deployment ID | Specific model alias in your Foundry resource |  
| AzureKeyCredential | SDK class for passing the API key |

**1. Entegrasyon Yöntemleri**

**REST API Tabanlı Entegrasyon**

* **Ne Zaman Kullanılır?**  
  Platformdan bağımsız istemciler (web, mobil, IoT) ile doğrudan iletişim kurmak istediğinde.
* **Nasıl Çalışır?**  
  Uygulaman senaryoya uygun istek gövdesini JSON formatında endpoint’e gönderir, aldığı JSON yanıtı işler.
* **Avantajlar:**
  + Dil veya çerçeve bağımsızdır.
  + Swagger/OpenAPI tanımı sayesinde hızlı dokümantasyon ve test imkânı.

**SDK Tabanlı Entegrasyon**

* **Ne Zaman Kullanılır?**  
  .NET, Python, Java gibi desteklenen dillerde derin entegrasyon ve geliştirme yaparken.
* **Nasıl Çalışır?**  
  Azure’un sunduğu SDK kütüphanelerini projenize ekleyerek, tip güvenli metodlarla AI çağrılarını gerçekleştirirsiniz.
* **Avantajlar:**
  + Kod tamamlama ve IntelliSense gibi geliştirme desteği.
  + Hata yönetimi ve yeniden deneme (retry) mekanizmaları SDK tarafından sağlanır.

**2. Kimlik Doğrulama ve Güvenlik**

**API Key & Endpoint**

* Projeye ait **endpoint URL** ve **API anahtarı**, Foundry portalının “Endpoints and keys” bölümünden alınır.
* Temel senaryoda bu anahtarı doğrudan HTTP başlığına ekleyerek kimliğinizi kanıtlar, ancak bu yöntem ile anahtarın kodda veya yapılandırma dosyasında görünür olması risktir.

**Managed Identity & Key Vault**

* **Managed Identity:** Azure kaynaklarına ait kimliği, kullanıcı müdahalesi olmadan Azure AD üzerinden kimlik doğrulaması yapar.
* **Key Vault:** API anahtarlarını sakladığınız merkezî gizli depodur. Uygulamanız, Managed Identity aracılığıyla Key Vault’a bağlanır ve anahtarı oradan çeker.
* **Faydaları:**
  + Anahtar hiç kimsenin göremeyeceği bir ortamda saklanır.
  + Anahtar rotasyonu ve erişim politikaları Azure portal üzerinden yönetilir.

**3. Ağ ve Erişim Kontrolleri**

**Public vs. Private Access**

* **Public Access:** İnternetten her yerden erişime açıktır; hızlı test ve prototip için uygundur ama güvenlik riski taşır.
* **Private Endpoint:** Sadece belirli bir sanal ağa (VNet) entegre olur; kurumsal içeriden güvenli erişim sağlar.

**IP Tabanlı Güvenlik Duvarı**

* Foundry kaynağına yalnızca belli IP aralıklarından erişim izni vererek “minimum erişim” ilkesini uygularsınız.

**4. CI/CD ve Altyapı Otomasyonu**

**Altyapıyı Kodla Tanımlama**

* **ARM/Bicep veya Terraform** gibi araçlarla; Foundry kaynağı, kimlik atamaları, ağ kuralları, Key Vault entegrasyonu gibi tüm bileşenleri tanımlarsınız.
* Bu tanımlar, sürüm kontrolüne alınır, ekip içindeki herkes aynı ortamı koddan oluşturur.

**Sürekli Teslimat Süreçleri**

* GitHub Actions veya Azure DevOps pipeline’larıyla:
  1. Kod ve altyapı tanımlarını sürüm kontrolünden çeker,
  2. Gerekli testleri ve güvenlik taramalarını yapar,
  3. Ortamı oluşturan veya güncelleyen otomatik adımları tetikler.
* Böylece “insan hatası” minimize edilir, tekrar üretilebilir ve izlenebilir bir dağıtım süreci kurulur.

**5. Gerçek Dünya Kullanım Senaryoları**

1. **Müşteri Destek Botu:**
   * GPT modelleriyle sık sorulan sorulara yanıt veren, gerektiğinde arka planda müşteri veritabanına sorgu atan bir sohbet robotu.
2. **Otomatik İçerik Üretimi:**
   * DALL·E görsel oluşturma ve GPT–4 özetleme kombinasyonuyla e-ticaret ürün açıklamaları ve pazarlama metinlerini otomatik üretme.
3. **Eğitim ve Danışmanlık Araçları:**
   * Akademik platforma entegre, öğrenci sorularını matematiksel veya tarihsel konularda yanıtlayan interaktif bir asistan.
4. **Kurumsal Bilgi Arama:**
   * Azure Cognitive Search ile kuruluş içi dokümanlardan oluşan bir vektör tabanlı semantik arama portalı.

**6. AI-102 Sınavı İçin Odak Noktaları**

* **Entegrasyon Seçimi:** REST vs. SDK avantaj/dezavantajları.
* **Güvenlik:** API Key yerine Managed Identity + Key Vault senaryosunu adım adım açıklayabilme.
* **Ağ:** Public vs. Private Endpoint farkları ve firewall kuralları.
* **Altyapı Otomasyonu:** Kodla tanımın (IaC) neden önemli olduğu ve hangi araçların kullanıldığı.
* **Senaryo Soruları:** Yukarıdaki gerçek dünya örneklerinden yola çıkarak “hangi Azure AI servisi, nasıl eklenir, nasıl güvenli hale getirilir” sorularına hazırlıklı ol.

Bu kavramsal çerçeve seni hem pratik projelerde hem de AI-102 sınavındaki senaryo tabanlı sorularda güçlü kılacaktır.

ChatGPT’ye sor