O'REILLY®

Azure Certified AI Engineer Associate
Crash Course

Reza Salehi

August/2020

Reza Salehi

Cloud Consultant and Trainer
Pluralsight author, O'Reilly Media instructor, Udemy instructor

@zaalion

linkedin.com/in/rezasalehi2008

Microsoft CERTIFIED Trainer
2008 - 2018

Microsoft CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

Microsoft CERTIFIED
AZURE AI ENGINEER
ASSOCIATE

Microsoft CERTIFIED
AZURE IOT DEVELOPER
SPECIALTY

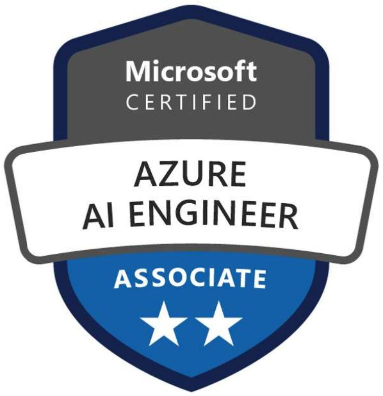
Course Overview

Agenda: Course Overview

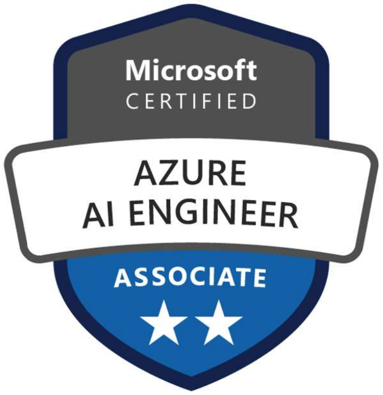
- Who can write AI-100 test? (candidate profile)
- Expectation from “Azure AI Engineer” (the role)
- Which skills are measured in the AI-100 exam?
- What is Machine Learning?
- How this course is structured?

AI-100 Candidate Profile

- Should have subject matter expertise in:
  - Using Azure Cognitive Service,
  - Azure Machine Learning,
  - Other related Azure services (storage, security, integration, monitoring, etc.)



Azure Security Engineer Role



Use the Azure Machine Learning product family, and

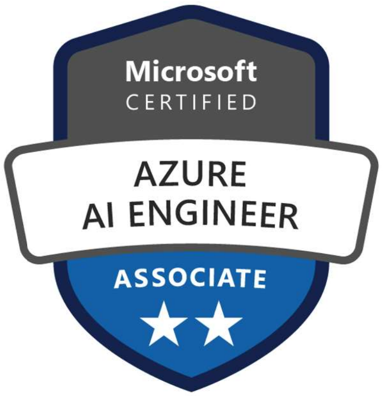
Other Azure services to develop AI solutions.

- Data ingestion, preparation
- Security
- Integration
- Monitoring

Skills Measured on AI-100

- Azure Cognitive Services
- Azure Machine Learning
- Azure Bot Service (framework)
- Azure Cognitive Search
- Data storage options in Azure
- Security (data and AI services)

- Solid general knowledge of Azure services
  - Similar to an architecture exam (AZ-300, AZ-301)



AI (Artificial Intelligence)

Enables machines to do tasks which are normally done by humans.

- Language translation
- Process images and audio
- Mathematic-based predictions
- ...

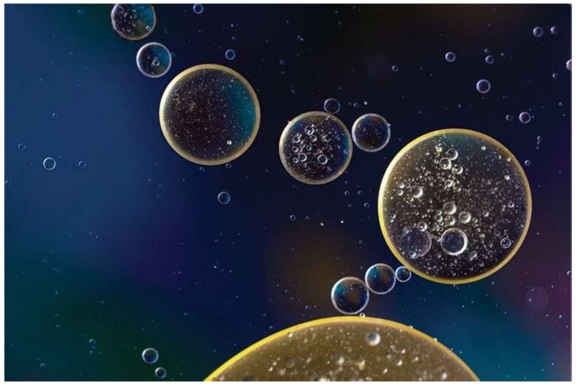
Machine Learning

- Is a subset of AI.
- Enables computers to use data from past to forecast future behaviors or trends.
- Machine learning enables computers to learn without being-explicitly programmed.

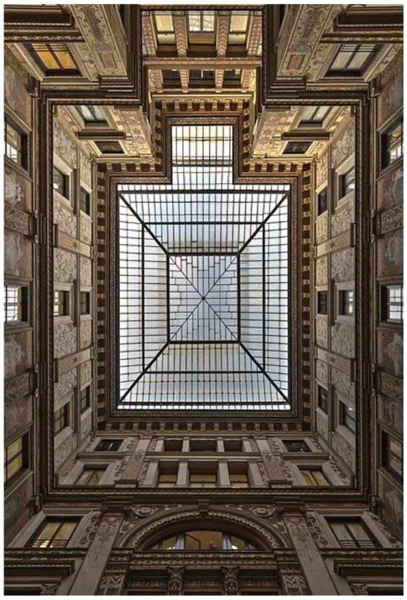
Machine Learning

- ML Scenarios
  - Classification
  - Regression
  - Predictions
  - ...

Machine Learning



Machine Learning



Machine Learning

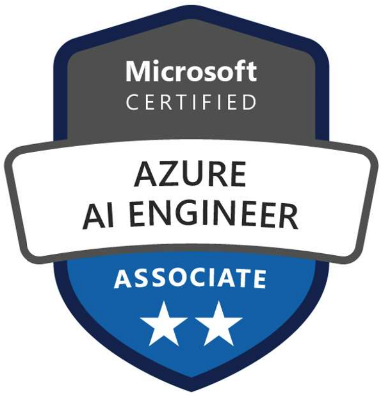
Machine Learning

- Workflow
  - Collect data; lots of it !
  - Prepare, clean up the data
  - Choose the right ML algorithm for your scenario
  - Train the algorithm with your data to get a “**trained model**”
  - Deploy and use the “model”

You are not expected to be a “Data Scientist” or have deep Machine Learning expertise to pass AI-100.

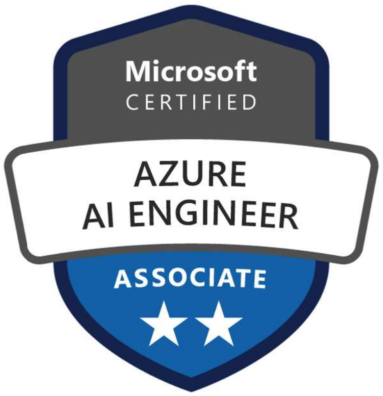
The Course Structure

- Lots of demos !
- We will cover a lot !
  - AI-100 is similar to the architecture exam
  - AI, storage, security, compliance, monitoring
- The topics are based on the exam blueprint.
  - https://docs.microsoft.com/en-us/learn/certifications/exams/ai-100



Questions & Resources

- Post questions in the Q & A box
- Resources in the course repository
  - https://github.com/zaalion/oreilly-ai-100
  - *(Within 24 hrs)*
- Reach out to me here:
  - Twitter: **@zaalion**
  - LinkedIn: **rezasalehi2008**



Analyze Solution Requirements

Recommend Azure Cognitive Services APIs

- Microsoft offers several AI products
    - Available processing architectures for AI solutions
    - Available data processing technologies
    - Identify automation options

Available Processing Architectures for AI Solutions

- IaaS
  - Manage VM > Create AI Experiments > Use the AI model
- PaaS
  - Create AI Experiments > Use the AI model
- SaaS
  - Use the pre-trained AI model

Available Processing Architectures for AI Solutions

- IaaS
  - Microsoft Machine Learning Server
  - SQL Server Machine Learning Services

- Also available as Azure VMs

Available Processing Architectures for AI Solutions

- PaaS
  - Azure Machine Learning (v2)
  - Azure Machine Learning Studio (v1, classic)
  - Azure Databricks
- Client
  - Azure Data Science Virtual Machine

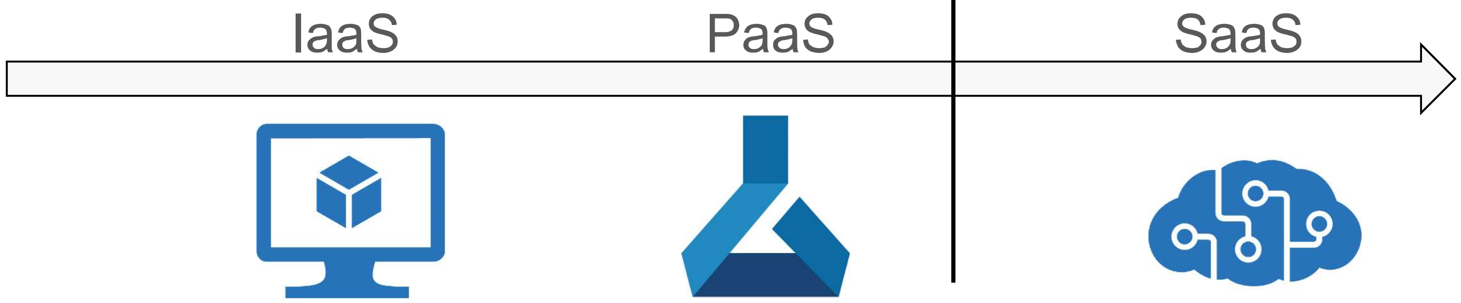
Available Processing Architectures for AI Solutions

- SaaS
  - Azure Cognitive Services

Available Processing Architectures for AI Solutions

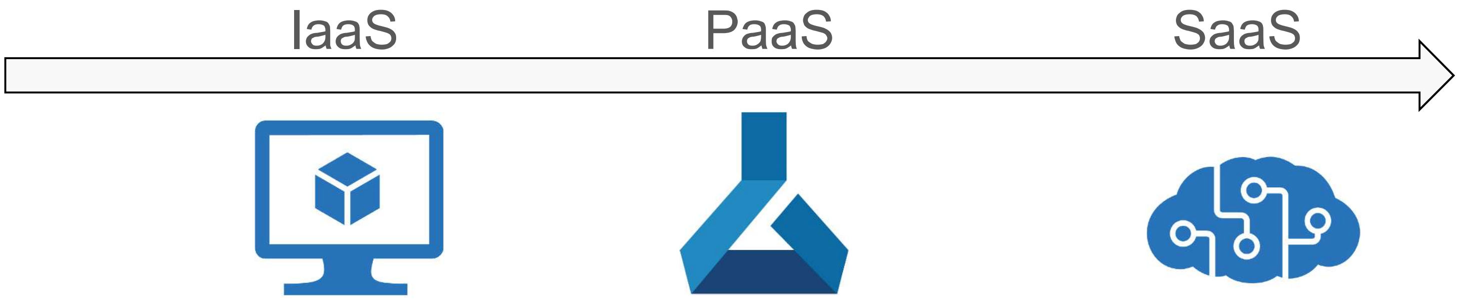
- Harder to use. Data science and ML expertise is required.
- Very flexible, more AI tasks can be solved

- Easier to use, less domain expertise is needed.
- Less flexibility, generalized AI tasks



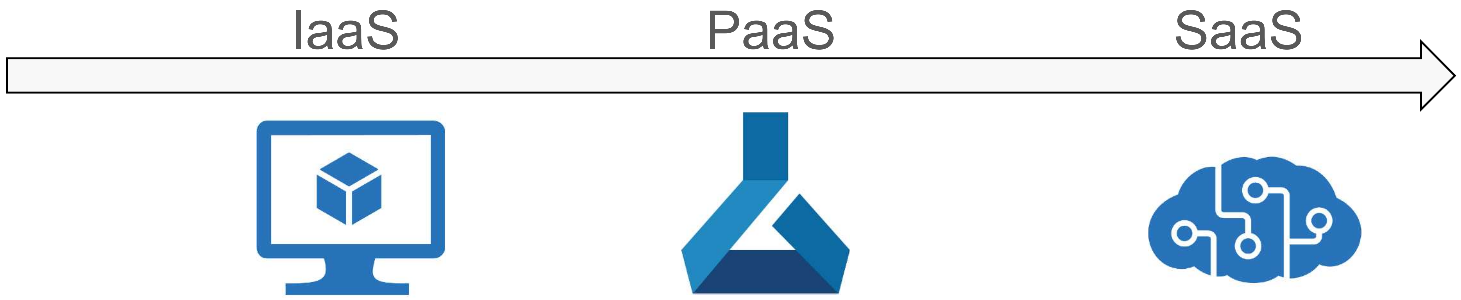
Available Processing Architectures for AI Solutions

- AI-100 focus is on:
  - ○ Azure Cognitive Services, and
  - ○ Azure Machine Learning



Recommend an AI Processing Architectures

- Start looking in Azure Cognitive Services.
- If no luck, try other Azure machine learning options
  - PaaS first



Recommend an AI Processing Architectures

- Azure Machine Learning
  - Can be used for any kind of machine learning
    - classical ML, deep learning, supervised, and unsupervised learning.
  - Provides all the tools developers and data scientists need for their machine learning workflows

Recommend an AI Processing Architectures

- Azure Machine Learning versions:
  - V2: Azure Machine Learning
  - V1: Azure Machine Learning Studio (classic)

Recommend an AI Processing Architectures

- Connect to Azure Machine Learning models:
  - REST API
- You will need
  - API endpoint & API key or token

Recommend an AI Processing Architectures

- Azure Cognitive Services
  - No ML or data science expertise
  - Models are pre-trained by Microsoft
  - Simply use the trained models
  - Covering general use cases
  - There is a level of customization
  - Five main categories

Recommend an AI Processing Architectures

- Azure Cognitive Services
  - Vision
  - Speech
  - Language
  - Decision
  - Web Search *(formerly Search)*

Recommend an AI Processing Architectures

- Use the Azure Cognitive Services
  - REST API
  - SDK (language specific)
- You will need
  - API endpoint & API key or token
  - Azure Active Directory authentication (RBAC)

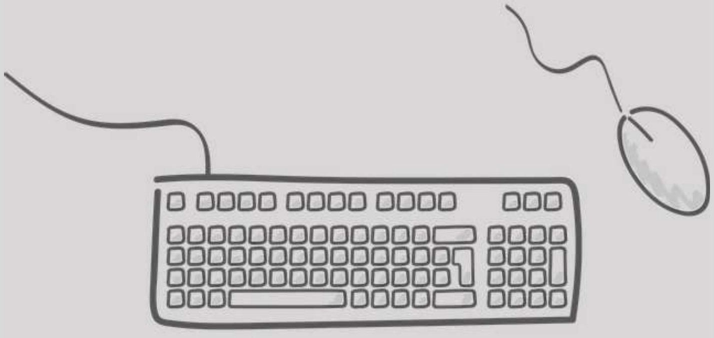
Recommend an AI Processing Architectures

- Both Azure Cognitive Services & Azure Machine Learning models can be deployed to *Docker* containers.
  - Deploy to on-premises machines
  - Deploy to Azure AKS
  - Deploy to Azure ACI
  - Deploy to an IoT edge device
    - Why?

Azure Machine Learning gives you a trained model file.

You can download it and deploy it anywhere you desire!

Demo



- Provisioning
  - Azure Machine Learning
  - Azure Machine Learning Studio (classic)
  - Azure Cognitive Services
  - Azure Data Science Virtual Machine

Choosing the Right Data Storage

- Relational databases
- Document databases
- Key/Value databases
- Graph databases
- Column family databases

- Object storage
- File share
- Data analytics databases
- Search Engine databases
- Time Series databases

Choosing the Right Data Storage

- Store logs / Azure Cognitive Services output
  - Azure Blob Storage
- Low latency document database
  - Azure Cosmos DB Core API
- Database for social media
  - Azure Cosmos DB Graph API
- Migrating from MongoDB
  - Azure Cosmos MongoDB API

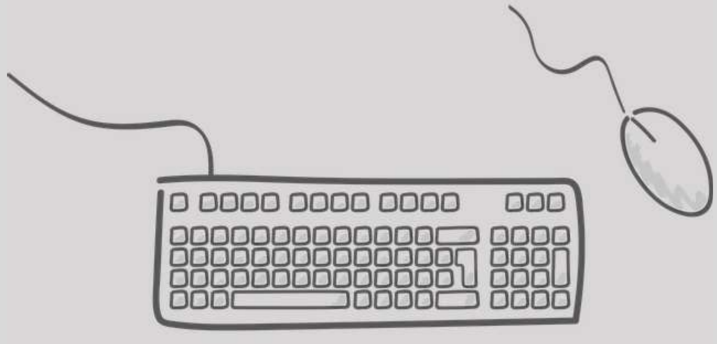
Choosing the Right Data Storage

- Building search around your existing data
  - Azure Cognitive Search
- Fast cache store
  - Azure Cache for Redis (Azure Redis)
- Highly relational data
  - Azure SQL Database
- Cheap column database
  - Azure Table Storage

Choosing the Right Data Storage

- Structured data
  - Azure SQL Database, MySQL, PostgreSQL, MariaDB
- Unstructured data
  - Azure Cosmos DB, Azure Table Storage
- Blobs / files
  - Azure Blob Storage, Data Lake Gen 2

Demo

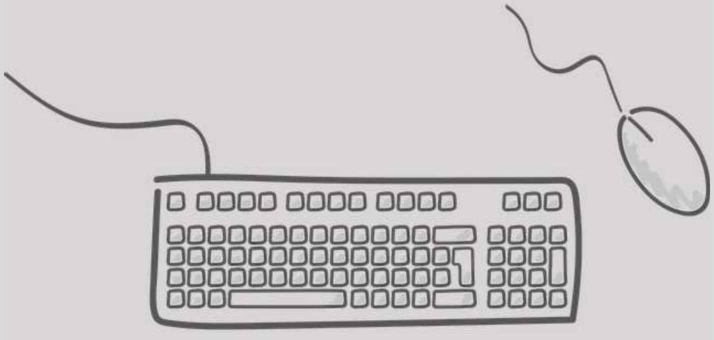


- Provisioning
  - Azure SQL Database
  - Azure Storage Account (Azure Data Lake Gen 2)
  - Azure Cosmos DB (multi-model)
  - Azure Cognitive Search

Automation Options

- Provisioning and deployment automation
    - You can create an Azure resource:
        - Azure Portal
        - Azure CLI / PowerShell / ARM templates / REST
    - Automate your AI solution deployment
        - Azure Automation Runbooks
        - Azure Blueprints

Demo



- Use Azure Automation to create an AI resource
- Azure Blueprints to create an AI resource

Securing Azure AI Solutions

1. Securing AI APIs and interfaces
2. Protecting customer data
    a. Protecting AI solution data
    b. Data privacy and regulatory compliance
3. Auditing

Securing AI APIs and Interfaces

- Azure Machine Learning
    - REST API
        - API key, or
        - Security token
            - Keep them safe (in Azure Key Vault)

Securing AI APIs and Interfaces

- Azure Cognitive Services
    - REST API or SDK
        - API key, or
        - Security token (time sensitive), or
        - Azure Active Directory authentication (RBAC)

Securing AI APIs and Interfaces

- Azure Cognitive Services
  - API key
    - All Services support keys.
    - They don’t expire but can be rotated.
    - Keep them safe (Azure Key Vault)

Securing AI APIs and Interfaces

- Azure Cognitive Services
  - API security tokens
    - Obtain them on-the-fly using an API key
    - They expire after 10 minutes
    - Keep them safe (in Azure Key Vault)

Securing AI APIs and Interfaces

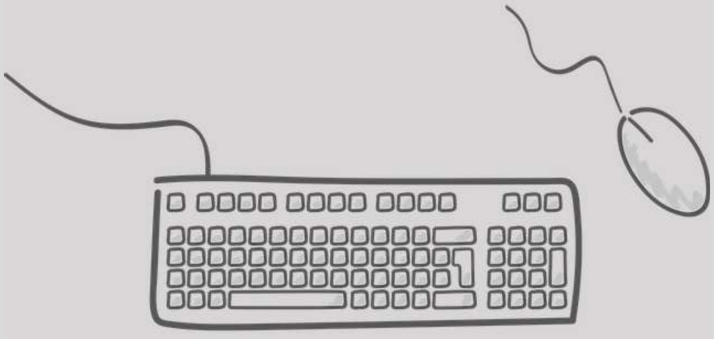
- Azure Cognitive Services
  - Azure Active Directory
    - Create a service principal or Managed Identity
    - Assign permission over the service to this identity
    - Can apply RBAC

Not all Azure Cognitive Services support security tokens or Azure Active Directory authentication!

Securing AI APIs and Interfaces

- Azure Cognitive Services
    - Azure Active Directory authentication
        - Computer Vision, Face, Text Analytics, Immersive Reader
    - Security token (time sensitive)
        - Text translation, speech-to-text, text-to-speech
    - API key
        - All services

Demo



- Securing Cognitive Services using
    - The API key
    - The security token
    - Azure Active Directory
- Securing Azure Machine Learning using
    - The API key
    - The security token

Protecting Customer Data

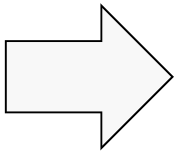
- Azure helps you protect client data
  - Data storage authentication/authorization
  - Data storage firewall
  - Data storage private endpoint
  - At-rest data protection
  - In-transit data protection

Protecting Customer Data

- Azure helps you protect client data
  - Data segregation
  - Data redundancy
  - Data retention
  - Data destruction

Data Storage Authentication/Authorization

- Azure SQL Database
- Azure Storage Account
- Azure Cosmos DB
- Azure Cognitive Search
- Azure Cache for Redis
- MariaDB
- etc.



- Database keys
- DB Credentials
- AAD Managed Identity
- RBAC

Data Storage Firewall

- Azure SQL Database
- Azure Storage Account
- Azure Cosmos DB
- Azure Cognitive Search
- Azure Cache for Redis
- MariaDB
- etc.

→

- VNET integration
- Incoming IP addresses
- Allow Azure services

Data storage Private Endpoint

- Azure SQL Database
- Azure Storage Account
- Azure Cosmos DB
- Azure Cognitive Search
- Azure Cache for Redis
- MariaDB
- etc.

- Only private access

At-rest Data Protection

- Azure Storage Account SSE
- Azure SQL Database TDE
- Azure Disk Encryption
- Managed Disk Encryption
  - (+CMK)
- Azure Cosmos DB encryption

- Key management:
  - System managed
  - Customer managed

In-transit Data Protection

- All communications are encrypted using SSL/TLS
- TLS 1.2
- TLS version is configurable

Data Segregation

- Azure is a multi-tenant service
    - Multiple customer data is stored on the same hardware.
- Azure uses logical isolation to segregate customers’ data

Data Redundancy

- In-country / in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery purposes.

Data Redundancy

- Azure Storage Account
- Azure SQL Database
- Azure VM Backups
- Azure Cosmos DB

Data Retention

- How long to keep the data?
  - Azure Storage Accounts
  - Azure SQL Database backups
  - Logs
  - ...

Data Destruction

- When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse,
- As well as the physical destruction of decommissioned hardware

Data Ownership

- Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure
- Microsoft does not know what kind of data customers choose to store in Azure
- Microsoft does not claim data ownership over the customer information that's entered Azure.

Regulatory Compliance and Governance

- Regulatory compliance refers to the discipline and process of ensuring that a company follows the laws enforced by governing bodies in their geography.
  - The company follows government laws concerning customer data.
  - Changes by region
- Use Azure Policy to enforce compliance

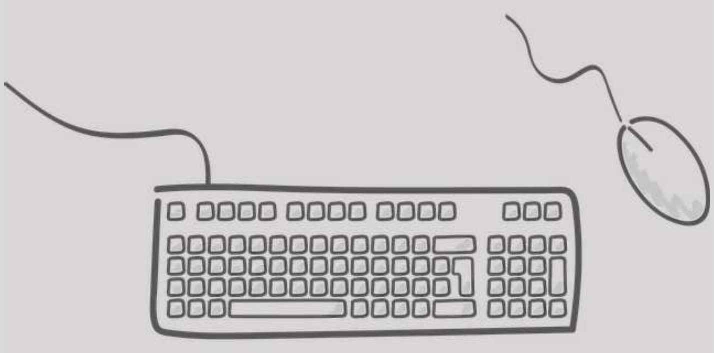
Regulatory Compliance and Governance

- Regulatory compliance
  - HIPAA
  - PCI
  - Personal data, PPI
  - GDPR
- Azure Data classification

Azure Policy to Enforce Compliance

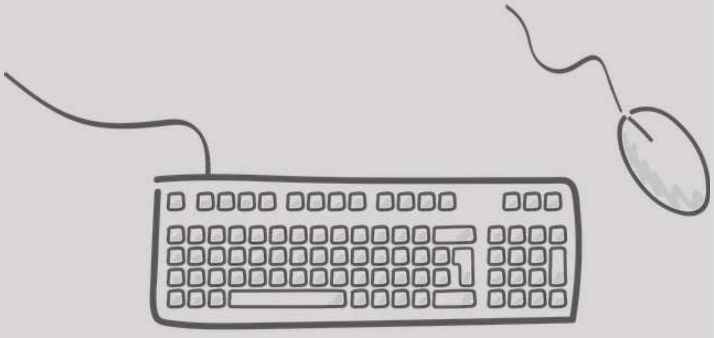
- Azure Policy can help you comply!
  - All resources should have taxonomy tags
  - No resource should be created outside USA
  - Only small VM sizes should be created for DEV
- Easy integration with Azure Blueprints

Demo



- Securing Azure SQL Database
- Securing Azure Storage Account
- Securing Azure Cosmos DB
- Microsoft Trust Center
    - Data locations, data sovereignty
- Azure Policy

Demo



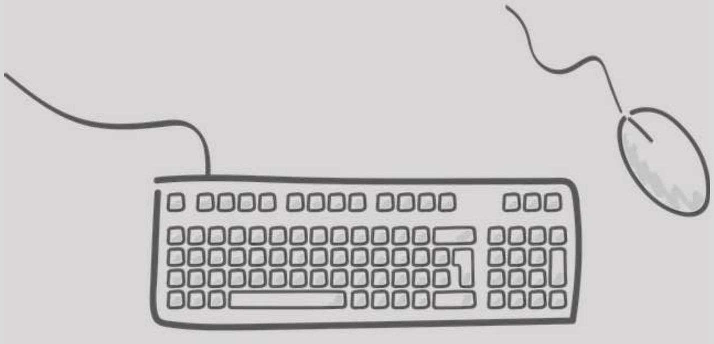
- Configuring data redundancy
- Data retention / destruction
- Immutable storage for Azure Blobs

Logs and Security Tools in Azure

- Azure Log Analytics Workspace
- App Insights
- Azure Monitor
- Azure Security Center
- Azure Sentinel

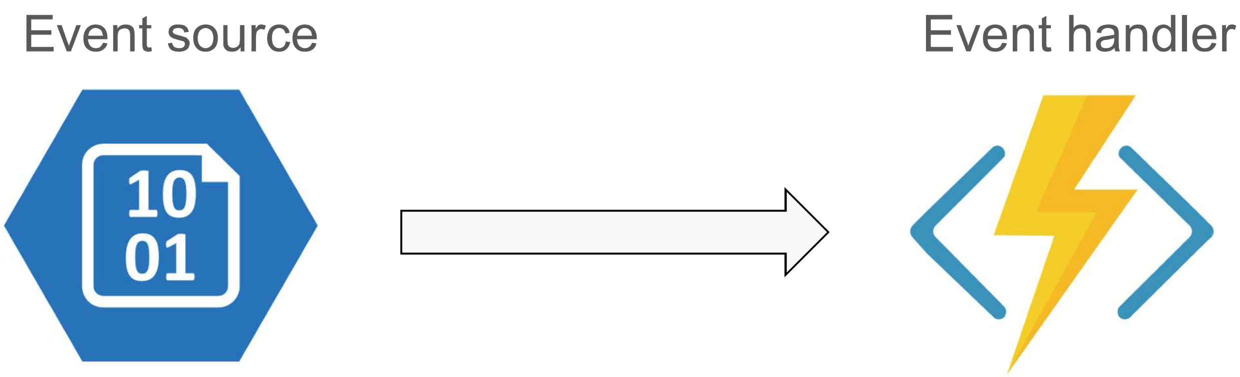
Demo

- Azure Log Analytics
- Azure Monitor
- Azure Security Center
- Azure Sentinel



Service and Data Integration

- Connect, chain multiple pipeline elements



Event source

Event handler

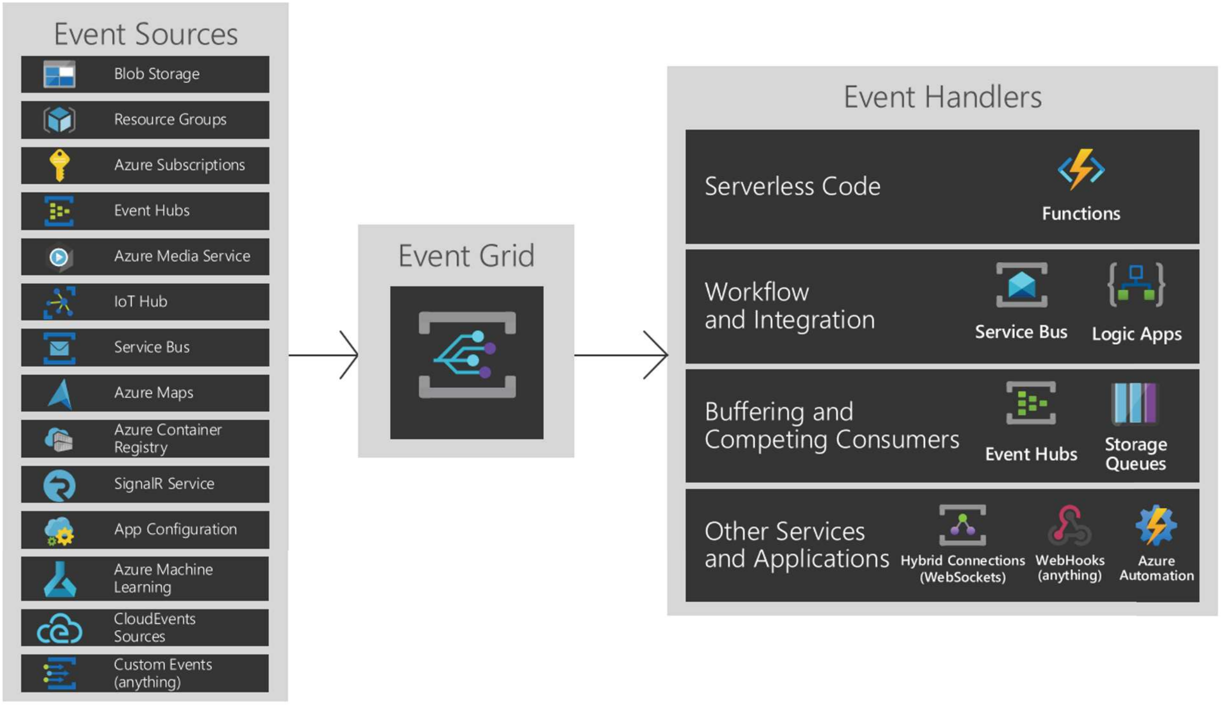
Service and Data Integration

- Connect, chain multiple pipeline elements
- Event source
  - Azure Event Hubs
  - Azure IoT Hub
  - Azure Storage Account
  - Azure Service Bus (queues, topics)
  - Azure Container Registry
  - ...

Service and Data Integration

- Connect, chain multiple pipeline elements
- Event handler
  - Azure Logic Apps
  - Azure Functions
  - Azure Stream Analytics
  - Azure Data Factory
  - Event Hubs
  - Azure Automation
  - ...

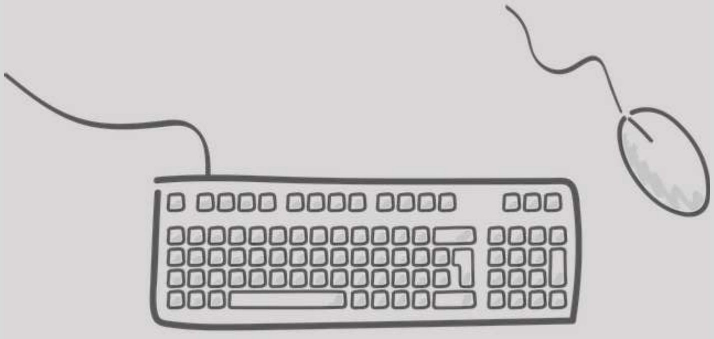
Service and Data Integration



https://docs.microsoft.com/en-us/azure/event-grid/overview

Demo

- Service and Data Integration
  - Start an ADF pipeline when a new text blob is uploaded.



Questions

Break (5 minutes)

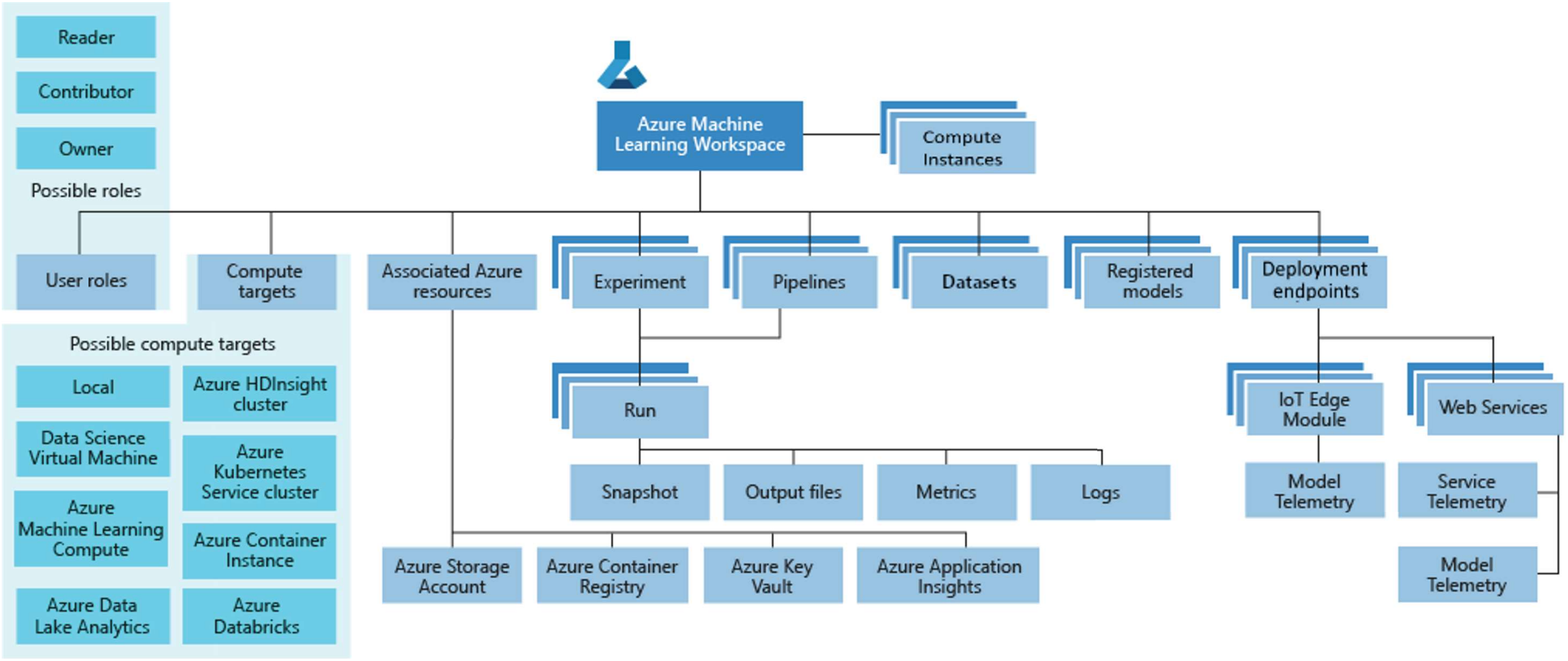
Design AI Solutions

Agenda: Design AI Solutions

- Define AI Workflows
- Design Cognitive Services solutions
- Design solutions using the Microsoft Bot Framework
- Design the compute infrastructure

Define AI Workflow

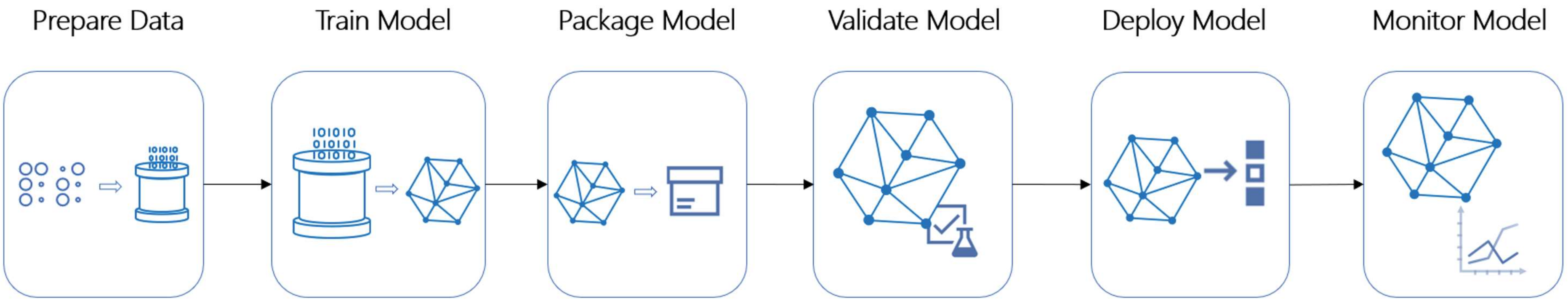
- Azure pipeline technologies
    - Azure Machine Learning Pipelines
        - Model orchestration (Train the model)
    - Azure Data Factory pipelines
        - Data orchestration (Data prep)
    - Azure DevOps Pipelines
        - Code & app orchestration (CI/CD)



https://docs.microsoft.com/en-us/azure/machine-learning/concept-workspace

Define AI Workflow

- Using Azure Machine Learning pipelines
    - Designer or Python/R SDK



Prepare Data → Train Model → Package Model → Validate Model → Deploy Model → Monitor Model

Define AI Workflow

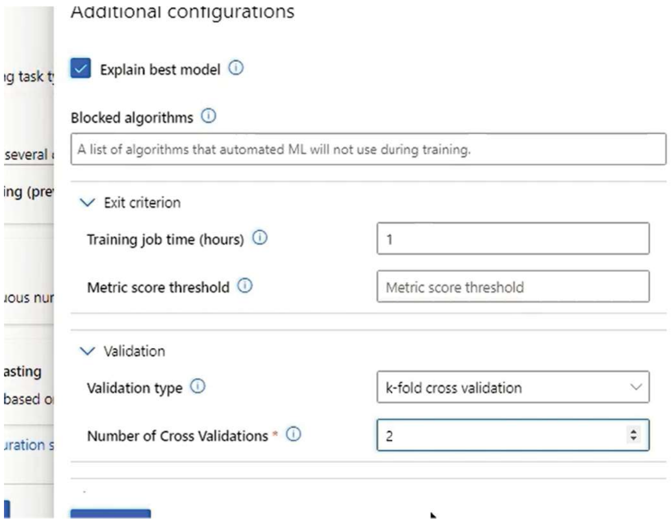
- Using Azure Machine Learning pipelines
    - Designer or Python/R SDK
        - Run in the context of an Azure ML Experiment
        - Prepare data, train and validate a model and deploy it

Define AI Workflow

- Building a pipeline in Azure Machine Learning workspace
  - Using Python / R SDKs
  - Using designer (preview)

Define AI Workflow

- Automated Machine Learning (preview)
  - How do you choose the best ML algorithm?



Additional configurations

☑ Explain best model ⓘ

Blocked algorithms ⓘ

A list of algorithms that automated ML will not use during training.

Exit criterion

Training job time (hours) ⓘ: 1

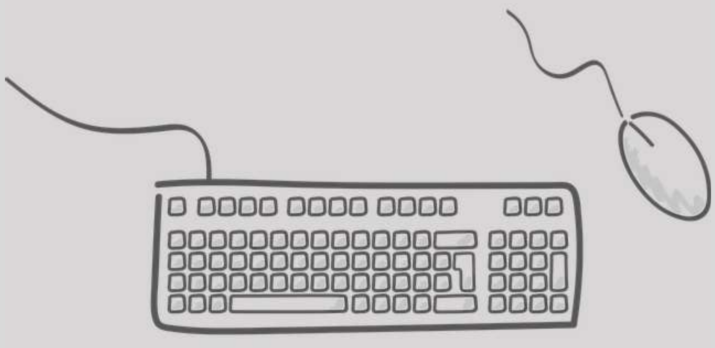
Metric score threshold ⓘ: Metric score threshold

Validation

Validation type ⓘ: k-fold cross validation

Number of Cross Validations * ⓘ: 2

Demo



- Creating a model in Azure Machine Learning
- Creating a model in Automated Machine Learning

Design Cognitive Services Solutions

- Azure Cognitive Services
  - Azure SaaS AI offering
  - Many general AI tasks can be addressed
  - Customizable to some level (will see later)
  - No AI or data science expertise is needed
  - Use REST APIs or SDKs (if applicable) to call the services

Design Cognitive Services Solutions

- Provisioning
  - Azure Portal
  - Azure CLI
  - Azure PowerShell
  - ARM
  - SDK (management)
  - REST API

Design Cognitive Services Solutions

- Authentication / Authorization
  - API Key, or
  - Bearer token, or
  - Azure Active Directory and RBAC
    - Only *Computer Vision, Face, Text Analytics, Immersive Reader, Form Recognizer, Anomaly Detector, and all Bing services except Bing Custom Search*