Internet of Things (IoT)

The Internet of Things (IoT) is a network of physical devices, sensors, and software connected to the internet, allowing them to collect, exchange, and act on data. IoT enables automation, monitoring, and analysis across various industries and applications.

- IoT Hub: A managed service in Azure that acts as a central message hub for bi-directional communication between IoT devices and the cloud. It securely connects, monitors, and manages millions of IoT devices.
- IoT Central: A fully managed SaaS (Software as a Service) solution in Azure that simplifies the deployment and management of IoT applications. It provides pre-built templates, dashboards, and analytics to reduce development complexity.
- IoT Edge: An Azure service that brings cloud intelligence to edge devices. It allows devices to process data locally using machine learning and custom logic, reducing latency and bandwidth requirements while enabling offline operations.

Container

A **Container** is a lightweight, standalone, and executable software package that includes everything needed to run an application: code, runtime, system tools, libraries, and settings. Containers allow applications to run consistently across different environments, such as development, testing, and production.

Big Data and Analytics

Big Data and Analytics refers to the collection, processing, and analysis of large volumes of data to uncover insights, trends, and patterns that help organizations make informed decisions.

Consists of:

- **Azure Synapse Analytics:** A limitless analytics service that brings together enterprise data warehousing and big data analytics. It enables querying data on your terms, using either serverless or provisioned resources.
- **HDInsight:** A fully managed cloud service that makes it easy to process massive amounts of data using popular open-source frameworks such as Hadoop, Spark, and Kafka.
- **Azure Databricks:** An Apache Spark-based analytics platform optimized for Azure that provides fast, collaborative big data analytics and AI/ML model development.

Artificial Intelligence (AI)

Artificial Intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning, reasoning, and self-correction.

- **Machine Learning (ML):** A subset of AI that enables systems to automatically learn and improve from experience without being explicitly programmed.
- **Deep Learning:** A subset of machine learning that uses neural networks with many layers to analyze complex patterns in large datasets.

Consists of:

- **Azure Machine Learning Service:** A cloud-based platform for building, training, and deploying machine learning models at scale.
- **Azure Machine Learning Studio:** A collaborative, drag-and-drop visual workspace for building, testing, and deploying machine learning models without extensive coding.

Serverless Computing

Serverless Computing is a cloud computing model in which the cloud provider automatically manages the infrastructure and dynamically allocates resources. Developers focus only on writing code without worrying about server management or scaling.

Consists of:

- **Azure Functions:** A serverless compute service that allows you to run event-driven code without provisioning or managing servers. Ideal for lightweight tasks, background processes, and microservices.
- **Logic Apps:** A cloud service that helps automate workflows and integrate apps, data, services, and systems across enterprises and organizations.
- **Event Grid:** A fully managed event routing service that allows event-driven architectures by enabling reactive programming and seamless communication between services and applications.

DevOps

DevOps is a set of practices that combines software development (Dev) and IT operations (Ops) to shorten the system development life cycle while delivering features, fixes, and updates frequently in close alignment with business objectives.

DevOps Tools and Services:

- GitHub: Version control and source code management.
- Azure Boards: Agile planning, work item tracking, and reporting.
- Visual Studio: Integrated development environment for building and debugging code.
- Azure Kubernetes Service (AKS): Orchestrates containerized applications.
- Azure Pipelines: CI/CD service for building, testing, and deploying code.
- Azure Monitor: Provides full-stack monitoring, analytics, and diagnostics for applications and infrastructure.

Core Azure Identity Services

Authorization vs Authentication:

- **Authentication:** Verifying the identity of a user or system.
- **Authorization:** Determining what an authenticated user or system is allowed to do.

Azure Entra: A Microsoft identity and access management solution that unifies Azure Active Directory and other identity services to manage access, identity governance, and secure authentication across cloud and on-premises environments.

- **Azure AD Entra Licenses:**
    - Azure Active Directory Free
    - Azure Active Directory Premium P1
    - Azure Active Directory Premium P2
    - Pay-as-you-go feature licenses

Azure Multi-Factor Authentication (MFA):

- **Two-factor:** Requires two different methods of verifying identity, such as a password plus a mobile verification code.
- **Three-factor:** Uses three types of authentication factors:
    - Something you have (e.g., smart card, mobile device)
    - Something you know (e.g., password, PIN)
    - Something you are (e.g., biometric like fingerprint or face recognition)

File Permissions: NTFS vs Shared

NTFS Permissions: - Apply to files and folders stored on an NTFS-formatted volume (local disk or network share). - Provide granular control (Read, Write, Modify, Full Control) over file and folder access. - Permissions are inherited by default from parent folders. - Affect both local and remote users. - Can be combined with shared permissions; the most restrictive permission always applies.

Shared Permissions: - Apply only to folders shared over a network. - Control network access levels: Read, Change, or Full Control. - Do not affect users accessing files locally. - Easier to configure but less granular than NTFS permissions. - Often used in combination with NTFS permissions for network security management.

Key Difference: NTFS permissions apply to both local and remote access, while shared permissions apply only to network access. The most restrictive permission between the two determines the user’s effective access.