SUMMARY

➢ Fundamentals

• **Training Course AI-900 :** Microsoft Azure AI Fundamentals

• **Training Course AZ-900 :** Microsoft Azure Fundamentals

• **Training Course DP-900** : Microsoft Azure Data Fundamentals

• **Training Course MS-900** : Microsoft 365 Fundamentals

• **Training Course PL-900** : Microsoft Power Platform Fundamentals

• **Training Course SC-900** : Microsoft Security, Compliance, and Identity Fundamentals

➢ Role Based

• **Training Course AZ-104 :** Microsoft Azure Administrator

• **Training Course AZ-204 :** Developing Solutions for Microsoft Azure

• **Training Course AZ-305 :** Designing Microsoft Azure Infrastructure Solutions

• **Training Course AZ-500 :** Microsoft Azure Security Technologies

• **Training Course SC-200** : Microsoft Security Operations Analyst

• **Training Course SC-300** : Microsoft Identity and Access Administrator

• **Training Course SC-400** : Administering Information Protection and Compliance in Microsoft 365

• **Training Course DP-203 :** Data Engineering on Microsoft Azure

• **Training Course MS-102 :** Microsoft 365 Administrator

• **Training Course PL-300 :** Microsoft Power BI Data Analyst

• **Training Course PL-400 :** Microsoft Power Platform Developer

• **Training Course AI-102** : Designing and Implementing a Microsoft Azure AI Solution

FUNDAMENTALS

AI-900

Training Course AI-900: Microsoft Azure

AI Fundamentals

Overview: This course introduces fundamentals concepts related to artificial intelligence (AI), and the services in Microsoft Azure that can be used to create AI solutions. The course is not designed to teach students to become professional data scientists or software developers, but rather to build awareness of common AI workloads and the ability to identify Azure services to support them.

Duration: 1 Day.

Audience Profile: The Azure AI Fundamentals course is designed for anyone interested in learning about the types of solution artificial intelligence (AI) makes possible, and the services on Microsoft Azure that you can use to create them. You don't need to have any experience of using Microsoft Azure before taking this course, but a basic level of familiarity with computer technology and the Internet is assumed. Some of the concepts covered in the course require a basic understanding of mathematics, such as the ability to interpret charts. The course includes hands-on activities that involve working with data and running code, so a knowledge of fundamental programming principles will be helpful.

Certification: This course prepares you for the AI-900: Azure AI Fundamentals.

Course Objectives: After completing this course, students will be able to:

- Get started with AI on Azure
- Use Automated Machine Learning in Azure Machine Learning
- Create a regression model with Azure Machine Learning designer.
- Create a classification model with Azure Machine Learning designer.
- Create a clustering model with Azure Machine Learning designer.
- Analyze images with the Computer Vision service.
- Classify images with the Custom Vision service.
- Detect objects in images with the Custom Vision service.
- Detect and analyze faces with the Face service.
- Read text with the Computer Vision service.
- Analyze receipts with the Form Recognizer service.

- Analyze text with the Language service.

- Recognize and synthesize speech.

- Translate text and speech.

- Create a language model with Conversational Language Understanding

- Build a bot with the Language Service and Azure Bot Service

<u>Course Outline:</u>

1- Get started with AI on Azure
   o In this module, you'll learn about the kinds of solution AI can make possible and considerations for responsible AI practices.
2- Use Automated Machine Learning in Azure Machine Learning
   o Learn how to use the automated machine learning user interface in Azure Machine Learning
3- Create a regression model with Azure Machine Learning designer.
   o Learn how to train and publish a regression model with Azure Machine Learning designer.
4- Create a classification model with Azure Machine Learning designer.
   o Train and publish a classification model with Azure Machine Learning designer.
5- Create a clustering model with Azure Machine Learning designer.
   o Train and publish a clustering model with Azure Machine Learning designer.
6- Analyze images with the Computer Vision service.
   o Learn how to use the Computer Vision cognitive service to analyze images.
7- Classify images with the Custom Vision service.
   o Learn how to use the Custom Vision service to create an image classification solution.
8- Detect objects in images with the Custom Vision service.
   o Learn how to use the Custom Vision service to create an object detection solution.
9- Detect and analyze faces with the Face service.
   o Learn how to use the Face cognitive service to detect and analyze faces in images.
10- Read text with the Computer Vision service.
   o Learn how to read text in images with the Computer Vision service.
11- Analyze receipts with the Form Recognizer service.
   o Learn how to use the built-in receipt processing capabilities of the Form Recognizer service.
12- Analyze text with the Language service.
   o Learn how to use the Language service for text analysis.
13- Recognize and synthesize speech.
   o Learn about speech recognition and synthesis.
   o Learn how to use the Speech cognitive service in Azure.
14- Translate text and speech.
   o After completing this module, you will be able to perform text and speech translation using Azure Cognitive Services.
15- Create a language model with Conversational Language Understanding
   o Learn what Conversational Language Understanding is.
   o Learn about key features, such as intents and utterances.
   o Build and publish a natural-language machine-learning model.

16- Build a bot with the Language Service and Azure Bot Service.
 - o After completing this module, you'll be able to create a knowledge base with an Azure Bot Service bot.

AZ-900

Training Course AZ-900: Microsoft Azure Fundamentals

Overview: This course will provide foundational level knowledge on cloud concepts; core Azure services; and Azure management and governance features and tools.

Duration: 1 Day.

Audience Profile: This course is suitable for IT personnel who are just beginning to work with Azure. This audience wants to learn about our offerings and get hands-on experience with the product. This course primarily uses the Azure portal and command line interface to create resources and does not require scripting skills. Students on this course will gain confidence to take other role-based courses and certifications, such as Azure Administrator.

Certification: This course prepares you for the AZ-900: Azure Fundamentals.

Course Objectives: After completing this course, students will be able to:

- Describe cloud concepts.
- Describe Azure architecture and services.
- Describe Azure management and governance.
- Learn about the basics of cloud computing and Azure.
- Learn about Azure architecture and core services.
- Learn about some of the core management and governance tools in Azure.

Course Outline:

1- Describe cloud computing.
  - Define cloud computing.
  - Describe the shared responsibility model.
  - Define cloud models, including public, private, and hybrid.
  - Identify appropriate use cases for each cloud model.
  - Describe the consumption-based model.
  - Compare cloud pricing models.
2- Describe the benefits of using cloud services.
  - Describe the benefits of high availability and scalability in the cloud.
  - Describe the benefits of reliability and predictability in the cloud.
  - Describe the benefits of security and governance in the cloud.
  - Describe the benefits of manageability in the cloud.
3- Describe cloud service types.
  - Describe Infrastructure as a Service (IaaS).
  - Describe Platform as a Service (PaaS).
  - Describe Software as a Service (SaaS).

- Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS)
4- Describe the core architectural components of Azure.
  - Describe Azure regions, region pairs, and sovereign regions.
  - Describe Availability Zones.
  - Describe Azure datacenters.
  - Describe Azure resources and Resource Groups.
  - Describe subscriptions.
  - Describe management groups.
  - Describe the hierarchy of resource groups, subscriptions, and management groups.
5- Describe Azure compute and networking services.
  - Compare compute types, including container instances, virtual machines, and functions.
  - Describe virtual machine (VM) options, including VMs, virtual machine scale sets, availability sets, Azure Virtual Desktop.
  - Describe resources required for virtual machines.
  - Describe application hosting options, including Azure Web Apps, containers, and virtual machines.
  - Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, VPN Gateway, and ExpressRoute.
  - Define public and private endpoints.
6- Describe Azure storage services.
  - Compare Azure storage services.
  - Describe storage tiers.
  - Describe redundancy options.
  - Describe storage account options and storage types.
  - Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync.
  - Describe migration options, including Azure Migrate and Azure Data Box.
7- Describe Azure identity, access, and security.
  - Describe directory services in Azure, including Azure Active Directory (AD) and Azure AD DS.
  - Describe authentication methods in Azure, including single sign-on (SSO), multifactor. authentication (MFA), and passwordless.
  - Describe external identities and guest access in Azure.
  - Describe Azure AD Conditional Access.
  - Describe Azure Role Based Access Control (RBAC).
  - Describe the concept of Zero Trust.
  - Describe the purpose of the defense in depth model.
  - Describe the purpose of Microsoft Defender for Cloud.
8- Describe cost management in Azure.
  - Describe factors that can affect costs in Azure.
  - Compare the Pricing calculator and Total Cost of Ownership (TCO) calculator.
  - Describe Azure Cost Management Tool.
  - Describe the purpose of tags.
9- Describe features and tools in Azure for governance and compliance.
  - Describe the purpose of Azure Blueprints.

- o Describe the purpose of Azure Policy.
- o Describe the purpose of resource locks.
- o Describe the purpose of the Service Trust portal.
10- Describe features and tools for managing and deploying Azure resources.
- o Describe Azure portal.
- o Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell.
- o Describe the purpose of Azure Arc.
- o Describe Azure Resource Manager (ARM) and Azure ARM templates.
11- Describe monitoring tools in Azure.
- o Describe the purpose of Azure Advisor.
- o Describe Azure Service Health.
- o Describe Azure Monitor, including Azure Log Analytics, Azure Monitor Alerts, and Application Insights.

DP-900

Training Course DP-900: Microsoft Power Platform Fundamentals

Overview: In this course, students will gain foundational knowledge of core data concepts and related Microsoft Azure data services. Students will learn about core data concepts such as relational, non-relational, big data, and analytics, and build their foundational knowledge of cloud data services within Microsoft Azure. Students will explore fundamental relational data concepts and relational database services in Azure. They will explore Azure storage for non-relational data and the fundamentals of Azure Cosmos DB. Students will learn about large-scale data warehousing, real-time analytics, and data visualization.

Duration: 1 Day.

Audience Profile: The audience for this course is individuals who want to learn the fundamentals of database concepts in a cloud environment, get basic skilling in cloud data services, and build their foundational knowledge of cloud data services within Microsoft Azure.

Certification: This course prepares you for the DP-900: Microsoft Azure Data Fundamentals.

Course Objectives: After completing this course, students will be able to:

- Describe core data concepts.
- Identify considerations for relational data on Azure.
- Describe considerations for working with non-relational data on Azure.
- Describe an analytics workload on Azure?

Course Outline:

1- Explore core data concepts.
    o Identify common data formats.
    o Describe options for storing data in files.
    o Describe options for storing data in databases.
    o Describe characteristics of transactional data processing solutions.
    o Describe characteristics of analytical data processing solutions.
2- Describe the benefits of using cloud services.
    o Identify common data professional roles.
    o Identify common cloud services used by data professionals.
3- Explore fundamental relational data concepts.
    o Identify characteristics of relational data.
    o Define normalization.
    o Identify types of SQL statement.
    o Identify common relational database objects.

4- Explore relational database services in Azure
   o Identify options for Azure SQL services.
   o Identify options for open-source databases in Azure.
   o Provision a database service on Azure.
5- Explore Azure Storage for non-relational data.
   o Describe features and capabilities of Azure blob storage.
   o Describe features and capabilities of Azure Data Lake Gen2.
   o Describe features and capabilities of Azure file storage.
   o Describe features and capabilities of Azure table storage.
   o Provision and use an Azure Storage account.

MS-900

Training Course MS-900: Microsoft Power Platform Fundamentals

Overview: This course introduces Microsoft 365, an integrated cloud platform that delivers industry-leading productivity apps along with intelligent cloud services, and world-class security. You'll learn foundational knowledge on the considerations and benefits of adopting cloud services and the Software as a Service (SaaS) cloud model, with a specific focus on Microsoft 365 cloud service offerings. You will begin by learning about cloud fundamentals, including an overview of cloud computing. You will be introduced to Microsoft 365 and learn how Microsoft 365 solutions improve productivity, facilitate collaboration, and optimize communications. The course then analyzes how security, compliance, privacy, and trust are handled in Microsoft 365, and it concludes with a review of Microsoft 365 subscriptions, licenses, billing, and support.

Duration: 1 Day.

Audience Profile: This course is designed for candidates looking to demonstrate foundational-level knowledge of cloud-based solutions to facilitate productivity and collaboration on-site, at home, or a combination of both. Candidates may have knowledge of cloud-based solutions or may be new to Microsoft 365.

Certification: This course prepares you for the MS-900: Microsoft 365 Fundamentals.

Course Objectives: After completing this course, students will be able to:

- Describe cloud computing.
- Describe the benefits of using cloud services.
- Describe cloud service types.
- What is Microsoft 365?
- Describe productivity solutions of Microsoft 365.
- Describe collaboration solutions of Microsoft 365.
- Describe endpoint modernization, management concepts, and deployment options in Microsoft 365.
- Describe analytics capabilities of Microsoft 365.
- Describe the services and identity types of Azure AD.
- Describe the access management capabilities of Azure AD.
- Describe threat protection with Microsoft 365 Defender.
- Describe security capabilities of Microsoft Sentinel.
- Describe the compliance management capabilities in Microsoft Purview.
- Describe the Service Trust Portal and privacy at Microsoft.
- Describe Microsoft 365 pricing, licensing, and billing options.
- Describe support offerings for Microsoft 365 services.

Course Outline:

1- Describe cloud computing.
   o Define cloud computing.
   o Describe the shared responsibility model.
   o Define cloud models, including public, private, and hybrid.
   o Identify appropriate use cases for each cloud model.
   o Describe the consumption-based model.
   o Compare cloud pricing models.
2- Describe the benefits of using cloud services.
   o Describe the benefits of high availability and scalability in the cloud.
   o Describe the benefits of reliability and predictability in the cloud.
   o Describe the benefits of security and governance in the cloud.
   o Describe the benefits of manageability in the cloud.
3- Describe cloud service types.
   o Describe Infrastructure as a Service (IaaS).
   o Describe Platform as a Service (PaaS).
   o Describe Software as a Service (SaaS).
   o Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS).
4- What is Microsoft 365?
   o Describe Office 365, Microsoft 365, and Windows 365.
   o Describe how Microsoft 365 empowers workers for hybrid and flexible work.
   o Create a Microsoft 365 trial organization.
5- Describe productivity solutions of Microsoft 365.
   o Describe how the capabilities of Microsoft 365 can boost productivity.
   o Describe how Microsoft 365 Apps help people craft compelling content in real-time.
   o Describe how the capabilities of the work management tools optimize operations.
   o Describe additional Microsoft 365 productivity apps.
6- Describe collaboration solutions of Microsoft 365.
   o Describe how the collaboration tools of Microsoft 365 promote synergy in the workplace.
   o Describe how Microsoft Teams helps boost teamwork.
   o Describe how Microsoft Viva helps organizations create thriving work cultures.
   o Describe how Yammer communities can help foster connections within your organization.
7- Describe endpoint modernization, management concepts, and deployment options in Microsoft 365.
   o Describe the endpoint modern management capabilities of Microsoft 365.
   o Describe the differences between Windows 365 and Azure Virtual Desktop.
   o Describe the deployment and release models for Windows-as-a-Service.
   o Describe the deployment methods and update channels for Microsoft 365 Apps.
8- Describe analytics capabilities of Microsoft 365
   o Describe how Viva Insights help people and organizations work smarter and achieve balance.
   o Describe the capabilities of the Microsoft 365 admin center and user portal.
   o Describe the reports available in the Microsoft 365 admin center and other admin centers.
9- Describe the services and identity types of Azure AD.
   o Describe what Azure AD does.

- o Describe the types of identities Azure AD supports.
10- Describe the access management capabilities of Azure AD
   - o Describe Conditional Access in Azure AD.
   - o Describe the benefits of Azure AD roles and role-based access control.
11- Describe threat protection with Microsoft 365 Defender
   - o Describe the Microsoft 365 Defender service.
   - o Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.
   - o Describe and explore Microsoft 365 Defender portal.
12- Describe security capabilities of Microsoft Sentinel.
   - o Describe the security concepts for SIEM and SOAR.
   - o Describe how Microsoft Sentinel provides integrated threat management.
   - o Describe the pricing models of Microsoft Sentinel.
13- Describe the compliance management capabilities in Microsoft Purview.
   - o Describe the Microsoft Purview compliance portal.
   - o Describe Compliance Manager.
   - o Describe the use and benefits of compliance score.
14- Describe the Service Trust Portal and privacy at Microsoft.
   - o Describe the offerings of the Service Trust Portal.
   - o Describe Microsoft's Privacy principles.
   - o Describe Microsoft Privacy.
15- Describe Microsoft 365 pricing, licensing, and billing options.
   - o Describe the pricing models available for Microsoft cloud services.
   - o Describe billing management features such as billing frequency and methods of payment.
   - o Describe the differences between base licensing and add-on licensing.
16- Describe support offerings for Microsoft 365 services.
   - o Describe the support offerings available for Microsoft 365 and how to create a support request.
   - o Describe service level agreement (SLAs) concepts.
   - o Identify how to track service health through the Microsoft 365 admin center.
   - o Describe how organizations can provide feedback on Microsoft 365 products and services.

PL-900

Training Course PL-900: Microsoft Power Platform Fundamentals

Overview: Learn the business value and product capabilities of Microsoft Power Platform. Create simple Power Apps, connect data with Dataverse, build a Power BI Dashboard, and automate processes with Power Automate.

Duration: 1 Day.

Audience Profile: Candidates for this course are users who aspire to improve productivity by automating business processes, analyzing data to produce business insights, and acting more effectively by creating simple app experiences.

Certification: This course prepares you for the PL-900: Power Platform Fundamentals.

Course Objectives: After completing this course, students will be able to:

- Describe the business value of the Microsoft Power Platform.
- Identify foundational components of Microsoft Power Platform.
- Describe how to build applications with Microsoft Power Apps.
- Describe building automation with Microsoft Power Automate.
- Describe the capabilities of Microsoft Power BI.
- Describe complementary Microsoft Power Platform solutions .

Course Outline:

1- Describe the business value of the Microsoft Power Platform
    o Examine Microsoft Power Platform.
    o Describe the business value of the Power Platform.
    o Explore connectors in Power Platform.
    o Review using Microsoft Dataverse to organize business data.
    o Examine how Power Platform works together with Microsoft 365 apps and services.
    o Explore solutions using Power Platform Microsoft Teams.
    o Describe how Power Platform works with Dynamics 365.
    o Describe how Power Platform solutions can consume Azure Services.
    o Explore how Power Platform apps work together to create solutions.
2- Identify foundational components of Microsoft Power Platform
    o Discover Microsoft Dataverse.
    o Learn about the Common Data Model.
    o Identify tables, columns, and relationships.
    o Learn about environments.
    o Discover business rules.
3- Describe how to build applications with Microsoft Power Apps

- o Examine Power Apps.
- o Explore canvas applications.
- o Explore model-driven applications.
- o Differentiate between canvas and model-driven applications.
- o Build a basic canvas app.
- o Build a basic model-driven app.
4- Describe building automation with Microsoft Power Automate
- o Examine the capabilities of Power Automate.
- o Explore the different Power Automate apps.
- o Examine the components of a cloud flow.
- o Examine Power Automate scenarios.
- o Build a basic cloud flow.
- o Build a basic desktop flow.
- o Examine the business value provided by Power Automate.
5- Describe the capabilities of Microsoft Power BI
- o Describe the business value and features of Power BI.
- o Compare and contrast the different components that make up Power BI.
- o Describe how to clean and transform data.
- o Examine how AI insights help detect anomalies and spot trends.
- o Build a basic dashboard.
- o Consume Power BI reports and dashboards.
6- Describe complementary Microsoft Power Platform solutions
- o Describe the capabilities of Power Virtual Agents and the business value it provides.
- o Examine the process of building a simple chatbot.
- o Describe the capabilities of Power Pages and the business value it provides.
- o Examine the process for building a basic site.
- o Describe the capabilities of AI Builder and the business value it provides.

SC-900

Training Course SC-900: Microsoft Security, Compliance, and Identity Fundamentals

Overview: This course provides foundational level knowledge on security, compliance, and identity concepts and related cloud-based Microsoft solutions.

Duration: 1 Day.

Audience Profile: The target audience for this course is individuals who want to become familiar with the fundamentals of security, compliance and identity (SCI) in cloud-based and related Microsoft services. The content of this course is aligned with the objective profile of the SC-900 exam. Candidates should be familiar with Microsoft Azure and Microsoft 365 and understand how Microsoft security, compliance and identity solutions can span across these solution areas to provide a holistic end-to-end solution.

Certification: This course prepares you for the SC-900: Fundamentals of Security, Compliance and Identity exam.

Course Objectives: After completing this course, students will be able to:

- Describe basic concepts of security, compliance, and identity.
- Describe the concepts and capabilities of Microsoft identity and access management solutions.
- Describe the capabilities of Microsoft security solutions.
- Describe the compliance management capabilities in Microsoft.

Course Outline:

1- Describe the basic concepts of security, compliance, and identity.
   o Describe security and compliance concepts and methods.
   o Describe identity concepts.
2- Describe the concepts and functions of Microsoft Identity & Access Management solutions.
   o Describe the basic services and identity types of Azure AD.
   o Describe the authentication features of Azure AD.
   o Describe the access management features of Azure AD.
   o Identity protection and governance features of Azure AD.
3- Describe the features of Microsoft security solutions.
   o Describe the basic security features of Azure.
   o Describe the security management features of Azure.
   o Describe the security features of Microsoft Sentinel.
   o Describe the threat protection features of Microsoft 365.
   o Describe the security management features of Microsoft 365.
   o Endpoint Security with Microsoft Intune.

4- Describe the features of Microsoft compliance solutions.
   o Describe the compliance management capabilities in Microsoft
   o Describe the information protection and governance features of Microsoft 365
   o Describe the insider risk features in Microsoft 365
   o Describe the eDiscovery and monitoring capabilities of Microsoft 365
   o Describe the resource governance capabilities in Azure

ROLE BASED

AZ-104

Training Course AZ-104: Microsoft Azure Administrator

Overview: This course teaches IT Professionals how to manage their Azure subscriptions, secure identities, administer the infrastructure, configure virtual networking, connect Azure and on-premises sites, manage network traffic, implement storage solutions, create and scale virtual machines, implement web apps and containers, back up and share data, and monitor your solution.

Duration: 4 Days.

Audience Profile: This course is for Azure Administrators. The Azure Administrator implements, manages, and monitors identity, governance, storage, compute, and virtual networks in a cloud environment. The Azure Administrator will provision, size, monitor, and adjust resources as appropriate.

Certification: This course prepares you for the AZ-104: Microsoft Azure Administrator.

Course Objectives: After completing this course, students will be able to:
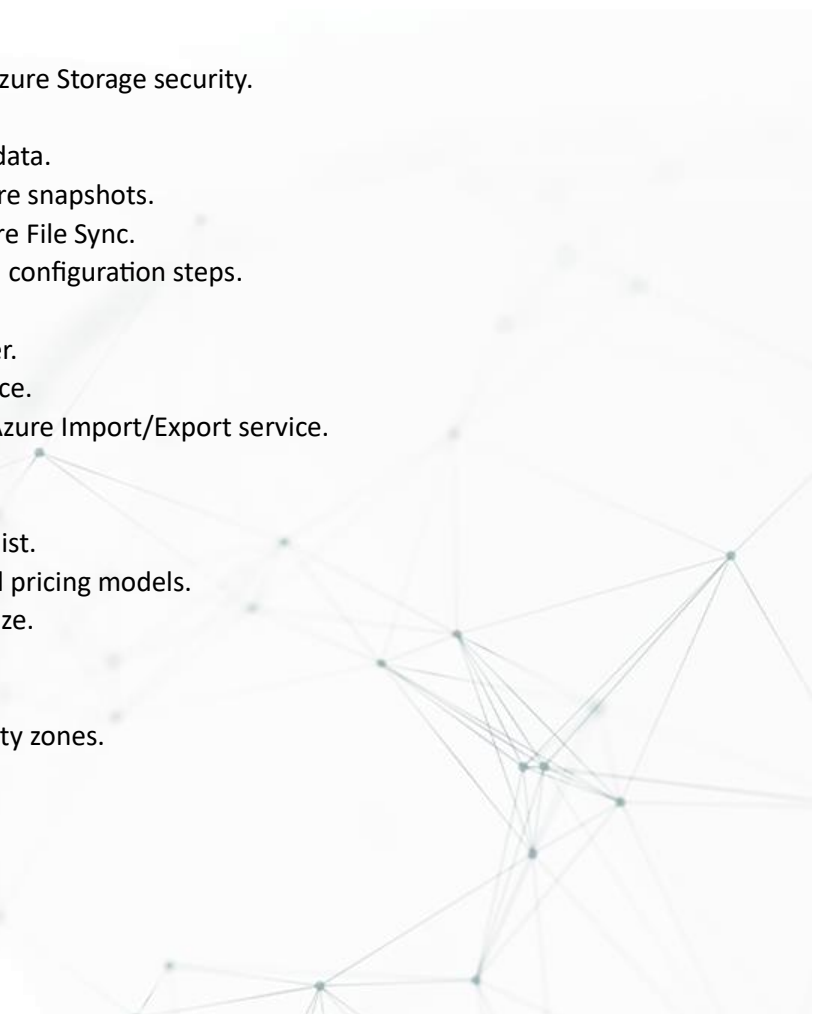
- Configure Azure Active Directory.
- Configure user and group accounts.
- Configure subscriptions.
- Configure Azure Policy.
- Configure role-based access control.
- Configure Azure resources with tools.
- Use Azure Resource Manager.
- Configure resources with Azure Resource Manager templates.
- Configure virtual networks.
- Configure network security groups.
- Configure Azure DNS.
- Configure Azure virtual network peering.
- Configure network routing and endpoints.
- Configure Azure Load Balancer.
- Configure Azure Application Gateway.
- Configure storage accounts.
- Configure Azure Blob Storage.
- Configure Azure Storage security.
- Configure Azure Files and Azure File Sync.
- Configure Azure Storage with tools.
- Configure virtual machines.
- Configure virtual machine availability.
- Configure virtual machine extensions.

- Configure Azure app service plans.
- Configure Azure App Service.
- Configure Azure Container Instances.
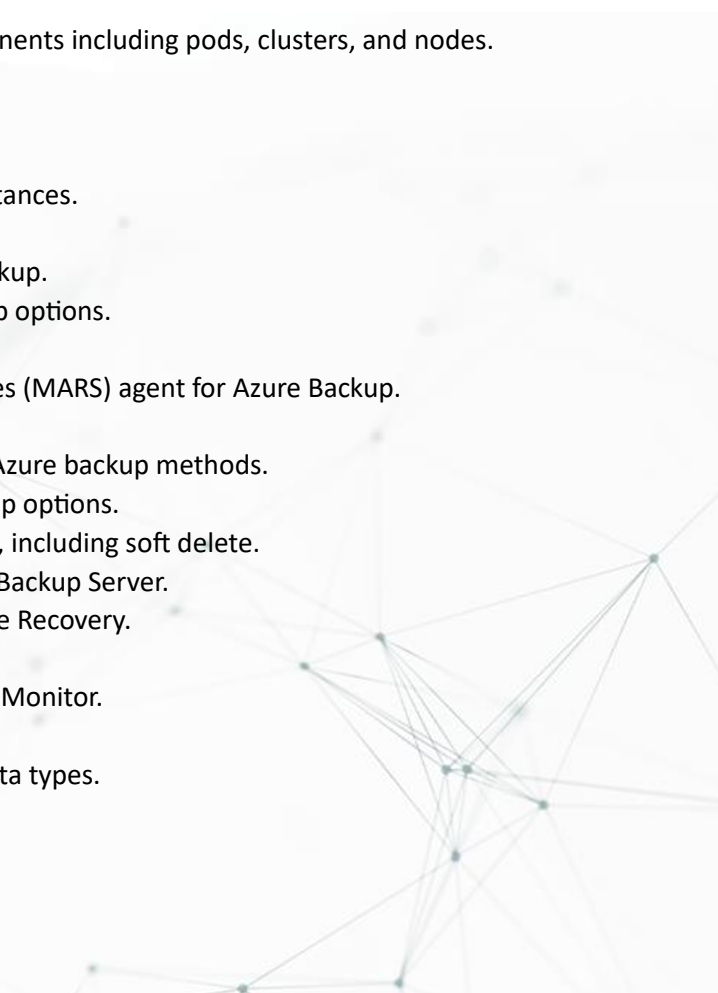- Configure Azure Kubernetes Service.
- Configure file and folder backups.
- Configure virtual machine backups.
- Configure Azure Monitor.
- Configure Azure alerts.
- Configure Log Analytics.
- Configure Azure Network Watcher.

Course Outline:

1- Configure Azure Active Directory.
   - Define Azure AD concepts, including identities, accounts, and tenants.
   - Describe Azure AD features to support different configurations.
   - Understand differences between Azure AD and Active Directory Domain Services (AD DS).
   - Choose between supported editions of Azure AD.
   - Implement the Azure AD join feature.
   - Use the Azure AD self-service password reset feature..
2- Configure user and group accounts.
   - Configure users accounts and user account properties.
   - Create new user accounts.
   - Import bulk user accounts with a template.
   - Configure group accounts and assignment types.
3- Configure subscriptions.
   - Determine the correct region to locate Azure services.
   - Review features and use cases for Azure subscriptions.
   - Obtain an Azure subscription.
   - Understand billing and features for different Azure subscriptions.
   - Use Microsoft Cost Management for cost analysis.
   - Discover when to use Azure resource tagging.
   - Identify ways to reduce costs.
4- Configure Azure Policy.
   - Create management groups to target policies and spending budgets.
   - Implement Azure Policy with policy and initiative definitions.
   - Scope Azure policies and determine compliance.
5- Configure role-based access control.
   - Identify features and use cases for role-based access control.
   - List and create role definitions.
   - Create role assignments.
   - Identify differences between Azure RBAC and Azure Active Directory roles.
   - Manage access to subscriptions with RBAC.
   - Review built-in Azure RBAC roles.
6- Configure Azure resources with tools.

- o Manage resources with the Azure portal.
- o Manage resources with Azure Cloud Shell.
- o Manage resources with Azure PowerShell.
- o Manage resources with Azure CLI.
7- Use Azure Resource Manager.
- o Identify the features and usage cases for Azure Resource Manager.
- o Describe each Azure Resource Manager component and its usage.
- o Organize your Azure resources with resource groups.
- o Apply Azure Resource Manager locks.
- o Move Azure resources between groups, subscriptions, and regions.
- o Remove resources and resource groups.
- o Apply and track resource limits.
8- Configure resources with Azure Resource Manager templates.
- o List the advantages of Azure templates.
- o Identify the Azure template schema components.
- o Specify Azure template parameters.
- o Locate and use Azure Quickstart Templates.
9- Configure virtual networks.
- o Describe Azure virtual network features and components.
- o Identify features and usage cases for subnets and subnetting.
- o Identify usage cases for private and public IP addresses.
- o Create and determine which resources require public IP addresses.
- o Create and determine which resources require private IP addresses.
- o Create virtual networks.
10- Configure network security groups.
- o Determine when to use network security groups.
- o Implement network security group rules.
- o Evaluate network security group effective rules.
- o Examine advantages of application security groups.
11- Configure Azure DNS.
- o Identify features and usage cases for domains, custom domains, and private zones.
- o Verify custom domain names using DNS records.
- o Implement DNS zones, DNS delegation, and DNS record sets.
12- Configure Azure virtual network peering.
- o Identify usage cases and product features of Azure virtual network peering.
- o Configure your network to implement Azure VPN Gateway for transit connectivity.
- o Extend peering by using a hub and spoke network with user-defined routes and service chaining.
13- Configure network routing and endpoints.
- o Implement system routes and user-defined routes.
- o Configure a custom route.
- o Implement service endpoints.
- o Identify features and usage cases for private links and endpoint services.
14- Configure Azure Load Balancer.

- o   Identify features and usage cases for Azure load balancer.
- o   Implement public and internal Azure load balancers.
- o   Compare features of load balancer SKUs and configuration differences.
- o   Configure back-end pools, load-balancing rules, session persistence, and health probes.

15- Configure Azure Application Gateway.
- o   Identify features and usage cases for Azure Application Gateway.
- o   Implement Azure Application Gateway, including selecting a routing method.
- o   Configure gateway components, such as listeners, health probes, and routing rules.

16- Configure storage accounts.
- o   Identify features and usage cases for Azure storage accounts.
- o   Select between different types of Azure Storage and storage accounts.
- o   Select a storage replication strategy.
- o   Configure network access to storage accounts.
- o   Secure storage endpoints.

17- Configure Azure Blob Storage.
- o   Identify features and usage cases for Azure Blob Storage.
- o   Configure Blob Storage and Blob access tiers.
- o   Configure Blob lifecycle management rules.
- o   Configure Blob object replication.
- o   Upload and price Blob Storage.

18- Configure Azure Storage security.
- o   Configure a shared access signature (SAS), including the uniform resource identifier (URI) and SAS parameters.
- o   Configure Azure Storage encryption.
- o   Implement customer-managed keys.
- o   Recommend opportunities to improve Azure Storage security.

19- Configure Azure Files and Azure File Sync.
- o   Identify storage for file shares and blob data.
- o   Configure Azure Files shares and file share snapshots.
- o   Identify features and usage cases of Azure File Sync.
- o   Identify Azure File Sync components and configuration steps.

20- Configure Azure Storage with tools.
- o   Configure and use Azure Storage Explorer.
- o   Configure the Azure Import/Export service.
- o   Use the WAImportExport tool with the Azure Import/Export service.
- o   Configure and use AZCopy.

21- Configure virtual machines.
- o   Create a virtual machine planning checklist.
- o   Determine virtual machine locations and pricing models.
- o   Determine the correct virtual machine size.
- o   Configure virtual machine storage.

22- Configure virtual machine availability.
- o   Implement availability sets and availability zones.
- o   Implement update and fault domains.

- o Implement Virtual Machine Scale Sets.
- o Autoscale virtual machines.

23- Configure virtual machine extensions.
- o Identify features and usage cases for virtual machine extensions.
- o Identify features and usage cases for custom script extensions.
- o Identify features and usage cases for desired state configuration.

24- Configure Azure app service plans.
- o Identify features and usage cases of the Azure App Service.
- o Select an appropriate Azure App Service plan pricing tier.
- o Scale the App Service Plan.
- o Scale out the App Service Plan.

25- Configure Azure App Services.
- o Identify features and usage cases for the Azure App Service.
- o Create an app with Azure App Service.
- o Configure deployment settings, specifically deployment slots.
- o Secure your Azure App Service app.
- o Configure custom domain names.
- o Backup and restore your Azure App Service app.
- o Configure Azure Application Insights.

26- Configure Azure Container Instances.
- o Identify when to use containers versus virtual machines.
- o Identify the features and usage cases of Azure Container Instances.
- o Implement Azure Container Groups.

27- Configure Azure Kubernetes Service.
- o Identify Azure Kubernetes Service (AKS) components including pods, clusters, and nodes.
- o Configure network connections for AKS.
- o Configure storage options for AKS.
- o Implement security options for AKS.
- o Scale AKS including adding Azure Container Instances.

28- Configure file and folder backups.
- o Identify features and usage cases for Azure Backup.
- o Configure Azure Recovery Services Vault backup options.
- o Implement on-premises file and folder backup.
- o Configure the Microsoft Azure Recovery Services (MARS) agent for Azure Backup.

29- Configure virtual machine backups.
- o Identify features and usage cases for different Azure backup methods.
- o Configure virtual machine snapshots and backup options.
- o Implement virtual machine backup and restore, including soft delete.
- o Compare the Azure Backup agent to the Azure Backup Server.
- o Perform site-to-site recovery by using Azure Site Recovery.

30- Configure Azure Monitor.
- o Identify the features and usage cases for Azure Monitor.
- o Configure and interpret metrics and logs.
- o Identify the Azure Monitor components and data types.

- o Configure the Azure Monitor Activity Log.
31- Configure Azure alerts.
  - o Identify Azure Monitor alerts, including alert types and alert states.
  - o Configure Azure Monitor alerts.
  - o Create alert rules and action groups.
32- Configure Log Analytics.
  - o Identify the features and usage cases for Log Analytics.
  - o Create a Log Analytics workspace.
  - o Structure a Log Analytics query and review results.
33- Configure Azure Network Watcher.
  - o Identify the features and usage cases for Azure Network Watcher.
  - o Configure diagnostic capabilities like IP Flow Verify, Next Hop, and Network Topology.

AZ-204

Training Course AZ-204: Developing Solutions for Microsoft Azure

Overview: This course teaches developers how to create end-to-end solutions in Microsoft Azure. Students will learn how to implement Azure compute solutions, create Azure Functions, implement and manage web apps, develop solutions utilizing Azure storage, implement authentication and authorization, and secure their solutions by using KeyVault and Managed Identities. Students will also learn how to connect to and consume Azure services and third-party services and include event- and message-based models in their solutions. The course also covers monitoring, troubleshooting, and optimizing Azure solutions.

Duration: 5 Days.

Audience Profile: Students in this course are interested in Azure development or in passing the Microsoft Azure Developer Associate certification exam.

Certification: This course prepares you for the AZ-204: Developing Solutions for Microsoft Azure
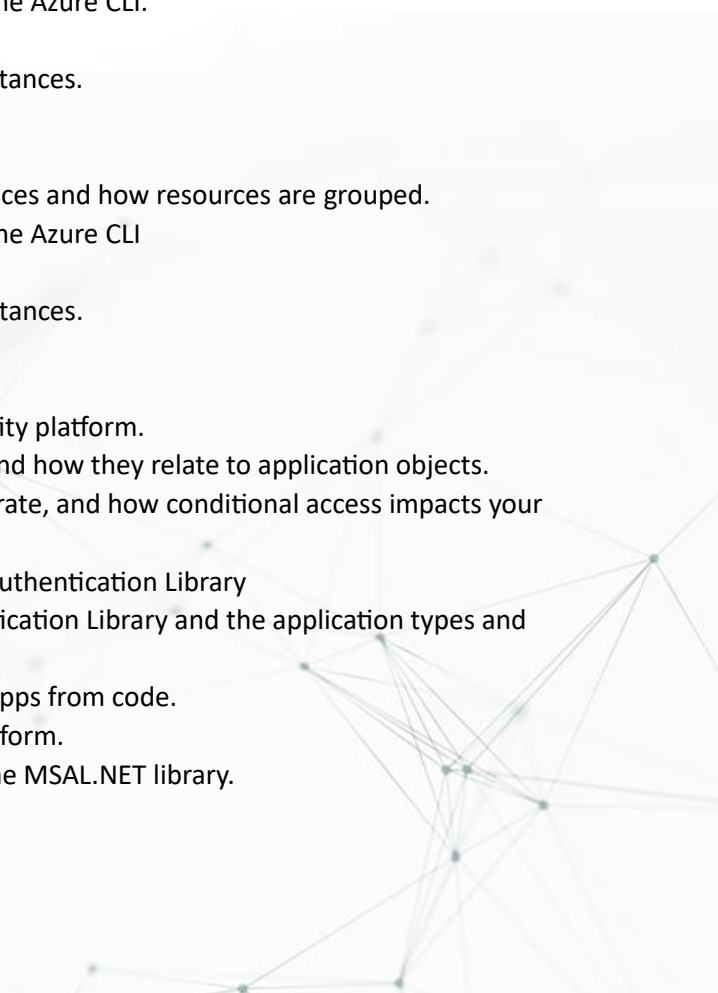
Course Objectives: After completing this course, students will be able to:
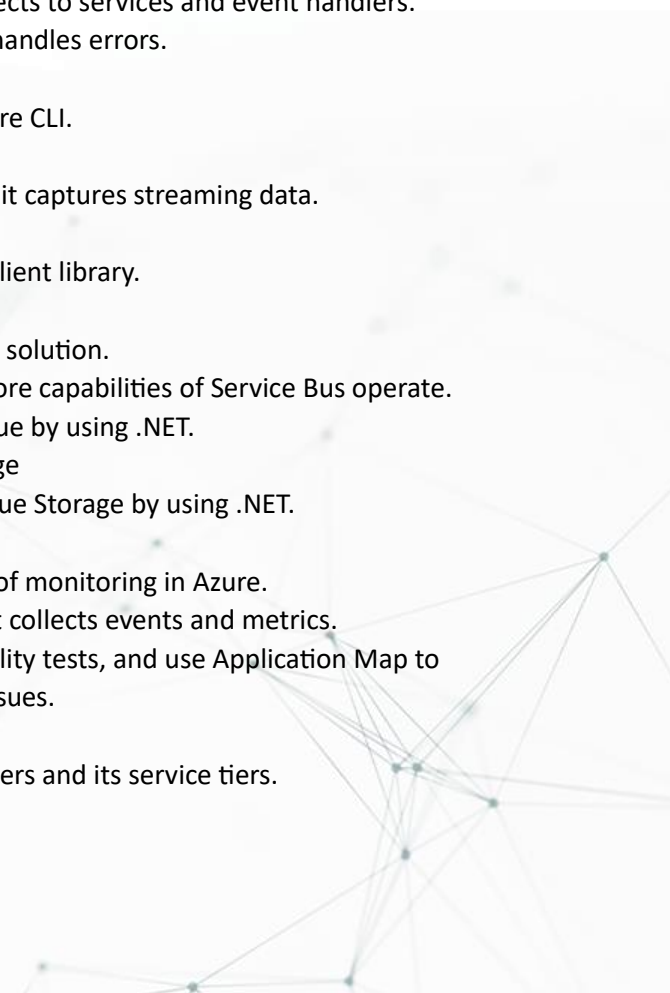
- Explore Azure App Service
- Configure web app settings.
- Scale apps in Azure App Service
- Explore Azure App Service deployment slots.
- Explore Azure Functions
- Develop Azure Functions
- Explore Azure Blob storage.
- Manage the Azure Blob storage lifecycle.
- Work with Azure Blob storage
- Explore Azure Cosmos DB
- Work with Azure Cosmos DB
- Manage container images in Azure Container Registry
- Run container images in Azure Container Instances
- Implement Azure Container Apps
- Explore the Microsoft identity platform.
- Implement authentication by using the Microsoft Authentication Library
- Implement shared access signatures.
- Explore Microsoft Graph
- Implement Azure Key Vault
- Implement managed identities.
- Implement Azure App Configuration
- Explore API Management
- Explore Azure Event Grid

- Explore Azure Event Hubs
- Discover Azure message queues.
- Monitor app performance
- Develop for Azure Cache for Redis
- Develop for storage on CDNs.

Course Outline

1- Explore Azure App Service
   o Describe Azure App Service key components and value.
   o Explain how Azure App Service manages authentication and authorization.
   o Identify methods to control inbound and outbound traffic to your web app.
   o Deploy an app-to-App Service using Azure CLI commands.
2- Configure web app settings.
   o Create application settings that are bound to deployment slots.
   o Explain the options for installing SSL/TLS certificates for your app.
   o Enable diagnostic logging for your app to aid in monitoring and debugging.
   o Create virtual app to directory mappings.
3- Scale apps in Azure App Service
   o Identify scenarios for which autoscaling is an appropriate solution.
   o Create autoscaling rules for a web app.
   o Monitor the effects of autoscaling.
4- Explore Azure App Service deployment slots.
   o Describe the benefits of using deployment slots.
   o Understand how slot swapping operates in App Service.
   o Perform manual swaps and enable auto swap.
   o Route traffic manually and automatically.
5- Explore Azure Functions
   o Explain functional differences between Azure Functions, Azure Logic Apps, and WebJobs
   o Describe Azure Functions hosting plan options.
   o Describe how Azure Functions scale to meet business needs.
6- Develop Azure Functions
   o Explain the key components of a function and how they are structured.
   o Create triggers and bindings to control when a function runs and where the output is directed.
   o Connect a function to services in Azure.
   o Create a function by using Visual Studio Code and the Azure Functions Core Tools
7- Explore Azure Blob storage.
   o Identify the different types of storage accounts and the resource hierarchy for blob storage.
   o Explain how data is securely stored and protected through redundancy.
   o Create a block blob storage account by using the Azure Cloud Shell.
8- Manage the Azure Blob storage lifecycle.
   o Describe how each of the access tiers are optimized.
   o Create and implement a lifecycle policy.
   o Rehydrate blob data stored in an archive tier.

9- Work with Azure Blob storage
   o Create an application to create and manipulate data by using the Azure Storage client library for Blob storage.
   o Manage container properties and metadata by using .NET and REST.
10- Explore Azure Cosmos DB
   o Identify the key benefits provided by Azure Cosmos DB
   o Describe the elements in an Azure Cosmos DB account and how they are organized.
   o Explain the different consistency levels and choose the correct one for your project.
   o Explore the APIs supported in Azure Cosmos DB and choose the appropriate API for your solution.
   o Describe how request units' impact costs.
   o Create Azure Cosmos DB resources by using the Azure portal.
11- Work with Azure Cosmos DB
   o Identify classes and methods used to create resources.
   o Create resources by using the Azure Cosmos DB .NET v3 SDK.
   o Write stored procedures, triggers, and user-defined functions by using JavaScript.
12- Manage container images in Azure Container Registry
   o Explain the features and benefits Azure Container Registry offers.
   o Describe how to use ACR Tasks to automate builds and deployments.
   o Explain the elements in a Dockerfile.
   o Build and run an image in the ACR by using Azure CLI.
13- Run container images in Azure Container Instances
   o Describe the benefits of Azure Container Instances and how resources are grouped.
   o Deploy a container instance in Azure by using the Azure CLI.
   o Start and stop containers using policies.
   o Set environment variables in your container instances.
   o Mount file shares in your container instances.
14- Implement Azure Container Apps.
   o Describe the benefits of Azure Container Instances and how resources are grouped.
   o Deploy a container instance in Azure by using the Azure CLI
   o Start and stop containers using policies.
   o Set environment variables in your container instances.
   o Mount file shares in your container instances
15- Explore the Microsoft identity platform.
   o Identify the components of the Microsoft identity platform.
   o Describe the three types of service principles and how they relate to application objects.
   o Explain how permissions and user consent operate, and how conditional access impacts your application.
16- Implement authentication by using the Microsoft Authentication Library
   o Explain the benefits of using Microsoft Authentication Library and the application types and scenarios it supports.
   o Instantiate both public and confidential client apps from code.
   o Register an app with the Microsoft identity platform.
   o Create an app that retrieves a token by using the MSAL.NET library.

17- Implement shared access signatures.
- Identify the three types of shared access signatures.
- Explain when to implement shared access signatures.
- Create a stored access policy.

18- Explore Microsoft Graph
- Explain the benefits of using Microsoft Graph.
- Perform operations on Microsoft Graph by using REST and SDKs.
- Apply best practices to help your applications get the most out of Microsoft Graph.

19- Implement Azure Key Vault.
- Describe the benefits of using Azure Key Vault.
- Explain how to authenticate to Azure Key Vault.
- Set and retrieve a secret from Azure Key Vault by using the Azure CLI.

20- Implement managed identities.
- Explain the differences between the two types of managed identities.
- Describe the flows for user- and system-assigned managed identities.
- Configure managed identities.
- Acquire access tokens by using REST and code.

21- Explore API Management
- Describe the components (and their functions) of the API Management service.
- Explain how API gateways can help manage calls to your APIs.
- Secure access to APIs by using subscriptions and certificates.
- Create a backend API.

22- Explore Azure Event Grid.
- Describe how Event Grid operates and how it connects to services and event handlers.
- Explain how Event Grid delivers events and how it handles errors.
- Implement authentication and authorization.
- Route custom events to web endpoint by using Azure CLI.

23- Explore Azure Event Hubs
- Describe the benefits of using Event Hubs and how it captures streaming data.
- Explain how to process events.
- Perform common operations with the Event Hubs client library.

24- Discover Azure message queues.
- Choose the appropriate queue mechanism for your solution.
- Explain how the messaging entities that form the core capabilities of Service Bus operate.
- Send and receive messages from a Service Bus queue by using .NET.
- Identify the key components of Azure Queue Storage
- Create queues and manage messages in Azure Queue Storage by using .NET.

25- Monitor app performance.
- Explain how Azure Monitor operates as the center of monitoring in Azure.
- Describe how Application Insights works and how it collects events and metrics.
- Instrument an app for monitoring, perform availability tests, and use Application Map to help you monitor performance and troubleshoot issues.

26- Develop for Azure Cache for Redis
- Explain the key scenarios Azure Cache for Redis covers and its service tiers.

- o Identify the key parameters for creating an Azure Cache for Redis instance and interact with the cache.
- o Connect an app to Azure Cache for Redis by using .NET Core.
27- Develop for storage on CDNs.
  - o Explain how the Azure Content Delivery Network works and how it can improve the user experience.
  - o Control caching behavior and purge content.
  - o Perform actions on Azure CDN by using the Azure CDN Library for .NET.

AZ-305

Training Course AZ-305: Designing Microsoft Azure Infrastructure Solutions

Overview: This course teaches Azure Solution Architects how to design infrastructure solutions. Course topics cover governance, compute, application architecture, storage, data integration, authentication, networks, business continuity, and migrations. The course combines lecture with case studies to demonstrate basic architect design principles.

Duration: 4 Days.

Audience Profile: Successful students have experience and knowledge in IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data platforms, and governance. Students also have experience designing and architecting solutions.

Certification: This course prepares you for the AZ-305: Designing Microsoft Azure Infrastructure Solutions.

Course Objectives: After completing this course, students will be able to:

- Design governance.
- Design an Azure compute solution.
- Design a data storage solution for non-relational data.
- Design a data storage solution for relational data.
- Design data integration.
- Design an application architecture.
- Design authentication and authorization solutions.
- Design a solution to log and monitor Azure resources.
- Design network solutions.
- Design a solution for backup and disaster recovery.
- Design migrations.
- Build great solutions with the Microsoft Azure Well-Architected Framework.
- Accelerate cloud adoption with the Microsoft Cloud Adoption Framework for Azure.
- Configure virtual machine extensions.
- Configure Azure app service plans.
- Configure Azure App Service.
- Configure Azure Container Instances.
- Configure Azure Kubernetes Service.
- Configure file and folder backups.
- Configure virtual machine backups.
- Configure Azure Monitor.
- Configure Azure alerts.

- Configure Log Analytics.
- Configure Azure Network Watcher.

Course Outline:

1- Design governance.
   o Design for governance.
   o Design for management groups.
   o Design for Azure subscriptions.
   o Design for resource groups.
   o Design for resource tagging.
   o Design for Azure policy.
   o Design for Azure role-based access control.
   o Design for Azure Blueprints.
2- Design an Azure compute solution.
   o Choose an Azure compute service.
   o Design for Azure Virtual Machines solutions.
   o Design for Azure Batch solutions.
   o Design for Azure App Service solutions.
   o Design for Azure Container Instances solutions.
   o Design for Azure Kubernetes Service solutions.
   o Design for Azure Functions solutions.
   o Design for Azure Logic Apps solutions.
3- Design a data storage solution for non-relational data.
   o Design for data storage.
   o Design for Azure storage accounts.
   o Design for Azure blob storage.
   o Design for data redundancy.
   o Design for Azure files.
   o Design an Azure disk solution.
   o Design for storage security.
4- Design a data storage solution for relational data.
   o Design for Azure SQL Database.
   o Design for Azure SQL Managed Instance.
   o Design for SQL Server on Azure Virtual Machines.
   o Recommend a solution for database scalability.
   o Recommend a solution for database availability.
   o Design protection for data at rest, data in transmission, and data in use.
   o Design for Azure SQL Edge.
   o Design for Azure Cosmos DB.
   o Design for Azure Table Storage
5- Design data integration.
   o Design a data integration solution with Azure Data Factory.
   o Design a data integration solution with Azure Data Lake.
   o Design a data integration and analytics solution with Azure Databricks.

- o Design a data integration and analytics solution with Azure Synapse Analytics.
- o Design strategies for hot, warm, and cold data paths.
- o Design an Azure Stream Analytics solution for data analysis.
6- Design an application architecture.
- o Describe message and event scenarios.
- o Design a messaging solution.
- o Design an Azure Event Hubs messaging solution.
- o Design an event-driven solution.
- o Design an automated app deployment solution.
- o Design API integration.
- o Design an application configuration management solution.
- o Design a caching solution.
7- Design authentication and authorization solutions.
- o Design for identity and access management.
- o Design for Azure Active Directory.
- o Design for Azure Active Directory business-to-business (B2B).
- o Design for Azure Active Directory B2C (business-to-customer).
- o Design for conditional access.
- o Design for identity protection.
- o Design for access reviews.
- o Design for managed identities.
- o Design for service principals for applications.
- o Design for Azure Key Vault.
8- Design a solution to log and monitor Azure resources.
- o Design for Azure Monitor data sources
- o Design for Azure Monitor Logs (Log Analytics) workspaces
- o Design for Azure Workbooks and Azure insights
- o Design for Azure Data Explorer.
9- Design network solutions.
- o Recommend a network architecture solution based on workload requirements
- o Design for on-premises connectivity to Azure Virtual Network
- o Design for Azure network connectivity services
- o Design for application delivery services
- o Design for application protection services.
10- Design a solution for backup and disaster recovery.
- o Design for backup and recovery.
- o Design for Azure Backup.
- o Design for Azure blob backup and recovery.
- o Design for Azure Files backup and recovery.
- o Design for Azure virtual machine backup and recovery.
- o Design for Azure SQL backup and recovery.
- o Design for Azure Site Recovery.
11- Design migrations.
- o Evaluate migration with the Microsoft Cloud Adoption Framework for Azure

- o Describe the Azure Migration and Modernization Program (Azure Migration Framework)
- o Assess your on-premises workloads
- o Select a migration tool
- o Migrate your databases
- o Select an online storage migration tool
- o Migrate offline data.

12- Build great solutions with the Microsoft Azure Well-Architected Framework.
- o You want to build great things on Azure, but you're not sure exactly what that means. Using key principles throughout your architecture, regardless of technology choice, can help you design, build, and continuously improve your architecture.

13- Accelerate cloud adoption with the Microsoft Cloud Adoption Framework for Azure.
- o Do you need a clear path forward for your cloud journey? This learning path includes best practice guidance to help you create a cloud strategy, define a cloud adoption plan, prepare your cloud environment with proper governance, and implement cloud operations in alignment with your organizational needs. Cloud architects and IT professionals will learn and engage with the proven best practices, tools, and documentation in the Cloud Adoption Framework for Azure to build the technical knowledge needed to help your organization successfully adopt the cloud and meet business goals.

AZ-500

Training Course AZ-500: Microsoft Azure Security Technologies

Overview: This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities. This course includes security for identity and access, platform protection, data and applications, and security operations.

Duration: 4 Days.

Audience Profile: This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Certification: This course prepares you for the AZ-500: Microsoft Azure Security Technologies.

Course Objectives: After completing this course, students will be able to:

- Secure Azure solutions with Azure Active Directory.
- Implement Hybrid identity.
- Deploy Azure AD identity protection.
- Configure Azure AD privileged identity management.
- Design an enterprise governance strategy.
- Implement perimeter security.
- Configure network security.
- Configure and manage host security.
- Enable Containers security.
- Deploy and secure Azure Key Vault.
- Configure application security features.
- Implement storage security.
- Configure and manage SQL database security.
- Configure and manage Azure Monitor.
- Enable and manage Microsoft Defender for Cloud.
- Configure and monitor Microsoft Sentinel.

Course Outline:

1- Secure Azure solutions with Azure Active Directory.
    o Configure Azure AD and Azure AD Domain Services for security.
    o Create users and groups that enable secure usage of your tenant.
    o Use MFA to protect user's identities.

- o   Configure passwordless security options.
2- Implement Hybrid identity.
   - o   Deploy Azure AD Connect
   - o   Pick and configure that best authentication option for your security needs
   - o   Configure password writeback.
3- Deploy Azure AD identity protection.
   - o   Deploy and configure Identity Protection.
   - o   Configure MFA for users, groups, and applications.
   - o   Create Conditional Access policies to ensure your security.
   - o   Create and follow an access review process.
4- Configure Azure AD privileged identity management.
   - o   Describe Zero Trust and how it impacts security.
   - o   Configure and deploy roles using Privileged Identity Management (PIM).
   - o   Evaluate the usefulness of each PIM setting as it relates to your security goals.
5- Design an enterprise governance strategy.
   - o   Explain the shared responsibility model and how it impacts your security configuration.
   - o   Create Azure policies to protect your solutions.
   - o   Configure and deploy access to services using RBAC.
6- Implement perimeter security.
   - o   Define defense in depth.
   - o   Protect your environment from denial-of-service attacks.
   - o   Secure your solutions using firewalls and VPNs.
   - o   Explore your end-to-end perimeter security configuration based on your security posture.
7- Configure network security.
   - o   Deploy and configure network security groups to protect your Azure solutions.
   - o   Configure and lockdown service endpoints and private links.
   - o   Secure your applications with Application Gateway, Web App Firewall, and Front Door.
   - o   Configure ExpressRoute to help protect your network traffic.
8- Configure and manage host security.
   - o   Configure and deploy Endpoint Protection.
   - o   Deploy a privileged access strategy for devices and privileged workstations.
   - o   Secure your virtual machines and access to them.
   - o   Deploy Windows Defender.
   - o   Practice layered security by reviewing and implementing Security Center and Security Benchmarks.
9- Enable Containers security.
   - o   Define the available security tools for containers in Azure.
   - o   Configure security settings for containers and Kubernetes services.
   - o   Lock down network, storage, and identity resources connected to your containers.
   - o   Deploy RBAC to control access to containers.
10- Deploy and secure Azure Key Vault.
   - o   Define what a key vault is and how it protects certificates and secrets.
   - o   Deploy and configure Azure Key Vault.
   - o   Secure access and administration of your key vault.

- o Store keys and secrets in your key vault.
- o Explore key security considers like key rotation and backup / recovery.
11- Configure application security features.
- o Register an application in Azure using app registration.
- o Select and configure which Azure AD users can access each application.
- o Configure and deploy web app certificates.
12- Implement storage security.
- o Define data sovereignty and how that is achieved in Azure.
- o Configure Azure Storage access in a secure and managed way.
- o Encrypt your data while it is at rest and in transit.
- o Apply rules for data retention.
13- Configure and manage SQL database security.
- o Configure which users and applications have access to your SQL databases.
- o Block access to your servers using firewalls.
- o Discover, classify, and audit the use of your data.
- o Encrypt and protect your data while is it stored in the database.
14- Configure and manage Azure Monitor.
- o Configure and monitor Azure Monitor.
- o Define metrics and logs you want to track for your Azure applications.
- o Connect data sources to and configure Log Analytics.
- o Create and monitor alerts associated with your solutions security.
15- Enable and manage Microsoft Defender for Cloud.
- o Define the most common types of cyber-attacks.
- o Configure Azure Security Center based on your security posture.
- o Review Secure Score and raise it.
- o Lock down your solutions using Security Center and Defender.
- o Enable Just-in-Time access and other security features.
16- Configure and monitor Microsoft Sentinel.
- o Explain what Azure Sentinel is and how it is used.
- o Deploy Azure Sentinel.
- o Connect data to Azure Sentinel, like Azure Logs, Azure AD, and others.
- o Track incidents using workbooks, playbooks, and hunting techniques.

SC-200

Training Course SC-200: Microsoft Security Operations Analyst

Overview: Microsoft Security Operations Analyst certification training focuses on developing skills to mitigate threats using Microsoft's security, compliance, and identity solutions. The course covers a range of topics including threat protection, security management, identity & access configuration and management. Participants learn to protect cloud and hybrid environments, configure Microsoft 365 Defender and Microsoft Defender for Endpoint, and understanding Microsoft's Zero Trust model. The training also involves hands-on labs for practical learning.

Duration: 4 Days.

Audience Profile: The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Certification: This course prepares you for the SC-200: Microsoft Security Operations Analyst.

Course Objectives: After completing this course, students will be able to:
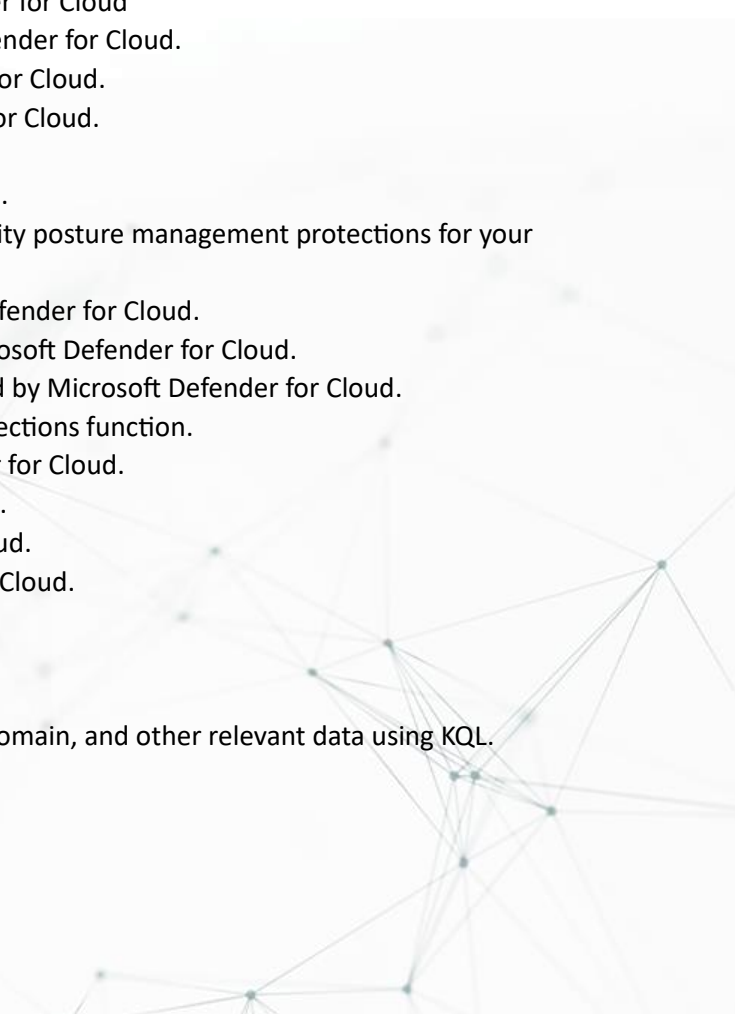
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Administer a Microsoft Defender for Endpoint environment.
- Configure Attack Surface Reduction rules on Windows devices.
- Perform actions on a device using Microsoft Defender for Endpoint.
- Investigate domains and IP addresses in Microsoft Defender for Endpoint.
- Investigate user accounts in Microsoft Defender for Endpoint.
- Configure alert settings in Microsoft 365 Defender.
- Conduct hunting in Microsoft 365 Defender.
- Manage incidents in Microsoft 365 Defender.
- Explain how Microsoft Defender for Identity can remediate risks in your environment.
- Investigate DLP alerts in Microsoft Defender for Cloud Apps.
- Explain the types of actions you can take on an insider risk management cases.
- Configure auto-provisioning in Microsoft Defender for Cloud Apps.
- Remediate alerts in Microsoft Defender for Cloud Apps.
- Construct KQL statements.

- Filter searches based on event time, severity, domain, and other relevant data using KQL.
- Extract data from unstructured string fields using KQL.
- Manage a Microsoft Sentinel workspace.
- Use KQL to access the watchlist in Microsoft Sentinel.
- Manage threat indicators in Microsoft Sentinel.
- Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel.
- Connect Azure Windows Virtual Machines to Microsoft Sentinel.
- Configure Log Analytics agent to collect Sysmon events.
- Create new analytics rules and queries using the analytics rule wizard.
- Create a playbook to automate an incident response.
- Use queries to hunt for threats.
- Observe threats over time with livestream.

Course Outline:

1- Introduction to Microsoft 365 threat protection.
   o Understand Microsoft 365 Defender solution by domain.
   o Understand Microsoft 365 Defender role in a Modern SOC.
2- Mitigate incidents using Microsoft 365 Defender.
   o Manage incidents in Microsoft 365 Defender.
   o Investigate incidents in Microsoft 365 Defender.
   o Conduct advanced hunting in Microsoft 365 Defender.
3- Protect your identities with Azure AD Identity Protection.
   o Describe the features of Azure Active Directory Identity Protection.
   o Describe the investigation and remediation features of Azure Active Directory Identity Protection
4- Remediate risks with Microsoft Defender for Office 365.
   o Define the capabilities of Microsoft Defender for Office 365.
   o Understand how to simulate attacks within your network.
   o Explain how Microsoft Defender for Office 365 can remediate risks in your environment.
5- Safeguard your environment with Microsoft Defender for Identity.
   o Define the capabilities of Microsoft Defender for Identity.
   o Understand how to configure Microsoft Defender for Identity sensors.
      o Explain how Microsoft Defender for Identity can remediate risks in your environment.
6- Secure your cloud apps and services with Microsoft Defender for Cloud Apps.
   o Define the Defender for Cloud Apps framework.
   o Explain how Cloud Discovery helps you see what's going on in your organization.
   o Understand how to use Conditional Access App Control policies to control access to the apps in your organization.
7- Respond to data loss prevention alerts using Microsoft 365.
   o Describe data loss prevention (DLP) components in Microsoft 365.
   o Investigate DLP alerts in the Microsoft Purview compliance portal.
   o Investigate DLP alerts in Microsoft Defender for Cloud Apps.
8- Manage insider risk in Microsoft Purview

- o Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- o Describe the types of built-in, pre-defined policy templates.
- o List the prerequisites that need to be met before creating insider risk policies.
- o Explain the types of actions you can take on an insider risk management case.

9- Investigate threats by using audit features in Microsoft 365 Defender and Microsoft Purview Standard
- o Describe the differences between Audit (Standard) and Audit (Premium).
- o Start recording user and admin activity in the Unified Audit Log (UAL).
- o Identify the core features of the Audit (Standard) solution.
- o Set up and implement audit log searching using the Audit (Standard) solution.
- o Export, configure, and view audit log records.
- o Use audit log searching to troubleshoot common support issues.

10- Investigate threats using audit in Microsoft 365 Defender and Microsoft Purview (Premium).
- o Describe the differences between Audit (Standard) and Audit (Premium).
- o Set up and implement Microsoft Purview Audit (Premium).
- o Create audit log retention policies.
- o Perform forensic investigations of compromised user accounts.

11- Investigate threats with Content search in Microsoft Purview
- o Describe how to use content search in the Microsoft Purview compliance portal.
- o Design and create a content search.
- o Preview the search results.
- o View the search statistics.
- o Export the search results and search report.
- o Configure search permission filtering.

12- Protect against threats with Microsoft Defender for Endpoint
- o Define the capabilities of Microsoft Defender for Endpoint.
- o Understand how to hunt threats within your network.
- o Explain how Microsoft Defender for Endpoint can remediate risks in your environment.

13- Deploy the Microsoft Defender for Endpoint environment.
- o Create a Microsoft Defender for Endpoint environment.
- o Onboard devices to be monitored by Microsoft Defender for Endpoint.
- o Configure Microsoft Defender for Endpoint environment settings.

14- Implement Windows security enhancements with Microsoft Defender for Endpoint
- o Explain Attack Surface Reduction in Windows.
- o Enable Attack Surface Reduction rules on Windows 10 devices.
- o Configure Attack Surface Reduction rules on Windows 10 devices.

15- Perform device investigations in Microsoft Defender for Endpoint.
- o Use the device page in Microsoft Defender for Endpoint.
- o Describe device forensics information collected by Microsoft Defender for Endpoint.
- o Describe behavioral blocking by Microsoft Defender for Endpoint.

16- Perform actions on a device using Microsoft Defender for Endpoint.
- o Perform actions on a device using Microsoft Defender for Endpoint.
- o Conduct forensics data collection using Microsoft Defender for Endpoint.

- o   Access devices remotely using Microsoft Defender for Endpoint.
17- Perform evidence and entities investigations using Microsoft Defender for Endpoint.
    - o   Investigate files in Microsoft Defender for Endpoint
    - o   Investigate domains and IP addresses in Microsoft Defender for Endpoint
    - o   Investigate user accounts in Microsoft Defender for Endpoint
18- Configure and manage automation using Microsoft Defender for Endpoint
    - o   Configure advanced features of Microsoft Defender for Endpoint.
    - o   Manage automation settings in Microsoft Defender for Endpoint.
19- Configure for alerts and detections in Microsoft Defender for Endpoint
    - o   Configure alert settings in Microsoft Defender for Endpoint.
    - o   Manage indicators in Microsoft Defender for Endpoint.
20- Utilize Vulnerability Management in Microsoft Defender for Endpoint.
    - o   Describe Vulnerability Management in Microsoft Defender for Endpoint.
    - o   Identify vulnerabilities on your devices with Microsoft Defender for Endpoint.
    - o   Track emerging threats in Microsoft Defender for Endpoint.
21- Plan for cloud workload protections using Microsoft Defender for Cloud
    - o   Describe Microsoft Defender for Cloud features.
    - o   Microsoft Defender for Cloud workload protections.
    - o   Enable Microsoft Defender for Cloud.
22- Connect Azure assets to Microsoft Defender for Cloud
    - o   Explore Azure assets.
    - o   Configure auto-provisioning in Microsoft Defender for Cloud.
    - o   Describe manual provisioning in Microsoft Defender for Cloud.
23- Connect non-Azure resources to Microsoft Defender for Cloud
    - o   Connect non-Azure machines to Microsoft Defender for Cloud.
    - o   Connect AWS accounts to Microsoft Defender for Cloud.
    - o   Connect GCP accounts to Microsoft Defender for Cloud.
24- Manage your cloud security posture management.
    - o   Describe Microsoft Defender for Cloud features.
    - o   Explain the Microsoft Defender for Cloud security posture management protections for your resources.
25- Explain cloud workload protections in Microsoft Defender for Cloud.
    - o   Explain which workloads are protected by Microsoft Defender for Cloud.
    - o   Describe the benefits of the protections offered by Microsoft Defender for Cloud.
    - o   Explain how Microsoft Defender for Cloud protections function.
26- Remediate security alerts using Microsoft Defender for Cloud.
    - o   Describe alerts in Microsoft Defender for Cloud.
    - o   Remediate alerts in Microsoft Defender for Cloud.
    - o   Automate responses in Microsoft Defender for Cloud.
27- Construct KQL statements for Microsoft Sentinel.
    - o   Construct KQL statements.
    - o   Search log files for security events using KQL.
    - o   Filter searches based on event time, severity, domain, and other relevant data using KQL.
28- Analyze query results using KQL.

- o   Summarize data using KQL statements.
- o   Render visualizations using KQL statements.
29- Build multi-table statements using KQL.
- o   Create queries using unions to view results across multiple tables using KQL.
- o   Merge two tables with the join operator using KQL.
30- Work with data in Microsoft Sentinel using Kusto Query Language.
- o   Extract data from unstructured string fields using KQL.
- o   Extract data from structured string data using KQL.
- o   Create Functions using KQL.
31- Introduction to Microsoft Sentinel.
- o   Identify the various components and functionality of Microsoft Sentinel.
- o   Identify use cases where Microsoft Sentinel would be a good solution.
32- Create and manage Microsoft Sentinel workspaces.
- o   Describe Microsoft Sentinel workspace architecture.
- o   Install Microsoft Sentinel workspace.
- o   Manage a Microsoft Sentinel workspace.
33- Query logs in Microsoft Sentinel.
- o   Use the Logs page to view data tables in Microsoft Sentinel.
- o   Query the most used tables using Microsoft Sentinel.
34- Use watchlists in Microsoft Sentinel.
- o   Create a watchlist in Microsoft Sentinel.
- o   Use KQL to access the watchlist in Microsoft Sentinel.
35- Utilize threat intelligence in Microsoft Sentinel.
- o   Manage threat indicators in Microsoft Sentinel.
- o   Use KQL to access threat indicators in Microsoft Sentinel.
36- Connect data to Microsoft Sentinel using data connectors.
- o   Explain the use of data connectors in Microsoft Sentinel.
- o   Describe the Microsoft Sentinel data connector providers.
- o   Explain the Common Event Format and Syslog connector differences in Microsoft Sentinel.
37- Connect Microsoft services to Microsoft Sentinel.
- o   Connect Microsoft service connectors.
- o   Explain how connectors auto-create incidents in Microsoft Sentinel.
38- Connect Microsoft 365 Defender to Microsoft Sentinel.
- o   Activate the Microsoft 365 Defender connector in Microsoft Sentinel.
- o   Activate the Microsoft Defender for Cloud connector in Microsoft Sentinel.
- o   Activate the Microsoft Defender for IoT connector in Microsoft Sentinel.
39- Connect Windows hosts to Microsoft Sentinel.
- o   Connect Azure Windows Virtual Machines to Microsoft Sentinel.
- o   Connect non-Azure Windows hosts to Microsoft Sentinel.
- o   Configure Log Analytics agent to collect Sysmon events.
40- Connect Common Event Format logs to Microsoft Sentinel.
- o   Explain the Common Event Format connector deployment options in Microsoft Sentinel.
- o   Run the deployment script for the Common Event Format connector.
41- Connect syslog data sources to Microsoft Sentinel.

- o Describe the Syslog connector deployment options in Microsoft Sentinel.
- o Run the connector deployment script to send data to Microsoft Sentinel.
- o Configure the Log Analytics agent integration for Microsoft Sentinel.
- o Create a parse using KQL in Microsoft Sentinel.

42- Connect threat indicators to Microsoft Sentinel.
- o Configure the TAXII connector in Microsoft Sentinel.
- o Configure the Threat Intelligence Platform connector in Microsoft Sentinel.
- o View threat indicators in Microsoft Sentinel.

43- Threat detection with Microsoft Sentinel analytics.
- o Explain the importance of Microsoft Sentinel Analytics.
- o Explain different types of analytics rules.
- o Create rules from templates.
- o Create new analytics rules and queries using the analytics rule wizard.
- o Manage rules with modifications.

44- Automation in Microsoft Sentinel.
- o Explain automation options in Microsoft Sentinel.
- o Create automation rules in Microsoft Sentinel.

45- Security incident management in Microsoft Sentinel.
- o Understand Microsoft Sentinel incident management.
- o Explore Microsoft Sentinel evidence and entity management.
- o Investigate and manage incident resolution.

46- Identify threats with Behavioral Analytics.
- o Explain User and Entity Behavior Analytics in Azure Sentinel.
- o Explore entities in Microsoft Sentinel.

47- Data normalization in Microsoft Sentinel.
- o Use ASIM Parsers.
- o Create ASIM Parser.
- o Create parameterized KQL functions.

48- Query, visualize, and monitor data in Microsoft Sentinel.
- o Visualize security data using Microsoft Sentinel Workbooks.
- o Understand how queries work.
- o Explore workbook capabilities.
- o Create a Microsoft Sentinel Workbook.

49- Manage content in Microsoft Sentinel.
- o Install a content hub solution in Microsoft Sentinel.
- o Connect a GitHub repository to Microsoft Sentinel.

50- Explain threat hunting concepts in Microsoft Sentinel.
- o Describe threat hunting concepts for use with Microsoft Sentinel.
- o Define a threat hunting hypothesis for use in Microsoft Sentinel.

51- Threat hunting with Microsoft Sentinel.
- o Use queries to hunt for threats.
- o Save key findings with bookmarks.
- o Observe threats over time with livestream.

52- Use Search jobs in Microsoft Sentinel.
- o Use Search Jobs in Microsoft Sentinel.
- o Restore archive logs in Microsoft Sentinel.
53- Hunt for threats using notebooks in Microsoft Sentinel.
- o Explore API libraries for advanced threat hunting in Microsoft Sentinel.
- o Describe notebooks in Microsoft Sentinel.
- o Create and use notebooks in Microsoft Sentinel.

SC-300

Training Course SC-300: Microsoft Identity and Access Administrator

Overview: The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Azure AD. Learn to manage tasks such as providing secure authentication and authorization access to enterprise applications. You will also learn to provide seamless experiences and self-service management capabilities for all users. Finally, learn to create adaptive access and governance of your identity and access management solutions ensuring you can troubleshoot, monitor, and report on your environment. The Identity and Access Administrator may be a single individual or a member of a larger team. Learn how this role collaborates with many other roles in the organization to drive strategic identity projects. The end goal is to provide you knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Duration: 4 Days.

Audience Profile: This course is for the Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job. This course would also be helpful to an administrator or engineer that wants to specialize in providing identity solutions and access management systems for Azure-based solutions; playing an integral role in protecting an organization.

Certification: This course prepares you for the SC-300: Microsoft Identity and Access Administrator.

Course Objectives: After completing this course, students will be able to:

- o Explore identity and Azure AD
- o Implement initial configuration of Azure Active Directory
- o Create, configure, and manage identities
- o Implement and manage external identities
- o Implement and manage hybrid identity
- o Secure Azure Active Directory users with Multi-Factor Authentication
- o Manage user authentication
- o Plan, implement, and administer Conditional Access
- o Manage Azure AD Identity Protection
- o Implement access management for Azure resources
- o Plan and design the integration of enterprise apps for SSO
- o Implement and monitor the integration of enterprise apps for SSO
- o Implement app registration

- o Plan and implement entitlement management
- o Plan, implement, and manage access review
- o Plan and implement privileged access
- o Monitor and maintain Azure Active Directory.

Course Outline:

1- Implement an identity management solution.
- o Define common identity terms and explain how they are used in the Microsoft Cloud.
- o Explore the common management tools and needs of an identity solution.
- o Review the goal of Zero Trust and how it is applied in the Microsoft Cloud.
- o Explore the available identity services in the Microsoft Cloud.

2- Implement initial configuration of Azure Active Directory
- o Implement initial configuration of Azure Active Directory.
- o Create, configure, and manage identities.
- o Implement and manage external identities (excluding B2C scenarios).
- o Implement and manage hybrid identity.

3- Create, configure, and manage identities.
- o Create, configure, and manage users.
- o Create, configure, and manage groups.
- o Manage licenses.
- o Explain custom security attributes and automatic user provisioning.

4- Implement and manage external identities.
- o Manage external collaboration settings in Azure Active Directory
- o Invite external users (individually or in bulk)
- o Manage external user accounts in Azure Active Directory
- o Configure identity providers (social and SAML/WS-fed)

5- Implement and manage hybrid identity.
- o Plan, design, and implement Azure Active Directory Connect (AADC)
- o Manage Azure Active Directory Connect (AADC)
- o Manage password hash synchronization (PHS)
- o Manage pass-through authentication (PTA)
- o Manage Seamless Single Sign-On (Seamless SSO)
- o Manage federation excluding manual ADFS deployments
- o Troubleshoot synchronization errors
- o Implement and manage Azure Active Directory Connect Health

6- Secure Azure Active Directory users with Multi-Factor Authentication
- o Learn about Azure AD Multi-Factor Authentication (Azure AD MFA)
- o Create a plan to deploy Azure AD MFA
- o Turn on Azure AD MFA for users and specific apps.

7- Manage user authentication.
- o Administer authentication methods (FIDO2 / Passwordless).
- o Implement an authentication solution based on Windows Hello for Business,
- o Configure and deploy self-service password reset.

- o Deploy and manage password protection.
- o Implement and manage tenant restrictions.

8- Plan, implement, and administer Conditional Access.
- o Plan and implement security defaults.
- o Plan conditional access policies.
- o Implement conditional access policy controls and assignments (targeting, applications, and conditions).
- o Test and troubleshoot conditional access policies.
- o Implement application controls.
- o Implement session management.
- o Configure smart lockout thresholds.

9- Manage Azure AD Identity Protection.
- o Implement and manage a user risk policy.
- o Implement and manage sign-in risk policies.
- o Implement and manage MFA registration policy.
- o Monitor, investigate, and remediate elevated risky users.

10- Implement access management for Azure resources.
- o Configure and use Azure roles within Azure AD.
- o Configure and managed identity and assign it to Azure resources.
- o Analyze the role permissions granted to or inherited by a user.
- o Configure access to data in Azure Key Vault using RBAC-policy.

11- Plan and design the integration of enterprise apps for SSO.
- o Discover apps by using MCAS or ADFS app report.
- o Design and implement access management for apps.
- o Design and implement app management roles.
- o Configure pre-integrated (gallery) SaaS apps.

12- Implement and monitor the integration of enterprise apps for SSO.
- o Implement token customizations.
- o Implement and configure consent settings.
- o Integrate on-premises apps by using Azure AD application proxy.
- o Integrate custom SaaS apps for SSO.
- o Implement application user provisioning.
- o Monitor and audit access/Sign-On to Azure Active Directory integrated enterprise applications.

13- Implement app registration.
- o Plan your line of business application registration strategy.
- o Implement application registrations.
- o Configure application permissions.
- o Plan and configure multi-tier application permissions.

14- Plan and implement entitlement management.
- o Define catalogs.
- o Define access packages.
- o Plan, implement and manage entitlements.
- o Implement and manage terms of use.

- o   Manage the lifecycle of external users in Azure AD Identity Governance settings.
15- Plan, implement, and manage access review.
  - o   Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds).
  - o   Configure Privileged Identity Management for Azure AD roles.
  - o   Configure Privileged Identity Management for Azure resources.
  - o   Assign roles.
  - o   Manage PIM requests.
  - o   Analyze PIM audit history and reports.
  - o   Create and manage emergency access accounts.
16- Plan and implement privileged access.
  - o   Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds).
  - o   Configure Privileged Identity Management for Azure AD roles.
  - o   Configure Privileged Identity Management for Azure resources.
  - o   Assign roles.
  - o   Manage PIM requests.
  - o   Analyze PIM audit history and reports.
  - o   Create and manage emergency access accounts.
17- Monitor and maintain Azure Active Directory.
  - o   Analyze and investigate sign in logs to troubleshoot access issues.
  - o   Review and monitor Azure AD audit logs.
  - o   Enable and integrate Azure AD diagnostic logs with Log Analytics / Azure Sentinel.
  - o   Export sign in and audit logs to a third-party SIEM (security information and event management).
  - o   Review Azure AD activity by using Log Analytics / Azure Sentinel, excluding KQL (Kusto Query Language) use.
  - o   Analyze Azure Active Directory workbooks / reporting.
  - o   Configure notifications.

SC-400

Training Course SC-400: Administering Information Protection and Compliance in Microsoft 365

Overview: Learn how to protect information in your Microsoft 365 deployment. This course focuses on data lifecycle management and information protection and compliance within your organization. The course covers implementation of data loss prevention policies, sensitive information types, sensitivity labels, data retention policies, Microsoft Purview Message Encryption, audit, eDiscovery, and insider risk among other related topics. The course helps learners prepare for the Microsoft Information Protection Administrator exam (SC-400).

Duration: 4 Days.

Audience Profile: The information protection administrator translates an organization's risk and compliance requirements into technical implementation. They are responsible for implementing and managing solutions for content classification, data loss prevention (DLP), information protection, data lifecycle management, records management, privacy, risk, and compliance. They also work with other roles that are responsible for governance, data, and security to evaluate and develop policies to address an organization's risk reduction and compliance goals. This role assists workload administrators, business application owners, human resources departments, and legal stakeholders to implement technology solutions that support the necessary policies and controls.

Certification: This course prepares you for the SC-400: Administering Information Protection and Compliance in Microsoft 365.

Course Objectives: After completing this course, students will be able to:

- Introduction to information protection and data lifecycle management in Microsoft Purview.
- Classify data for protection and governance.
- Create and manage sensitive information types.
- Understand Microsoft 365 encryption.
- Deploy Microsoft Purview Message Encryption.
- Protect information in Microsoft Purview.
- Apply and manage sensitivity labels.
- Prevent data loss in Microsoft Purview.
- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform.
- Manage data loss prevention policies and reports in Microsoft 365.
- Manage the data lifecycle in Microsoft Purview.

- Manage data retention in Microsoft 365 workloads.
- Manage records in Microsoft Purview.
- Explore compliance in Microsoft 365.
- Search for content in the Microsoft Purview compliance portal.
- Manage Microsoft Purview eDiscovery (Standard).
- Manage Microsoft Purview eDiscovery (Premium).
- Manage Microsoft Purview Audit (Standard).
- Prepare Microsoft Purview Communication Compliance.
- Manage insider risk in Microsoft Purview.
- Implement Microsoft Purview Information Barriers.
- Manage regulatory and privacy requirements with Microsoft Priva.
- Implement privileged access management.
- Manage Customer Lockbox.

Course Outline:

1- Introduction to information protection and data lifecycle management in Microsoft Purview.
   - o Discuss information protection and data lifecycle management and why it's important.
   - o Describe Microsoft's approach to information protection and data lifecycle management.
   - o Define key terms associated with Microsoft's information protection and data lifecycle management solutions.
   - o Identify the solutions that comprise information and data lifecycle management in Microsoft Purview.
2- Classify data for protection and governance.
   - o List the components of the Data Classification solution.
   - o Identify the cards available on the Data Classification overview tab.
   - o Explain the Content explorer and Activity explorer.
   - o Describe how to use sensitive information types and trainable classifiers.
3- Create and manage sensitive information types.
   - o Recognize the difference between built-in and custom sensitivity labels.
   - o Configure sensitive information types with exact data match-based classification.
   - o Implement document fingerprinting.
   - o Create custom keyword diction.
4- Understand Microsoft 365 encryption.
   - o Explain how encryption mitigates the risk of unauthorized data disclosure.
   - o Describe Microsoft data-at-rest and data-in-transit encryption solutions.
   - o Explain how Microsoft 365 implements service encryption to protect customer data at the application layer.
   - o Understand the differences between Microsoft managed keys and customer managed keys for use with service encryption.
5- Deploy Microsoft Purview Message Encryption.
   - o Configure Microsoft Purview Message Encryption for end users.
   - o Implement Microsoft Purview Advanced Message Encryption.
6- Protect information in Microsoft Purview.
   - o Discuss the information protection solution and its benefits.

- List the customer scenarios the information protection solution addresses.
- Describe the information protection configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

7- Apply and manage sensitivity labels.
- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.
- Monitor label usage using label analytics.
- Configure on-premises labeling.
- Manage protection settings and marking for applied sensitivity labels.
- Apply protections and restrictions to email.
- Apply protections and restrictions to files.

8- Prevent data loss in Microsoft Purview.
- Discuss the data loss prevention solution and its benefits.
- Describe the data loss prevention configuration process.
- Explain what users will experience when the solution is implemented.

9- Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform.
- Describe the integration of DLP with Microsoft Defender for Cloud Apps.
- Configure policies in Microsoft Defender for Cloud Apps.

10- Manage data loss prevention policies and reports in Microsoft 365.
- Review and analyze DLP reports.
- Manage permissions for DLP reports.
- Identify and mitigate DLP policy violations.
- Mitigate DLP violations in Microsoft Defender for Cloud Apps.

11- Manage the data lifecycle in Microsoft Purview.
- Discuss the Data Lifecycle Management solution and its benefits.
- List the customer scenarios the Data Lifecycle Management solution addresses.
- Describe the Data Lifecycle Management configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

12- Manage data retention in Microsoft 365 workloads.
- Describe the retention features in Microsoft 365 workloads.
- Configure retention settings in Microsoft Teams, Yammer, and SharePoint Online.
- Recover content protected by retention settings.
- Regain protected items from Exchange Mailboxes.

13- Manage records in Microsoft Purview.
- Discuss the Microsoft Purview Records Management solution and its benefits.
- List the customer scenarios the Microsoft Purview Records Management solution addresses.
- Describe the Microsoft Purview Records Management configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

14- Explore compliance in Microsoft 365.
- Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.

- o Plan your beginning compliance tasks in Microsoft Purview.
- o Manage your compliance requirements with Compliance Manager.
- o Manage compliance posture and improvement actions using the Compliance Manager dashboard.
- o Explain how an organization's compliance score is determined.

15- Search for content in the Microsoft Purview compliance portal.
- o Describe how to use content search in the Microsoft Purview compliance portal.
- o Design and create a content search.
- o Preview the search results.
- o View the search statistics.
- o Export the search results and search report.
- o Configure search permission filtering.

16- Manage Microsoft Purview eDiscovery (Standard).
- o Describe how Microsoft Purview eDiscovery (Standard) builds on the basic search and export functionality of Content search.
- o Describe the basic workflow of eDiscovery (Standard).
- o Create an eDiscovery case.
- o Create an eDiscovery hold for an eDiscovery case.
- o Search for content in a case and then export that content.
- o Close, reopen, and delete a case.

17- Manage Microsoft Purview eDiscovery (Premium).
- o Describe how Microsoft Purview eDiscovery (Premium) builds on eDiscovery (Standard).
- o Describe the basic workflow of eDiscovery (Premium).
- o Create and manage cases in eDiscovery (Premium).
- o Manage custodians and non-custodial data sources.
- o Analyze case content and use analytical tools to reduce the size of search result sets.

18- Manage Microsoft Purview Audit (Standard).
- o Describe the differences between Audit (Standard) and Audit (Premium).
- o Identify the core features of the Audit (Standard) solution.
- o Set up and implement audit log searching using the Audit (Standard) solution.
- o Export, configure, and view audit log records.
- o Use audit log searching to troubleshoot common support issues.

19- Prepare Microsoft Purview Communication Compliance.
- o List the enhancements in communication compliance over Office 365 Supervision policies, which it will replace.
- o Explain how to identify and remediate code-of-conduct policy violations.
- o List the prerequisites that need to be met before creating communication compliance policies.
- o Describe the types of built-in, pre-defined policy templates.

20- Manage insider risk in Microsoft Purview.
- o Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- o Describe the types of built-in, pre-defined policy templates.
- o List the prerequisites that need to be met before creating insider risk policies.

- o Explain the types of actions you can take on an insider risk management case.
21- Implement Microsoft Purview Information Barriers.
  - o Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
  - o Describe the components of an information barrier and how to enable information barriers.
  - o Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site.
  - o Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.
22- Manage regulatory and privacy requirements with Microsoft Privacy.
  - o Create and manage risk management policies for data overexposure, data transfer, and data minimization.
  - o Investigate and remediate risk alerts.
  - o Send user notifications.
  - o Create and manage Subject Rights Requests.
  - o Estimate and retrieve subject data.
  - o Review subject data.
  - o Create subject rights reports.
23- Implement privileged access management.
  - o Explain the difference between privileged access management and privileged identity management.
  - o Describe the privileged access management process flow.
  - o Describe how to configure and enable privileged access management.
24- Manage Customer Lockbox.
  - o Describe the Customer Lockbox workflow.
  - o Explain how to approve or deny a Customer Lockbox request.
  - o Explain how you can audit actions performed by Microsoft engineers when access requests are approved.

DP-203

Training Course DP-203: Data Engineering on Microsoft Azure

Overview: In this course, the student will learn about the data engineering patterns and practices as it pertains to working with batch and real-time analytical solutions using Azure data platform technologies. Participants will begin by understanding the core compute and storage technologies that are used to build an analytical solution. They will then explore how to design an analytical serving layer and focus on data engineering considerations for working with source files. Students will learn how to interactively explore data stored in files in a data lake. They will learn the various ingestion techniques that can be used to load data using the Apache Spark capability found in Azure Synapse Analytics or Azure Databricks, or how to ingest using Azure Data Factory or Azure Synapse pipelines. Attendees will also learn the various ways they can transform the data using the same technologies that are used to ingest data. Students will spend time on the course learning how to monitor and analyze the performance of an analytical system so that they can optimize the performance of data loads, or queries that are issued against the systems. They will understand the importance of implementing security to ensure that the data is protected at rest or in transit. Participants will then show how the data in an analytical system can be used to create dashboards or build predictive models in Azure Synapse Analytics.

Duration: 4 Days.

Audience Profile: The primary audience for this course is data professionals, data architects, and business intelligence professionals who want to learn about data engineering and building analytical solutions using data platform technologies that exist on Microsoft Azure. The secondary audience for this course data analysts and data scientists who work with analytical solutions built on Microsoft Azure.

Certification: This course prepares you for the DP-203: Data Engineering on Microsoft Azure.

Course Objectives: After completing this course, students will be able to:

- Explore compute and storage options for data engineering workloads in Azure.
- Run interactive queries using serverless SQL pools.
- Perform data Exploration and Transformation in Azure Databricks.
- Explore, transform, and load data into the Data Warehouse using Apache Spark.
- Ingest and load Data into the Data Warehouse.
- Transform Data with Azure Data Factory or Azure Synapse Pipelines.
- Integrate Data from Notebooks with Azure Data Factory or Azure Synapse Pipelines.
- Support Hybrid Transactional Analytical Processing (HTAP) with Azure Synapse Link.
- Perform end-to-end security with Azure Synapse Analytics.
- Perform real-time Stream Processing with Stream Analytics.
- Create a Stream Processing Solution with Event Hubs and Azure Databricks.

Course Outline

1- Introduction to data engineering on Azure.
   - Identify common data engineering tasks.
   - Describe common data engineering concepts.
   - Identify Azure services for data engineering.

2- Introduction to Azure Data Lake Storage Gen2.
   - Describe the key features and benefits of Azure Data Lake Storage Gen2.
   - Enable Azure Data Lake Storage Gen2 in an Azure Storage account.
   - Compare Azure Data Lake Storage Gen2 and Azure Blob storage.
   - Describe where Azure Data Lake Storage Gen2 fits in the stages of analytical processing.
   - Describe how Azure data Lake Storage Gen2 is used in common analytical workloads.
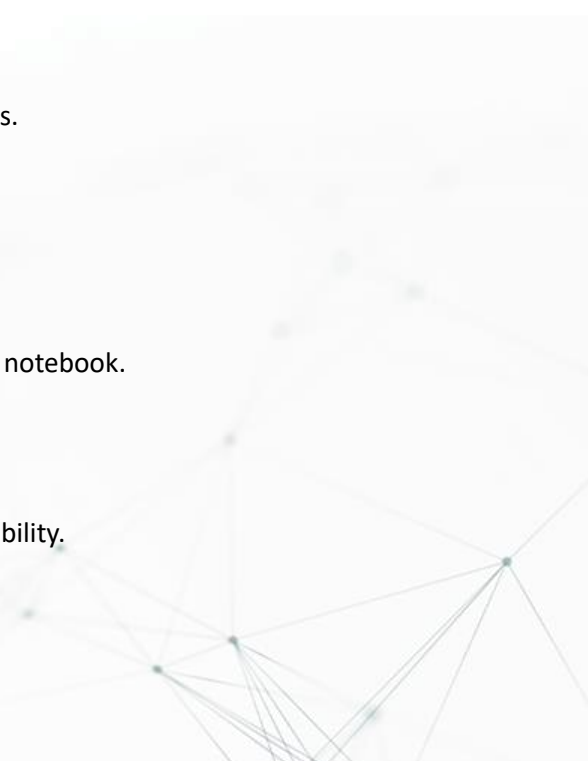
3- Introduction to Azure Synapse Analytics.
   - Identify the business problems that Azure Synapse Analytics addresses.
   - Describe core capabilities of Azure Synapse Analytics.
   - Determine when to use Azure Synapse Analytics.

4- Use Azure Synapse serverless SQL pool to query files in a data lake.
   - Identify capabilities and use cases for serverless SQL pools in Azure Synapse Analytics.
   - Query CSV, JSON, and Parquet files using a serverless SQL pool.
   - Create external database objects in a serverless SQL pool.

5- Use Azure Synapse serverless SQL pools to transform data in a data lake.
   - Use a CREATE EXTERNAL TABLE AS SELECT (CETAS) statement to transform data.
   - Encapsulate a CETAS statement in a stored procedure.
   - Include a data transformation stored procedure in a pipeline.

6- Create a lake database in Azure Synapse Analytics.
   - Understand lake database concepts and components.
   - Describe database templates in Azure Synapse Analytics.
   - Create a lake database.

7- Analyze data with Apache Spark in Azure Synapse Analytics.
   - Identify core features and capabilities of Apache Spark.
   - Configure a Spark pool in Azure Synapse Analytics.
   - Run code to load, analyze, and visualize data in a Spark notebook.

8- Transform data with Spark in Azure Synapse Analytics.
   - Use Apache Spark to modify and save dataframes.
   - Partition data files for improved performance and scalability.

- o Transform data with SQL.

9- Use Delta Lake in Azure Synapse Analytics.

- o Describe core features and capabilities of Delta Lake.
- o Create and use Delta Lake tables in a Synapse Analytics Spark pool.
- o Create Spark catalog tables for Delta Lake data.
- o Use Delta Lake tables for streaming data.
- o Query Delta Lake tables from a Synapse Analytics SQL pool.

10- Analyze data in a relational data warehouse.

- o Design a schema for a relational data warehouse.
- o Create fact, dimension, and staging tables.
- o Use SQL to load data into data warehouse tables.
- o Use SQL to query relational data warehouse tables.

11- Load data into a relational data warehouse.

- o Load staging tables in a data warehouse.
- o Load dimension tables in a data warehouse.
- o Load time dimensions in a data warehouse.
- o Load slowly changing dimensions in a data warehouse.
- o Load fact tables in a data warehouse.
- o Perform post-load optimizations in a data warehouse.

12- Build a data pipeline in Azure Synapse Analytics.

- o Describe core concepts for Azure Synapse Analytics pipelines.
- o Create a pipeline in Azure Synapse Studio.
- o Implement a data flow activity in a pipeline.
- o Initiate and monitor pipeline runs.

13- Use Spark Notebooks in an Azure Synapse Pipeline.

- o Describe notebook and pipeline integration.
- o Use a Synapse notebook activity in a pipeline.
- o Use parameters with a notebook activity.

14- Plan hybrid transactional and analytical processing using Azure Synapse Analytics.

- o Describe Hybrid Transactional / Analytical Processing patterns.
- o Identify Azure Synapse Link services for HTAP.

15- Implement Azure Synapse Link with Azure Cosmos DB.

- o Configure an Azure Cosmos DB Account to use Azure Synapse Link.
- o Create an analytical store enabled container.
- o Create a linked service for Azure Cosmos DB.

- o   Analyze linked data using Spark.
- o   Analyze linked data using Synapse SQL.

16- Implement Azure Synapse Link for SQL.

- o   Understand key concepts and capabilities of Azure Synapse Link for SQL.
- o   Configure Azure Synapse Link for Azure SQL Database.
- o   Configure Azure Synapse Link for Microsoft SQL Server.

17- Get started with Azure Stream Analytics.

- o   Understand data streams.
- o   Understand event processing.
- o   Understand window functions.
- o   Get started with Azure Stream Analytics.

18- Ingest streaming data using Azure Stream Analytics and Azure Synapse Analytics.

- o   Describe common stream ingestion scenarios for Azure Synapse Analytics.
- o   Configure inputs and outputs for an Azure Stream Analytics job.
- o   Define a query to ingest real-time data into Azure Synapse Analytics.
- o   Run a job to ingest real-time data, and consume that data in Azure Synapse Analytics.

19- Visualize real-time data with Azure Stream Analytics and Power BI.
- o   Configure a Stream Analytics output for Power BI.
- o   Use a Stream Analytics query to write data to Power BI.
- o   Create a real-time data visualization in Power BI.

20- Introduction to Microsoft Purview.
- o   Knowledge of Azure accounts and services
- o   Knowledge of various data sources such as SQL Server and Azure Cosmos DB
- o   Knowledge of the concepts around data governance.

21- Integrate Microsoft Purview and Azure Synapse Analytics.
- o   Catalog Azure Synapse Analytics database assets in Microsoft Purview.
- o   Configure Microsoft Purview integration in Azure Synapse Analytics.
- o   Search the Microsoft Purview catalog from Synapse Studio.
- o   Track data lineage in Azure Synapse Analytics pipelines activities.

22- Explore Azure Databricks.
- o   Provision an Azure Databricks workspace.
- o   Identify core workloads and personas for Azure Databricks.
- o   Describe key concepts of an Azure Databricks solution.

23- Use Apache Spark in Azure Databricks.
- o   Describe key elements of the Apache Spark architecture.
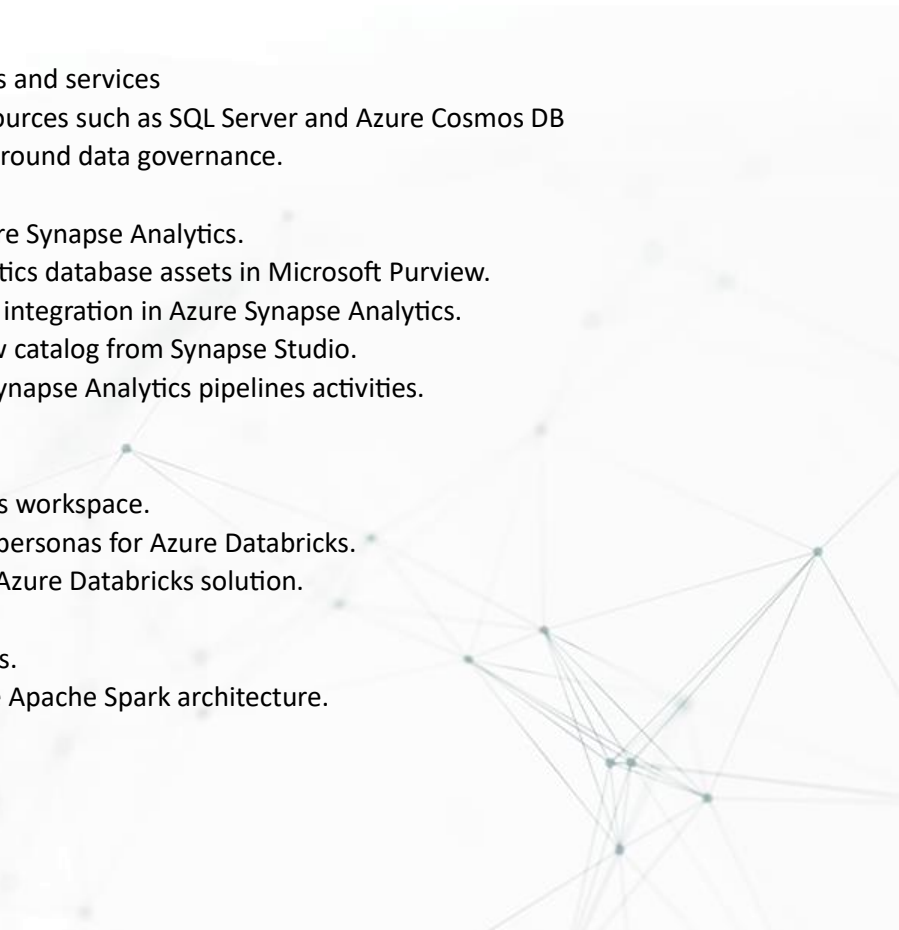
- o Create and configure a Spark cluster.
- o Describe use cases for Spark.
- o Use Spark to process and analyze data stored in files.
- o Use Spark to visualize data.

24- Run Azure Databricks Notebooks with Azure Data Factory.
- o Describe how Azure Databricks notebooks can be run in a pipeline.
- o Create an Azure Data Factory linked service for Azure Databricks.
- o Use a Notebook activity in a pipeline.
- o Pass parameters to a notebook.

MS-102

Training Course MS-102: Microsoft 365 Administrator

Overview: This course covers the following key elements of Microsoft 365 administration: Microsoft 365 tenant management, Microsoft 365 identity synchronization, and Microsoft 365 security and compliance.

Duration: 5 Days.

Audience Profile: This course is designed for persons aspiring to the Microsoft 365 Administrator role and have completed at least one of the Microsoft 365 role-based administrator certification paths.

Certification: This course prepares you for the MS-102: Microsoft 365 Administrator.

Course Objectives: After completing this course, students will be able to:

- o   Configure your Microsoft 365 experience.
- o   Manage users, licenses, and mail contacts in Microsoft 365
- o   Manage groups in Microsoft 365
- o   Add a custom domain in Microsoft 365
- o   Configure client connectivity to Microsoft 365
- o   Configure administrative roles in Microsoft 365
- o   Manage tenant health and services in Microsoft 365
- o   Deploy Microsoft 365 Apps for enterprise.
- o   Analyze your Microsoft 365 workplace data using Microsoft Viva Insights
- o   Explore identity synchronization.
- o   Prepare for identity synchronization to Microsoft 365
- o   Implement directory synchronization tools.
- o   Manage synchronized identities.
- o   Manage secure user access in Microsoft 365
- o   Examine threat vectors and data breaches.
- o   Explore the Zero Trust security model.
- o   Explore security solutions in Microsoft 365 Defender
- o   Examine Microsoft Secure Score

o   Examine Privileged Identity Management

o   Examine Azure Identity Protection

o   Examine Exchange Online Protection

o   Examine Microsoft Defender for Office 365

o   Manage Safe Attachments

o   Manage Safe Links

o   Explore threat intelligence in Microsoft 365 Defender

o   Implement app protection by using Microsoft Defender for Cloud Apps

o   Implement endpoint protection by using Microsoft Defender for Endpoint

o   Implement threat protection by using Microsoft Defender for Office 365

o   Examine data governance solutions in Microsoft Purview

o   Explore archiving and records management in Microsoft 365

o   Explore retention in Microsoft 365

o   Explore Microsoft Purview Message Encryption

o   Explore compliance in Microsoft 365

o   Implement Microsoft Purview Insider Risk Management

o   Implement Microsoft Purview Information Barriers

o   Explore Microsoft Purview Data Loss Prevention

o   Implement Microsoft Purview Data Loss Prevention

o   Implement data classification of sensitive information.

o   Explore sensitivity labels.

o   Implement sensitivity labels.

Course Outline:

1-   Configure your Microsoft 365 experience.

   o   Configure your company's organization profile, which is essential for setting up your company's tenant.

   o   Maintain minimum subscription requirements for your company.

   o   Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.

   o   Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs.

2-   Manage users, licenses, and mail contacts in Microsoft 365
   o   Identify which user identity model best suited for your organization.
   o   Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.

- o Manage user accounts and licenses in Microsoft 365.
- o Recover deleted user accounts in Microsoft 365.
- o Perform bulk user maintenance in Azure Active Directory.
- o Create and manage mail contacts from both the new Exchange admin center and Exchange Online PowerShell.

3- Manage groups in Microsoft 365
- o Describe the various types of groups available in Microsoft 365.
- o Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
- o Create and manage groups in Exchange Online and SharePoint Online.

4- Add a custom domain in Microsoft 365
- o Identify the factors that must be considered when adding a custom domain to Microsoft 365.
- o Plan the DNS zones used in a custom domain.
- o Plan the DNS record requirements for a custom domain.
- o Add a custom domain to your Microsoft 365 deployment.

5- Configure client connectivity to Microsoft 365
- o Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
- o Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process.
- o Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
- o Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.

6- Configure administrative roles in Microsoft 365
- o Describe the Azure RBAC permission model used in Microsoft 365.
- o Describe the most common Microsoft 365 admin roles.
- o Identify the key tasks assigned to the common Microsoft 365 admin roles.
- o Delegate admin roles to partners.
- o Manage permissions using administrative units in Azure Active Directory.
- o Elevate privileges to access admin centers by using Azure AD Privileged Identity Management.

7- Manage tenant health and services in Microsoft 365
- o Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
- o Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service.
- o Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support issues.

8- Deploy Microsoft 365 Apps for enterprise.
- o Describe the Microsoft 365 Apps for enterprise functionality.
- o Configure the Readiness Toolkit.
- o Plan a deployment strategy for Microsoft 365 Apps for enterprise.

- o   Complete a user-driven installation of Microsoft 365 Apps for enterprise.
- o   Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager.
- o   Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
- o   Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
- o   Describe how to manage Microsoft 365 Apps for enterprise updates.
- o   Determine which update channel and application method applies for your organization.

9-   Analyze your Microsoft 365 workplace data using Microsoft Viva Insights
- o   Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
- o   Discover the sources of data used in Microsoft Viva Insights.
- o   Explain the high-level insights available through Microsoft Viva Insights.
- o   Create custom analysis with Microsoft Viva Insights.
- o   Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy.

10- Explore identity synchronization
- o   Describe the Microsoft 365 authentication and provisioning options
- o   Explain the two identity models in Microsoft 365 - cloud-only identity and hybrid identity
- o   Explain the three authentication methods in the hybrid identity model - Password hash synchronization, Pass-through authentication, and federated authentication
- o   Describe how Microsoft 365 commonly uses directory synchronization

11- Prepare for identity synchronization to Microsoft 365
- o   Identify the tasks necessary to configure your Azure Active Directory environment.
- o   Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
- o   Identify the features of Azure AD Connect sync and Azure AD Connect Cloud Sync.
- o   Choose which directory synchronization best fits your environment and business needs.

12- Implement directory synchronization tools
- o   Configure Azure AD Connect and Azure AD Connect Cloud Sync prerequisites
- o   Set up Azure AD Connect and Azure AD Connect Cloud Sync
- o   Monitor synchronization services using Azure AD Connect Health

13- Manage synchronized identities

- o   Ensure users synchronize efficiently
- o   Manage groups with directory synchronization
- o   Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
- o   Configure object filters for directory synchronization
- o   Troubleshoot directory synchronization using various troubleshooting tasks and tools

14- Manage secure user access in Microsoft 365

- o   Manage user passwords
- o   Describe pass-through authentication

- o Enable multifactor authentication
- o Describe self-service password management
- o Implement Azure AD Smart Lockout
- o Implement entitlement packages in Azure AD Identity Governance
- o Implement conditional access policies
- o Create and perform an access review

15- Examine threat vectors and data breaches

- o Describe techniques hackers use to compromise user accounts through email
- o Describe techniques hackers use to gain control over resources
- o Describe techniques hackers use to compromise data
- o Mitigate an account breach
- o Prevent an elevation of privilege attack
- o Prevent data exfiltration, data deletion, and data spillage

16- Explore the Zero Trust security model

- o Describe the Zero Trust approach to security in Microsoft 365
- o Describe the principles and components of the Zero Trust security model
- o Describe the five steps to implementing a Zero Trust security model in your organization
- o Explain Microsoft's story and strategy around Zero Trust networking

17- Explore security solutions in Microsoft 365 Defender

- o Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
- o Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
- o Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- o Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization's security officers and administrators
- o Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas

18- Examine Microsoft Secure Score

- o Describe the benefits of Secure Score and what kind of services can be analyzed
- o Describe how to collect data using the Secure Score API
- o Describe how to use the tool to identify gaps between your current state and where you would like to be regarding security
- o Identify actions that increase your security by mitigating risks
- o Explain where to look to determine the threats each action mitigates and the impact it has on users

19- Examine Privileged Identity Management

- o Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization
- o Configure Privileged Identity Management for use in your organization
- o Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
- o Explain how Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments
- o Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365

20- Examine Azure Identity Protection

- o Describe Azure Identity Protection (AIP) and what kind of identities can be protected
- o Enable the three default protection policies in AIP
- o Identify the vulnerabilities and risk events detected by AIP
- o Plan your investigation in protecting cloud-based identities
- o Plan how to protect your Azure Active Directory environment from security breaches

21- Examine Exchange Online Protection

- o Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection.
- o List several mechanisms used by Exchange Online Protection to filter spam and malware.
- o Describe other solutions administrators may implement to provide extra protection against phishing and spoofing.
- o Understand how EOP provides protection against outbound spam.

22- Examine Microsoft Defender for Office 365

- o Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents.
- o Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites.
- o Create outbound spam filtering policies.
- o Unblock users who violated spam filtering policies so they can resume sending emails.

23- Manage Safe Attachments

- o Create and modify a Safe Attachments policy using Microsoft 365 Defender
- o Create a Safe Attachments policy by using PowerShell
- o Configure a Safe Attachments policy
- o Describe how a transport rule can disable a Safe Attachments policy
- o Describe the end-user experience when an email attachment is scanned and found to be malicious

24- Manage Safe Links

- o Create and modify a Safe Links policy using Microsoft 365 Defender

- o Create a Safe Links policy using PowerShell
- o Configure a Safe Links policy
- o Describe how a transport rule can disable a Safe Links policy
- o Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email, and a link to a malicious file hosted on a website

25- Explore threat intelligence in Microsoft 365 Defender

- o Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- o Create alerts that can identify malicious or suspicious events.
- o Understand how the Microsoft 365 Defender's Automated investigation and response process works.
- o Describe how threat hunting enables security operators to identify cybersecurity threats.
- o Describe how Advanced hunting in Microsoft 365 Defender proactively inspects events in your network to locate threat indicators and entities.

26- Implement app protection by using Microsoft Defender for Cloud Apps

- o Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications.
- o Explain how to deploy Microsoft Defender for Cloud Apps.
- o Control your cloud apps with file policies.
- o Manage and respond to alerts generated by those policies.
- o Configure and troubleshoot Cloud Discovery

27- Implement endpoint protection by using Microsoft Defender for Endpoint

- o Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats.
- o Onboard supported devices to Microsoft Defender for Endpoint.
- o Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses.
- o Configure device discovery to help find unmanaged devices connected to your corporate network.
- o Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations.

28- Implement threat protection by using Microsoft Defender for Office 365

- o Describe the protection stack provided by Microsoft Defender for Office 365.
- o Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.
- o Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company.
- o Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.

29- Examine data governance solutions in Microsoft Purview

- o Protect sensitive data with Microsoft Purview Information Protection.
- o Govern organizational data using Microsoft Purview Data Lifecycle Management.
- o Minimize internal risks with Microsoft Purview Insider Risk Management.
- o Explain the Microsoft Purview eDiscovery solutions.

30- Explore archiving and records management in Microsoft 365

- o Enable and disable an archive mailbox in the Microsoft Purview compliance portal and through Windows PowerShell.
- o Run diagnostic tests on an archive mailbox.
- o Learn how retention labels can be used to allow or block actions when documents and emails are declared records.
- o Create your file plan for retention and deletion settings and actions.
- o Determine when items should be marked as records by importing an existing plan (if you already have one) or create new retention labels. Restore deleted data in Exchange Online and SharePoint Online.

31- Explore retention in Microsoft 365

- o Explain how retention policies and retention labels work.
- o Identify the capabilities of both retention policies and retention labels.
- o Select the appropriate scope for a policy depending on business requirements.
- o Explain the principles of retention.
- o Identify the differences between retention settings and eDiscovery holds.
- o Restrict retention changes by using preservation lock.

32- Explore Microsoft Purview Message Encryption

- o Describe the features of Microsoft Purview Message Encryption.
- o Explain how Microsoft Purview Message Encryption works and how to set it up.
- o Define mail flow rules that apply branding and encryption templates to encrypt email messages.
- o Add organizational branding to encrypted email messages.
- o Explain the extra capabilities provided by Microsoft Purview Advanced Message Encryption.

33- Explore compliance in Microsoft 365

- o Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
- o Plan your beginning compliance tasks in Microsoft Purview.
- o Manage your compliance requirements with Compliance Manager.
- o Manage compliance posture and improvement actions using the Compliance Manager dashboard.
- o Explain how an organization's compliance score is determined.

34- Implement Microsoft Purview Insider Risk Management

o Describe insider risk management functionality in Microsoft 365.
o Develop a plan to implement the Microsoft Purview Insider Risk Management solution.
o Create insider risk management policies.
o Manage insider risk management alerts and cases.

35- Implement Microsoft Purview Information Barriers

o Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
o Describe the components of an information barrier and how to enable information barriers.
o Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site.
o Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.

36- Explore Microsoft Purview Data Loss Prevention

o Describe how Data Loss Prevention (DLP) is managed in Microsoft 365
o Understand how DLP in Microsoft 365 uses sensitive information types and search patterns
o Describe how Microsoft Endpoint DLP extends the DLP activity monitoring and protection capabilities.
o Describe what a DLP policy is and what it contains
o View DLP policy results using both queries and reports

37- Implement Microsoft Purview Data Loss Prevention

o Create a data loss prevention implementation plan. Implement Microsoft 365's default DLP policy
o Create a custom DLP policy from a DLP template and from scratch.
o Create email notifications and policy tips for users when a DLP rule applies.
o Create policy tips for users when a DLP rule applies
o Configure email notifications for DLP policies
o Implement data classification of sensitive information
o Explain the benefits and pain points of creating a data classification framework.
o Identify how data classification of sensitive items is handled in Microsoft 365.
o Understand how Microsoft 365 uses trainable classifiers to protect sensitive data.
o Create and then retrain custom trainable classifiers.
o Analyze the results of your data classification efforts in Content explorer and Activity explorer.
o Implement Document Fingerprinting to protect sensitive information being sent through Exchange Online.

38- Explore sensitivity labels

o Describe how sensitivity labels let you classify and protect your organization's data
o Identify the common reasons why organizations use sensitivity labels
o Explain what a sensitivity label is and what they can do for an organization
o Configure a sensitivity label's scope
o Explain why the order of sensitivity labels in your admin center is important

- o   Describe what label policies can do

39- Implement sensitivity labels

- o   Describe the overall process to create, configure, and publish sensitivity labels
- o   Identify the administrative permissions that must be assigned to compliance team members to implement sensitivity labels
- o   Develop a data classification framework that provides the foundation for your sensitivity labels
- o   Create and configure sensitivity labels
- o   Publish sensitivity labels by creating a label policy
- o   Identify the differences between removing and deleting sensitivity labels

PL-300

Training Course PL-300: Microsoft Power BI Data Analyst

Overview: This course covers the various methods and best practices that are in line with business and technical requirements for modeling, visualizing, and analyzing data with Power BI. The course will show how to access and process data from a range of data sources including both relational and non-relational sources. Finally, this course will also discuss how to manage and deploy reports and dashboards for sharing and content distribution.

Duration: 3 Days.

Audience Profile: The audience for this course are data professionals and business intelligence professionals who want to learn how to accurately perform data analysis using Power BI. This course is also targeted toward those individuals who develop reports that visualize data from the data platform technologies that exist on both in the cloud and on-premises.

Certification: This course prepares you for the PL-300: Microsoft Power BI Data Analyst.

Course Objectives: After completing this course, students will be able to:

- Discover data analysis.
- Get started building with Power BI
- Get data in Power BI
- Clean, transform, and load data in Power BI
- Design a data model in Power BI
- Add measures to Power BI Desktop models.
- Add calculated tables and columns to Power BI Desktop models.
- Use DAX time intelligence functions in Power BI Desktop models.
- Optimize a model for performance in Power BI
- Design Power BI reports
- Configure Power BI report filters.
- Enhance Power BI report designs for the user experience.
- Perform analytics in Power BI
- Create and manage workspaces in Power BI
- Manage datasets in Power BI
- Create dashboards in Power BI
- Implement row-level security.

Course Outline

1- Discover data analysis.
   - Learn about the roles in data.
   - Learn about the tasks of a data analyst.

2- Get started building with Power BI

- o Learn how Power BI services and applications work together.
- o Explore how Power BI can make your business more efficient.
- o Learn how to create compelling visuals and reports.

3- Get data in Power BI

- o Identify and connect to a data source.
- o Get data from a relational database, like Microsoft SQL Server
- o Get data from a file, like Microsoft Excel
- o Get data from applications.
- o Get data from Azure Analysis Services
- o Select a storage mode.
- o Fix performance issues
- o Resolve data import errors.

4- Clean, transform, and load data in Power BI

- o Resolve inconsistencies, unexpected or null values, and data quality issues.
- o Apply user-friendly value replacements.
- o Profile data so you can learn more about a specific column before using it.
- o Evaluate and transform column data types.
- o Apply data shape transformations to table structures.
- o Combine queries.
- o Apply user-friendly naming conventions to columns and queries.
- o Edit M code in the Advanced Editor.

5- Design a data model in Power BI

- o Create common date tables.
- o Configure many-to-many relationships.
- o Resolve circular relationships.
- o Design star schemas

6- Add measures to Power BI Desktop models.

- o Determine when to use implicit and explicit measures.
- o Create simple measures.
- o Create compound measures.
- o Create quick measures.
- o Describe similarities of, and differences between, a calculated column and a measure.

7- Add calculated tables and columns to Power BI Desktop models.

- o Create calculated tables.
- o Create calculated columns.
- o Identify row context.

- Determine when to use a calculated column in place of a Power Query custom column.
- Add a date table to your model by using DAX calculations.

8- Use DAX time intelligence functions in Power BI Desktop models.

- Define time intelligence.
- Use common DAX time intelligence functions.
- Create useful intelligence calculations.

9- Optimize a model for performance in Power BI

- Review the performance of measures, relationships, and visuals.
- Use variables to improve performance and troubleshooting.
- Improve performance by reducing cardinality levels.
- Optimize Direct Query models with table level storage.
- Create and manage aggregations.

10- Design Power BI reports

- Learn about the structure of a Power BI report.
- Learn about report objects.
- Select the appropriate visual type to use.

11- Configure Power BI report filters.

- Design reports for filtering.
- Design reports with slicers.
- Design reports by using advanced filtering techniques.
- Apply consumption-time filtering.
- Select appropriate report filtering techniques.

12- Enhance Power BI report designs for the user experience.

- Design reports to show details.
- Design reports to highlight values.
- Design reports that behave like apps.
- Work with bookmarks.
- Design reports for navigation.
- Work with visual headers.
- Design reports with built-in assistance.
- Use specialized visuals.

13- Perform analytics in Power BI

- Explore statistical summary.
- Identify outliers with Power BI visuals.
- Group and bin data for analysis.
- Apply clustering techniques.

- o   Conduct time series analysis.
- o   Use the Analyze feature.
- o   Use advanced analytics custom visuals.
- o   Review Quick insights.
- o   Apply AI Insights.

14- Create and manage workspaces in Power BI

- o   Create and manage Power BI workspaces and items.
- o   Distribute a report or dashboard.
- o   Monitor usage and performance.
- o   Recommend a development lifecycle strategy.
- o   Troubleshoot data by viewing its lineage.
- o   Configure data protection.

15- Manage datasets in Power BI

- o   Use a Power BI gateway to connect to on-premises data sources.
- o   Configure a scheduled refresh for a dataset.
- o   Configure incremental refresh settings.
- o   Manage and promote datasets.
- o   Troubleshoot service connectivity.
- o   Boost performance with query caching (Premium).

16- Create dashboards in Power BI

- o   Set a mobile view.
- o   Add a theme to the visuals in your dashboard.
- o   Configure data classification.
- o   Add real-time dataset visuals to your dashboards.
- o   Pin a live report page to a dashboard.

17- Implement row-level security.

- o   Configure row-level security by using a static method.
- o   Configure row-level security by using a dynamic method.

PL-400

Training Course PL-400: Microsoft Power Platform Developer

Overview: The Microsoft Power Platform helps organizations optimize their operations by simplifying, automating, and transforming business tasks and processes. In this course, students will learn how to build Power Apps, Automate Flows and extend the platform to complete business requirements and solve complex business problems.

Duration: 5 Days.

Audience Profile: Candidates for this course design, develop, secure, and troubleshoot Power Platform solutions. Candidates implement components of a solution that include application enhancements, custom user experience, system integrations, data conversions, custom process automation, and custom visualizations. Candidates will gain applied knowledge of Power Platform services, including in-depth understanding of capabilities, boundaries, and constraints. Candidates should have development experience that includes JavaScript, JSON, TypeScript, C#, HTML, .NET, Microsoft Azure, Microsoft 365, RESTful Web Services, ASP.NET, and Power BI.

Certification: This course prepares you for the PL-400: Microsoft Power Platform Developer
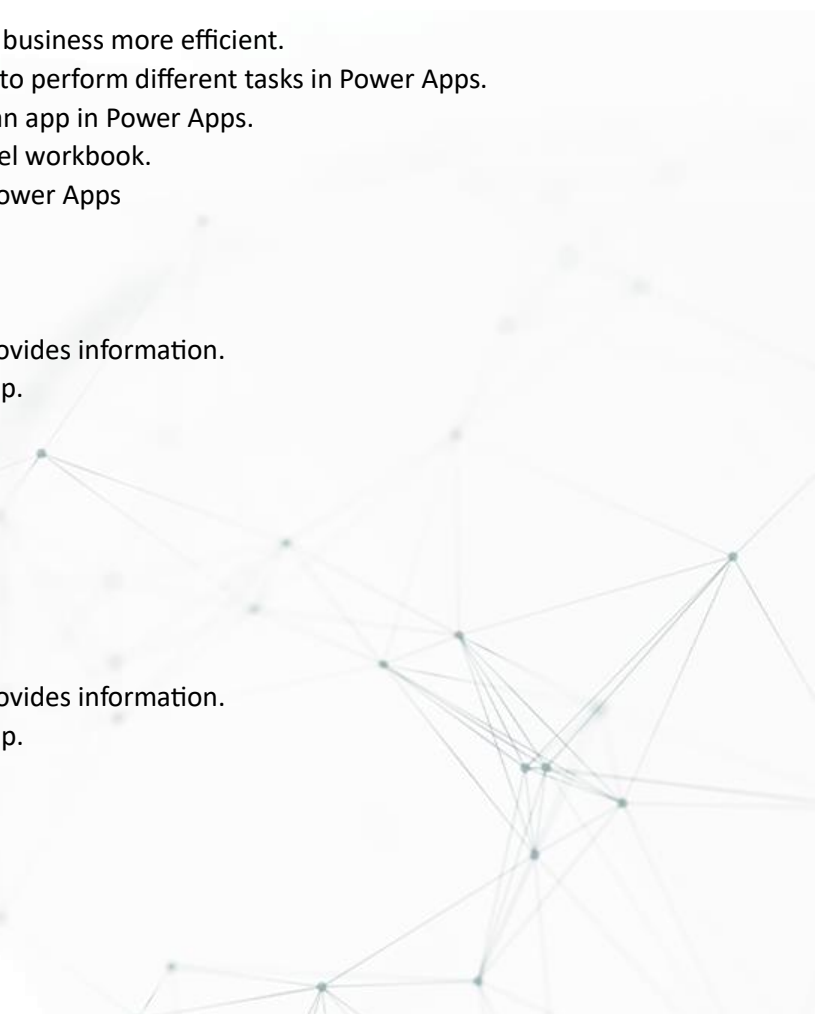
Course Objectives: After completing this course, students will be able to:

- How to build your first model-driven app with Dataverse.
- Get started with model-driven apps in Power Apps.
- Manage tables in Dataverse.
- Create and manage columns within a table in Dataverse.
- Working with choices in Dataverse.
- Create a relationship between tables in Dataverse.
- Define and create business rules in Dataverse.
- Create and define calculation or rollup columns in Dataverse.
- Get started with security roles in Dataverse.
- Get started with Power Apps canvas apps.
- Customize a canvas app in Power Apps
- Manage apps in Power Apps.
- Navigation in a canvas app in Power Apps.
- How to build the UI in a canvas app in Power Apps.
- Use and understand Controls in a canvas app in Power Apps.
- Document and test your Power Apps application.
- Use imperative development techniques for canvas apps in Power Apps
- Create formulas that use tables, records, and collections in a canvas app in Power Apps
- Perform custom updates in a Power Apps canvas app.
- Complete testing and performance checks in a Power Apps canvas app
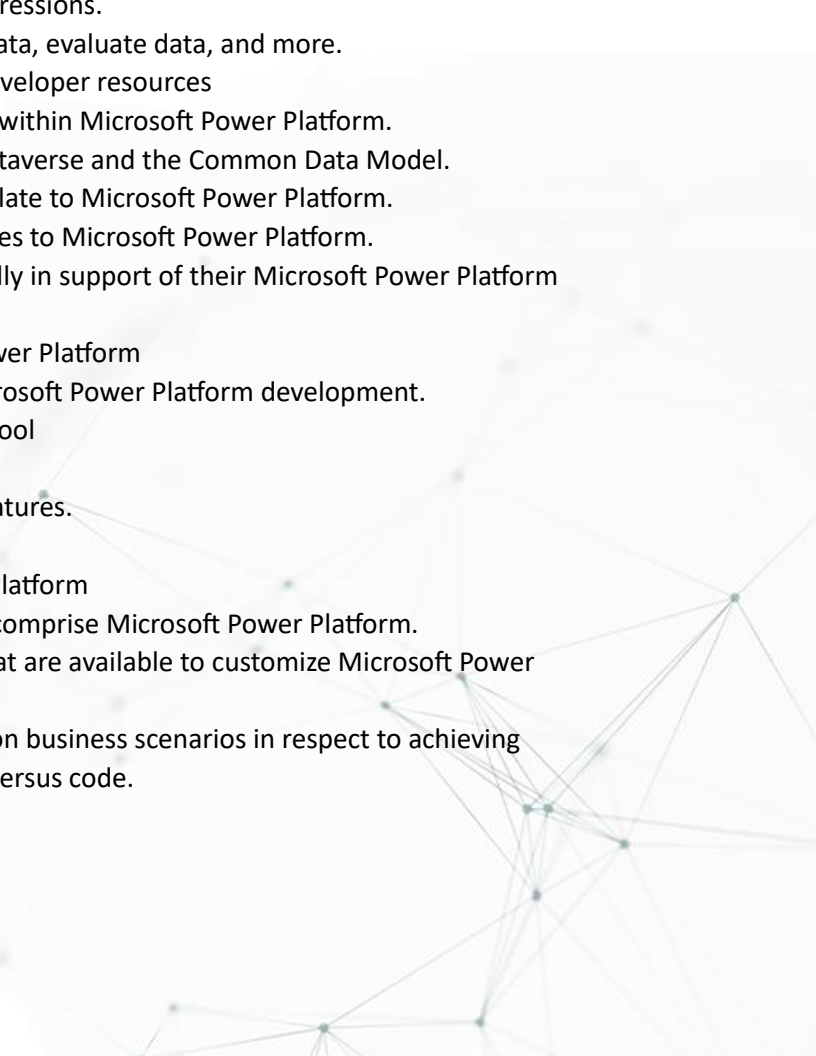- Work with relational data in a Power Apps canvas app.

- Work with data source limits (delegation limits) in a Power Apps canvas app
- Connect to other data in a Power Apps canvas app.
- Use custom connectors in a Power Apps canvas app.
- Get started with Power Automate.
- Build approval flows with Power Automate.
- Introduction to expressions in Power Automate.
- Introduction to Microsoft Power Platform developer resources.
- Use developer tools to extend Microsoft Power Platform.
- Introduction to extending Microsoft Power Platform.
- Introduction to Dataverse for developers.
- Extend plug-ins.
- Performing common actions with client script.
- Automated business process flows with client script.
- Get started with Power Apps component framework.
- Build a Power Apps component.
- Use advanced features with Power Apps component framework.
- Work with Dataverse Web API.
- Integrate Dataverse Azure solutions.

Course Outline

1- How to build your first model-driven app with Dataverse
   o Discover the value and key features of Dataverse.
   o Learn about the value and key features of model-driven apps.
   o Explore sample model-driven template apps.
2- Get started with model-driven apps in Power Apps
   o Learn about model-driven app design.
3- Manage tables in Dataverse.
   o Tables in Dataverse.
   o Types of tables that are available in Dataverse.
   o Creating a custom table.
   o Enabling attachments within a table.
   o Which licensing requirements to apply to use each type of table.
4- Create and manage columns within a table in Dataverse.
   o Learn what a column is in Dataverse.
   o Learn about the types of columns that are available in Dataverse.
   o Add a column to a table.
   o Learn what a primary name column is in Dataverse.
   o Identify restrictions that are associated with columns.
   o Create an auto-numbering column.
   o Create an alternate key.
5- Working with choices in Dataverse
   o Learn about choices.
   o Explore the standard choices.

- o   Create a new choice or modify an existing one.
6- Create a relationship between tables in Dataverse.
    - o   Why you should segment data that is used by your solutions into many tables.
    - o   Why you need to relate one table to another.
    - o   How to build relationships between tables.
    - o   How to select the proper relationship type when you're building solutions with Dataverse.
7- Define and create business rules in Dataverse.
    - o   Define business rules in Dataverse.
    - o   Create and manage business rules in Dataverse.
8- Create and define calculation or rollup columns in Dataverse.
    - o   Define a rollup column.
    - o   Create a rollup column.
    - o   Identify a calculation column.
    - o   Create a calculation column.
9- Get started with security roles in Dataverse.
    - o   Learn about security roles and apply them to users in an environment.
    - o   Learn how to add users to an environment.
    - o   Understand security concepts in Dataverse.
    - o   Identify default security roles.
    - o   Create a custom role.
    - o   Create a custom security role and assign it to entities and users.
    - o   Learn how to configure Dataverse teams for security.
    - o   Learn how to configure Dataverse group teams for security.
10- Get started with Power Apps canvas apps.
    - o   Explore how Power Apps can make your business more efficient.
    - o   Learn how to use different technologies to perform different tasks in Power Apps.
    - o   Learn about the different ways to build an app in Power Apps.
    - o   Create your first app from data in an Excel workbook.
    - o   Module 11: Customize a canvas app in Power Apps
    - o   Change the layout of a gallery.
    - o   Change the data that a control shows.
    - o   Change the order in which fields appear.
    - o   Change the control with which a user provides information.
    - o   Explore controls on each screen of an app.
    - o   Format a number as a price.
    - o   Color prices based on their values.
    - o   Explore formulas in a generated app.
11- Customize a canvas app in Power Apps.
    - o   Change the layout of a gallery.
    - o   Change the data that a control shows.
    - o   Change the order in which fields appear.
    - o   Change the control with which a user provides information.
    - o   Explore controls on each screen of an app.
    - o   Format a number as a price.

- o Color prices based on their values.
- o Explore formulas in a generated app.
12- Manage apps in Power Apps
- o Learn how to view and restore app versions.
- o Explore how to share an app, including permissions and notifications.
- o Learn about what environments are, how to create them, and how to manage security.
- o Find more information about Power Apps.
13- Navigation in a canvas app in Power Apps
- o Understand how navigation works in a canvas app.
- o Use the Navigate and Back functions.
- o Understand the different ways these functions can be invoked.
14- How to build the UI in a canvas app in Power Apps
- o Understand the basics of building the UI through themes, icons, control customization, and images.
- o Use personalization in a canvas app.
- o Understand the differences between the Tablet and Mobile form factors.
15- Use and understand Controls in a canvas app in Power Apps
- o Understand how to use controls in a canvas app.
- o Use the different types of controls.
- o Understand how Galleries and Forms related to controls.
16- Document and test your Power Apps application.
- o Learn about the different types of test plans and components of a good test plan.
- o Identify and discuss optimization tools and performance tuning.
- o Learn about the benefits of documenting your application.
17- Use imperative development techniques for canvas apps in Power Apps
- o Understand imperative vs. declarative development.
- o Understand the variables in Power Apps
- o Understand when to utilize each of the three different types of variables.
18- Create formulas that use tables, records, and collections in a canvas app in Power Apps
- o Utilize formulas that process multiple records.
- o Use the Concat function to combine text from multiple records.
- o Utilize the Countrows, CountIf, ForAll
- o Perform math operations on data in a table.
19- Perform custom updates in a Power Apps canvas app
- o Use the Patch function to update your data.
- o Understand how the Defaults function is used to create new records with Patch.
- o Utilize the Remove and RemoveIf functions to delete records.
- o Determine whether to use Clear and Collect or ClearCollect in their scenario.
20- Complete testing and performance checks in a Power Apps canvas app
- o Use best practices to improve the performance of your app.
- o Understand how to best test an app.
- o Use fiddler for troubleshooting.
21- Work with relational data in a Power Apps canvas app
- o Understand relational data.

- o Use relational data to improve an app user's experience in Power Apps
- o Understand how to use relational data in Microsoft Dataverse
22- Work with data source limits (delegation limits) in a Power Apps canvas app
- o Understand the different limits of different data sources.
- o Understand how functions, predicates, and operators all play roles in the limits.
- o Use this new understanding to choose the best data source for an app.
23- Connect to other data in a Power Apps canvas app.
- o Understand and use action-based connectors.
- o Integrate user information and user-profile information into a canvas app.
- o Use Power Automate with Power Apps
24- Use custom connectors in a Power Apps canvas app.
- o Understand custom connectors and the basics of how to build one.
- o Understand the custom connector lifecycle.
- o Use postman with a custom connector.
25- Get started with Power Automate.
- o Create a flow that automatically saves email attachments.
- o Learn how to create a button flow to send yourself a reminder.
26- Build approval flows with Power Automate
- o Create and process approval requests.
- o Build a flow that runs at recurring time intervals.
- o Create a business process flow with conditions.
27- Introduction to expressions in Power Automate
- o Use one or more functions to create expressions.
- o Use functions to retrieve data, change data, evaluate data, and more.
28- Introduction to Microsoft Power Platform developer resources
- o Explain what solution components exist within Microsoft Power Platform.
- o Explain key components of Microsoft Dataverse and the Common Data Model.
- o Explain what Azure solution elements relate to Microsoft Power Platform.
- o Explain what AI Solutions exist as it relates to Microsoft Power Platform.
- o Navigate the Developer Guide successfully in support of their Microsoft Power Platform development efforts.
29- Use developer tools to extend Microsoft Power Platform
- o Install NuGet packages available for Microsoft Power Platform development.
- o Work with the Configuration Migration tool
- o Work with Package Deployer
- o Leverage Solution Packager to isolate features.
- o Run the Plugin Registration Tool
30- Introduction to extending Microsoft Power Platform
- o Identify which elements architecturally comprise Microsoft Power Platform.
- o Learn about the areas of extensibility that are available to customize Microsoft Power Platform through code.
- o Discover different approaches to common business scenarios in respect to achieving extensibility by means of configuration versus code.
31- Introduction to Dataverse for developers

- o Explain what functions can be executed against Microsoft Power Platform via Microsoft Power Platform SDKs.
- o Perform basic operations against Microsoft Power Platform such as create/read/update/delete operations.

32- Extend plug-ins.
- o Learn how to extend plug-ins.

33- Performing common actions with client script
- o Write client script to perform common actions as listed in the module units.

34- Automate business process flows with client script.
- o Automate business process flow actions by using JavaScript/TypeScript API methods.

35- Get started with Power Apps component framework.
- o Learn about Power Apps component framework architecture.
- o Learn about Power Apps component tooling.

36- Build a Power Apps component.
- o Create a custom Power Apps component.
- o Create a code component solution package.
- o Test and debug a code component.
- o Learn key concepts of Dataverse auditing.

37- Use advanced features with Power Apps component framework.
- o Use formatting API in a Power Apps component.
- o Use Dataverse web API in a Power Apps component.

38- Work with Dataverse Web API
- o Interact with Dataverse Web API by using Postman.
- o Authorize against Dataverse with OAuth.
- o Use OData to query data.

39- Integrate Dataverse Azure solutions
- o Publish Dataverse events to Microsoft Azure Service Bus.
- o Write a Service Bus Event Listener that consumes Dataverse events.

AI-102

Training Course AI-102: Designing and Implementing a Microsoft Azure AI Solution

Overview: AI-102 Designing and Implementing an Azure AI Solution is intended for software developers wanting to build AI infused applications that leverage Azure Cognitive Services, Azure Cognitive Search, and Microsoft Bot Framework. The course will use C# or Python as the programming language.

Duration: 4 Days.

Audience Profile: Software engineers concerned with building, managing and deploying AI solutions that leverage Azure Cognitive Services, Azure Cognitive Search, and Microsoft Bot Framework. They are familiar with C# or Python and have knowledge on using REST-based APIs to build computer vision, language analysis, knowledge mining, intelligent search, and conversational AI solutions on Azure.

Certification: This course prepares you for the AI-102: Designing and Implementing a Microsoft Azure AI Solution.

Course Objectives: After completing this course, students will be able to:

- Prepare to develop AI solutions on Azure.
- Create and consume Cognitive Services.
- Secure Cognitive Services.
- Monitor Cognitive Services.
- Deploy cognitive services in containers.
- Extract insights from text with the Language service.
- Translate text with the Translator service.
- Create speech-enabled apps with the Speech service.
- Translate speech with the speech service.
- Build a Language Understanding model.
- Publish and use a Language Understanding app.
- Build a question answering solution.
- Create a bot with the Bot Framework SDK.
- Create a Bot with the Bot Framework Composer.
- Analyze images.
- Analyze video.
- Classify images.
- Detect objects in images.
- Detect, analyze, and recognize faces.
- Read Text in Images and Documents with the Computer Vision Service.
- Extract data from forms with Form Recognizer.
- Create an Azure Cognitive Search solution.

- Create a custom skill for Azure Cognitive Search.
- Create a knowledge store with Azure Cognitive Search.

Course Outline

1- Prepare to develop AI solutions on Azure.
   - Define artificial intelligence.
   - Understand AI-related terms.
   - Understand considerations for AI Engineers.
   - Understand considerations for responsible AI.
   - Understand capabilities of Azure Machine Learning.
   - Understand capabilities of Azure AI Services.
   - Understand capabilities of the Azure Bot Service.
   - Understand capabilities of Azure Cognitive Search.

2- Create and consume Azure AI Services.
   - Provision Azure AI Services resources in an Azure subscription.
   - Identify endpoints, keys, and locations required to consume an Azure AI Services resource.
   - Use a REST API to consume an Azure AI service.
   - Use an SDK to consume an Azure AI service.

3- Secure Azure AI Services.
   - Consider authentication for Azure AI Services
   - Manage network security for Azure AI Services.

4- Monitor Azure AI Services.
   - Monitor Azure AI Services costs.
   - Create alerts.
   - View metrics.
   - Manage diagnostic logging.

5- Deploy Azure AI services in containers.
   - Create Containers for Reuse
   - Deploy to a Container
   - Secure a Container
   - Consume Azure AI Services from a Container.

6- Extract insights from text with the Azure AI Language service.
   - Detect language.
   - Extract key phrases.
   - Analyze sentiment.
   - Extract entities.

- o   Extract linked entities.

7- Translate text with Azure AI Translator service.

- o   Provision a Translator resource.
- o   Understand language detection, translation, and transliteration.
- o   Specify translation options.
- o   Define custom translations.

8- Create speech-enabled apps with Azure AI services.

- o   Provision an Azure resource for the Azure AI Speech service.
- o   Use the Azure AI Speech to text API to implement speech recognition.
- o   Use the Text to speech API to implement speech synthesis.
- o   Configure audio format and voices.
- o   Use Speech Synthesis Markup Language (SSML).

9- Translate speech with the Azure AI Speech service.

- o   Provision Azure resources for speech translation.
- o   Generate text translation from speech.
- o   Synthesize spoken translations.

10- Build a conversational language understanding model.

- o   Provision Azure resources for Azure AI Language resource.
- o   Define intents, utterances, and entities.
- o   Use patterns to differentiate similar utterances.
- o   Use pre-built entity components.
- o   Train, test, publish, and review an Azure AI Language model.

11- Develop an app with Azure AI Language.

- o   Understand capabilities of an Azure AI Language Understanding model.
- o   Process predictions from an Azure AI Language in your app.

12- Build a question answering solution.

- o   Understand question answering.
- o   Compare question answering to language understanding.
- o   Create a knowledge base.
- o   Implement multi-turn conversation.
- o   Test and publish a knowledge base.
- o   Consume a knowledge base.
- o   Implement active learning.
- o   Create a question answering bot.

13- Create a bot with the Bot Framework SDK.

- o   Understand principles of bot design.
- o   Use the Bot Framework SDK to build a bot.
- o   Deploy a bot to Azure.

14- Create a Bot with the Bot Framework Composer.

- o   Understand dialogs.
- o   Plan conversational flow.
- o   Design the user experience.
- o   Create a bot with the Bot Framework Composer.

15- Analyze images.

- o   Provision an Azure AI Vision resource.
- o   Analyze an image.
- o   Generate a smart-cropped thumbnail.

16- Analyze video.

- o   Describe Azure Video Indexer capabilities.
- o   Extract custom insights.
- o   Use Azure Video Indexer widgets and APIs.

17- Classify images.

- o   Provision Azure resources for Azure AI Custom Vision.
- o   Understand image classification.
- o   Train an image classifier.

18- Detect objects in images.

- o   Provision Azure resources for Azure AI Custom Vision.
- o   Understand object detection.
- o   Train an object detector.
- o   Consider options for labeling images.

19- Detect, analyze, and recognize faces.
- o   Identify options for face detection, analysis, and identification.
- o   Understand considerations for face analysis.
- o   Detect faces with the Azure AI Vision service.
- o   Understand capabilities of the Face service.
- o   Compare and match detected faces.
- o   Implement facial recognition.

20- Read Text in Images and Documents with the Azure AI Vision Service.
- o   Read text from images with the Read API.
- o   Use the Azure AI Vision service with SDKs and the REST API.

o   Develop an application that can read printed and handwritten text.

21- Extract data from forms with Azure Document Intelligence.
o   Identify how Azure Document Intelligence's layout service, prebuilt models, and custom service can automate processes.
o   Use Azure Document Intelligence's Optical Character Recognition (OCR) capabilities with SDKs, REST API, and Azure Document Intelligence Studio.
o   Develop and test custom models.

22- Create an Azure Cognitive Search solution.
o   Create an Azure Cognitive Search solution.
o   Develop a search application.

23- Create a custom skill for Azure Cognitive Search.
o   Implement a custom skill for Azure Cognitive Search
o   Integrate a custom skill into an Azure Cognitive Search skillset.

24- Create a knowledge store with Azure Cognitive Search.
o   Create a knowledge store from an Azure Cognitive Search pipeline.
o   View data in projections in a knowledge store.