- The code.md file provides an overview of what the template does
- azuredeploy.json defines the resources that will be deployed.
- The azuredeploy.parameters.json file provides the values the template needs.

~~Microsoft Azure fundamentals: Describe azure architecture and services~~

Understand Microsoft entra ID

Examine Microsoft entra ID

- Active Directory
  - Directive service that provide methods for storing directory data such as users accounts and passwords
  - It makes this data available to network users, administrators and other devices and services.
  - It runs on a windows server(domain controller).
  - Part of the PAAS and is managed by microsoft so we cannot do changes to it.
  - With this service you have features not available in the normal AD such as multi-factor auth, identity protection and self-service password reset.
  - We can use this to provide more secure access to cloud resources by:
    - Config access to applications
    - Config single sign-on (SSO) to cloud based SAAS applications.
    - Managing users and groups.
    - Provisioning users.
    - Enabling federation between orgs
    - Providing an identity management solution.

- Identifying irregular sign-in activity.
- Configuring multi-factor authentication.
- Extending existing on-premise active directory implementations to Microsoft Entra ID.
- Configuring application proxy for cloud and locked applications.
- Configuring conditional access for users and devices.

- Microsoft Entra is a service that you usually get as a bundle up package in any microsoft subscription although usually you will only come with free features.
- You can have multiple tenants for test access you can only use one and by making the association you can do RBAC.
- Basicly you can create multiple tenants and associate one per each subscription.
- Each tenant has one DNS that is related to the user.

Microsoft entra schema

Microsoft entra ID vs Active Directory

A Characteristics of AD DS
- Traditional deployment of windows server-based active directory on a physical or virtual server.
- It has multiple services such as:
  - Active directory certificate services
  - Active directory lightweight directory services

- Active directory Federation Services
- Active directory rights management services
- characteristics
  - AD DS is a true directory service, with a hierarchical x.500 - based structure
  - AD DS uses DNS for locating resources such as domain controllers
  - You can query and manage AD DS by using Lightweight Directory Access Protocol (LDAP)
  - AD DS primarily uses the Kerberos protocol for auth.
  - AD DS uses ou, and GPOs for management
  - AD DS includes computer objects representing computers that join an active directory domain.
  - AD DS uses trusts between domains for delegated management
  - We can deploy AD DS on cloud for scalability but that does not turn into a microsoft entra ID.

characteristics of microsoft Entra ID

- Many similarities with AD but different.
- Is primarily a Identity solution, its designed for internet-based applications by using HTTP (port 80) and HTTPS (port 443) communications.
- Is a multi-tenant directory service.
- users are created in a flat structure, and there are no ou's or GPOs.

- You can't query on it using LDAP, it uses instead Rest API over HTTP and HTTPS
- It does not use Kerberos it uses HTTP and HTTPS such as SAML WS-federation, OpenID connect for authentication and oauth for authorization.
- Includes federation services and third party services such as Facebook are federated with and trust Microsoft Entra ID.

Microsoft entra ID as a directory service for cloud apps:

- So we resources in azure require authentication and usually by using the service the service itself creates its own microsoft entra tenant
- We can use the same microsoft entra tenant for various services which create a sso experience (one login for various services).
- We can apply this auth to custom solutions!
- We can assign this to a web service making only people with those credentials enter a website.

Compare Microsoft Entra P1 and P2

- This plans are better that the one that comes with microsoft office

P1 Service

- Self service group management
- To simplify the administration of group.

- Advanced security reports and alert
- detailed logs and data that help in managing security.
- multifactor authentication
- works with everything, even on-premises.
- Microsoft Identity Manager (MIM) licensing
- Hybrid identity solutions by bridging multiple authentication stores.
- Enterprise SLA of 99.9%.
- you are guaranteed 99.9% availability of this service.
- Password Reset with writeback
- It follows the AD on premises password policy.
- cloud App Discovery feature of Microsoft Entra ID
- Discovers the most used cloud-based apps.
- Conditional Access based on device, group or location.
- Make Conditions over the access of resources.
- Microsoft Entra connect Health
- operational insights over the Microsoft MA tool.

P2

- P1 but with Extras.
- Microsoft Entra ID Protection
- Enhanced functionalities for monitoring and protecting user accounts.
- Microsoft Entra Privileged Identity management
- Additional security levels for privileged users.

Microsoft extra domain services

- Some people want to deploy AD DS based authentications on cloud and to do that they either just deploy AD communicate with their local AD DS on they deploy them AD DS in the cloud in VMs
- A different approach is a service called "extra domain services".
- This services come with P1 as P2 services and provide domain services that are compatible with local AD DS.

create user accounts

- there are