Implement role-based access control

- RBAC is a role based access control mecanism that helps you manage who can access your Azure resources.

Things you can do with RBAC

- Allow a app to access all resources in a resource group.
- Allow one user to manage VMs in a subscription and allow another user to manage virtual networks.
- Allow a database administrator (DBA) to manage sql databases in a subscription.
- Allow users to manage all resources in a resource group, such as VMs, websites and subnets.

Core Components

★ Security Principal
- An object that represents something that requests acces to resources
- (User, group, managed identity).

★ Role definition
- A set of permissions that lists the allowed operations.
- Azure RBAC comes with buildin role definitions, but we can create custom ones (Reader, Contributor, owner, User Access administrator etc...).

★ Scope
- the boundary for the request level of access or "how much" access is granted.
- Management group, subscription, resource group, resource

★ Role Assignment
- an assignment attaches a role to a security principal at a particular scope

Considerations
- consider who are your requestors
- consider your Roles
- consider the scope of the permissions
- consider built-in or custom definitions.

Create a role definition
- This is defined in Json
- ~~Actions~~ Parameters
  - Actions
    - what you are allowed to do
  - NotActions
    - what you are not allowed to do.
  - DataActions
    - How can data be changed or used.
  - AssignableScopes
    - The scopes where a role definition can be assigned.

ex:
contributor
"Actions": [
"*"
],
"NotActions": [
"Authorization/*/Delete" → deny all deletes
],
"DataActions": []
"NotDataActions": []
"AssignableScopes": ["/"] → all scopes level of data.

* means all

Role Permissions

Things to consider when creating Roles
- consider using built-in Roles
- consider creating custom defini-

tions.
- Consider limiting access scope
- Consider controlling changes to data
- Consider applying deny assignments

Create a role Assignment
- the purpose of it is to have control & access.
- the limits can be available for those that belong to that role.
- Access can be removed by removing the role.
- A resource inherits the role access of its parent.

Compare Azure Roles to Microsoft Entra roles
* Types of roles for access management in azure
  - Classic subscription administrator roles
  - Azure role-based access control (RBAC) roles
  - Microsoft Entra Administrator roles

Apply role-based access control

- You can apply Entra ID Admin roles and Azure RBAC roles.

Entra Id admin Roles

/

/root

Azure RBAC

Root Management Group

Management group

RBAC Roles — Subscription

Resource group

Resources

Azure account

LAB simulation

- create management group
- Add subscription
- create json role def
- upload json with powershell
- create new users
- assign this role to that user
- test user permissions