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 them locally AD DS on they deploy them AD DS in the cloud in VMs
- A different approach is using 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.

Cloud users and group accounts

create user accounts

- there are 3 types of accounts

Cloud identity

- only for Microsoft Entra id users

Directory-Synchronized identity

- users that come from a on-premise network (usually sync of AD and Microsoft extra id

Guest user

- users outside of AZURE (ex: users from another cloud provider).

things to consider when creating users

- consider where users are defined.
- consider support for external authentications
- consider a combination of user accounts

manage user accounts

- We can add users using Azure portal, Microsoft 365 (only internal users), windows admin center (on-

and Azure cli cmdlets.

create Bulk user accounts

- can be done in azure portal with csv or credentials and a csv with the creation details.

create group accounts

- There are 2 types of grps.

Security groups

- Group for manage member and compute access to shared resources of a group of users.
- By managing groups we can set permissions for group of members

Microsoft 365 groups

- For collaboration opportunities
- Basicly a non-adm group.

ways to add users

- Adding specifically
- Dynamic user way which you put rules and it assigns rules based on the
- Dynamic device (only for security groups) adds and removes users based on rules.

create administrative units

Microsoft admin center

Azure portal

Administrative units

Powershell

Microsoft Graph

Business sched

School of engineering

Security team

Execution team