Compiled by Dr T Oberholster
DP-900 version: March 2021

- Authentication central ID management
  - Database users
  - Permission management
- Specify who/what resources need access
- Azure Role Based Access Control (RBAC)
  - 1 user to manage VMs & another to manage VN (per subscription)
  - 1 administrator group manage SQL DB (per subscription)
  - 1 user manage all resources in resource group
  - 1 app access all resources in resource group

Azure Active Directory

- Security principle: object (user/group/service principle/managed ID) requesting access
- Role definition: collection of permissions & lists operations performed (read/write/delete). High level names/specific roles
  - Owner: full access & delegate permissions
  - Contributor: Create & manage resources, no permissions
  - Reader: View resources
  - User Access Administrator: Mange user access to resources
- Scope: Set of resources access applies to. Assign roles & limit access

- Add roles through Access control (IAM) page

Parameters

- Azure relational data services
  - Default: disable public access

Firewall & Connectivity

Azure Virtual Network

- Virtual machines & Azure services connected
- Isolated
- Routes traffic to resources
- Connect to on-prem by configuring firewall & add IP address
- Exceptions setting allows non-isolated service access (via Virtual Network/IP address rules)

Advanced Security

- Threat protection & assessments
- Security intelligence: Detect harmful/compromising activities on services
- Identify vulnerabilities
- Recommended mitigation actions

Azure Private End Point

- Network interface private/secure service connection
- Private IP address for VN
- Firewall + VN => lock down user/app public access