70-534 Security Study Guide

**Securing Resources Using Managed Identities**

* Describe difference between AD on Prem and Azure AD (test a change)

|  |  |
| --- | --- |
| On Prem | Azure AD |
| Authentication | Authentication |
| Single tenant | Multi-tenant |
| Hierarchical; users, computers, OUs, groups, services | Flat; users and groups only |
| GPO, DNS | N/A |
| Accessed via LDAP | Graph API |
| Kerberos | SAML, WS-Federation, and OAUTH |
| VMs join domain | VMs can’t join domain (except Win10) |
| AD DS Forest, Trees, Domains contoso.net | Azure AD Tenants, contoso.onmicrosoft.com |

* + Azure AD
    - Multi-tenant
    - Cloud-based
    - Identity management already integrated with other SaaS solutions such as
      * Office 365
      * Dynamics CRM
      * Salesforce
      * FB
      * Twitter, etc.
    - All Microsoft Online businesses use Azure AD
    - Flat structure
    - Geo distributed in 28 data centers w/ automatic failover
  + On Prem AD
    - Single tenant
    - On prem data center(s)
* Azure AD versions
  + https://azure.microsoft.com/en-us/pricing/details/active-directory
  + Free
    - 500,000 objects
    - 10 apps per user
    - No group based access
    - No self-service password
    - No branding
    - No app proxy
    - No SLA
  + Basic
    - Unlimited objects
    - 10 apps per user
  + Premium 1 and Premium 2
    - No object or app limits
    - Advanced security reports
    - Other same features as Basic
    - Self-service password with write back
    - Device 2 way sync
  + Premium 2
* Programmatically access Azure AD using Graph API
  + REST API endpoints are OData 3.0 compliant
  + Supports common CRUD operations
    - Create user
    - Read properties
    - Update properties
    - Disable or Delete account
  + 3 steps
    - Add app w/ client secret
    - Use secret and other info to authenticate and get a token
    - Use token to make requests to API endpoint
    - https://graph.windows.net/{tenantId}/{resourcePath}?{apiVersion}
* Secure access to resources from Azure AD applications using OAuth and OpenID Connect