**Pluralsight Azure Secure Resources:**

Objectives

* Secure resource by using managed identities
  + Describe the differences between Active Directory on-premises and Azure AD
  + Programmatically access Azure AD using Graph API
  + Secure access to resources from Azure AD applications using OAuth and OpenID Connect
* Secure resources by using hybrid identities
  + Use SAML claims to authenticate on-premises
  + Describe DirSync synchronization
  + Implement federated identities using Azure Access Control service (ACS) and Active Directory Federation Services (ADFS)
* Secure resources by using identity providers
  + Provide access to resources using identity providers, such as Microsoft account, Facebook, Google, and Yahoo!
* Identity an appropriate data security solution
  + Use the appropriate Access Control List(ACL)
  + Identity security requirements for data in transit and data at rest
* Design a role-based access control
  + Secure resource scopes, such as the ability to create VMs and websites

Describe the differences between Active Directory on-premises and Azure AD

On-Premise AD

Supports only one directory

Moving target

Domain controller – running a certain OS with functions

User accounts, computer, accounts, group accounts, etc

Domain – logical boundary in a forest

Forest – collection of domains

Schema – collection of AD attributes

Site – set of AD computers by a network

Organizational Unit – obtain AD objects

Domain partition – collection of AD objects.

Attribute – username, password

Windows Server 2012 R2 (70-410) Administer Active Directory

Windows Server 2012 R2 (70-411) Configure Active Directory

Azure AD (as a Service)

Uses Office 365 and Microsoft Intune. Can join Windows 10 machines. Can support multiple directories. Roles don’t transfer to other directories.

Free edition

* User account management
* Sync with on-premises AD
* SSO with Intune and Office 365

Basic

* Group based access management
* Self-service password reset
* Azure AD application proxy

Premium

* Self service group management
* Advanced security reports and alerts
* Multi-factor authentication
* Microsoft Identity Manager Use rights
* Password reset with write-back
* Azure AD connect health

Domain Services

Replacement for Azure IaaS DC VM. Will only work with VM configured in Azure

Can do:

* Support complex schema extensions
* Support domain join/LDAP/Kerberos/NTLM/GPO
* Function as DNS server
* Works with AD connect

Can’t do:

* No accessible AD DS domain administrator account from AD DS tools. Can only view objects.
* Can only create users and groups from console or Azure Powershell
* Can edit computers gpo, users gpo
* Can’t edit default domain GPO, Default Domain Controllers GPO

Which computers are subject to Azure AD Domain Services domain policies?

VMs that are located on a specific Azure virtual network and which are joined to the Azure AD Domain Services domain are subject to Azure AD DS domain policies.

Which Azure AD Domain Services GPOs can be edited?

AADDC Computer GPO

AADDC Users GPO

Accessing Azure AD using Graph API

Programming application. OData 3.0 which allows objects to be modified and read. Single endpoint with access token via HTTP requests. May include JSON payload. Requires headers.

Tasks

List/search AD users/groups

Determine user groups

Determine report relationships

Update information

Set user passwords

Must be configured with OAuth 2.0 permissions scopes on the application

**Must know –** [**https://graph.windows.net/{tenant\_id}/{resource\_path}?{api\_version}**](https://graph.windows.net/%7btenant_id%7d/%7bresource_path%7d?%7bapi_version%7d) **endpoint addressing**

* <https://graph.windows.net> **is the service root**
* **{tenant\_id} identifier for the tenant where the requests will be served (GUID, Registered domain name, myorganization alias, me alias when delegated permissions scope)**
* **{resource\_path} – specific resource to the path – resource path table shown**
  + **Can display resource collection**
  + **Specific resource like user**
  + **Display a property of a specific resource**
  + **Target a function**
  + **Target a function on a resource**
* **{api\_version} – beta, 1.6, 1.5, 2013/11/08 types.**

Questions

What is the current version of the Azure AD Graph API? 1.6 as of December 2015