**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

Securing Access to Resources from Azure AD Applications Using OAuth and Open ID Connect

**OAuth**

* Open standard for authorization
* Authorize 3rd party access without requiring credentials
  + Special tokens used by the authorization server
* Pluralsight Courses – Oauth2, OpenID Connect, and JSON Web Tokens (JWT) (Dominick Baier)
* Azure AD complies with OAuth 2.0 RFC 6749
  + Authorizes web API’s and web applications

**Authorization Code Grant Flow**

* Done through OAuth 2.0 from Azure AD
* User delegates access to client application
  + Client application initiates flow by redirecting user to Azure AD authorization endpoint. User consent if necessary
  + Azure AD endpoint redirects user agent to client application with an authorization code
  + User agent returns an authorization code to client application redirect URI
  + Client application requests an access token from Azure AD token issuance endpoint
  + Azure AD token issuance point issues an access token and a refresh token. **Refresh token** can be used to request additional access tokens.
    - Azure AD uses a single refresh token to request access to multiple resources
  + Client application uses access token to authenticate to Web API
  + Web API returns data.
* Transaction is mediated and protected by a code grant
* Code grant is exchanged for an access token
* Client application never sees user credentials
* User agent never sees access token

**OAuth 2.0 Client Credentials Grant Flow** – allows a web service to use its own credentials for authentication when interacting with another web service rather than impersonating a user.

* Authenticates to Azure AD token issue and requests the access token
* Azure AD issuance endpoint issues an access token
* Access token is used to authenticate to secured resourced
* Data from secured resource returned to client application

**OAuth 2.0 Error Handling**

Invalid\_request, unauthorized\_client, access\_denied, unsupported\_response\_type, server\_error, temporarily\_unavailable, invalid\_resource.

400:invalid\_request, 401:invalid\_token, 403:insufficient\_scope, 403:insufficient\_access

Best Practices:

Use Authorization Code Grant Flow to prevent (CSRF) Cross-Site Request Forgery

* Client application generates a pseudo-random value
* Parameter and value sent by client in request
* Response should include state parameter and same pseudo-random value
* Client verifies that pseudo-random values are identical.

Best to cache access tokens

Clear cache if web API is called (invalid\_token)

During Authorization Code Grant Flow can generate interaction\_required or invalid\_grant codes

OpenID Connect 1.0 – allows you to use OAuth 2.0 with Azure AD for SSO. Authentication protocol. Returns an **id\_token** to authenticate a user.

What type of token does OpenID Connect return that allows a user to authenticate? Id\_token.

DirSync and Azure AD Connect

**DirSync** – a way to take on premise users and groups to Azure AD by sync and the other way around

* **Retired 2015**
* Azure AD Sync – retired 2015

**Azure AD Connect** – Current Tool

* Self-service password reset
* Sync custom AD attributes to Azure AD
* Password write-back
* Upgrade from DirSync/AAD Sync

Security requirements:

* Install SQL Express or SQL Server
* Using account that is local administrator on computer hosting the Azure AD Connect Role
* Global Admin rights account with Azure
* AD account with Enterprise Admin Rights

Multiple forests can be synced to a single Azure AD directory. Azure AD connect per forest.

What role must the account used for Azure AD Connect have? Global Admin Role

What group membership must the on-premises account used for Azure AD Connect have? Enterprise Admin Group in the forest.

Secure Resources

Azure ACS (Azure Access Control Service)

* Depreciated but still supported
* Merged into Azure AD

AZ FS (Federation Services)

* Syncs onpremise to Azure AD and use Azure AD to sync
* SSO with corporate network with policies that can be set.
* Use it when you need conditional access for onpremi/cloud and restricting sync of password with hash.
* Can setup now with Azure AD Connect with FS and web application proxy.
  + web application proxy should be accessible to the internet.

Enable –PSRemoting –force

What role service, besides AD FS, is required when federating on-premises Active Directory with Azure AD when using Azure AD Connect with Windows Server 2012 R2? Web application porxy role and accessible to the internet.