spanlabs
Enabling Talent Transformation

Windows Azure Question-Answer Part V- Azure Active Directory

KRUNAL TRIVEDI

MCT, MCT INDIA REGIONAL LEAD

TRAINER, WRITER, SPEAKER

www.techtrainingpoint.com

Krunal Trivedi
MCT – INDIA Regional Lead
www.techtrainingpoint.com

WINDOWS AZURE QUESTION-ANSWER

Windows Azure Active Directory

WHAT IS AZURE ACTIVE DIRECTORY?

- Windows Azure is all about services. It offers numerous services like Virtual Machines , Websites , Databases , Storage Services etc.
- For on-premises application and environment Active Directory serves the purpose of data store for identities management , same way Azure AD is a repository for all of your organization's directory data in the cloud , so that it can be readily available to all the services you have subscribed to.
- Azure Active Directory offers you the identity and access capabilities of Active Directory with your applications regardless of cloud-hosted or on-premises app.
- You can consider Azure AD as an identity provider which offers identity and access management functionality for your applications or SaaS applications like Dropbox, Skype, Intuit etc...
- It implements Single-Sign-On (SSO) to your application.
- It also supports identity sync functionality. As a result, your existing corporate credentials can be used to authenticate to new or existing applications that are hosted in cloud.
- Azure AD comes with a portal where your users can optionally manage their own passwords or groups. Password write-back feature of the Azure AD, the updated password hash is then duplicated to your on-premises Active Directory Instance.

HOW DEVELOPERS CAN LEVERAGE AZURE AD?

- Azure AD is a logical way to group your application and users.
- Developers can user Azure AD as an identity provider in their custom line-of-business applications and get benefits of SSO[Single-Sign-On].
- Developers can also update existing applications to use specific Azure AD tenant for identity.

- Third party cloud applications can interact with your data in Azure AD by using Graph API.

EXPLAIN THE MAIN FEATURES OF AZURE ACTIVE DIRECTORY?

Azure AD is composed of multiple features. Two main features of Azure AD are:

- Multi-Factor Authentication
- Directory Services

Multi-Factor Authentication: MFA offers another layer of authentication for your application that is completely managed. Administrator need to configure Multi-Factor Authentication and your application can take advantage of the feature by using Azure AD as the authentication (identity) provider. Multi-Factor Authentication supports authentication from text messages, mobile applications or phone calls.

Directory Services: Azure AD provides conceptual directories where you can store related accounts. One can sync identities from on-premises systems, identities created in Azure and third-party identities. These identities can be later configured to use with SaaS application.

-

WHAT ARE THE DIFFERENT WAYS TO INTEREACT WITH AZURE AD?

- One can manage organization's tenant data in Azure AD using either of these three tools:
    - Microsoft Azure AD Portal
    - Office 365 Account Portal
    - Windows intune Account Portal
    - Office 365 Account Portal

Krunal Trivedi
MCT – INDIA Regional Lead
www.techtrainingpoint.com

WHAT IS INTEGRATING ON-PREMISES DIRECTORIES WITH AZURE AD?

- Organization's existing on-premises directory service you can integrate with your Azure AD .
- There are number of ways of setting up directory integration capabilities like directory sync or SSO.
- Once you configured the sync operations, all the cloud services that you have subscribed to in your Azure AD tenant can utilize the data that is now provisioned and updated in your cloud.
- You have various options available like :
    - Syncing identities from Active directory to Azure AD
    - Syncing identity and password hash from AD to Azure AD
    - Syncing identity and password hash from AD to Azure AD and enabling password writeback.

WHAT IS PASSWORD WRITEBACK?

- Password writeback feature allows your existing AD identity to be updated when a change occurs in Azure AD.
- Identity and password hash sync process generates two identities.
- While designing authentication schemes for cloud applications, writeback functionality is key factor to be considered.

WHAT IS SINGLE SIGN-ON?

- Single Sign-On enables the users in your organization to be automatically signed into any third-party SaaS application using their Azure AD credentials.
- This functionality provides users with the convenience of remembering a single password and also increase the organization's security by providing users with access to only their applications.

.

WHAT IS AZURE AD GRAPH?

- Azure AD Graph is a REST based API which provides programmatic access to your Azure AD.
- This API can be used to store and retrieve metadata about your users that is not part of the typical user profile in Active Directory.

- Applications use the Graph API to perform CRUD operations on directory objects in your Azure AD instance.
- For example,
    - Create a new user in a specified directory,
    - Get detailed properties for a user
    - Check group membership for a user
    - Delete or disable a user account
    - Update the profile of a user
    - Similar operations are supported for groups and applications

EXPLAIN THE SCENARIO WHERE YOU NEED TO WORK WITH AD GRAPH API?

- Sometimes you application needs metadata and properties for each user that is not typically stored in standard Active Directory user profile.
- The Graph API allows you to register and then use extended properties.
- For example , if you need to store and then retrieve the Xbox Live ID for each user in a gaming application , you must first register the new property in the directory. You can then use this property in subsequent operations because it is not available for every user object in the directory.

EXPLAIN THE SCENARIO WHERE YOU NEED TO WORK WITH AD GRAPH API?

- Sometimes you application needs metadata and properties for each user that is not typically stored in standard Active Directory user profile.
- The Graph API allows you to register and then use extended properties.
- For example , if you need to store and then retrieve the Xbox Live ID for each user in a gaming application , you must first register the new property in the directory. You can then use this property in subsequent operations because it is not available for every user object in the directory.

Krunal Trivedi
MCT – INDIA Regional Lead
www.techtrainingpoint.com

EXPLAIN AZURE MULTIFACTOR-AUTHENTICATION?

- Multifactor-Authentication feature of Azure AD is used to provide an additional layer of authorizations like mobile code or a phone call to your existing directory accounts.
- It is an extra layer of authentication along with your credentials.
- It can be used for both on-premises applications and cloud applications.
- Multi-factor authentication can protect applications from unauthorized access if a user's credentials are compromised.
- Multi-factor authentication is usually defined by password (something you know) and trusted device (phone)
- If a user's credentials are compromised, a malicious user would still require a trusted device that is assigned to the same user to compromise the application or its data. If a user loses a trusted device, they report it immediately and the device can be de-authorized.
- Multi-Factor authentication can be used with either Azure AD or on-premises directory. The second form of authentication can be a smartphone, a phone number that supports text message or a phone call or a custom application.
- Multi-Factor Authentication service with Azure AD can have multi-factor authentication for each individual user.
- The MFA supports up to three phone numbers that are authorized for use as a second from of authentication.
- A SDK is available to integrate your custom application with Azure AD multi-factor authentication. The SDK allows you to use the Multi-Factor Authentication phone call or text message verification as a part of your custom application's sign-in process.

About The Author

- Krunal Trivedi is a Microsoft Certified Trainer as well as MCT INDIA Regional Lead
- *Krunal delivers training on various Microsoft technologies like .NET Framework , ASP.NET MVC Framework , SharePoint Server , Windows Azure – PaaS and IaaS,Office 365.*
- *He is having extensive experience of delivering IT technical training to thousands of participants In various software MNCs.*
- *He writes articles on his personal website www.techtrainingpoint.com on various Microsoft as well as JavaScript technologies including Angular JS , KnockoutJS and Angular2.*

spanlabs
Enabling Talent Transformation

- *Spanlabs is one of the premier Information Technology and Soft-Skills training organization.*
- *Spanlabs has the privilege of working with some of the leading players in the IT & ITES space.*
- *The company can proudly claim to have imparted training on many niche programs, complex technologies, products, applications and domains.*
- *We also provide advisory and consultancy services to our clients in their niche areas.*

FOLLOW US ON

Facebook Connect

Web Site: www.spanlabs.in