Assignment

Class Name and Teacher

Name

2023-07-14

Contents

1 Abstract

1.1 Lab 1: Create Azure Users & Group in Azure Active Directory

In this lab you are in the position of a global administrator for Azure Active Directory and is in the process of adding a development team along with an external design organization to ultimately collaborate a shared website in the Azure active directory environment. Throughout the lab you will be adding users in the Azure AD environment, managing resources and applications with Azure AD groups, and permitting guest access by the use of Azure AD's B2B. After performing the lab, the final results were mundane because access was not granted to create a tenant in the Azure AD environment.

1.2 Lab 2: Secure Your Application by using OpenID Connect and Azure AD

In this lab you will provide users with access to a secure application while minimizing the complexity of user interaction. A transportation company is building an application for drivers to help manage their schedule. The goal is to provide users ease of access by utilizing their existing Azure Active Directory accounts reducing overall complexity of signing up. You will use OpenID Connect and Azure AD as authentication methods allowing for a single account across many different applications in the Azure AD environment. The results were commonplace because access was not granted to create a tenant in the Azure AD environment.

1.3 Lab3: Allow Users to Reset Their Password with Azure AD Self-service Password Reset

In this lab you will set up a self-service password reset Azure active directory for a retail organization. By setting up the self-service password reset the administrator's overall productivity will increase because they no longer have to take the time and do manual password resets. In this lab you will implement and configure self-service password reset meeting specific requirements. The results were dull because access was not granted to create a tenant in the Azure AD environment.

2 Introduction

2.1 Lab 1: Create Azure Users & Group in Azure Active Directory

Identity management gives you the ability to control access of user accounts in the Azure active directory environment. Ultimately there are three types of user accounts when it comes to Azure AD.

One being administrators that have elevated privileges to maintain and create different resources. Two, member users which are the people who will be using the Azure AD environment to perform the work. Lastly, we have guest users that come with restricted permissions and are usually viewed as temporary and mostly used for external collaboration. The administrators will mostly manage the identity tasking so assigning the correct roles is necessary for security, maintain compliance, and the integrity of proprietary data. By implementing effective access control Azure AD can effectively collaborate with internal and external entities which can include stakeholders, other companies, or customers. In this lab, you will learn the basics of user management, access control, and how you can use collaboration in the Azure AD environment for a project that consists of website development.

2.2 Lab2: Secure Your Application by using OpenID Connect and Azure AD

In this lab you will be setting up a modern authentication method, a transportation will need to access their new app without any creation of new accounts. In Azure Active Directory you will review the OAuth 2.0 authentication method and then expand your knowledge of OpenID Connect providing an even more secure way of authentication. Simply put, you will authenticate to the application in two steps. Your identity will first be verified by Azure AD the environment, once verified a token will be issued. After you receive your token from verifying your identity, it will be sent to the application and the application will also verify the token that was issued and provide appropriate access from there. OpenID Connect takes OAuth 2.0 to the next level with an extra step adding signed JSON Web Tokens (JWTs) along with identity tokens. By using OpenID's authentication method, organizations can authenticate users securely and seamlessly with less complexity on the user side. In this lab you will use the modern authentication method of OpenID for single sign on, create another Azure tenant, and deploy an application. Largely, this lab will give you some skills to implement secure and user-friendly authentication methods in applications connected to Azure AD.

2.3 Lab3: Allow Users to Reset Their Password with Azure AD Self-service Password Reset

In this lab you will set up self-service password reset (SSPR) in Azure Active Directory for an organization. The retail organization in question is trying to reduce helpdesk costs and help users get more out of their service with SSPR. Users will be able to reset their passwords without the help of helpdesk overall improving productivity on the user end and organization end. You will learn SSPR process, ways to authenticate, options for customization, the requirements for licensing, and explore different deployment options. In this lab you will learn how to enable SSPR in the Azure AD environment, augment the management of passwords, and better the user experience.

3 Objectives

3.1 Lab 1: Create Azure Users & Group in Azure Active Directory

- Learn to add users to the Azure active directory environment.
- Learn to manage resources and applications through Azure active directory groups.
- Learn how to provision guest accounts with Azure Business to Business (B2b)

3.2 Lab2: Secure Your Application by using OpenID Connect and Azure AD

- Learn the different needs of modern authentication methods.
- Learn how to configure application registration for your application in your Azure tenant.
- Learn how to deploy an application with the OpenID connect authentication method in Azure AD.

3.3 Lab3: Allow Users to Reset Their Password with Azure AD Self-service Password Reset

- Learn when to implement SSPR.
- Learn how to deploy SSPR to meet requirements and configure SSPR to customize the experience.

4 Proceedures

4.1 Lab 1: Create Azure Users & Group in Azure Active Directory

In this lab you start out creating an Azure active directory organization. When creating the Azure AD tenant you select the type, organization name, and original domain name. Once the tenant is created, it requires you to sign up for a free Azure Premium subscription, when done signing up you proceed with the creation of the user. After you create your user in the Tenant with your free premium subscription, the next step is to delete the user. Once the user is deleted you need to recover the user, this is possible only if the deletion occurred within the last thirty days, otherwise the user and data along with the user will be gone forever. Your next task is to add a new group to the Azure Tenant you created. You will add a new group by providing the group type, group name, and group description. Once the group is created you will use direct assignment to assign the user to the group. The next step is to modify the group to use dynamic assignment. When using group dynamic assignments, a user will only be added if they meet the rules you set. In the case of this lab, you a user will be assigned to the dynamic user

group based on country. Once completed, you will change the group back from dynamic assigned to assigned. The last exercise in this lab is setting up a B2B connection to allow guests to collaborate on projects. First you will go to your Tenant and click “New User” and then “Invite external user”, enter the users name and email address. The user will receive an email and the “all users” pane will appear with the user you just entered as type guest. From here you will add the user to the group you created earlier as well as add them to the application Docusign. The way you add the user to Docusign is by selecting “select role” and then assigning them to the Docusign application. If the user never received the invitation, you could resend the invitation by selecting the user and selecting resend invitation.

4.2 Lab2: Secure Your Application by using OpenID Connect and Azure AD

In this lab the first step is to create an Azure tenant specifying type, organization type, domain name, and country region. When you are done creating your Azure tenant, the next step is to register an application by navigating to the manage tab and selecting app registration. Select new registration and the register an application page will appear. Here you will select the name of who can use this application (Accounts in this organizational directory only (Learn Module AAD Tenant only - Single tenant) and specify the URI and hit register. Once registered the WebApp-OpenIDConnect-DotNet pane will appear and you will see the application (client) ID and the Directory (tenant) ID, make sure to save these. Next you will configure and deploy an application that uses OpenID connect. Login to Azure CLI and create a resource group. After the resource group is created you will clone a Github repository, this is your application you are deploying. Change directory into the applications repository you just cloned and open the appsettings.json file in a code editor to change some json values. You will change the domain name, application (client) ID and the Directory (tenant) ID you got earlier from the application registered Azure page. Save the file and then run the deploy command in Azure CLI to deploy the application. Navigate back to your tenant you originally created and select the WebApp-OpenIDConnect-DotNet application that you created. Now under the manage tab select authentication and under redirect URI paste in the URL from the application you deployed and click save. The final part is to test the authentication method you set up in the application, you should be prompted with a sign in requesting permission to access the application.

4.3 Lab3: Allow Users to Reset Their Password with Azure AD Self-service Password Reset

Starting this lab, you will configure your Azure AD organization tenant; this procedure can be found in Lab 1. After you configure your tenant, you will create a group and user account, this procedure can also be found in Lab 1. Once you have your tenant, group and user account, it is time to enable SSPR. You do this by going to the manage tab and selecting “password reset”. In the password reset page

select the “select” option and then select the SSPRTesters group option and save. Next you will go back to the manage tab and select customization and then navigate to the Custom helpdesk email / URL text box and enter “admin@theorganizationyoucreated” and select save. At this point the SSPR configuration is complete the next step is to register a phone number for the user you created. Now navigate to https://aka.ms/ssprsetup, you will be asked to change your password and authenticate your phone, set it up and select text. Next, we will test the SSPR, navigate to https://aka.ms/sspr, enter the “user@theorganizationyoucreated”, complete the captcha, enter your number, select text, enter the pass code you received in your text, and finally enter your new password. For the final task in this lab, you will customize Azure AD organization branding. Go to your tenant you created and under the manage tab select company branding > configure. In the company branding configure tab you can set you sign in background and Banner logo. Once those are set browse to https://login.microsoft.com/ and see if things have propagated correctly. Select forgot my password and follow the steps above to see it SSPR is still working.

5 Results

5.1 Lab 1: Create Azure Users & Group in Azure Active Directory

There are no results for this lab due to not having access to create an organizational tenant (Figure 1). This is the first step of the lab, and I was unable to complete it.

5.2 Lab2: Secure Your Application by using OpenID Connect and Azure AD

There are no results for this lab due to not having access to create an organizational tenant (Figure 1). This is the first step of the lab, and I was unable to complete it.

5.3 Lab3: Allow Users to Reset Their Password with Azure AD Self-service Password Reset

There are no results for this lab due to not having access to create an organizational tenant (Figure 1). This is the first step of the lab, and I was unable to complete it.

6 Conclusion and Recomendations

6.1 Lab 1: Create Azure Users & Group in Azure Active Directory

Overall, this lab would have been a good exercise but again I did not have access to do the lab. I did learn quite a bit reading over the lab and writing up the procedure. I like the fact that it is really easy to add guest users to the account and how easy it is to assign them roles in the group. Learning how to assign dynamic groups and add users to them based on rules and provided good insight into ways users might stumble upon things they should not have access to. This taught me to be very careful when creating and assigning users to dynamic groups.

6.2 Lab2: Secure Your Application by using OpenID Connect and Azure AD

I would have really liked to do this lab and go through the actual hands-on motion of setting up a single sign on application. I gained a better understanding of OAuth and OpenID connect authentication methods. Understanding these modern authentication methods is crucial for modern web applications.

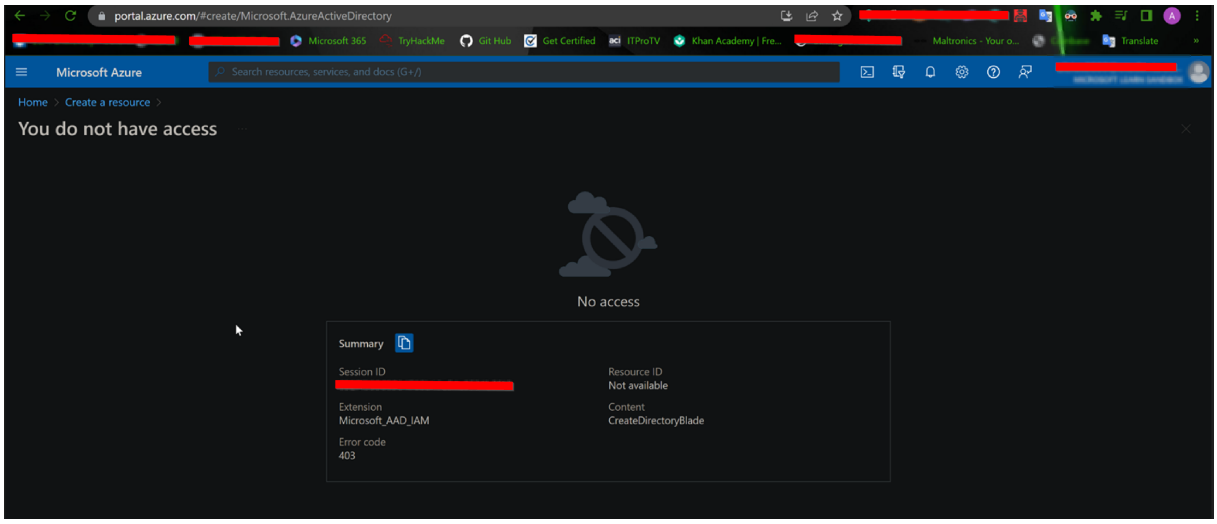
6.3 Lab3: Allow Users to Reset Their Password with Azure AD Self-service Password Reset

Again, I would have really liked to do this lab, but I did not have access to complete the first step. Learning the setup of SSPR and writing out the procedure gave me a better understanding of the process and security behind it. I think a lab implementing all these topics together would be great practice and would give me an all-around scope of authentication practices in Azure.

7 Appendix

7.1 Lab 1,2,3

7.1.1 Figue 1



References

Microsoft. (2023a). Create Azure users and groups in Azure Active Directory: Introduction. Microsoft Learn.line https://learn.microsoft.com/en-us/training/modules/create-users-and-groups-in-azure-active-directory/

Microsoft. (2023b). Secure your application by using OpenID Connect and Azure AD: Introduction. Microsoft Learn https://learn.microsoft.com/en-us/training/modules/secure-app-with-oidc-and-azure-ad/

Microsoft. (2023c). Allow users to reset their password with Azure Active Directory self-service password reset: Introduction. Microsoft Learn. https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/