## Lab 6-01: Azure Entra ID

### Service Introduction

CloudHealth, a leading cloud management platform provider, faced a growing challenge: managing complex access across multiple cloud providers and on-premises infrastructure. Their existing identity system, fragmented and manual, hindered collaboration, created security risks and slowed down onboarding.

### Problem

CloudHealth's existing system relied on a patchwork of on-premises directories and disparate cloud provider solutions, making access control inconsistent and difficult to manage. The complex process of adding users and granting access hampered collaboration and slowed down new customer acquisition.

### Solution

CloudHealth partnered with Microsoft to implement Azure Entra ID, a comprehensive identity and access management (IAM) solution, as their single source of truth for user identities and access control. Azure Entra ID consolidated all identities, from employees to partners, into a single, centralized platform, simplifying management and access control.

|  |
| --- |
| Task 1: Create Azure Entra ID  1. Log in to the **Microsoft Azure** portal and go to the portal menu.      1. Click on **Microsoft Entra ID** from the portal menu.      1. Now click on **Users** from the left sidebar of the default directory.      1. The **Users** tab displays the list of all users currently in the tenant.      1. To add a new user to this active directory, click on the **+ New user** tab.      1. Write the username, first name, and last name of your choice.      1. After filling out the names section, click on **Auto-generated password** in the **Password** option.      1. Then, click **Create.**      1. After clicking **Create,** the notification of “Successfully created user” will appears.      1. Now, click on “**New\_user”** to see the entered details. |

## Lab 6-02: Multi-Factor Authentication

### Service Introduction

Azure Multi-Factor Authentication (MFA) is a security feature provided by Microsoft Azure that adds an extra layer of protection to user logins. By requiring users to verify their identity through a second authentication method beyond just a password, such as a phone call, text message, or mobile app notification, Azure MFA significantly enhances the security posture of applications and resources. This additional layer helps safeguard against unauthorized access, even if passwords are compromised. Azure MFA can be easily integrated with various Azure services, applications, and on-premises resources, providing a flexible and comprehensive solution for organizations aiming to strengthen their authentication mechanisms and protect sensitive data from unauthorized access.

Top of Form

### Problem

The organization has recently shifted its resources from on-premises to the Azure cloud platform. The security and access management department wants to use a service that keeps things simple for users while securing access to data and apps. How would it be possible?

### Solution

Using an Azure service called Multi-Factor Authentication (MFA), the organization can easily fulfill the requirement to safeguard access to data and apps. MFA also delivers robust authentication using various simple validation methods and adds security by requiring a second form of verification.

|  |
| --- |
| Task: Multi-Factor Authentication   1. Log in to Azure Portal using your credentials.      1. From the home page, select Azure Entra ID. The Default Directory Overview page will appear.      1. From the left side given menu, click on Security under Manage.      1. From the Getting Started page, select Conditional Access present inside Protect.      1. From the Getting Started page, select **Conditional Access** present inside **Protect.**      1. Select the **+New policy.** You can also use the Preview option to create a policy.      1. To create a policy, select a category and click **Next.**      1. Select the option to apply MFA, or you can select the template provided by the preview option. 2. Click on **Next.**     **Note:** Here, we are enabling MFA for all users.   1. After reviewing the settings, click on **Create Policy.**     **Note:** Within a few minutes, your policy for MFA will be successfully created.   1. You can restrict access to your account by the given steps. Go to the home page and search and open **Multifactor authentication.**      1. The overview page will appear. Go to the **Block/unblock users** from the Settings section.      1. Click on **+Add** to add a user you want to block.      1. Write the User name and provide a reason to block.     **Note:** You will shortly observe that the user will be added to the list of **Blocked users.**   1. To unblock the user and provide access to the service, you need to click on **Actions.**      1. Provide a reason to unblock the user and click on **OK.**     **Note:** You will shortly be observed that the user will now be removed from the blocked list. |