Azure Security Concepts, Skill Labs

Course Specifications

Course Number: ACI76-025SL_rev1.0
Lab Length: Approximately 3 hours

Using Azure Key Vault (PLAB-AZ4)

Introduction
Objective

Welcome to the Using Azure Key Vault practice lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Azure Key Vault is a service that assists infrastructure administrators to manage security keys, Hardware Security Modules (HSMs), and security certificates in one central location in Azure.

Overview
Learning Outcomes:

In this module, you will complete the following exercises:

- Exercise 1 – Using Azure Key Vault

After completing this lab, you will be able to:

- Enable and configure Azure Key Vault.
- Create security keys, secrets, and certificates using Azure Key Vault.

Admin Tools (PLAB-AZ4)

Introduction
Objective

Welcome to the Admin Tools practice lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

Microsoft Azure provides security tools on the Azure portal. The Azure Windows Admin Center can be used to assess the security posture of the resources hosted on the Azure platform.

In this module, different security assessment tools in the Azure Windows Admin Center will be explored.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 – Exploring the Azure Windows Admin Center

After completing this lab, you will be able to:

- Create a virtual machine (VM).

- Explore Azure Windows Admin Security Center.

Network Security (PLAB-AZ4)

Introduction
Objective

Welcome to the Network Security in Azure practice lab. In this lab, you will be provided with the instructions and devices needed to develop your hands-on skills.

One common authorization method is Access Control Lists (ACLs) to manage access to resources. An ACL is a list attached to a resource, allocating permissions or rules to specific users granting them access.

It's essential to recognize that network ACLs have different functionality than ACLs used on a host file system or application. Instead of specifying what users can access a specific file or resource, a network ACL specifies what type of network traffic is allowed to pass through a device like a router or a firewall.

Different vendors may use different terms, but the important thing is that a network ACL restricts unwanted traffic from passing through a device. This application of network ACLs is called packet filtering, and it's one of the oldest and most common ways of restricting network traffic for security purposes.

For example, if a particular IP address has been used for repeated attacks against your network, you could create an ACL that blocks traffic from that address. Similarly, you can prevent users from accessing known phishing sites. In that case, you could block access to the IP address using an ACL. Inbound and outbound rules are typically on separate ACLs.

Overview
Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 – Network Connection Security

After completing this lab, you will be able to:

- Create a virtual network in Azure.
- Create a network security group in Azure.
- Configure a network security group in Azure.
- Create network security rules in Azure.