Lab Exercise: Day 2 - Advanced Azure Infrastructure, Security, and Management

Objective:

This lab focuses on deepening participants' understanding of Azure's infrastructure capabilities beyond virtual machines, emphasizing availability configurations, security, governance, identity management, and automation of Azure resources. By completing this exercise, participants will gain hands-on experience with Azure's management tools, security practices, and governance policies, empowering them to build a secure, highly available, and compliant Azure environment.

Expected Outcome:

- Proficiency in configuring Availability Zones, Availability Sets, and Resource Groups for optimized resource organization and application reliability.
- Comprehensive knowledge of Azure's security and governance frameworks, including Azure Active Directory, Azure Policy, and Role-based Access Control (RBAC).
- Skills in utilizing Azure Portal, Cloud Shell, Azure PowerShell, and CLI for efficient resource management.
- Ability to securely manage sensitive information using Azure Key Vault.

Prerequisites:

- An active Microsoft Azure account.
- Basic understanding of cloud computing concepts and familiarity with Azure services.

Lab Exercise Details:

Part 1: Azure Infrastructure Configuration

- **Task 1.1:** Create Resource Groups based on different project environments (e.g., Development, Testing, Production). Explain the organizational benefits of using Resource Groups.
- **Task 1.2:** Explore and document the purpose and usage of Availability Zones and Availability Sets in ensuring application reliability, without creating VMs.

Part 2: Security and Governance Overview

- **Task 2.1:** Navigate to Azure Security Center. Review and summarize the key security features and recommendations provided for your Azure subscription.
- **Task 2.2:** Implement Azure Policy to enforce tagging standards across your resources. Create a compliance report based on your policy assignments.

Part 3: Identity, Azure Active Directory, Users & Groups

- **Task 3.1:** Create a new Azure Active Directory (AAD) instance, add new users, and organize these users into groups reflecting hypothetical organizational roles.
- **Task 3.2:** Configure Role-based Access Control (RBAC) for a Resource Group, assigning different roles to the users created. Verify access restrictions.

Part 4: Subscriptions and Accounts, Azure Policy, RBAC

- **Task 4.1:** Within Azure Policy, create a policy that requires all resources in a specific subscription to utilize a particular network security group.
- **Task 4.2:** Experiment with RBAC by creating custom roles tailored to specific needs within your organization and apply these roles at different scopes.

Part 5: Azure Automation Tools

- **Task 5.1:** Use Azure Cloud Shell to automate the creation of a Resource Group and a storage account. Document the process and the commands used.
- **Task 5.2:** Explore Azure PowerShell and CLI by scripting a sequence to create and configure Azure Key Vault, including setting up secrets and permissions.

Part 6: Azure Key Vault Service

- **Task 6.1:** Securely store and manage a secret in Azure Key Vault. Demonstrate how to access this secret using Azure CLI or PowerShell.
- **Task 6.2:** Document how Azure Key Vault can be integrated into Azure services for secure management of keys, secrets, and certificates without exposing them in code or configuration files.

Submission Guidelines:

- Document the execution of each task, including command-line inputs/outputs, configuration settings, and any scripts written. Include screenshots where applicable.

- Reflect on how each task contributes to building and managing a secure and efficient cloud infrastructure. Discuss any challenges faced and how they were overcome.
- Submit your report through the designated submission platform or via email to the instructor, adhering to any specified formatting or content requirements.