**CST8912 – Cloud Solution Architecture**

**Graded Lab Activity #5**

1. Employ industry standards and best practice guidelines when creating cloud-based architectural solutions. (1,5)
2. Identify the techniques for automation and orchestration of resources
3. Evaluate programming, deployment and failure considerations when programming the cloud.
4. Examine the prerequisite to implement elasticity to handle increased traffic load
5. Evaluate decoupling strategies to create flexible, modular and scalable cloud solutions
6. Describe and evaluate cloud software deployment considerations for optimizing cost.
7. Identify security, organizational standards, and policies for securing platforms

**Lab Scenario:**

**Part 1:** In order to allow users to authenticate by using Azure AD, you have been tasked with provisioning users and group accounts. Membership of the groups should be updated automatically based on the user job titles. You also need to create a test Azure AD tenant with a test user account and grant that account limited permissions to resources in the Azure subscription.

Microsoft Entra ID is a cloud-based identity and access management service. Microsoft Entra ID enables your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Microsoft Entra ID also helps them access internal resources like apps on your corporate intranet, and any cloud apps developed for your own organization.

In this lab, you will:

* Create and configure users
* Create groups with assigned and dynamic membership
* Create a conditional access policy for a user in AD
* Test the access policy
* Clean the resources after use

**Purpose of this hands-on Lab that can be simulated for any Cloud Provider**:

In this lab you will:

Task 1: Create and configure Azure AD users for Canada central region /7

Steps to follow:

1. Go to azure portal and search for azure active directory
2. Create a tenant and choose tenant type “Microsoft Entra ID”
3. Choose the organization name and domain name and location as “Canada”
4. Once tenant is created, search **Microsoft Entra ID in portal**
5. On the Microsoft Entra ID blade, scroll down to the Manage section, click User settings, and review available configuration options.
6. On the Microsoft Entra ID blade, in the Manage section, click Users, and then click your user account to display its Profile settings
7. Navigate back to the Users - All users blade, and then click + New user
   * **user principal name:** 8912user1
   * **display name**: 8912user1
   * Auto-generate password: **checked**
   * Account enabled: checked
   * Job title (Properties tab): **IT Administrator**
   * Department (Properties tab): **IT**
   * **Usage location: Canada**
8. In the list of users, click the newly created user account to display its blade
9. Review the options available in the Manage section and note that you can identify the roles assigned to the user account as well as the user account’s permissions to Azure resources.
10. Invite an external user
11. In the New user drop-down select Invite an external user.

|  |  |
| --- | --- |
| Setting | Value |
| Email | your email address |
| Display name | your name |
| Send invite message | check the box |
| Message | Welcome to Azure and our group project |

1. Move to the Properties tab. Complete the basic information, including these fields.

|  |  |
| --- | --- |
| Setting | Value |
| Job title | **IT Administrator** |
| Department | IT |
| Usage location (Properties tab) | Canada |

1. Select Review + invite, and then Invite.
2. Refresh the page and confirm the invited user was created. You should receive the invitation email shortly.

Task 2: Create groups and add members /7

In this task, you create a group account. Group accounts can include user accounts or devices. These are two basic ways members are assigned to groups: Statically and Dynamically. Static groups require administrators to add and remove members manually. Dynamic groups update automatically based on the properties of a user account or device. For example, job title.

1. In the Azure portal, search for and select Groups.
2. Take a minute to familiarize yourself with the group settings in the left pane.
3. Expiration lets you configure a group lifetime in days. After that time the group must be renewed by the owner.
4. Naming policy lets you configure blocked words and add a prefix or suffix to group names.
5. In the All groups blade, select + New group and create a new group.

|  |  |
| --- | --- |
| Setting | Value |
| Group type | Security |
| Group name | IT Administrator |
| Group description | Administrators that manage the IT lab |
| Membership type | Assigned |

Note: An Entra ID Premium P1 or P2 license is required for dynamic membership. If other Membership types are available, the options will show up in the drop-down.

1. Screenshot of create assigned group.
2. Select No owners selected.
3. In the Add owners page, search for and select yourself (shown in the top right corner) as the owner. Notice you can have more than one owner.
4. Select No members selected.
5. In the Add members pane, search for and select the 8912user1 and the guest user you invited. Add both of the users to the group.
6. Select Create to deploy the group.
7. Refresh the page and ensure your group was created.
8. Select the new group and review the Members and Owners information.

Task3: Implement Management Groups /3

In this task, you will create and configure management groups. Management groups are used to logically organize and segment subscriptions. They allow for RBAC and Azure Policy to be assigned and inherited to other management groups and subscriptions. For example, if your organization has a dedicated support team for Europe, you can organize European subscriptions into a management group to provide the support staff access to those subscriptions (without providing individual access to all subscriptions).

1. Sign in to the Azure portal - https://portal.azure.com.
2. Search for and select Microsoft Entra ID.
3. In the Manage blade, select Properties.
4. Review the Access management for Azure resources area. Ensure you can manage access to all Azure subscriptions and management groups in the tenant.
5. Search for and select Management groups.
6. On the Management groups blade, click + Create.
7. Create a management group with the following settings. Select Submit when you are done.
8. Refresh the management group page to ensure your new management group displays

|  |  |
| --- | --- |
| Setting | Value |
| Management group ID | 8912-mg1 (must be unique in the directory) |
| Management group display name | 8912-mg1 |

Task4: Review and assign a built-in Azure role /2

1. Select the 8912-mg1 management group.
2. Select the Access control (IAM) blade, and then the Roles tab.
3. Scroll through the built-in role definitions that are available. View a role to get detailed information about the Permissions, JSON, and Assignments. You will often use owner, contributor, and reader.
4. Select + Add, from the drop-down menu, select Add role assignment.
5. On the Add role assignment blade, search for and select the Virtual Machine Contributor. The Virtual machine contributor role lets you manage virtual machines, but not access their operating system or manage the virtual network and storage account they are connected to. This is a good role for the Help Desk. Select Next.
6. On the Members tab, Select Members.
7. Note: The next step assigns the role to the helpdesk group. If you do not have a Help Desk group, take a minute to create it.
8. Search for and select the helpdesk group. Click Select.
9. Click Review + assign twice to create the role assignment.
10. Continue on the Access control (IAM) blade. On the Role assignments tab, confirm the helpdesk group has the Virtual Machine Contributor role.

Task 5: Clean up the resources created during the lab and document all the steps in the lab report /1

.