Лабораторна робота №4

ОЗНАЙОМЛЕННЯ З ПРИНЦИПАМИ РОБОТИ ENTRA ID ТА ЙОГО ОСНОВНИМИ ФУНКЦІЯМИ

Мета: ознайомитися з принципами роботи Microsoft Entra ID (Azure AD) та основними функціями які використовуються в щоденній роботі адміністратора Microsoft Entra ID (Azure AD)

Хід роботи

1. Створити Entra ID тенент.
   https://portal.azure.com/#view/Microsoft_AAD_IAM/CreateDirectoryBlade/releaseCreateOperation~/
   https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-create-new-tenant#create-a-new-microsoft-entra-tenant
2. Створити одного користувача в новоствореному тененті, використовуючи графічний метод.
   https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/AllUsers/menuId/
   Відправити запрошення одному користувачеві поза тенентом (external user), пошта якого буде @gmail.com, @outlook.com, тощо.
   https://learn.microsoft.com/en-us/entra/external-id/b2b-quickstart-add-guest-users-portal
   Додати двох користувачів, використовуючи Bulk Create.
   https://learn.microsoft.com/en-us/entra/identity/users/users-bulk-add
3. Зайти на myapplications.microsoft.com, використовуючи дані першого користувача та додати у звіт скріншот з початковою сторінкою Apps Dashboard.
4. Створити дві Security Group з назвами «Developers» та «QA». В результаті виконання попереднього завдання ми маємо мати 4-х новостворених користувачів. В довільному порядку додати по два користувача в кожну групу. https://learn.microsoft.com/en-us/entra/fundamentals/groups-view-azure-portal
5. Перемістити Subscription у створений в завданні 1 тенент. Якщо при спробі переміщенні Subscription у новий тенент виникає помилка, то варто спробувати перезайти у свій обліковий запис або спробувати

спробу пізніше. Створити Resource Group, використовуючи метод зазначений у табл.1 згідно варіанту. Назва Resource group буде мати наступний вигляд: rg-aaa-xxx-yyy-zzz, де aaa – скорочена назва ресурсу, який буде створено, згідно з офіційними рекомендаціями щодо скороченого іменування ресурсів, xxx – скорочена назва одного з 5 доступних регіонів зідно політики, яка застосовується для навчальних Subscriptions Azure for Students, в якій вказані регіони, в яких можна створювати ресурси, використовуючи скорочену назву регіону, відповідно до цього файлу, що містить відповідність між повною та скороченою назвою регіону, а yyy – ініціали студента, zzz – номер варіанту. Згідно даних створити ресурс, заданий в табл.1 всередині даної Resource group. Назва ресурсу буде наступного формату: aaaxxxyyyzzz, де значення aaa, xxx, yyy, zzz співпадає з умовами іменування Resource group.

6. Дублювати існуючі політики Allowed resource types та Add a tag to resources, додавши до їх імені префікс [Custom]. Об'єднати політики у Policy Initiative definition. Назва Policy Initiative Definition має бути [Custom] Policy Initiative definition – xxx, yyy, zzz, де xxx, yyy, zzz будуть співпадати зі значенням для іменування групи ресурсів. В параметрах політики Allowed resource types потрібно додати тип Microsoft.Authorization/locks, а також тип ресурсу вказаний у завданні завдання 5, згідно варіанту. В політиці Add a tag to resources вказати в параметр Tag Name значення Variant, а в Tag Value – номер варіанту. Застосувати Policy Initiative definition на Scope студентської Subscription. Якщо не виконати призначення Policy Initiative, то вона просто буде створена та не мати ніякого ефекту. Протестувати політики, спробувавши створити в Resource groups ресурс, який ви дозволяєте створити в політиці явно, переконавшись, що ви дійсно можете їх створювати та спробувати створити ресурс, який відсутній в дозволяючій політиці та, очікувано, отримати помилку. Переконатись, що в створеному ресурсі буде наявний тег, який буде додано політикою.
7. В результаті виконання завдань 5 та 6 у вас має бути Resource group, всередині якої будуть два ресурси однакового типу. На рівні Resouce group створити Resource lock ReadOnly з довільною назвою. Після

його створення, спробуйте видалити один з ресурсів. Спробуйте виконати наступні дії:

- додати довільний тег до Resource group
- додати довільний тег до ресурсу в Resource group
- видалити один з ресурсів

Зафіксувати результати.

Видаліть ReadOnly Resouce lock та створіть новий з типом CanNotDelete та довільною назвою. Спробуйте повторити попередні 3 дії та зафіксуйте результати.

8. Надати одному довільному попередньо створеному користувачеві роль Contributor, іншому Reader. Від імені користувача, що має права Contributor, спробувати створити ресурс, в існуючі Resource group ресурс, такого типу, який вказаний в дозволяючій політиці. Переглянути список усіх ресурсів. Від імені користувача, що має права Reader спробувати створити ще один ресурс такого ж типу. Зафіксувати результати. Створити кастомну роль, яка буде називатись Technical Support та буде призначена на Scope рівня Subscription. Серед дозволів вказати наступні:

- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listKeys/action
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/secrets/read

Назначити цю роль довільному користувачеві з попередніх завдань та вказати Scope – Subscription.

Табл.1

Ресурси та метод їх створення, згідно варіанту

№ варіанту	Ресурс	Метод створення ресурсів
1	Azure Virtual Network	Azure CLI
2	Azure Storage Account	Azure PowerShell
3	Azure Key Vault	ARM Template
4	Azure Virtual Network	Azure PowerShell
5	Azure Storage Account	Azure CLI
6	Azure Key Vault	Azure CLI
7	Azure Virtual Network	ARM Template
8	Azure Storage Account	ARM Template
9	Azure Key Vault	Azure PowerShell
10	Azure Virtual Network	Azure CLI
11	Azure Storage Account	Azure PowerShell
12	Azure Key Vault	ARM Template
13	Azure Virtual Network	PowerShell
14	Azure Storage Account	ARM Template
15	Azure Key Vault	Azure CLI
16	Azure Virtual Network	Azure CLI
17	Azure Storage Account	Azure PowerShell
18	Azure Key Vault	Azure PowerShell
19	Azure Virtual Network	ARM Template
20	Azure Storage Account	Azure CLI

Контрольні запитання

1. Що таке Microsoft Entra ID (раніше Azure Active Directory) і яку роль відіграє створення окремого тенанта у процесі керування доступом до ресурсів Azure?
2. У чому полягає різниця між внутрішнім користувачем тенанта та зовнішнім (external/guest user), і яким чином здійснюється їхнє додавання через портал Microsoft Entra?
3. Яке призначення мають Security Groups у Microsoft Entra ID і як вони можуть використовуватись для спрощення призначення ролей або політик у межах Azure?
4. Яким чином можна перемістити існуючу підписку (Subscription) до нового тенанта, і які обмеження або наслідки можуть виникнути після такого переміщення?
5. Поясніть логіку формування імен для ресурсів і груп ресурсів у завданні. Чому стандартизовані схеми найменування (наприклад, rg-aaa-xxx-yyy-zzz) є важливими для управління корпоративним середовищем Azure?
6. Яке призначення політик Allowed resource types та Add a tag to resources, і як їхнє дублювання з префіксом [Custom] допомагає у створенні власних ініціатив комплаєнсу (Policy Initiative Definition)?
7. Як працює Resource Lock у режимах ReadOnly та CanNotDelete? У чому полягає різниця між цими двома типами блокувань і які саме дії користувач не може виконати в кожному випадку?
8. Які відмінності у правах і можливостях мають користувачі з ролями Contributor і Reader у межах однієї Resource Group, і як це впливає на їхню здатність створювати або змінювати ресурси?
8. Яку роль виконує створена кастомна роль Technical Support, які дозволи вона надає користувачу та чому її призначення на рівні Scope Subscription є доцільним?
10. Як Azure RBAC, Azure Policy та Resource Locks взаємодіють між собою у забезпеченні цілісної системи контролю доступів, комплаєнсу та захисту ресурсів у середовищі Azure?