Chmurowisko

Szkolenie Terraform: Dzień 5

1. Zadanie: Tworzenie użytkownika w Azure AD

Należy stworzyć konto użytkownika w domenie „chmurowiskolab.onmicrosoft.com". Do wygenerowanie hasła możesz wykorzystać zasób „*random_password*", w ramach providera *random.* Użyj hasła o długości 20 i z wykorzystaniem znaków specjalnymi.

Do zadania potrzebny będzie provider *azread.*

Zasoby które należy utworzyć (w kolejności):

- Losowo generowane hasło
- Konto użytkownika

Przydatne linki:
Terraform dokumentacja User
https://registry.terraform.io/providers/hashicorp/azuread/latest/docs/resources/user

Terraform dokumentacja Password
https://registry.terraform.io/providers/hashicorp/random/latest/docs/resources/password

2. Zadanie: Tworzenie własnych definicji ról oraz przypisanie ich do stworzonego użytkownika

Należy stworzyć 2 własne, dowolne definicje ról lub skorzystać z tych zapisanych w kodzie do zadania. Następnie należy przypisać role do użytkownika stworzonego w poprzednim zadaniu. Przypisanie powinno być zrobione na poziomie grupy zasobów, którą zarządzamy.

Zachęcamy do stworzenia własnych definicji ról. W tym celu warto skorzystać z dokumentacji Microsoftu, w której można znaleźć opis poszczególnych akcji dotyczących różnych zasobów.

Na końcu należy sprawdzić działanie przypisanych ról. Można to zrobić za pomocą portalu logując się kontem użytkownika stworzonym przez nas a następnie spróbować wykonać akcję, którą przypisaliśmy wraz z rolą np. spróbować stworzyć grupę zasobów jeśli nadana rola powinna uprawnić do tego użytkownika.

Zasoby które należy utworzyć (w kolejności):

- 2 definicje dowolnych ról
- Role Assigment

Przydatne linki:
Terraform dokumentacja Role Definition
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/role_definition

Terraform dokumentacja Role Assigment
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/role_assignment

Azure dokumentacja operacji zasobów
https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

3. Zadanie: stworzenie własnej tożsamości Managed Identity oraz użycie jej do uzyskania dostępu do Storage Account

W tym zadaniu skupimy się na skorzystaniu z tożsamości Managed Identity „przypiętej" do danego zasobu, która pozwoli nam odczytać testowy plik w innym zasobie. W tym przypadku będzie to maszyna wirtualna, do której zostanie „przypięta" wcześniej stworzona tożsamość Managed Identity typu „User Assigned", a następnie utworzymy zasób Storage Account, z którego za pomocą wcześniej utworzonej tożsamości spróbujemy odczytać jego zawartość.

Zasoby które należy utworzyć (w kolejności):

- Sieć wirtualna + podstawowy subnet
- Storage Account
- Maszyna wirtualna (Linux)
- Managed Identity typu **User Assigned** w raz z przypisaniem tożsamości do maszyny wirtualnej
- Nadanie roli dla Managed Identity, która pozwoli uzyskać dostęp do plików przetrzymywanych w Storage Account – Storage Blob Data Reader

Przydatne linki:
Terraform dokumentacja Linux Virtual Machine
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/linux_virtual_machine

Terraform dokumentacja Azure Role Assignment
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/linux_virtual_machine

Terraform dokumentacja User Assigned Managed Identity
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/user_assigned_identity