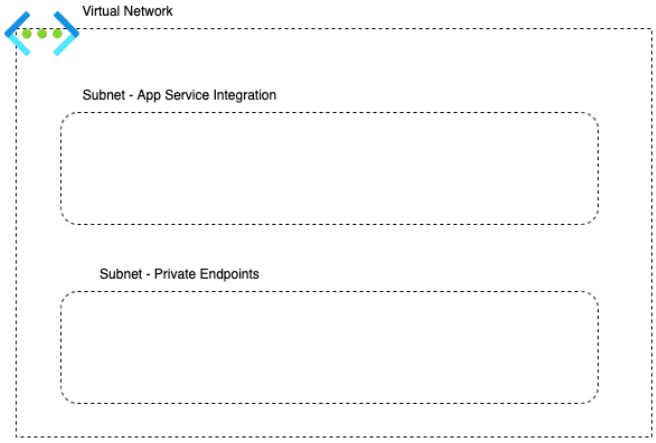
Chmurowisko

Szkolenie Terraform: Dzień 3

1. Zadanie: Budowa sieci pod aplikacje Ghost



Rys. 1 Architektura sieciowa Zad 1.

Wszystkie zasoby podczas warsztatów utwórz w przygotowanej dla Ciebie grupie zasobów.

Należy utworzyć sieć wirtualną oraz dwie podsieci (pod aplikacje i prywatne punkty końcowe). Podsieć przeznaczoną dla aplikacji należy oddelegować do wykorzystania przez usługę App Service. Należy tutaj wykorzystać blok „delegation" w definicji zasobu podsieć.
Podsieć przeznaczona dla prywatnych punktów końcowych musi mieć argument „enforce_private_link_endpoint_network_policies" na wartość „true".

Przykładowa adresacja sieci:

- Vnet – 10.0.0.0/16
- Subnet App Service – 10.0.0.0/24
- Subnet Private Endpoints – 10.0.1.0/24

Zasoby które należy utworzyć:

- Sieć wirtualna Vnet
- Subnet pod App Service w sieci wirtualnej Vnet
- Subnet pod Private Endpoints sieci wirtualnej Vnet

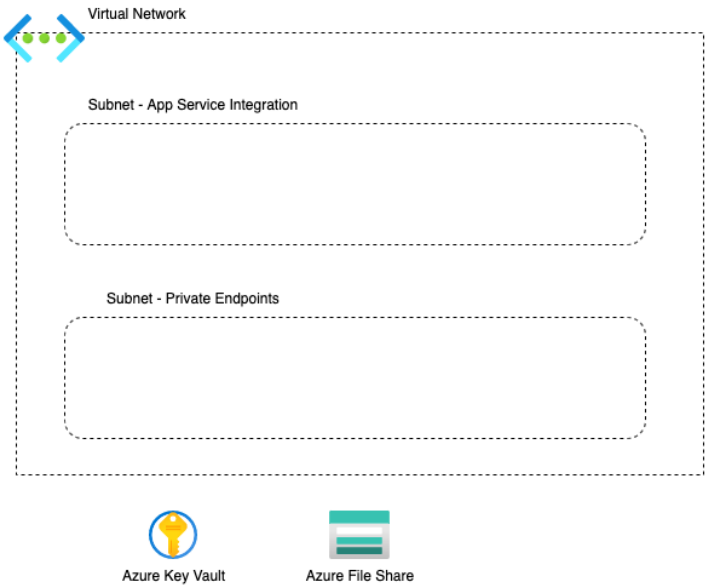
Przydatne linki:

Terraform dokumentacja sieci wirtualnych
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/virtual_network

Terraform dokumentacja subnetów
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/subnet

Przykładowe rozwiązanie znajduje się w folderze „1-VNet"

2. Zadanie: Utworzenie Azure Key Vault i Storage Account



Rys. 2 Architektura Zad 2.

Należy utworzyć Azure Key Vault. Podczas tworzenia Key Vault nadaj uprawnienia swojemu użytkownikowi wykorzystując Access Policy. (Wartości object_id oraz tenant_id dla swojego użytkownika może pobrać z portalu lub wykorzystując data source „azurerm_client_config".

Do utworzonego Azure Key Vault utwórz sekret, który będzie przechowywać hasło. Hasło to zostanie wykorzystane przy tworzeniu serwera bazy danych MySQL w kolejnym zadaniu. Hasło możesz wygenerować korzystając z zasobu „random_password", w ramach providera „random".

W kolejnym kroku utwórz Azure Storage Account, po czym dodaj do niego Azure Storage Share. Azure Storage File Share zostanie podłączony do utworzonej aplikacji w celu przechowywania plików statycznych.

Zasoby które należy utworzyć (w kolejności):

- Azure Key Vault (sku: standard)
- Azure Key Vault Secret (hasło)
- Azure Storage Account
- Azure Storage Account Share (quota: 50gb)

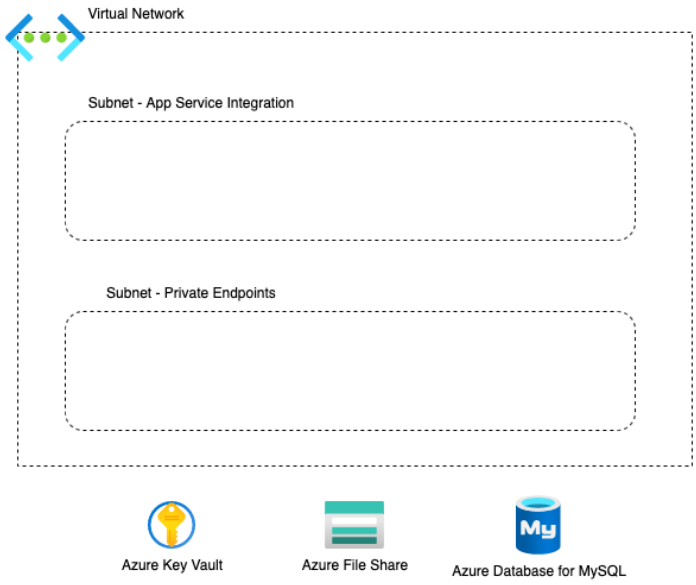
Przydatne linki:
Terraform dokumentacja key vault
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/key_vault

Terraform dokumentacja key vault secret
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/key_vault

Terraform dokumentacja storage account
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/storage_account

Terraform dokumentacja storage account share
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/storage_share

3. Zadanie: Utworzenie bazy danych MySQL



Rys. 3 Architektura Zad 3.

W tym zadaniu utworzymy serwer bazy danych MySQL i bazę danych pod aplikację. Podczas tworzenia serwera bazy danych jako hasło wskaż, te samą wartość, która znajdują się w Azure Key Vault Secret.

Wartości, które należy wskazać podczas tworzenia serwera bazy danych:

- sku_name = "GP_Gen5_2"
- storage_mb = 5120
- version = "5.7"
- auto_grow_enabled = true
- backup_retention_days = 7
- geo_redundant_backup_enabled = false
- infrastructure_encryption_enabled = false
- public_network_access_enabled = false
- ssl_enforcement_enabled = true
- ssl_minimal_tls_version_enforced = "TLSEnforcementDisabled"

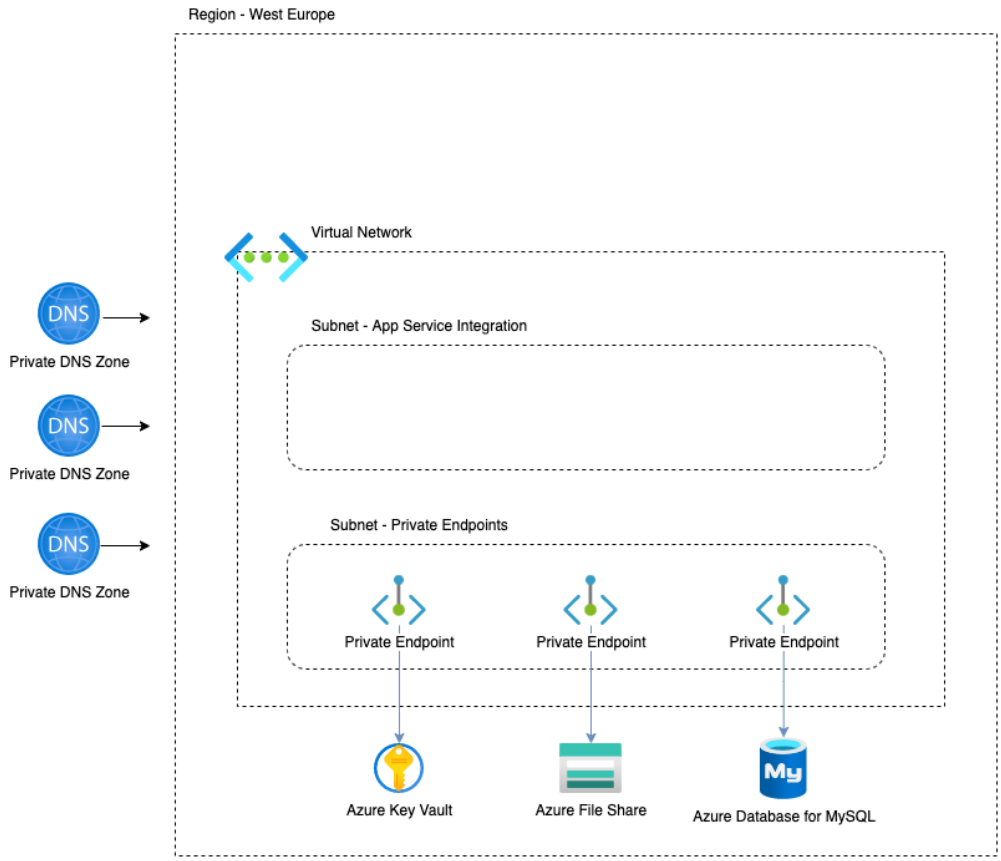
Zasoby które należy utworzyć (w kolejności):

- Azure MySQL Server
- Azure MySQL Server Database

Przydatne linki:
Terraform dokumentacja Azure MySQL Server
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/mysql_server

Terraform dokumentacja Azure MySQL Server Database
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/mysql_database

4. Zadanie: Utworzenie prywatnych punktów końcowych



Rys. 4 Architektura Zad 4.

W tym zadaniu utworzymy prywatne punkty końcowe dla Azure File Share, Azure MySQL Server, Azure Key Vault. Dzięki temu wszystkie komponenty naszej aplikacji, będą wykorzystywały sieć prywatną przy komunikacji.

Przed przystąpieniem do utworzenia prywatnych punktów końcowych, należy utworzyć prywatne strefy DNS oraz powiązać te strefy DNS z naszą siecią wirtualną.

Prywatne strefy DNS wykorzystywane przez prywatne punkty końcowe powinny korzystać z zalecanych nazw.

W naszym przypadku utworzymy 3 strefy DNS o nazwach:

- privatelink.vaultcore.azure.net
- privatelink.file.core.windows.net
- privatelink.mysql.database.azure.com

Więcej informacji na temat zalecanych nazw prywatnych stref DNS dla usług Azure znajdziesz tutaj: https://docs.microsoft.com/pl-pl/azure/private-link/private-endpoint-dns#azure-services-dns-zone-configuration.

W kolejnym kroku należy utworzone prywatne strefy DNS powiązać z siecią wirtualną utworzoną w zadaniu 1.

Ostatnim krokiem tego zadania jest utworzenie trzech prywatnych punktów końcowych dla usług Azure Key Vault, Azure Storage Account, Azure MySQL Server.

Przy tworzeniu prywatnego punktu końcowego należy wskazać:

- w bloku private_service_connection – id zasobu, dla którego tworzymy endpoint oraz nazwę zasobu podrzędnego (więcej informacji znajdziesz tutaj https://docs.microsoft.com/en-gb/azure/private-link/private-endpoint-overview#private-link-resource)
- w bloku private_dns_zone_group – należy wskazać id prywatnej strefy dns, dzięki temu odpowiedni rekord A wskazujący na interfejs sieciowy endpointu zostanie automatycznie dodany
- w argumencie subnet_id należy wskazać podsieć przeznaczą na punkty końcowe.

Zasoby które należy utworzyć (w kolejności):

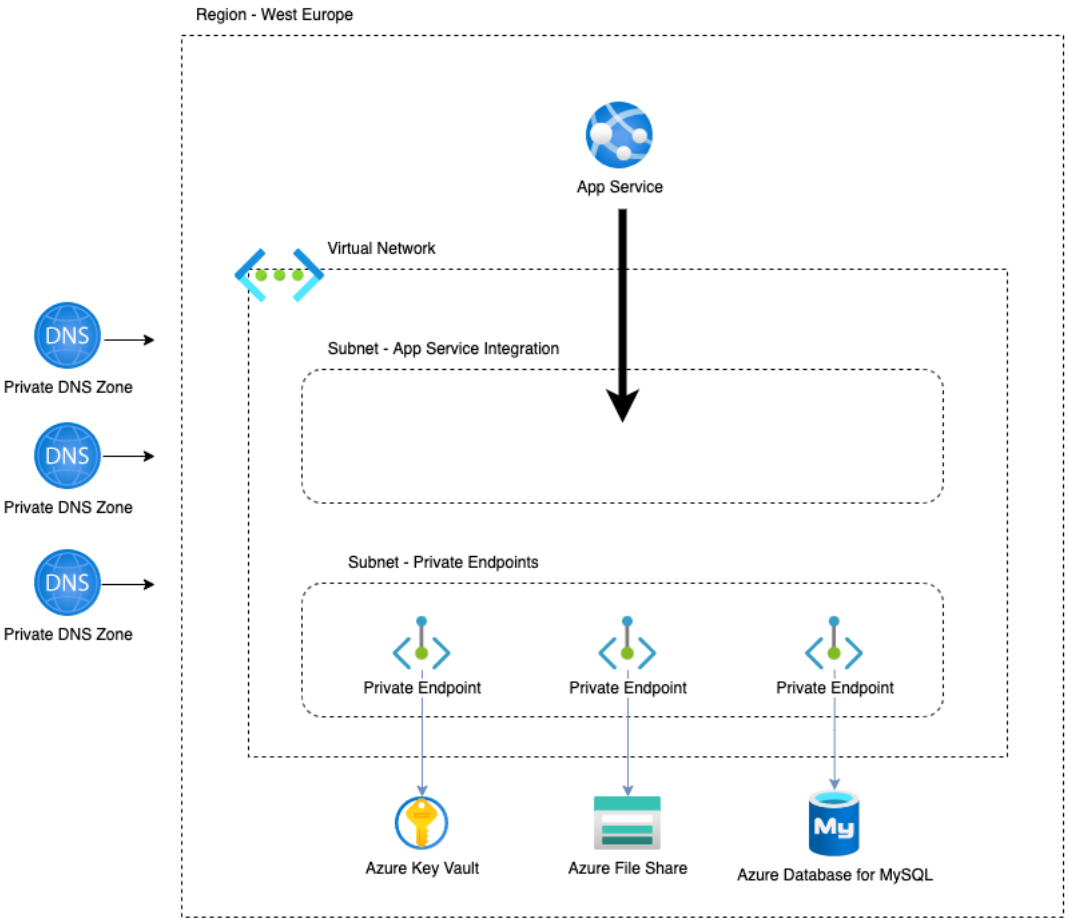
- 3x Private DNS Zone
- 3x Private DNS Zone Virtual Network Link
- 3x Private Endpoint

Przydatne linki:
Terraform dokumentacja Private DNS Zone
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/private_dns_zone

Terraform dokumentacja Private DNS Zone Virtual Network Link
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/private_dns_zone_virtual_network_link

Terraform dokumentacja Private Endpoint
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/private_endpoint

5. Zadanie: Utworzenie Azure App Service



Rys. 5 Architektura Zad 5.

W tym zadaniu utworzymy App Service pod naszą aplikacje Ghost.

W pierwszym kroku utwórz Service Plan wykorzystujący system „Linux" i plan „P2v3". Do utworzenia tego zasobu wykorzystaj „azurerm_linux_web_app".

Następnym krokiem jest utworzenie App Service wykorzystujący utworzony wcześniej Service Plan. Podczas tworzenia aplikacji skonfiguruj:

- Ustawienia aplikacji:
  "database__client" : "mysql",
  "database__connection__database" : __REFERENCJA_DO_NAZWY_BAZY__,
  "database__connection__host" : __REFERENCJA_DO_HOSTA__ (wykorzystaj nazwę serwera oraz nazwę prywatnej strefy DNS).
  "database__connection__password" :
  "@Microsoft.KeyVault(VaultName=__WSTAW__NAZWE__KEY__VAULT__;SecretName=__WSTAW_NAZWE_SEKRETU__)"
  "database__connection__ssl" : "true",
  "database__connection__user" : __TUTAJ_LOGIN__@__TUTAJ_NAZWA_BAZY__
  "paths_contentPath" : "/var/lib/storage",

"WEBSITES_ENABLE_APP_SERVICE_STORAGE" : "true",

- Ustawienia strony:
  always_on = true
  https2_enable = true
  docker_image = ghost
  docker_image_tag = 3.42.8
- W bloku identity wskaż type “SystemAssigned”. Zostanie on wykorzystany w kolejnym kroku do nadania dostępu aplikacji do Key Vaulta.
- W bloku storage_account skonfiguruj połącznie z file share. Jako ścieżkę wskaż: „/var/lib/storage”.
- Korzystając z virtual_network_subnet_id, wskaż podsieć z jakiej ma korzystać app service.

W następnym kroku utwórz Azure Key Vault Access Policy i nadaj uprawnienia tożsamości przypisanej do App Service uprawnienia do sekretów w Key Vault.

Zasoby które należy utworzyć (w kolejności):

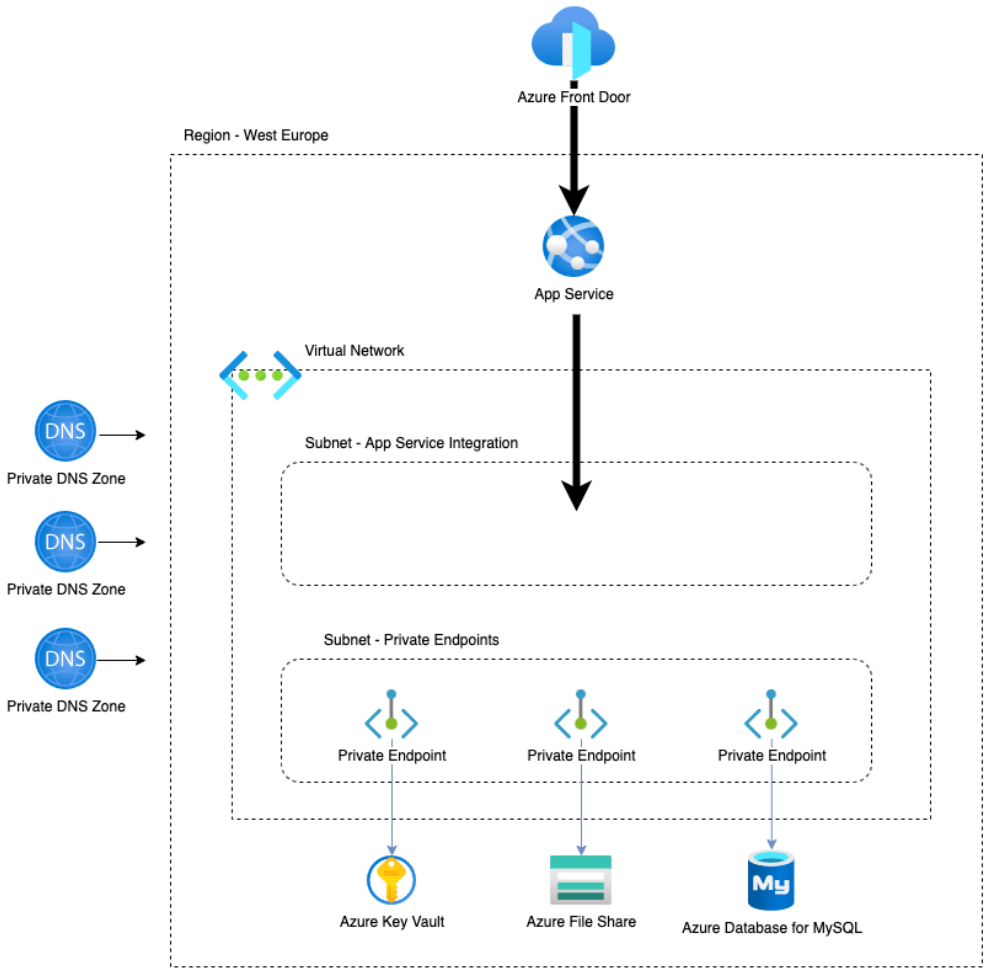
- App Service Plan
- App Service
- Azure Key Vault Access Policy

Przydatne linki:
Terraform dokumentacja App Service Plan
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/service_plan

Terraform dokumentacja App Service
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/linux_web_app

Terraform dokumentacja Azure Key Vault Access Policy
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/key_vault_access_policy

6. Zadanie: Utworzenie Azure Front Door



Rys. 6 Architektura Zad 6.

W ostatnim zadaniu utworzymy Azure Front Door.

Korzystając z dokumentacji zasobu, spróbuj odpowiednio skonfigurować wszystkie wymagane parametry.

Przydatne linki:
Terraform dokumentacja Azure Front Door
https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/frontdoor