

Dokumentacja wdrożenia infrastruktury Azure (Terraform) - Hub & Spoke

Data: 03.01.2026

Część 1: Prompty infrastrukturalne (Chronologicznie)

Poniżej znajdują się polecenia (prompty) wydane przez użytkownika, dotyczące tworzenia i modyfikacji zasobów infrastrukturalnych.

1. Inicjalizacja środowiska (Hub-Spoke, VNet, VM):

"jesteś specjalistą od azure , aks piszesz kod w terraformie wygeneruj mi na początek plik zdefinicja providera azure rm , tak baby w uruchomieniu terraforma podawać jako zmienną id subskrypcji , kod będę uruchomił lokalnie z laptopa , zaczne od az login , potem terraform init , na początek plik z providerem , szliet variables.tf , terraform ma definiować : 1.siec vnet - hub zmaszyną virtualną ubuntu , 2- siec spoke z 3 podsieciami , w której mają się mieścić AKS, nody i w trzeciej sieci będę umieszczał private endpointy od storage , kv vault ,i bazy danych , na tę chwilę generuj sieci i vm bez aks i pas"

2. Konfiguracja bezpieczeństwa (NSG i SSH):

"popraw definicje nsg nsg-hub-vm ssh na vm source [USER_IP_ADDRESS] destination ip address vm , dodaj zmienną w variable i tvar my_ipaddress"

3. Storage Account (Private Link, SMB):

"dodaj teraz do definicji storage account , lwr , file storage po smb , dostęp tylko prywatny , private link w sieci spoke snet-private-endpoints, utwórz private dns zone dla storage file i dodaj linki do dwóch sieci hub i spoke"

4. Poprawka dostępu sieciowego do Storage (Błąd 403):

"zrób tak , ustaw access do storage tylko z wybranych ip , gdzie wybrany ip to jest mój ip i popraw kod , popraw kod w związku z 'Usunąć cały zasób azure_rm_private_dns_a_record.storage_file - nie jest potrzebny, bo private endpoint to robi automatycznie przez private_dns_zone_group'"

5. Poprawka Service Endpoints vs Private Endpoint:

"używamy tylko Private Endpoint , usuń subnety z z network_rules.virtual_network_subnet_ids i zostaw tylko ip_rules. popraw kod"

6. Uszczelnienie NSG dla Private Endpoints:

"uszczelniamy nsg-spoke-private-endpoints ruch inbound do subnetu 1. usuwamy regułę że otarty dla wszystkich sieci i podsieci azurowych , 100 AllowVnetInbound Any Any VirtualNetwork VirtualNetwork Allow dodajemy że https, http wybranego mojego adresu ip i adresu serwera ubuntu w spoke , smb tylko z serwera w spoke."

7. Key Vault (RBAC, Private Link):

"analogicznie do storage zrób key vault , dostęp z publicznej sieci tylko po moim ip , private link w spoke-private-endpoints , private dns dla key vaulta podlinkowane do dwóch sieci spoke i hub , key vault ma używać do od stępu nie policy , dla testu nie ma mieć retencji , chce go kasować i reużywać nazwe , robimy testy nie produkcje"

8. Managed Identities:

"stwórz user managment identity 1 dla całego AKS , 2 dla kubelet identity , 3 dla podód do testowania workload identity na podach"

9. Azure Kubernetes Service (AKS) - Konfiguracja wstępna:

"teraz potrzebuje kod dla azure kubernetes , dostęp publiczny ale tylkozmojego adresu ip , AKS musi używać Azure CNI (VNET mode) + Azure Network Policy Manager nody i pody w sieci spoke w podsieci snet-aks-nodes , sam aks w sieci snet-aks , dwie node poole - system 1 skalowany do 3 nodów w podsieci - snet-aks , work skalowany od 1 do 3 w snet-aks-nodes , nody po taniości seria B 2 cpu 4-8 GB ram , czy można zrobić cluster z dostępem mieszanym po publicznym i prywatnym (private link) ?"

10. Poprawka uprawnień AKS Identity:

"tak dodaj" (W kontekście dodania roli 'Managed Identity Operator').

11. Azure SQL Database (Wymagania i Implementacja):

"potrzebuje najtańszy sql server , ale wspierający azure ad plus można go zarządzać przez azure identity user, co proponujesz nie pisz kodu"
"zrób to w kodzie tylko prywatny dostęp po private linku , private link w snet privateendpoint , dns private zone podlinkowane do dwóch sieci" (Wybór opcji Serverless).

12. Weryfikacja dostępu do Internetu (Outbound):

"w obecnej konfiguracji jak nody pody uzyskują dostęp do internetu"
"zrób opcje 2 Opcja 2: Azure Load Balancer Outbound Rules [...] moje wątpliwości budzi fakt że powstał load balancer w rg z nodami ma jakieś backendy ma outbound rules"

13. Zmiana modelu sieciowego AKS (Usunięcie Overlay):

"popraw policy bo nody i pody miały dostawać adresy z subnetów a nie z wewnętrzne z clustra"

14. Aktualizacja NSG dla SQL:

"nsg-spoke-private-endpoints do tej nsg dodaj reguły odnośnie dostępu do serwera sql z stacji w spoke oraz z podsieci gdzie będą pody z nodów work"

Część 2: Analiza błędów Terraform

Zestawienie błędów napotkanych podczas wdrożenia wraz z wyjaśnieniem i zastosowanym rozwiązaniem.

Błąd 1: Literówka w konfiguracji Storage

- **Komunikat:** Error: expected account_replication_type to be one of ["LRS" ...], got LZR
- **Opis:** Użyto niepoprawnego kodu dla typu replikacji.
- **Rozwiązanie:** Zmiana LZR na LRS.

Błąd 2: Blokada tworzenia File Share (Network Access)

- **Komunikat:** unexpected status 403 ... This request is not authorized to perform this operation.
- **Opis:** Storage Account został utworzony z zablokowanym dostępem publicznym (public_network_access_enabled = false), co uniemożliwiło Terraformowi (uruchamianemu z lokalnego IP) utworzenie zasobu File Share.
- **Rozwiązanie:** Dodanie reguł sieciowych (network_rules) zezwalających na dostęp z adresu IP użytkownika.

Błąd 3: Konflikt rekordów DNS

- **Komunikat:** Error: A resource with the ID ../privateDnsZones/.../A/... already exists
- **Opis:** Terraform próbował utworzyć rekord A w strefie DNS, który został już automatycznie utworzony przez zasób Private Endpoint.
- **Rozwiązanie:** Usunięcie manualnej definicji zasobu azurerm_private_dns_a_record.

Błąd 4: Brak Service Endpoints dla reguł VNet

- **Komunikat:** SubnetsHaveNoServiceEndpointsConfigured ... Add Microsoft.Storage to subnet's ServiceEndpoints collection
- **Opis:** Próba dodania podsieci do ACL Storage Account, podczas gdy podsieć nie miała włączonego Service Endpoint dla Storage.
- **Rozwiązanie:** Użytkownik zdecydował o usunięciu podsieci z ACL i poleganiu wyłącznie na Private Endpoint.

Błąd 5: Niepoprawny argument w AKS

- **Komunikat:** Error: Unsupported argument ... An argument named "automatic_upgrade_channel" is not expected here.
- **Opis:** Użyto nazwy parametru niekompatybilnej z wersją providera.
- **Rozwiązanie:** Zmiana na automatic_channel_upgrade.

Błąd 6: Brak uprawnień tożsamości klastra

- **Komunikat:** CustomKubeletIdentityMissingPermissionError ... must be granted 'Managed Identity Operator' role
 - **Opis:** Tożsamość "Control Plane" klastra AKS nie miała uprawnień do przypisywania tożsamości "Kubelet Identity" do maszyn wirtualnych (nodów).
 - **Rozwiązanie:** Dodanie zasobu azurerm_role_assignment nadającego rolę "Managed Identity Operator".
-

Część 3: Pełny zapis rozmowy (Zanonimizowany)

rmarszolek: jesteś specjalistą od azure , aks piszesz kod w terraformie wygeneruj mi na początek plik zdefinicja providera azure rm , tak baby w uruchomieniu terraforma podawać jako zmienna id subskrypcji , kod będę uruchomił lokalnie z laptopa , zaczne od az login , potem terraform init , na początek plik z providerem , szczerze variables.tf , terraform ma definiować : 1.siec vnet - hub zmaszyną virtualną ubuntu , 2- siec spoke z 3 podsieciami , w której mają się mieścić AKS, nody i w trzeciej sieci będę umieszczał private endpointy od storage , kv vault ,i bazy danych , na tę chwilę generuj sieci i vm bez aks i pas

GitHub Copilot: Rozumiem! Stworzę dla Ciebie infrastrukturę w Terraform z topologią hub-spoke. (Generowanie plików: *provider.tf, variables.tf, main.tf, network-hub.tf, network-spoke.tf, peering, outputs*)

rmarszolek: popraw definicje nsg nsg-hub-vm ssh na vm source [USER_IP_ADDRESS] destination ip address vm , dodaj zmienna w variable i tvar my_ipaddress

GitHub Copilot: Poprawię konfigurację NSG dla SSH, aby używać konkretnego IP zamiast "*". (Aktualizacja *variables.tf, network-hub.tf*)

rmarszolek: dodaj teraz do defini storage account , lzo , file storage po smb , dostęp tylko prywatny , private link w sieci spoke subnet-private-endpoints, utwórz private dns zone dla storage file i dodaj linki do dwóch sie hub i spoke ,

GitHub Copilot: Dodam storage account z Azure Files (SMB), private endpoint w sieci spoke oraz Private DNS Zone. (Generowanie *storage.tf*)

rmarszolek: popraw ten błąd jest literów Error: expected account_replication_type to be one of ["LRS" "ZRS" "GRS" "RAGRS" "GZRS" "RAGZRS"], got LZR

GitHub Copilot: Poprawione! Zmieniłem LZR na LRS.

rmarszolek: błędy są " |

| Error: checking for existing File Share "fileshare" ... unexpected status 403 ...

| Error: A resource with the ID .../privateDnsZones/privatelink.file.core.windows.net/A/stdevrn51p5" already exists ...

" | " nie poprawiaj kodu tylko analizuj

GitHub Copilot: Analizuję błędy:

1. 403 Authorization Failure - Storage ma zablokowany dostęp publiczny, Terraform nie może utworzyć share.
2. Rekord DNS A już istnieje - Private Endpoint tworzy go automatycznie.

rmarszolek: zrób tak , ustaw access do storage tylko z wybranych ip , gdzie wybrany ip to jest mój ip i popraw kod , popraw kod w związku z "Usunąć cały zasób azurerm_private_dns_a_record.storage_file - nie jest potrzebny, bo private endpoint to robi automatycznie przez private_dns_zone_group"

GitHub Copilot: Poprawione! Dodałem network_rules i usunąłem manualny rekord DNS.

rmarszolek: o co chodzi w tym błędzie Error: updating Storage Account ... NetworkAclsValidationFailure: ... SubnetsHaveNoServiceEndpointsConfigured ...

GitHub Copilot: Problem: Brak Service Endpoints na podsieciach, które próbujesz dodać do ACL Storage Account.

rmarszolek: używamy tylko Private Endpoint , usuń subnety z z network_rules.virtual_network_subnet_ids i zostaw tylko ip_rules. popraw kod

GitHub Copilot: Poprawione! Usunąłem podsieci z reguł, zostawiłem tylko IP.

rmarszolek: uszczelniamy nsg-spoke-private-endpoints ruch inbound do subnetu 1. usuwamy regułę że otarty dla wszystkich sieci i podsieci azurowych [...] dodajemy że https, http wybranego mojego adresu ip i adresu serwera ubuntu w spoke , smb tylko zservera w spoke.

GitHub Copilot: Poprawione! Uszczelnię NSG dla subnet-private-endpoints.

rmarszolek: analogicznie do storage zrób key vault , dostęp z publicznej sieci tylko po moim ip , private link w spoke-private-endpoints , private dns dla key vaulta podlinkowane do dwóch sieci spoke i hub , key vault ma używaćbac do od stępu nie policy [...]

GitHub Copilot: Gotowe! Dodałem Key Vault z RBAC, soft-delete i Private Endpoint.

rmarszolek: stwórz user management identity 1 dla całego AKS , 2 dla kubelet identity , 3 dla podód do testowania workload identity na podach

GitHub Copilot: Gotowe! Stworzyłem 3 tożsamości (User Assigned Managed Identities).

rmarszolek: teraz potrzebuje kod dla azure kubernetes , dostęp publiczny ale tylkozmojego adresu ip , AKS musi używać Azure CNI (VNET mode) + Azure Network Policy Manager nody i pody w sieci spoke w podsieci subnet-aks-nodes , sam aks w sieci subnet-aks [...]

GitHub Copilot: Gotowe! Stworzyłem klaster AKS z odpowiednią konfiguracją sieciową i Node Pools.

rmarszolek: sprawdź ten błąd , nie poprawiał kodu
| Error: Unsupported argument ... automatic_upgrade_channel = "patch" ...

GitHub Copilot: Błąd wynika z użycia złej nazwy parametru. Powinno być automatic_channel_upgrade.

rmarszolek: tak podmien kod

GitHub Copilot: Poprawione.

rmarszolek: potrzebuje najtańszy sql server , ale wspierający azure ad plus można go zarządzać przez azure identity user, co proponujesz nie pisz kodu

GitHub Copilot: Proponuję Azure SQL Database - Serverless (General Purpose). Płacisz tylko za użycie, posiada auto-pause.

rmarszolek: wracamy do kodu jest błąd "Error: creating Kubernetes Cluster ... CustomKubeletIdentityMissingPermissionError ...

GitHub Copilot: Problem: Cluster Identity nie ma uprawnień do przypisywania Kubelet Identity. Trzeba dodać rolę "Managed Identity Operator".

rmarszolek: tak dodaj

GitHub Copilot: Dodano Role Assignment.

rmarszolek: podaj az cli do sprawdzanie jakie wersja aks mogą mieć w west europe

GitHub Copilot: az aks get-versions --location westeurope --output table

rmarszolek: 1. Azure SQL Database - Serverless (NAJLEPSZA OPCJA) [...] zrób to w kodzie tylko prywatny dostęp po private linku , private link w subnet privateendpoint , dns private zone podlinkowane

do dówch sieci

GitHub Copilot: Gotowe! Dodałem SQL Database Serverless z Private Link i integracją Azure AD.

rmarszolek: w obecnej konfiguracji jak nody pody uzyskują dostęp do internetu

GitHub Copilot: W obecnej konfiguracji nody mogą mieć dostęp przez domyślny Load Balancer (jeśli Standard SKU), ale pody zależnie od CNI. Domyślnie w AKS Standard LB tworzy outbound rules.

rmarszolek: zrób opcje 2 Opcja 2: Azure Load Balancer Outbound Rules [...] moje wątpliwości budzi fakt że powstał load balancer w rg z nodami ma jakieś backendy ma outbound rules

GitHub Copilot: Potwierdzam, że AKS domyślnie tworzy Load Balancer z regułami wyjściowymi. Można to skonfigurować dokładniej przez load_balancer_profile, ale dostęp już powinien działać.

rmarszolek: popraw policy bo nody i pody miały dostawać adresy z subnetów a nie z wewnętrzne z clustra

GitHub Copilot: Poprawione! Usunąłem network_plugin_mode = "overlay". Teraz używamy czystego Azure CNI, gdzie pody pobierają IP bezpośrednio z VNet.

rmarszolek: nsg-spoke-private-endpoints do tej nsg dodaj reguły odnośnie dostępu do serwera sql z stacji w spoke oraz z podsieci gdzie będą pody z nodów work ,

GitHub Copilot: Zaktualizowano NSG o reguły dla SQL.