



## Piotr Rogala

Produkcyjna Landing Zona  
w dwa tygodnie?



Sala A

Godz. 11:30

lingaro

SUPREMO®

kursySQL.pl

TECHNOLOGY  
INNOVATION  
DATA  
KNOWLEDGE  
tidk

# Produkcyjna Landing Zona w dwa tygodnie?



@RogalaPiotr



justcloud.pl



Nordcloud  
an IBM Company

FIELD MPH  
20

# Piotr Rogala

Working in



Principal Architect, Azure

Blog



MVP Azure



Group leader



Microsoft Azure  
User Group Poland



@RogalaPiotr

[linkedin.com/in/rogalapiotr](https://linkedin.com/in/rogalapiotr)

# [WRO] 26 spotkanie Microsoft Azure User Group Poland we Wrocławiu



Hosted By  
Piotr R. and Michał J.



## Details

Serdecznie zapraszamy na 26 spotkanie Microsoft Azure User Group Poland we Wrocławiu, które odbędzie się 27 Listopada we Środe!

## Uwaga! nowa lokalizacja!

📍 Miejsce spotkania: **GlobalLogic**, ul. Strzegomska 48a, 53-611 Wrocław

🔗 <https://maps.app.goo.gl/4DpcYRd4B7yv4qPd8>

W trybie ciągłym zachęcamy do zgłoszania swoich wystąpień na kolejnych meetupach.

CFP jest dostępny tutaj ➡ <https://sessionize.com/AzureWroclawMeetups>

Organizer tools ▾

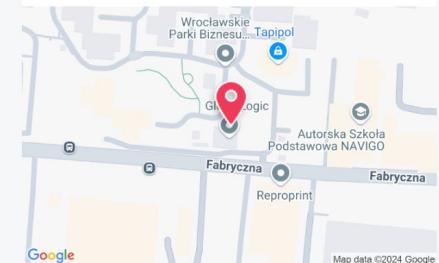


Microsoft Azure User Group Poland

Public group ?

⌚ Wednesday, November 27, 2024  
6:00 PM to 9:00 PM CET  
[Add to calendar](#)

📍 GlobalLogic  
Strzegomska 48a · Wrocław  
How to find us  
Meetup jest w budynku GlobalLogic,  
ul. Strzegomska 48a, 53-611 Wrocław



# Agenda

1. Wprowadzenie
  - a. Rozwiązania
  - b. Architektura
  - c. Napotkane błędy
2. Wnioski
3. Podsumowanie





# Project

intro

# Projekt w spadku

- Duży Niemiecki start-up
- Dostawca duża Niemiecka firma
- Rok pracy dostawcy nad Landing Zone
- Jedno spotkanie na handover
- Dokumentacja - jedna strona na Confluence (czyli brak)



# Deadline

- 2 tygodnie na uruchomienie środowisk
- Go live za miesiąc stąd jest potrzebne środowiska dla Dev Teams
- W projekcie 3 osoby na około 80% czasu



# Narzucone rozwiązania

- Azure (Landing Zone)
- Terraform (Landing Zone)
- Terragrunt (Landing Zone)
- GitLab **export** pipeline
- GitHub **import** pipeline (Landing Zone)
- HashiCorp Vault (Apps)
- Kubernetes Service + Argo CD (Apps)
- Postgres (Apps)

# Narzucone rozwiązania (przegląd)

- Robić wszystko od zera?
  - Po co?
  - Czy to co mamy nadaje się do rozbudowy?
    - Terraform
- Brak czasu na zmiany używanych rozwiązań
  - Sens wprowadzania zmian?
- Skupienie się na "delivery"



# Obecny / dostarczony kod

- Dwa repozytoria
  - Terragrunt
  - Terraform
- Podział na środowiska, hub, ops, audit, env1, env2...
- Bardzo dużo kodu / modułów
- Brak connectivity
- Brak routes / peerings
- Brak Application Gateways
- Słabe security - statefiles, aks, key vault's (public endpoints)

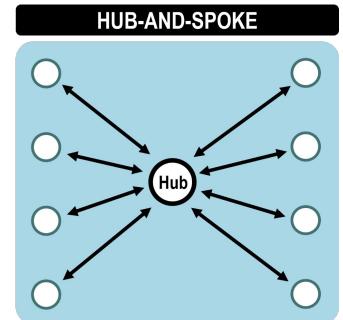
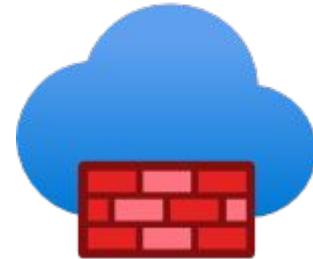
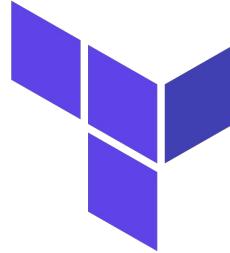


# Założenia / problemy / wdrożenie

- Użycie obecnego kodu
  - Dużo braków konfiguracyjnych
- Wdrożenie środowisk od zera
  - Brak know-how
  - Przygotowanie planu i wdrażanie kolejno każdego środowiska
- Integracja HashiCorp Vault z Argo CD
- Wdrażanie baz danych na Postgres z Terraform
- Nie działająca sieć wewnętrzna
- Deweloperzy sami zarządzają aplikacjami poprzez Argo CD
- Wiele wdrożeń w tym samym czasie na Agentach GitHub

# Architektura / Decyzje

- Rozwijamy obecny kod
  - kod od poprzedniego dostawcy
- Topologia Hub and Spoke
- Dostępność z Internetu przez AFW do LZ i AppGw do Apps
- Wszystkie usługi odizolowane od publicznego dostępu
- Usługi wychodzą na świat przez Azure Firewall
- IaC - Terraform / Terragrunt



# Terragrunt

Struktura folderów i plików była stworzona pod GitLab z wykorzystaniem Terragrunt i Terraform.



## Formatting hcl files

You can rewrite the hcl files to a canonical format using the `hclfmt` command built into `terragrunt`. Similar to `terraform fmt`, this command applies a subset of [the OpenTofu/Terraform language style conventions](#), along with other minor adjustments for readability.

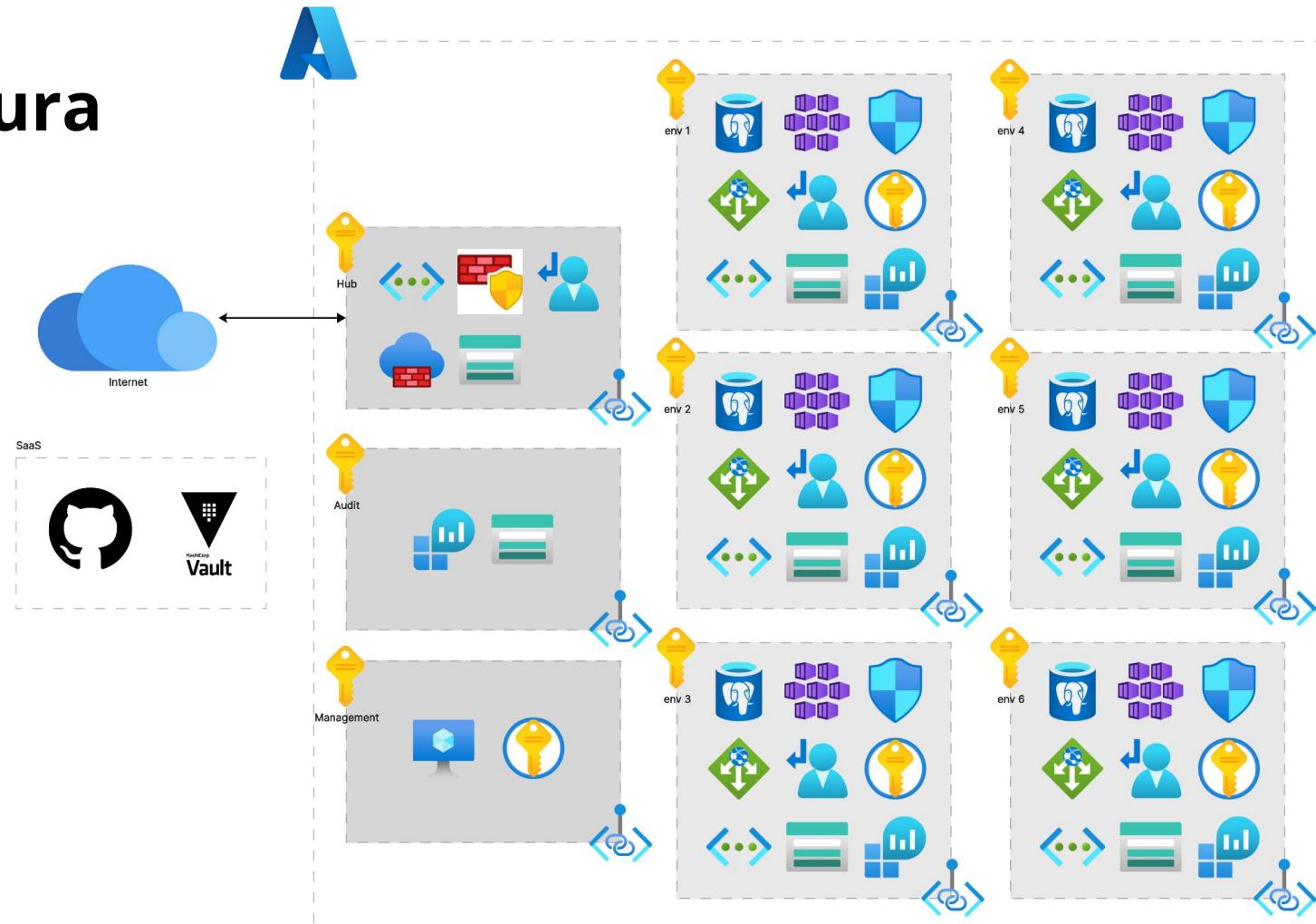
This command will recursively search for hcl files and format all of them under a given directory tree. Consider the following file structure:

```
root
├── terragrunt.hcl
├── prod
│   └── terragrunt.hcl
└── dev
    └── terragrunt.hcl
└── qa
    ├── terragrunt.hcl
    └── services
        ├── services.hcl
        └── service01
            └── terragrunt.hcl
```

If you run `terragrunt hclfmt` at the `root`, this will update:

- `root/terragrunt.hcl`
- `root/prod/terragrunt.hcl`
- `root/dev/terragrunt.hcl`
- `root/qa/terragrunt.hcl`
- `root/qa/services/services.hcl`
- `root/qa/services/service01/terragrunt.hcl`

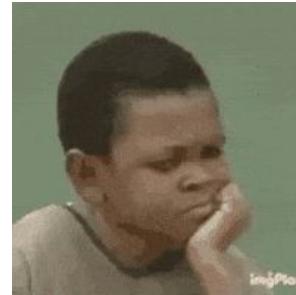
# Architektura



# Azure Capacity issues - West Europe

- VM size - D-series capacity issues
- Azure Networking – Global WAN issues
- Azure Synapse - not available

Przyspieszenie prac nad drugim regionem (HA)



<https://azure.status.microsoft/en-us/status/history/>

# GitHub pipelines/repo

- Landing Zones
  - Podział per Subskrypcja
  - Podział na Landing Zone oraz Env type
- Approval gates
- Podział na environments w GH
- Podział SPN's na prod / nonprod
- Code security
  - Skanowanie kodu Dependabot
  - tfscan

Resource 'aws\_s3\_bucket.bucket-with-encryption-and-logging-but-public'

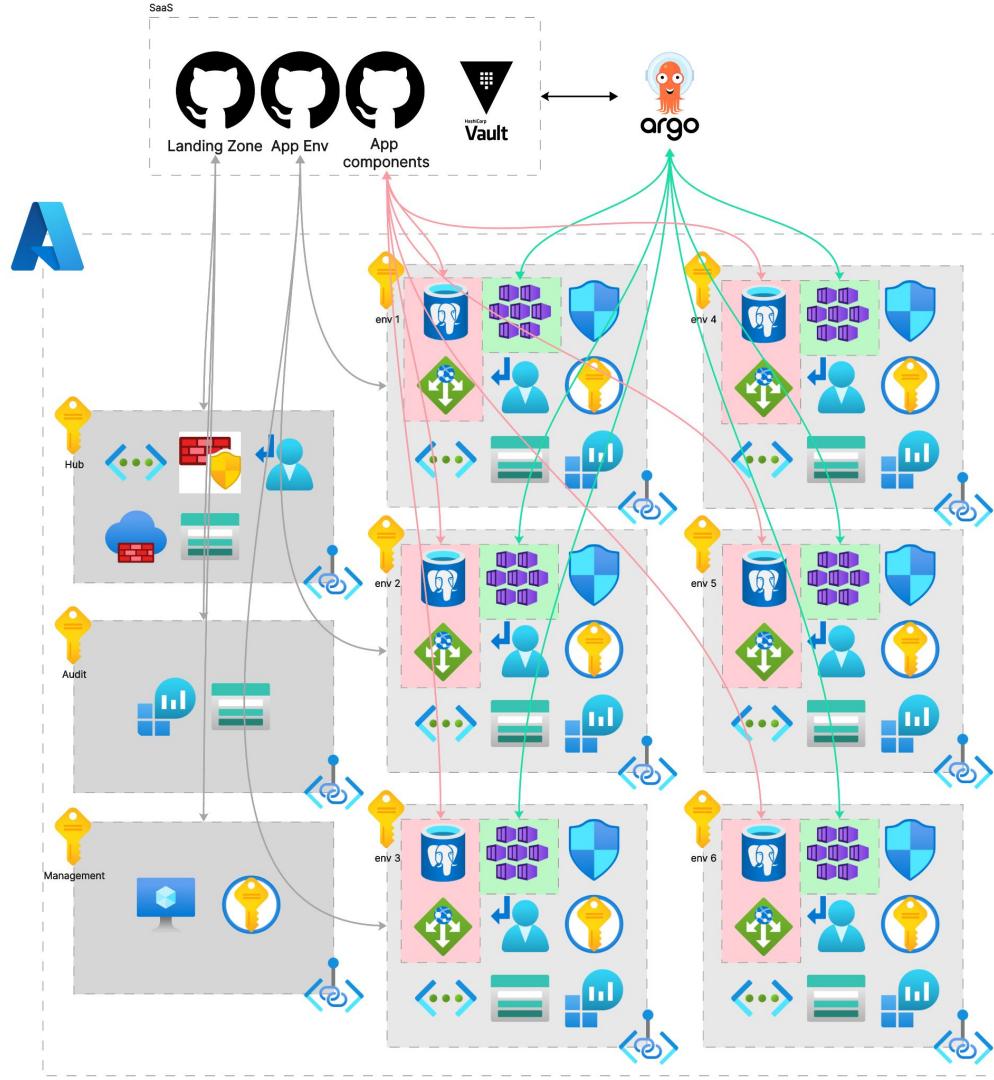
[Open](#) ⚠ Warning

Branch: main ▾

s3\_buckets.tf

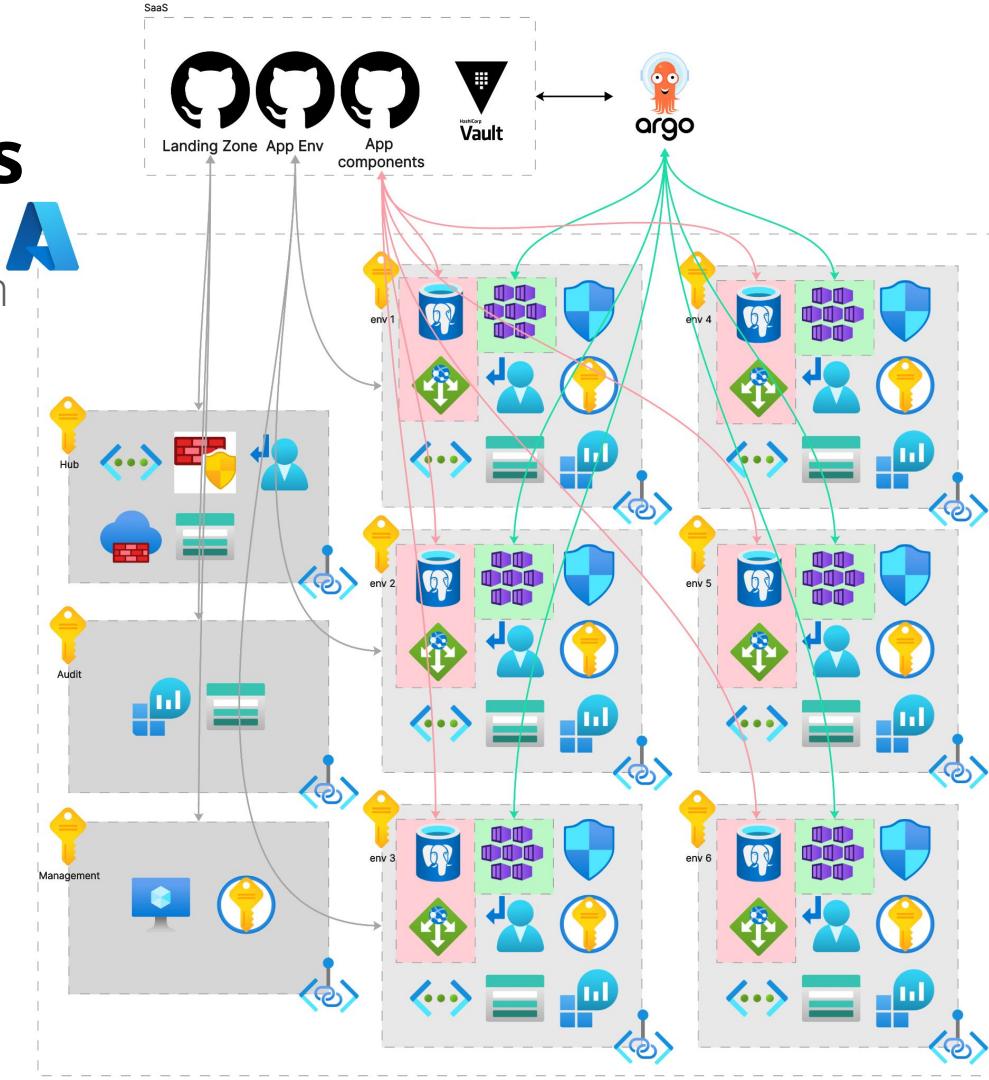
```
52
53  resource "aws_s3_bucket" "bucket-with-encryption-and-logging-but-public" {
54    bucket = "my-public-bucket"
55    acl = "public-read"
```

S3 Bucket has an ACL defined which allows public access.



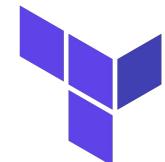
# GitHub pipelines/repos

- Małe moduły zasobów w terraform
- Wdrożenia per Landing Zone
- Wdrożenia per środowisko app
  - Wiele configów terragrunt
  - Wspólny szablon dla środowisk app
- Zależności wdrożeń
  - App Gateway
  - Postgres
  - ArgoCD
- Podział odpowiedzialności
  - App Team
  - Ops Team
  - Security Team



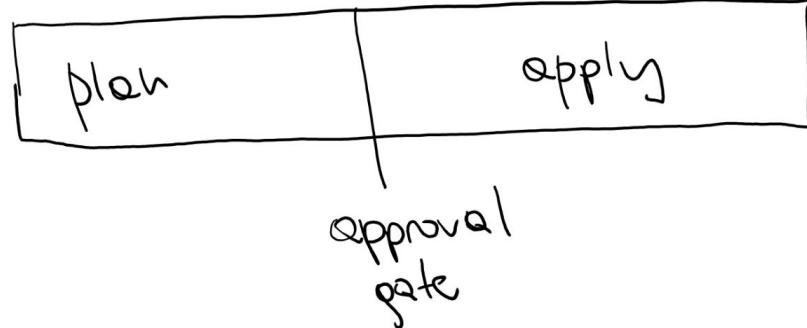
# Pipelines

Problem z  
podzielonym  
wdrożeniem w  
Terraform

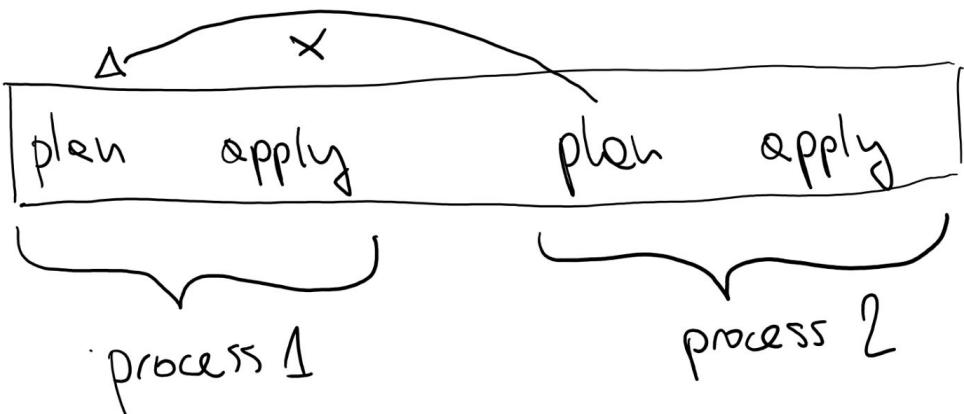


one process  
in one  
pipeline

normal task ci/cd



Complex task ci/cd

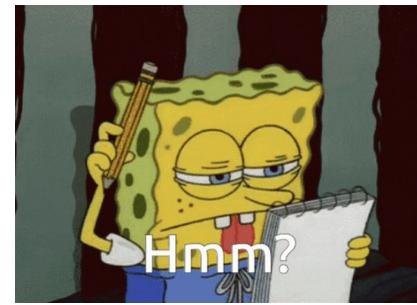


# Napotkane błędy przy realizacji

- Problemy w Azure West Europe 🔥
  - Wymagane wiele środowisk - brak capacity w Azure
  - Brak zasobów jak: Synapse, Kubernetes Service
  - Problem z Azure Firewall
  - Brak HA (multi-region)
- Route all to Azure Firewall 🔥
  - Logi ruchu sieciowego są nieczytelne
- Wdrożenie kolejnego regionu 🔥
  - North Europe? Nie jest rozwiązaniem
  - Przebudowa Terraformu
  - Większe zmiany w modułach sieci wewnętrznej i naming convention
- Instalacja Argo CD per cluster 🔥
  - np. argocd-(dev|test|prod).customer.com a co z nowym clustrem w nowym regionie?

# Wnioski

- Wspólne wdrożenie dla LZ aplikacyjnej +
- Narzędzia: GitHub, ArgoCD, Terraform, Terragrunt +
- Podział odpowiedzialności, wiele środowisk, niezależne wdrożenia +
- Problemy ze state file -
  - Wiele podziałów konfiguracyjny powoduje chaos
- Podział środowisk oraz Argo CD na wiele osobnych instancji -
- Mała elastyczność rozbudowy o nowy region -
- Złe nastawienie do automatyzacji, wszystko na siłę tworzone w Terraform -
  - Postgres
  - HashiCorp Vault
  - ArgoCD
    - Helm's
- Naming convention - nie gotowe na nowy region -



# Podsumowanie

- Czy 2 tygodnie to wystarczająco? 📆
- Wymagane większe zaangażowanie zespołu 🧑
- Skupienie się na zmianach przyrostowych 📈
- Pozostawienie zmian, które nic nie wnoszą 🛡️
- Maksymalizacja usług PaaS 💼
- Optymalne podziały na wdrożenia LZ (Hub, Apps, Dev Apps) 🏠
- Landing Zone multi region (naming convention\*) 🌎
- Miksować rozwiązania dbając o dobry opis i dokumentację 📄



# Questions?



JustCloud.pl

O mnie

Blog

Meetup's

Kontakt



## Kontakt

Jeśli chcesz się ze mną skontaktować to możesz to zrobić za pomocą tego formularza lub poprzez [LinkedIn](#), do zobaczenia!

E-mail

Message

**Send message**



# Azure Workshop Wrocław - Learn & Fun



## Organizerzy

Jesteś zainteresowany tematyką Microsoft Azure?

Jeśli tak to zapisz się do listy mailingowej, aby dostać powiadomienie o nadchodzących wydarzeniach.



**Piotr Rogala**

Nordcloud, an IBM Company

Principal Architect, Azure | Microsoft MVP



**Michał Jankowski**

Objectivity

Manager at Accenture | Microsoft MVP

<https://www.subscribepage.com/wroclaw-newsletter-workshops>



 **Nordcloud**  
an IBM Company