infoShare ACADEMY

AWS Cloud

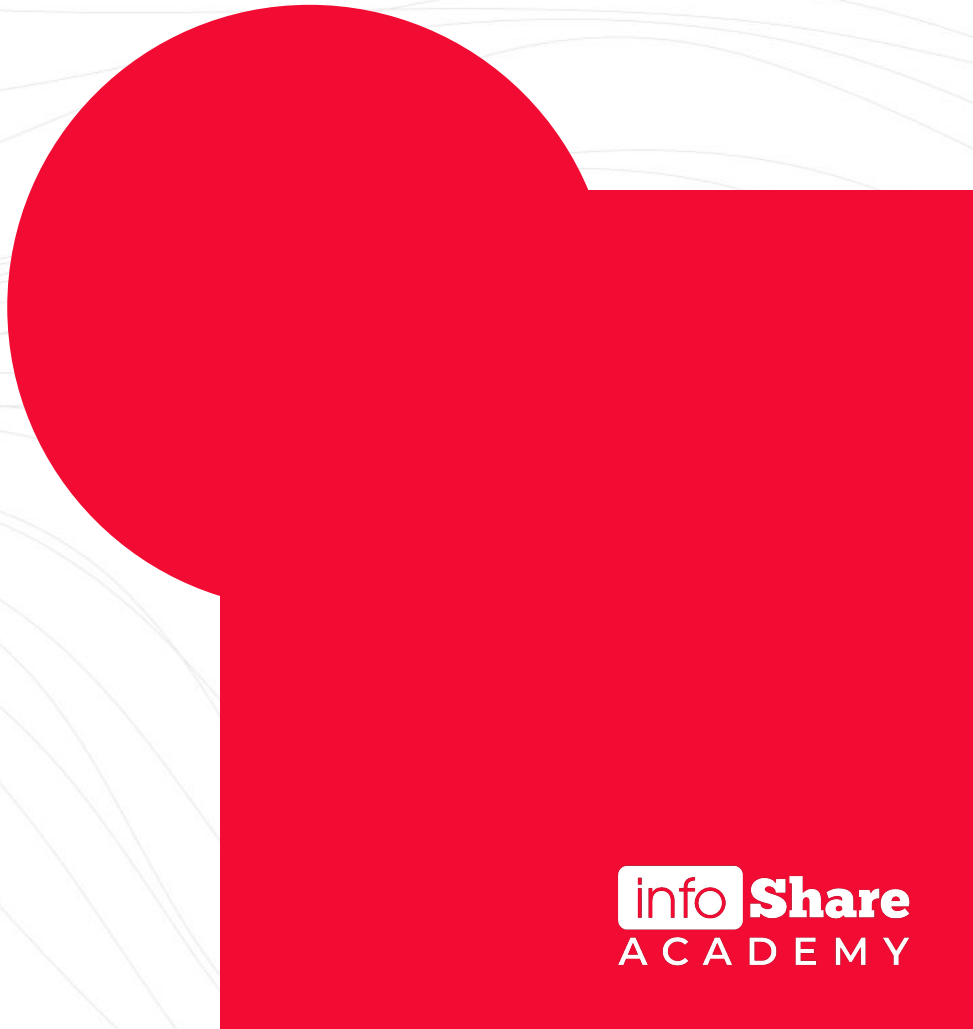
infoShare Academy

infoShareAcademy.com

HELLO

Maciej Małek

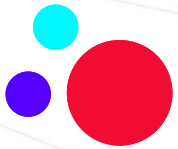
From SysAdmin to AWS DevOps Engineer and Architect



Amazon Web Services

Podstawowe informacje.

infoShareAcademy.com



Konta AWS

Numer konta AWS to ciąg 12 cyfr, ale nie jest numerem w sensie matematycznym.

Konto AWS nie służy do separacji sieciowej.

Konta AWS służą do podziału funkcjonalnego

- na role - konto dla zespołu Security, dla kopii zapasowych (backup), dla wspólnych usług (autoryzacja, DNS), konto administracyjne.
- na przeznaczenie - konto produkcyjne, konta dla programistów, konta dla testerów

infoShare ACADEMY

Regions / Availability Zones

Region

- obszar geograficzny w którym znajdują się serwerownie AWS
- w sumie jest 31 regiony (marzec 2023)
- jest 32 Local Zones (ograniczona ilość serwisów)
- przykład regionu - eu-west-1 Europe (Ireland)

Serwerownia - Data Center / Availability Zone

- w każdym regionie jest od 2 do 6 AZs
- średnio to 3 AZs w regionie
- przykład eu-central-1a (lub AZ ID = uec1-az2)
- oddzielone max. 100km od siebie

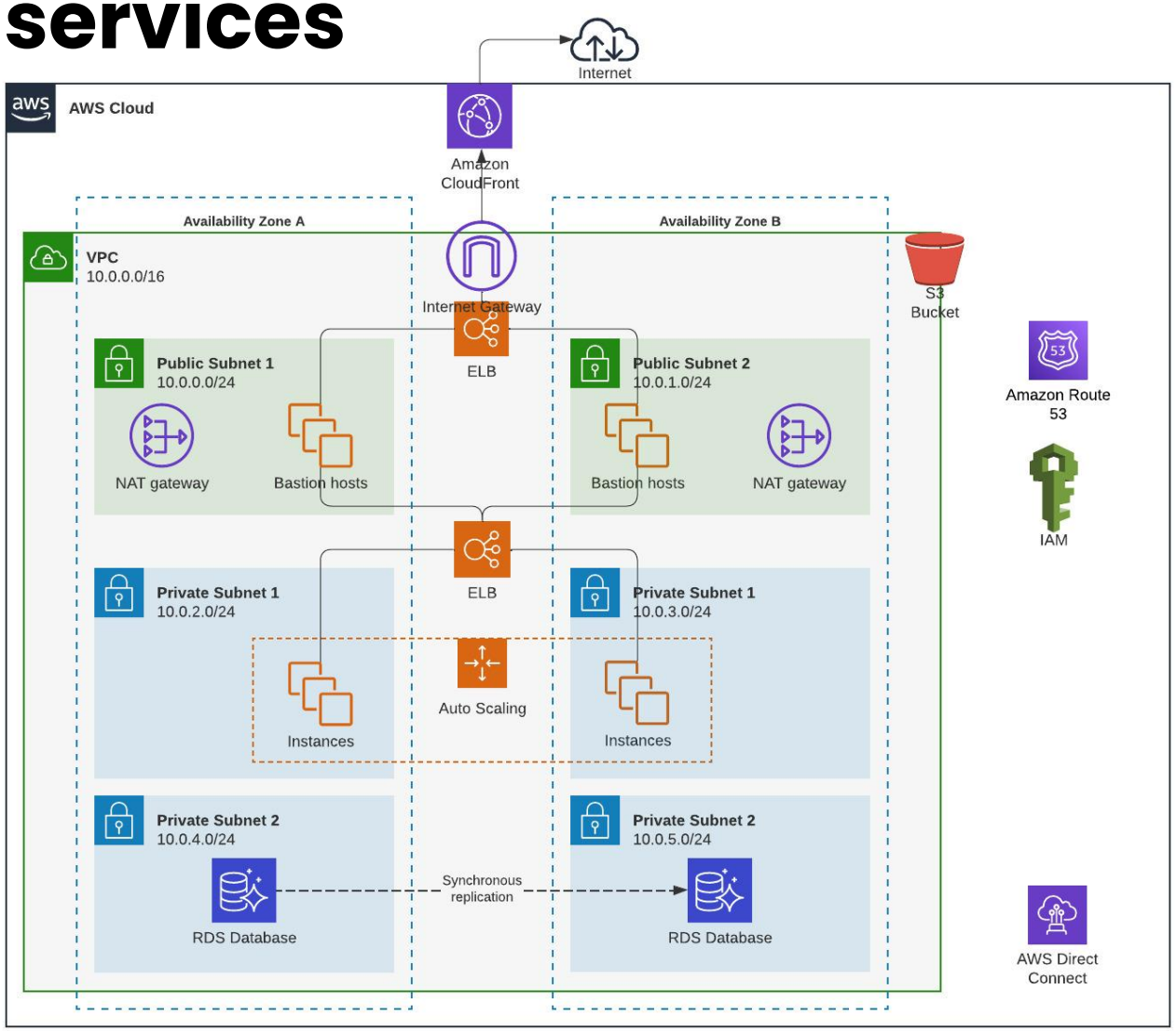
infoShare ACADEMY

Regional vs Global services

Aktualnie AWS oferuje ponad 200 serwisów.

Non-regional / Global services

- Amazon CloudFront
- Amazon Route53
- IAM
- S3
- AWS Support Center
- Trusted Advisor
- AWS Direct Connect
- AWS Cost Management



02. Network

infoShareAcademy.com

VPC / Subnets

VPC – Virtual Private Cloud

Służy do separacji sieciowej na najwyższym poziomie np.

- dla systemów dostępnych z Internetu,
- dla systemów tylko wewnątrz firmy
- dedykowane dla konkretnych aplikacji lub zespołów.

Najczęściej używamy następujących zakresów adresów IP.

- Sieć prywatna klasa A - 10.0.0.0/8 (zakres od 10.0.0.1 do 10.255.255.254) lub jej części
- Sieć prywatna klasa B - 172.16.0.0/12 (zakres od 172.16.0.1 do 172.31.254.254) lub jej części

VPC musi znajdować się tylko w jednym regionie (np. EU Frankfurt)

Subnets

Subnet czyli podsieć - najmniejsza część sieci zlokalizowana w jednej serwerowni (Availability Zone) wewnątrz VPC.

To w niej znajdują się karty sieciowe (NICs) podłączone do serwerów.

Jej zakres adresacji musi mieścić się wewnątrz wyznaczonego VPC.

Subnet jest zlokalizowany tylko w jednym AZ (np. eu-central-1b)

infoShare ACADEMY

Inne elementy sieciowe

Internet Gateway

- urządzenie sieciowe (router), które pozwala na ruch wchodzący z Internetu do VPC jak i ruch wychodzący z VPC do Internetu

NAT Gateway

- urządzenie, które pozwala na ruch wychodzący z VPC do Internetu.

Route Table (tablica routingu)

- spis tras w pomiędzy subnetem a Internet Gateway / NAT Gateway / Gateway Endpoint

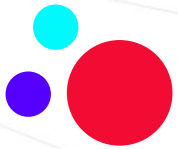
Elastic IPs

- statyczny, zewnętrzny adres IP

Peering connection

- połączenie w warstwie 3 między dwoma VPC (mogą być w różnych kontach i w różnych regionach)
- zakresy sieciowe nie mogą na siebie nachodzić
- nie można tworzyć połączeń szeregowych, do tego jest Transit Gateway

infoShare ACADEMY



Cwiczenie

Tworzymy VPC w wybrany regionie (10.0.0.0/24)
Tworzymy 2 x Subnet'y (10.0.0.0/26 oraz 10.0.0.64/26)

Opcja 1 - manualnie przy pomocy AWS Management Console
Opcja 2 - przy pomocy Terraform

infoShare ACADEMY

Inne elementy sieciowe – Endpoints

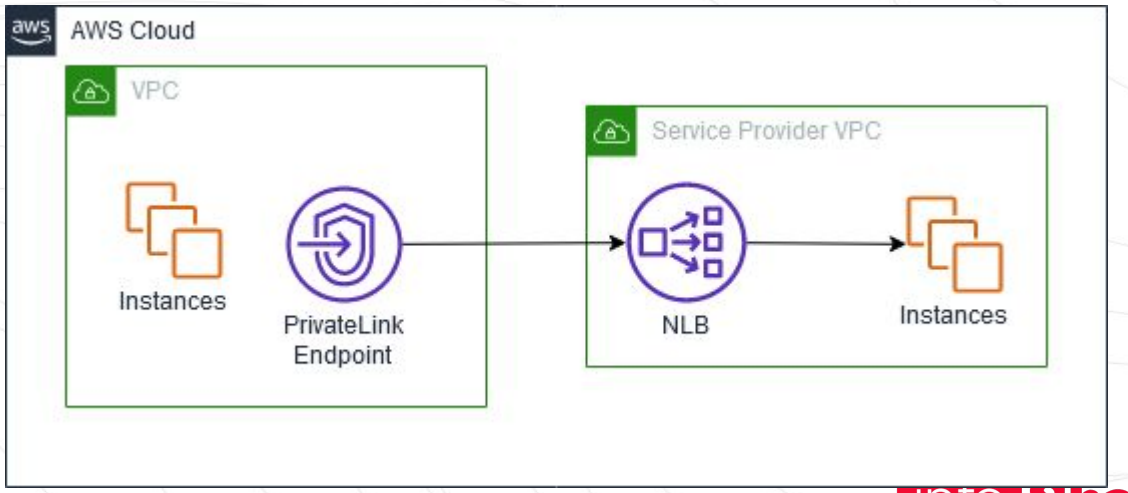
Endpoints

- połączenie do serwisów AWS
  - Interface (Lambda, ECS, ECR, SSM)
  - Gateway (S3, DynamoDB)
- połączenie do service endpoints (VPC Private Link)

Endpoint services

- udostępnianie swojego serwisu, aplikacji d

VPC Private Link - tunel do aplikacji / serwisu



InfoShare ACADEMY

Cwiczenie

Tworzymy VPC Endpoints

- SSM
- SSMMESSAGES
- EC2MESSAGES
- S3

infoShare ACADEMY

Inne elementy sieciowe

NACL - Network Access Control List

- stosuje się aby kontrolować ruch do i z subnetow
- **stateless** - czyli nie zachowuje stanu połączenia
- **default - wszystko odblokowane**
  https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#default-network-acl

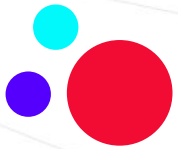
Security Group

- stosuje się aby kontrolować ruch do i z urządzeń / resource'ow (np. instancji EC2, baza danych RDS, Lambda działająca w VPC)
- **stateful** - zachowuje stan połączenia, czyli kiedy otwieramy połączenie na port 80 to nie musimy już definiować ruchu wychodzącego.
- **default - wszystko zablokowane**, regułki na ingres i egress odblokowywuja dostep.

infoShare ACADEMY

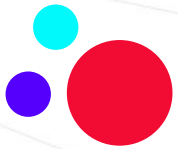
03. Security

infoShareAcademy.com



Security, Management & Governance

- CloudTrail - śledzenie wszystkich API calls na koncie
- Config - śledzenie zmian wszystkich resourców na koncie
- AWS Health Dashboard - monitoring serwisów AWS'owych
- AWS Organizations - zarządzanie kontami AWS
- Key Management Service (KMS) - zarządzanie kluczami szyfrującymi
- Certificate Manager - certyfikaty SSL dla Load Balancers i CloudFront
- Guard Duty - Intelligent Threat Detection
- WAF & Shield - ochrona przed atakami m.in. DDos
- AWS Inspector - skanowanie EC2 i ECR pod względem znanych podatności (np. CVEs)
- oraz ....



IAM - Identity and Access Management

IAM Users

- dla ludzi
- możliwość logowania się do AWS Management Console (login / haslo)
- programowalny dostęp przy pomocy Security Credentials (Access Key ID i Secret Access Key)
- w korporacjach nie są używane

IAM Roles

- może być używane przez instancje (z IAM EC2 Profile), serwisy, funkcje lub pośrednio przez ludzi (Federated Access do AWS Management Console)
- służy do nadawania uprawnień resource'om lub serwisom AWS
- służy do tymczasowej zmiany uprawnień (assume role)

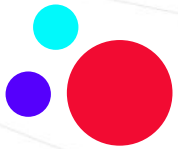
IAM Policies

- zestaw uprawnień (allow lub deny) który można podłączyć do roli lub użytkownika / grupy

Root user

- nie uzywac do normalnej pracy, tylko w sytacji awaryjnej (np. zablokowanie dostępu do S3 bucketa)
- MFA - tak
- programmatic keys - nie

infoShare ACADEMY



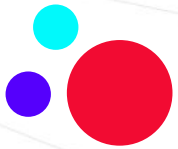
Cwiczenie

Tworzymy

- IAM Rolę dla EC2 (z EC2 IAM Profile)
- IAM Policy
  - uprawnienia do pobierania obiektów z S3 bucket'a **(s3:GetObject)**
  - uprawnienia do listowania obiektów z S3 bucket'a **(s3:ListBucket)**
- Podłączamy stworzone przez siebie policy do IAM Role
- Podłączamy AWS managed policy do IAM Role
  - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

infoShare ACADEMY

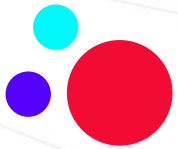
05. Elastic Compute Cloud



EC2 - Elastic Compute Cloud

- Serwery wirtualne
- Podział na klasy
  - General Purpose
    - T - brustable
    - M - standard
    - A - AWS Graviton
    - Mac
  - Compute Optimized
    - C - CPU optimized
  - Memory Optimized
    - R - memory
    - X - in-memory apps
    - Z - high compute, high memory
  - Accelerated Computing
    - P - GPU
    - G - GPU, Machine learning
    - DL1, Trn1 Inf1, F1, VT1
  - Storage Optimized
    - I - NVMe SSD local drives
    - D - HDD local drives

infoShare ACADEMY



EC2 - Instancje

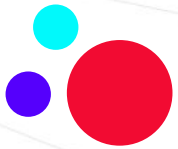
Możliwości uruchomienia instancji:

- on-demand - standardowe wirtualne serwery, naliczanie sekundowe (lub godzine w przypadku niektórych typów serwerów)
- spot - giełda wirtualnych maszyn
- dedicated - wirtualny serwer uruchomiony zarezerwowanym tylko dla nas hardwarze.

Dostęp do wirtualnych serwerów:

- klucze RSA - logowanie SSH do Linux'a
- klucz RSA - haslo przy logowaniu do Windows
- **AWS SSM Session Manager - terminal przez AWS Management Console**
- EC2 Serial Console - mozliwosc podlaczenia sie do serial port wirtualne maszyny
- EC2 Instance Connect - logowanie przez SSH kiedy serwer ma publiczny adres

infoShare ACADEMY



EC2 - EBS - Elastic Block Storage

Sieciowy system umożliwiający podłączenie dysków do serwerów wirtualnych EC2

Możliwość tworzenia backup'ow poprzez snapshoty (przechowywane na S3)

Rodzaje:

- General Purpose SSD (gp2, gp3)
- Provisioned IOPS SSD (io1, io2)
- Cold HDD (sc1)
- Throughput Optimized HDD (st1)
- Magnetic (standard)

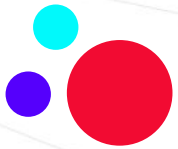
Tworzone per AZ

Można tworzyć czyste dyski lub ze snapshot'ow

Szyfrowanie

infoShare ACADEMY

06. Bazy danych



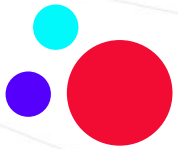
SQL vs noSQL

- RDS - Managed Relational Database Service
- DynamoDB - Managed NoSQL Database
- Amazon DocumentDB - Managed MongoDB

- ElasticCache - Redis / Memcache
- Amazon MemoryDB for Redis

- Amazon Keyspaces - baza danych kompatybilna z Cassandra
- Neptune - graph database
- Amazon QLDB - blockchain database
- Amazon Timestream - baza danych dla IoT do przechowywania serii danych czasowych

infoShare ACADEMY



RDS

W pełni zarządzane przez AWS relacyjne bazy danych

Silniki:

- PostgreSQL
- MySQL
- MariaDB
- Oracle
- SQL Server
- Aurora
  - MySQL
  - PostgreSQL

infoShare ACADEMY

07. DevOps services

infoShareAcademy.com

DevOps Services

CloudWatch

- Logs
- Metrics
- Insights

Event Bridge

CloudTrail

Athena + Quicksight

SNS + SQS

Code Pipeline + Code Build + Code Deploy

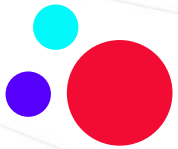
AWS Systems Manager Automations / Documents

Lambda

AWS Organizations

IAM

infoShare ACADEMY



Developer Services

Lambda + Lambda Layers

EC2 + ALB + ASG

RDS / DynamoDB

ElasticCache

ECS + ECR +ALB

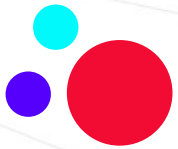
API Gateway + Lambda

Cognito

EKS + ECR

AWS Certificate Manager

infoShare ACADEMY



CloudWatch

Monitoring, logi, alarmy, metryki

Tworzenie własnych dashboardow

Możliwość tworzenia własnych metryk i konfigurowania już istniejących

Zbieranie i analiza logów (Logs i Logs Insights)

infoShare ACADEMY

Dziękuję za uwagę!

infoShareAcademy.com

06. Auto Scaling

infoShareAcademy.com

EC2 - Auto Scaling

Składniki:

- Auto Scaling Groups
- Launch Configuration (LCs)
  - niezmienne
  - stare, niepolecane - nie używać dla nowych ASGs
- Launch Templates (LTs)
  - możliwe wersjonowanie
  - nowe, zalecane
  - możliwość uruchamiania serwerów spot i on-deman w tym samym ASG

- Skalowalność (zwiększamy/zmniejszamy ilość serwerów a nie ich wielkość)
- Dostępność
- Monitoring
- Dane muszą być przechowywane poza serwerem (DynamoDB, RDS, EFS)

infoShare ACADEMY

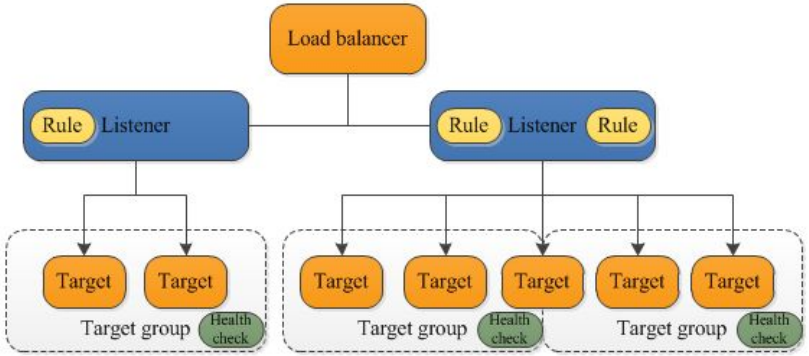
05. Load Balancers

infoShareAcademy.com

EC2 - Load Balancers

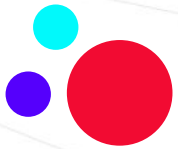
Typy:

- Application Load Balancer
  - najbardziej wszechstronny
  - funkcjonuje na warstwie aplikacyjnej (Model OSI - 7)
  - zmienne adresy IP listenerow
  - rutowanie po path, host, nagłówkach http
  - instancje EC2, kontenery ECS lub funkcje Lambda jako targety
  - rozpakowywanie SSL (przechowywane w AWS Certificate Manc
- Network Load Balancer
  - najbardziej wydajny
  - funkcjonuje na warstwie transportowej (Model OSI - 4)
  - stałe adresy IP listenerow
  - instancje EC2, kontenery ECS jako targety
  - wsparcie dla TCP i UDP
  - możliwość mapowania do VPC Endpoint Service
- Gateway Load Balancer
  - funkcjonuje na warstwie sieciowej (Model OSI - 3)
  - używany z urządzeniami sieciowymi (firewalls, intrusion detection and prevention systems, deep packet inspection systems)
- Classic Load Balancer
  - pierwsza generacja load balancer'a w AWS



https://aws.amazon.com/elasticloadbalancing/features/#Product_comparisons

infoShare ACADEMY



Application Load Balancer

Obsługa IPv4 oraz dualstack (IPv4 + IPv6)

Minimalna liczba AZ - 2

Minimalna liczba wolnych adresów IP w AZ - 8

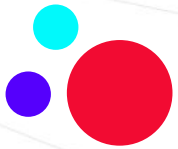
Zarządzany przez AWS

Stały DNS endpoint, **adresy IP zmienne**.

Elementy

- Listener
- Target group
- Launch template

infoShare ACADEMY



ALB - Listener

Frontend dla load balancera - jest to proces nasłuchujący na zdefiniowanych portach (min. 1)

Obsługa certyfikatów SSL z AWS Certificate Manager

Możliwość ustawiania reguł do danego portu + domyślna reguła

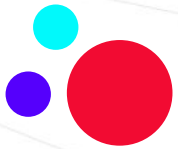
Reguły są przetwarzane wg. ustalonej kolejnosci (priority)

Rodzaje akcji dla reguł:

- Fixed-response - stała odpowiedź
- Forward - przekazanie ruchu do np. maszyny
- Redirect - przekierowanie (301, 302)
- Authenticate -> Cognito - uwierzytelnianie w AWS Cognito (tylko HTTPS)
- Authenticate -> OIDC - uwierzytelnianie przez OpenID (tylko HTTPS)

Warunki regul

infoShare ACADEMY



ALB - Listeners

Warunki reguł:

- host-header - nazwa domeny (nagłówek Host)
- http-header - inny dowolny nagłówek HTTP
- http-request-method - metoda HTTP (get, post, delete, update, put)
- path-pattern - ścieżka żądania (np. /admin/)
- query-string - ścieżka żądania (np. /admin/?key=value)
- source-ip - adres IP klienta

infoShare ACADEMY

ALB - Target Groups

Backend dla load balancera - tutaj kierowany jest ruch zgodnie z regułami ustawionym na Listenerach

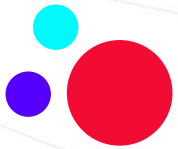
Targets:

- Instance EC2 (wewnatrz VPC w ktorym jest ALB)
- Adresy IP (dowolne adresy IP, rownież on-prem
- Funkcje Lambda - przekierowanie do pojedynczej lambdy
- Inny Application Load Balancer (ma zastosowanie kiedy Target Group jest podlaczona do NLB)

Health Checks - weryfikacja stanu uslugi

- TCP
- HTTP
- HTTPS

infoShare ACADEMY



Network Load Balancer

Przekierowanie ruchu na warstwie 4

Obsługa IPv4 oraz dualstack (IPv4 + IPv6)

Obsługiwane protokoły

- TCP
- UDP
- TLS

Stale 2 adresy IP per NLB

Możliwość ustawienia ALB jako target - przydaje się przy konfigurowaniu VPC Endpoint Service.

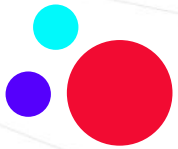
info Share ACADEMY

Dziękuję za uwagę!

infoShareAcademy.com

06. Simple Storage Service

infoShareAcademy.com



S3 - Simple Storage Service

Główne funkcje

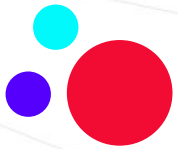
- Przechowywanie danych
- Kopie zapasowe
- Archiwizacja danych (Glacier)
- Jezioro danych (data lake)
- Hosting statycznych stron www

Główne właściwości:

- nieograniczona powierzchnia
- max. rozmiar obiektu to 5TB
- niskie koszty
- trwałości i wysoka dostępność

“Easy to Learn, Hard to Master”

infoShare ACADEMY



S3 - szczegóły

Bucket

- nazwa jest unikatowa w skali całego AWS (nikt na żadnym koncie, w żadnym regionie nie może mieć bucketu o takiej samej nazwie)
- uwaga na usuwanie i ponowne tworzenie bucketu o tej samej nazwie - synchronizacja trwa ok. 1 godzinę!

Object / key

- plik z danymi (S3 to nie jest filesystem)
- Metadata - zestaw par nazwa-wartość, czesciowo definiowane przez użytkownika https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingMetadata.html
- może być wersjonowany

infoShare ACADEMY

Ćwiczenie

Tworzymy S3 bucket

- default encryption - Amazon S3-managed keys (SSE-S3)
- versioning disabled
- region - taki sam jak VPC
- ACLs disabled
- Block all public access

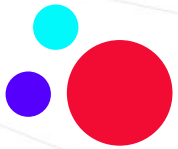
infoShare ACADEMY

Dziękuję za uwagę!

infoShareAcademy.com

Elastic Container Registry

infoShareAcademy.com



ECR

Elastic Container Registry (w skrócie: ECR) jest zarządzanym prywatnym rejestrem obrazów Docker.

Działa na podobnej zasadzie co Docker Hub z tą różnicą, że w ECR mówimy tylko PRYWATNYCH obrazach, czyli takich do których bez uwierzytelnienia nie mamy dostępu.

Do rejestru można zapisywać obrazy przy pomocy Docker CLI (po wcześniejszej autoryzacji)

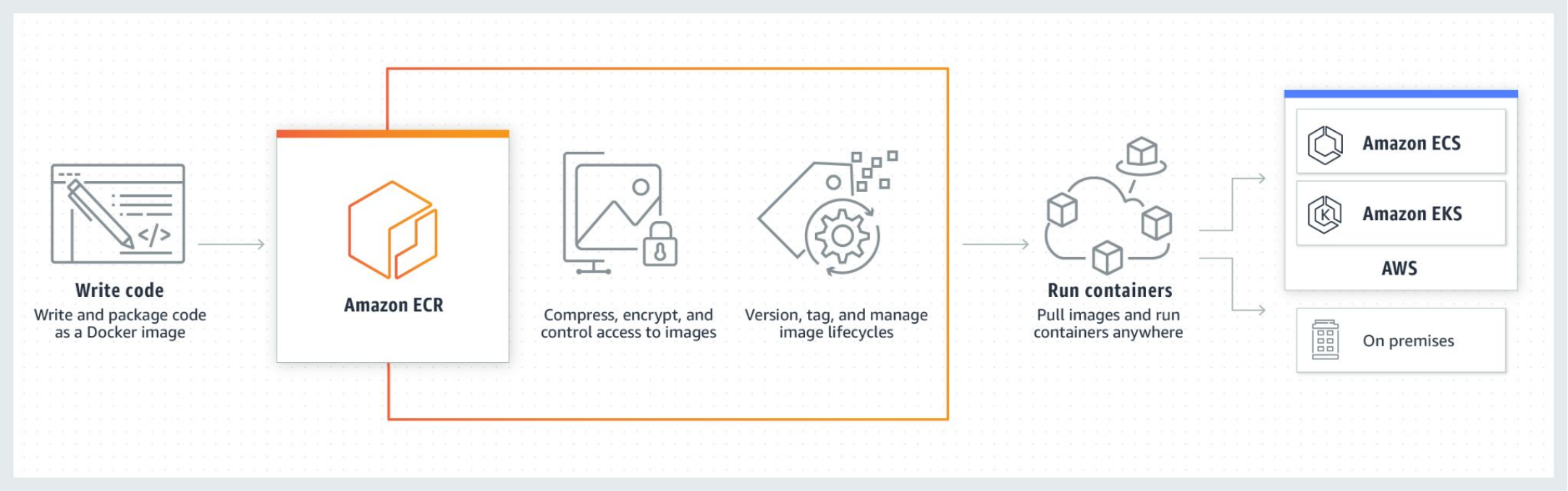
```
aws ecr get-login-password --region <REGION> --profile <PROFILE-NAME> | docker login --username AWS
--password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<REGION>.amazonaws.com/<REPO-NAME>
```

```
docker push 844187532425.dkr.ecr.eu-west-1.amazonaws.com/<REPO-NAME>:<TAG>
```

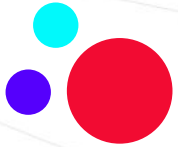
infoShare ACADEMY

ECR

- Wiele repozytoriów
- Integracja z innymi usługami AWS (ECS, EKS, AWS Lambda, AWS Elastic Beanstalk)



infoShare ACADEMY



ECR

Dodatkowe funkcjonalności ECR:

Helm Chart – ECR wspiera także publikację artefaktów **Open Container Initiative** (OCI), dlatego możliwa jest publikacja artefaktu w postaci Helm Chartu;

Lifecycle policies – Definicja cyklu życia obrazu. Za pomocą reguł można zdefiniować, kiedy dane obrazy mają zostać usunięte w sposób automatyczny z rejestru;

Image scanning – Obrazy w rejestrze, mogą być skanowane pod kątem wykrywania luk bezpieczeństwa w oprogramowaniu, które wykorzystywane jest w obrazie;

Tag immutability – Obrazy w rejestrze nie mogą być zmieniane. Oznacza to tyle, że otagowany obraz nie może zostać nadpisany.

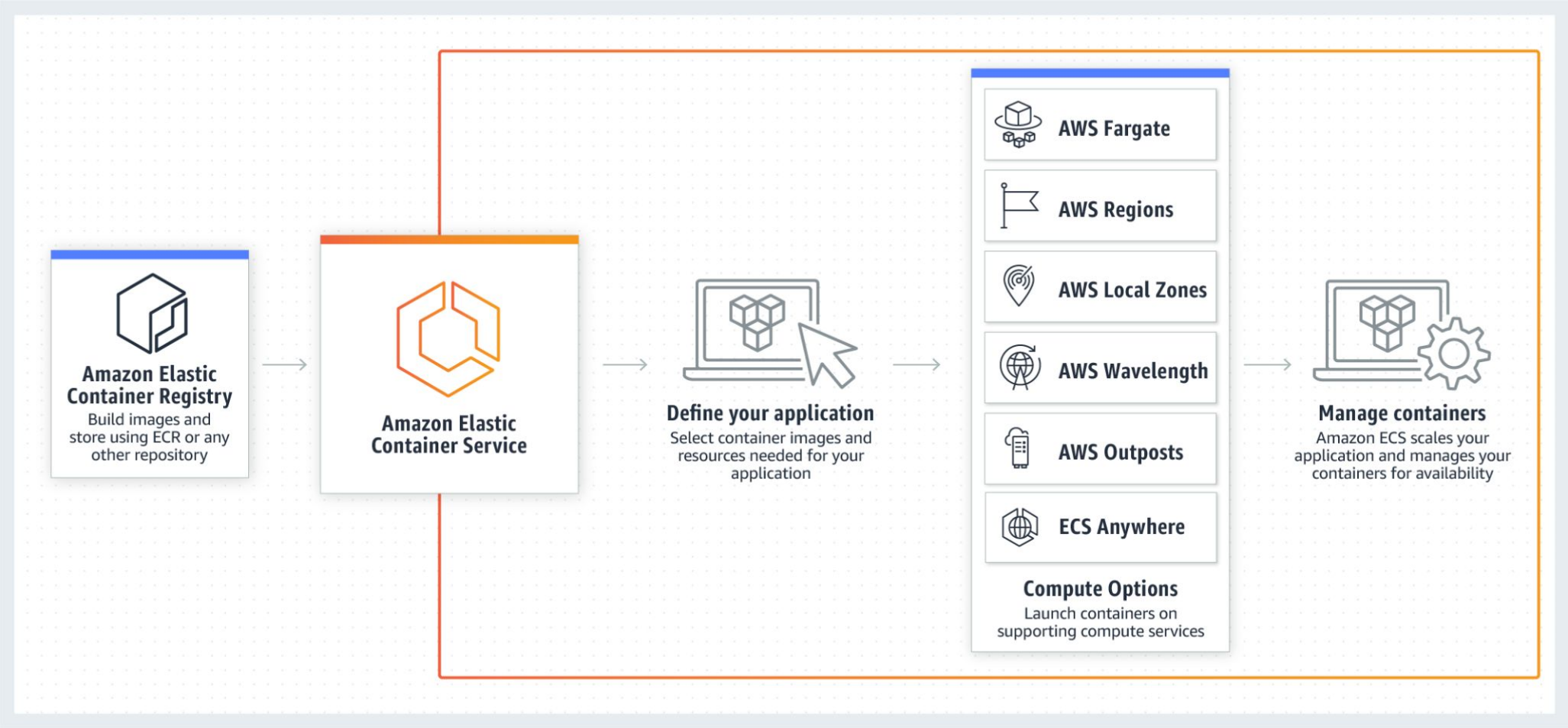
Elastic Container Service

infoShareAcademy.com

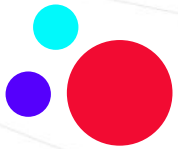
ECS

System orkiestracji kontenerów zarządzany przez AWS.

ECS EC2 vs Fargate (serverless)



infoShare ACADEMY

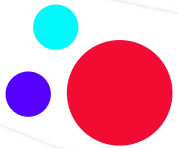


ECS

Części składowe:

- Cluster - nadrzędna jednostka, logiczne grupowanie task'ów i service'ów
- Task - jeden lub więcej działających kontenerów
  - można uruchomić ręcznie lub poprzez poprzez cron/scheduler
  - uruchamianie bezpośrednie przydaje się do pojedynczych zadań, które się kończą.
- Task Definition - konfiguracja jak ma być uruchomiony kontener (lub więcej) jako Task
  - zawiera informacje o wymagania dot. CPU i pamięci
  - jak mają być zbierane logi
  - mapowanie portów
  - mapowanie dysków
- Service - używany do uruchamiania Tasków które mają działać non-stop
  - ECS dba aby ilość działających tasków była zgodna z wymaganiami
  - można podłączyć Application Load Balancer
  - możliwość automatycznego skalowania (zwiększania/zmniejszania) ilości Tasków

infoShare ACADEMY

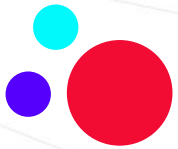


ECS - Demo

https://github.com/infoshareacademy/dor3-materialy/tree/master/aws/part-4/terraform

10. AWS Lambda

infoShareAcademy.com

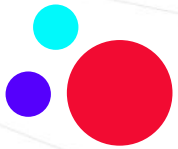


Lambda

Co to jest ?

- Bezserwerowa usługa obliczeniowa
- Możliwość uruchamiania kodu bez zarządzania infrastruktura serwerową
- Wspierane języki programowania
  - Java
  - Go
  - PowerShell
  - Node.js
  - C#
  - Python
  - Ruby
- Możliwość uruchamiania kontenerów
  - Docker Image Manifest V2 Schema 2 (Docker werja 1.10+)
  - Open Container Initiative (OCI) Spec (v1.0+)
  - Maksymalna wielkość kontenera to 10GB.

infoShare ACADEMY



Lambda

Wady - zalety

Zalety:

- wszechstronność (używane do integracji między usługami, do transformacji na plikach, backend dla aplikacji webowych, IoT)
- cena
- bardzo szybkie wykonywanie kodu
- wsparcie dla x86 i arm
- skalowalność
- możliwość uruchamiania w VPC jak poza

Wady

- maksymalny czas działania - 15 minut
- wielkość dysku /tmp jest ograniczona do 3GB
- maksymalna ilość pamięci to 3GB
- monitoring

infoShare ACADEMY

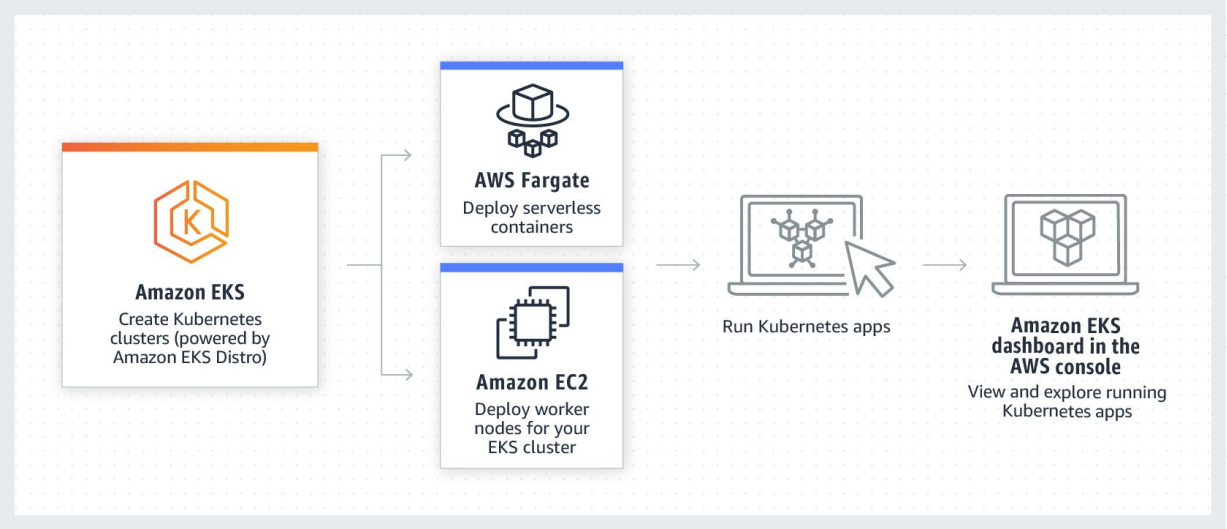
Elastic Kubernetes Service

infoShareAcademy.com

EKS

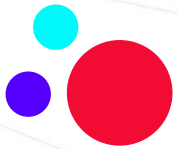
Kubernetes as a Service

- Control plane
- Wspierane są 4 wersje.
  - Nowe wersje wychodzą co około 3 miesiące.
  - Aktualne wsparcie dla wersji
    - 1.22.9
    - 1.21.12
    - 1.20.15
    - 1.19.16
  - Projekt Kubernetes wspiera:
    - 1.24
    - 1.23
    - 1.22



- Obsługa EKS na EC2 (dedykowane obrazy amazon-eks-optimzed) lub Fargate
- EKS Outposts / EKS Anywhere

infoShare ACADEMY

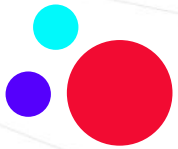


EKS

Cluster Add-on

- Amazon VPC CNI - natywne wsparcie dla VPC, pody mają adresy IP z VPC
- CoreDNS
- kube-proxy
- ADOT - AWS Distro for OpenTelemetry - ułatwia wysyłanie metryk do CloudWatch'a / Prometeus / X-Ray
- Amazon EBS CSI - Amazon Elastic Block Store (Amazon EBS) Container Storage Interface (CSI) - możliwość montowania dysków EBS do podów (ale tylko EKS EC2)

infoShare ACADEMY

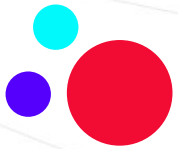


EKS

Zarządzanie

- kubectl - operacje wykonywane wewnątrz klastra, deployment
- eksctl - skalowanie, modyfikacja klastra (używane wtedy gdy nie stosujemy IaC)
- aws cli - uzyskanie dostępu i modyfikacja parametrów od strony AWS

infoShare ACADEMY



Containers

- Red Hat OpenShift Service on AWS
- AWS App Mesh (na bazie Envoy proxy) - służy do kontroli komunikacji sieciowej miedzy microservicami
- AWS Cloud Mesh - service discovery

https://aws.amazon.com/containers/

infoShare ACADEMY