GoDaddy

Uvod u Amazon Web Services (AWS)

Miljenko Rebernišak

19. Maj 2019

Agenda

- Zašto cloud ?
- Zašto AWS ?
- Network layer
- Compute layer
- Database layer
- Storage layer
- Security layer
- Live demo

GoDaddy

Zašto cloud ?

Zašto cloud ?

- Fleksibilnost
- Cena
- Skalabilnost i performance
- Pouzdanost
- Sigurnost

Tipovi cloud provajdera

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

GoDaddy

Zašto AWS ?

AWS Global Infrastructure Map

The AWS Cloud spans 66 Availability Zones within 21 geographic Regions around the world, with announced plans for 12 more Availability Zones and four more Regions in Bahrain, Cape Town, Jakarta, and Milan.

Kako početi ?

- https://aws.amazon.com/free/

apps

Types of offers

Explore more than 60 products and start building on AWS using the free tier. Three different types of free offers are available depending on the product used. See below for details on each product.

Always free

These free tier offers do not expire and are available to all AWS customers

12 months free

Enjoy these offers for 12-months following your initial sign-up date to AWS

Trials

Short-term free trial offers are available through many different software solutions

GoDaddy

GoDaddy

Network layer

Network layer

- VPC – Virtual Private Cloud
- Subnets
- Route Tables
- Internet Gateways
- NAT
- Elastic IP Addresses
- Security groups / NACL
- DNS
- VPC Endpoints
- VPC Peering
- VPN connection

GoDaddy

VPC – Virtual Private Cloud

- Virtualna mreža dodeljena nalogu
- Logički izolovana od drugih AWS mreža
- Mesto gde pokrećete vaše resurse
- IPv4 / IPv6
- PCI DSS
- Pokriva više AZ
- Tipični opsezi
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

GoDaddy

Subnets

- Manji segment mreže dodeljen jednoj AZ
- Javni ili privatni subneti
- Opciona IPv6 podrška
- Uobičajna notacija CIDR

Route Tables

- Set pravila (routes) koji određuje putanju saobraćaja
- Svaki subnet unutar VPC mora da ima route tabelu koja kontroliše protok
- Subnet može da pripada samo jednoj route tabeli
- Route tabela može da sadrži više subnet
- VPC ima glavnu route tabelu
- Glavna route tabela se ne može obrisati
- Route tabela sadrži destinacioni CIDR format i odredište
- Loklana ruta za svaki IPv4 CIDR blok

GoDaddy

Internet Gateways

- Horizontalno skaliran
- Redudantan
- Highly available
- IPv4 / IPv6
- Pruža uslugu eksternog saobraćaja unutar VPC
- Koristi se za 0.0.0.0/0 saobraćaj

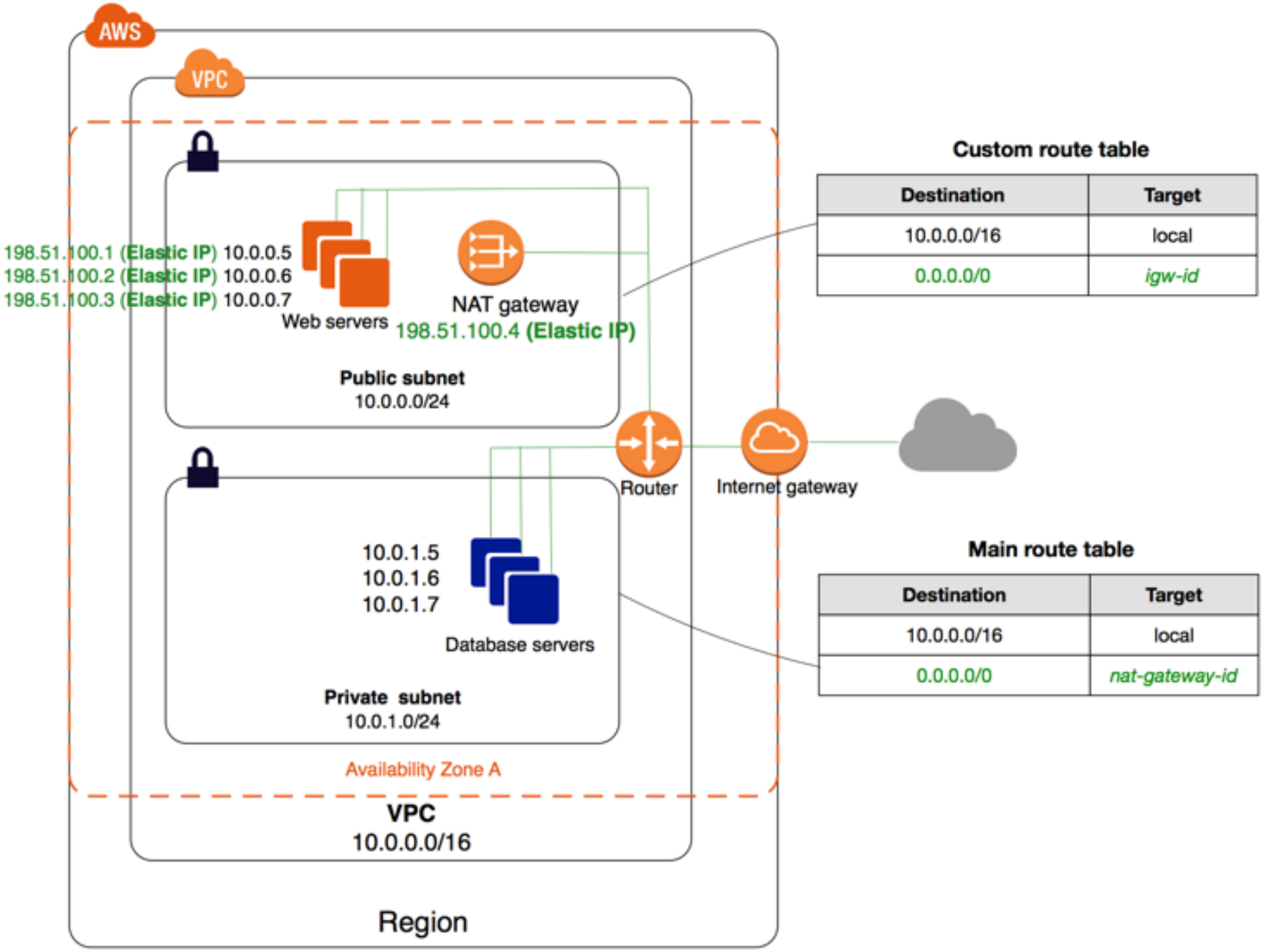
NAT - network address translation

- Omogućava izlaz na internet bez, ali ne pruža konekciju ka resursima unutar VPC sa spoljne mreže
  - Ažuriranja softwera
- NAT gateways
  - Skalabilni servis
  - AWS održava
  - IPv4 podrška
- NAT instances
  - Korisnik radi administraciju instance
  - Ne postoji skalabilnost

EIP - Elastic IP address

- Statična, javna IPv4 adresa
- Dizajnirana za cloud
- Vezana za AWS nalog
- Može se dodeliti instacama ili mrežnim interfejsima
- Mogućnost brzog remapiranja u slučaju pada pozadinskog servisa
- Mapiranjem na eth0 mrežni interfejs, EIP postaje izvor za sav internet saobraćaj
- 1:1 NAT sa privatnom IP adresom

GoDaddy



Custom route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Main route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-gateway-id*

GoDaddy

Security groups / NACL

- Security group – virtualni firewall
  - Kontrola ulazno/izlaznog saobraćaja
  - Kontrola na nivou instance
  - Pravila dozvole samo
  - Prazna grupa ne podrazumeva dozvoljeni saobraćaj
  - Različita pravila za ulaz / izlaz
  - Pamti stanje saobraćaja (stateful)
- NACL – network access control list
  - Opcioni nivo zaštite na nivou jednog ili više subnet-a
  - Pravila po prioritetu
  - Odvojena ulazno / izlazna pravila
  - Mogućnost pravila dozvole ili zabrane (deny)
  - Ne pamti stanje saobraćaja (stateless)

GoDaddy

DNS

- Servis omogućen unutar VPC od strane AWS
- Limitiran na 1024 paketa po sekundi po interfejsu
- Mogućnost korišćena sopstvenog DNS servera
- Javno DNS ime dodeljeno instance kada se startuje u javnom subnetu
- Unutar VPC privatno DNS ime

GoDaddy

VPC Endpoints

- Privatna konekcija unutar VPC do AWS servisa
  - Skalabilna
  - Redudanta
  - Visoko dostupna
  - Ne utiče na network saobraćaj
- Nije potreban izlaz na internet
- Sva komunikacija se obavlja unutar VPC
- Podržano preko 30+ servisa
- Dva tipa endpointa
  - Interfejs – virtualni uređaj
  - Gateways – HTTP

GoDaddy

VPC Peering

- Mogućnost spajanja dva ili više VPC
- Mogućnost rutiranja saobraćaja između VPC-a privatno
- Podržan je VPC peering
  - Unutar istog naloga
  - VPC unutar drugog naloga
  - VPC u drugom region
- Nije Site-to-Site VPN, niti poseban hardware

VPN connection

- Mogućnost spajanja VPC sa drugim fizičkim mrežama
- Podržani tipovi konekcija
  - AWS Site-to-Site VPN - IPsec VPN
  - AWS Client VPN – OpenVPN VPN klijent
  - AWS VPN CloudHub – mogućnost spajanja više kancelarija putem AWS
  - Third party software VPN appliance – VPN server podignut na instanci

GoDaddy

Compute layer

Compute layer

- EC2 - Elastic Compute Cloud
- Lightsail – Virtual server
- ECR - Elastic Container Registry
- ECS - Elastic Container Service
- EKS - Elastic Container Service for Kubernetes
- Lambda - serverless

EC2

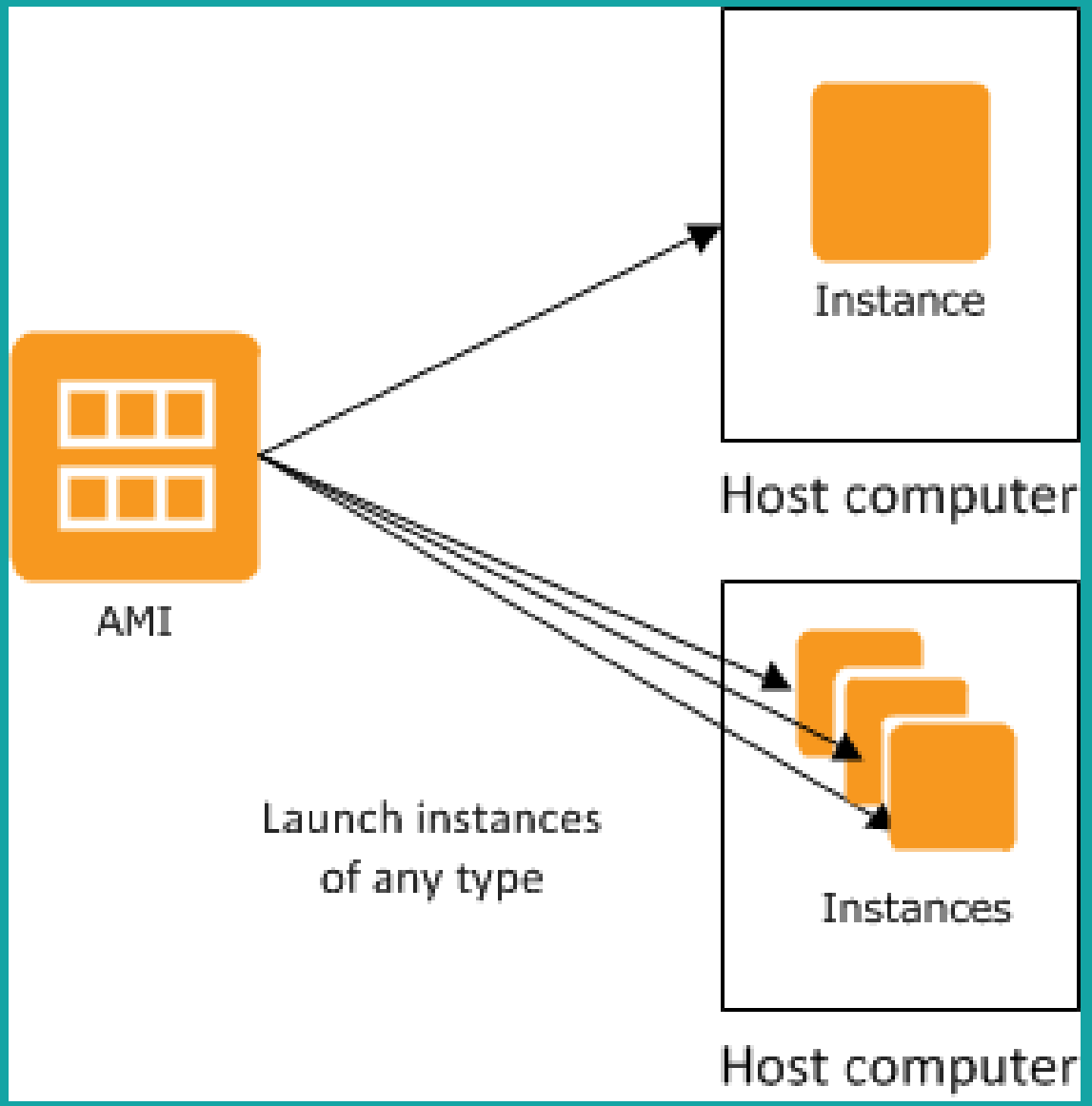
- Skalabilni virtualni server
- Različite konfiguracije CPU, Memorije, storage, mreže
- Različite vrste operativnih Sistema
  - AMI - Amazon Machine Images

EC2 – Tipovi instanca

- Generalna namena
- CPU optimizovane
- Memorijski optimizovane
- Storage optimizovane
- GPU optimizovane

EC2 – AMI

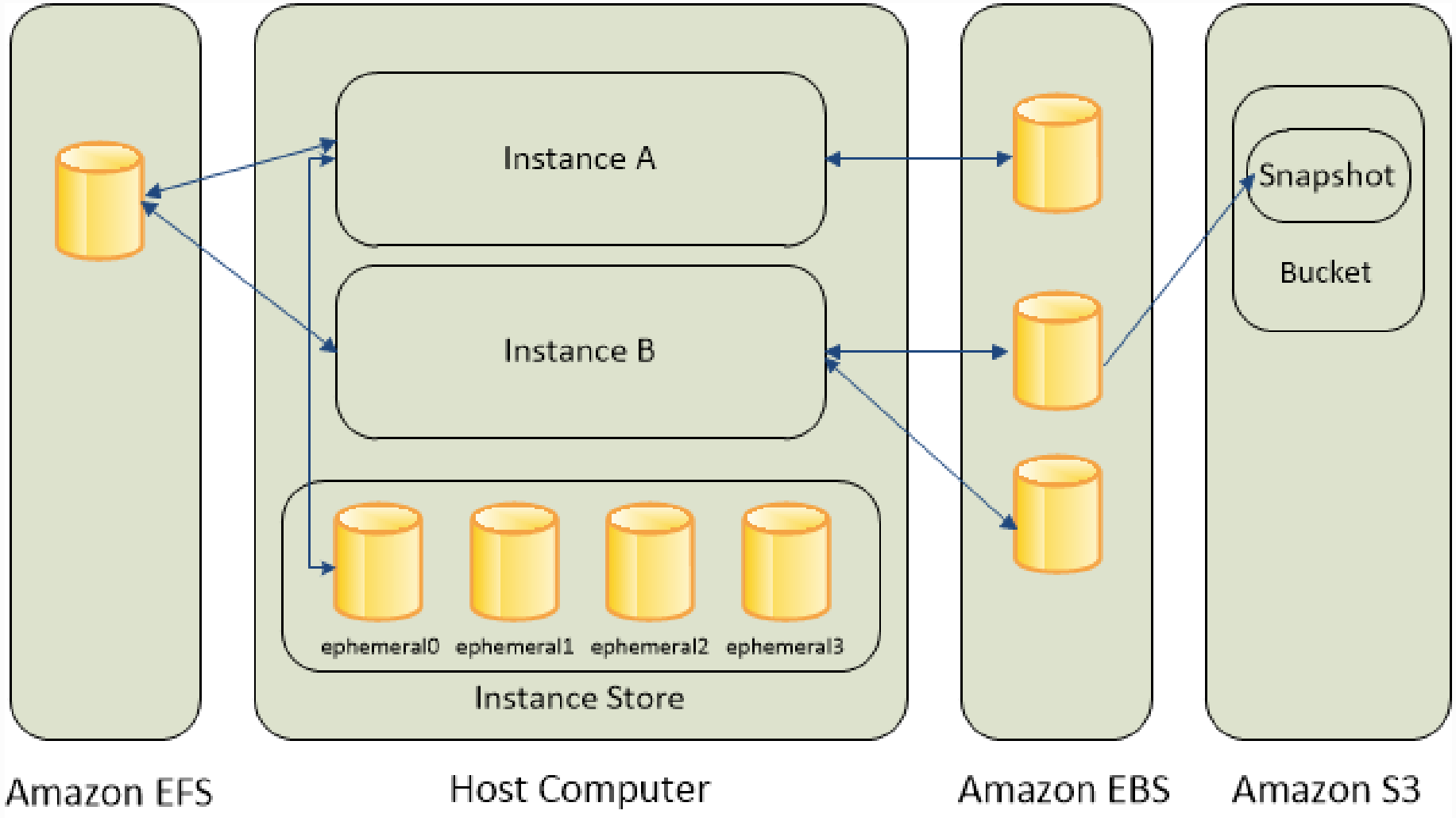
- AMI sadrži
  - Operativni system
  - Aplikacije
- Više instance može da pokreće jedan AMI
- Mogućnost pravljenja sopstvenog AMI
- Mogućnost korišćena plaćenih AMI (Marketplace)



EC2 – Storage

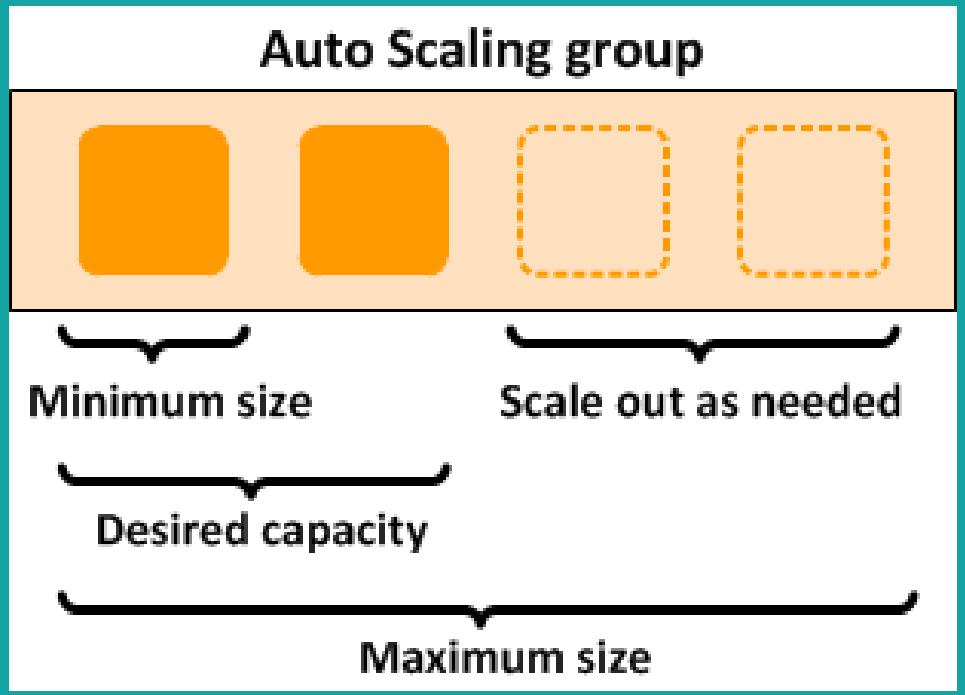
- EBS
  - Trajni mrežni disk
  - Samo jedna instance
  - Neformatiran
  - Više diskova može na jednu instance
- Instance Store
  - Privremeno mesto dokle instanca radi
- EFS File System
  - Mrežni disk za linux sisteme
  - Više instanci može koristiti jedan disk

EC2 – Storage

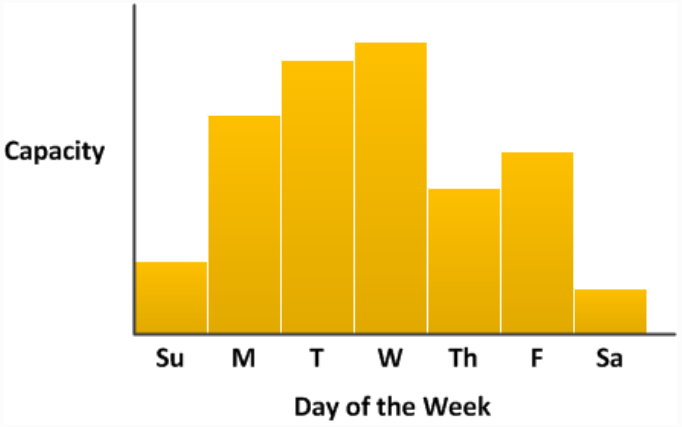


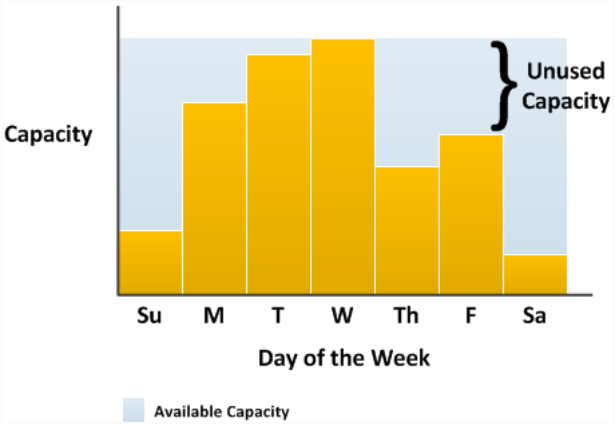
EC2 – Auto Scaling

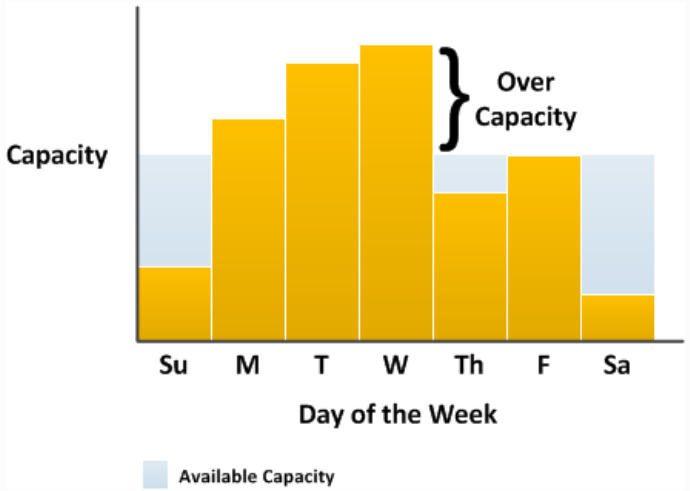
- AWS održavani servis koji pokreće ili zaustavlja EC2 istance
- Obezbeđuje minimum ili maksimum kapaciteta
- Prati parameter instance na osnovu pravila (alarms) i preduzima akcije
- Pokreće instance prema unapred zadatim pravilima – Launch template

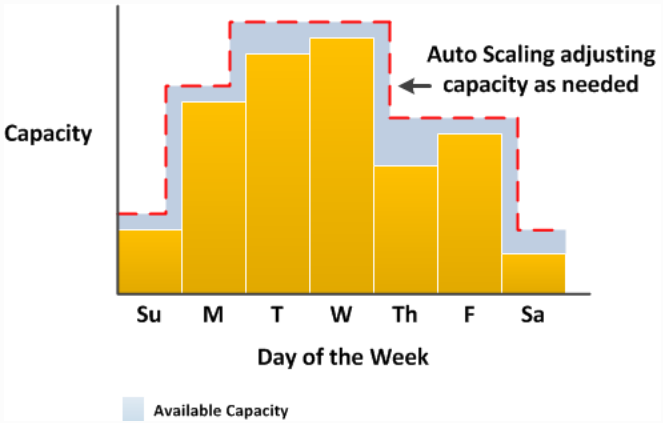


EC2 – Auto Scaling





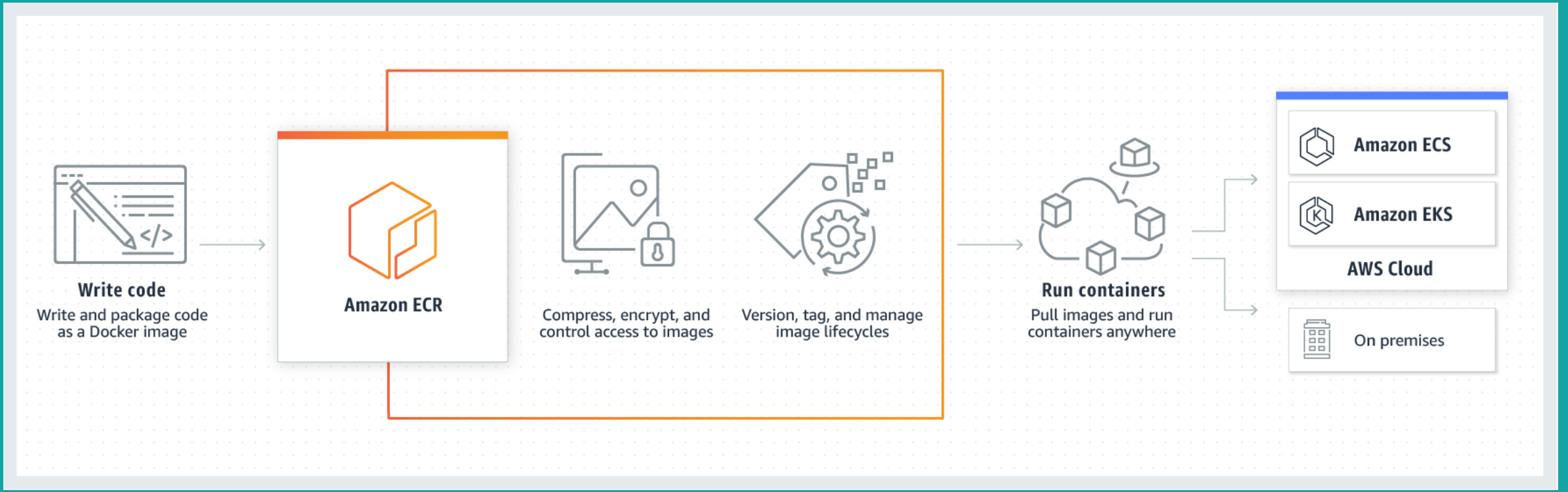




GoDaddy

ECR - Elastic Container Registry

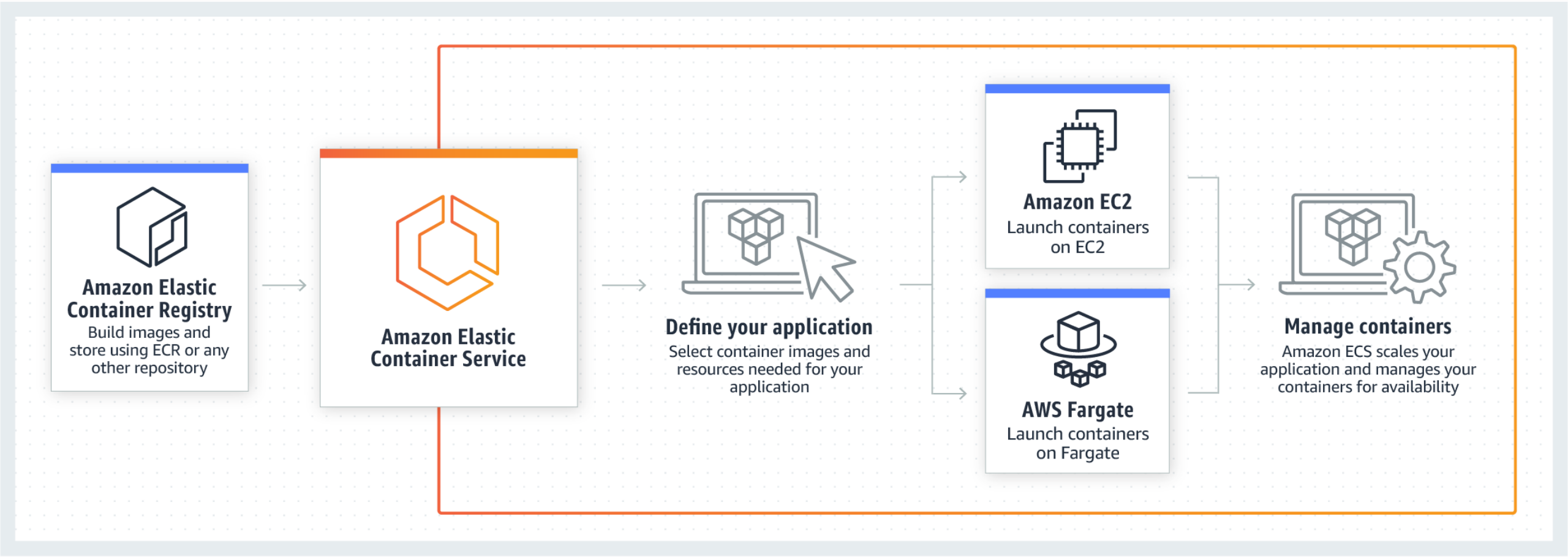
- AWS održavani registar doker kontejnera
- Integrisan sa ECS



ECS - Elastic Container Service

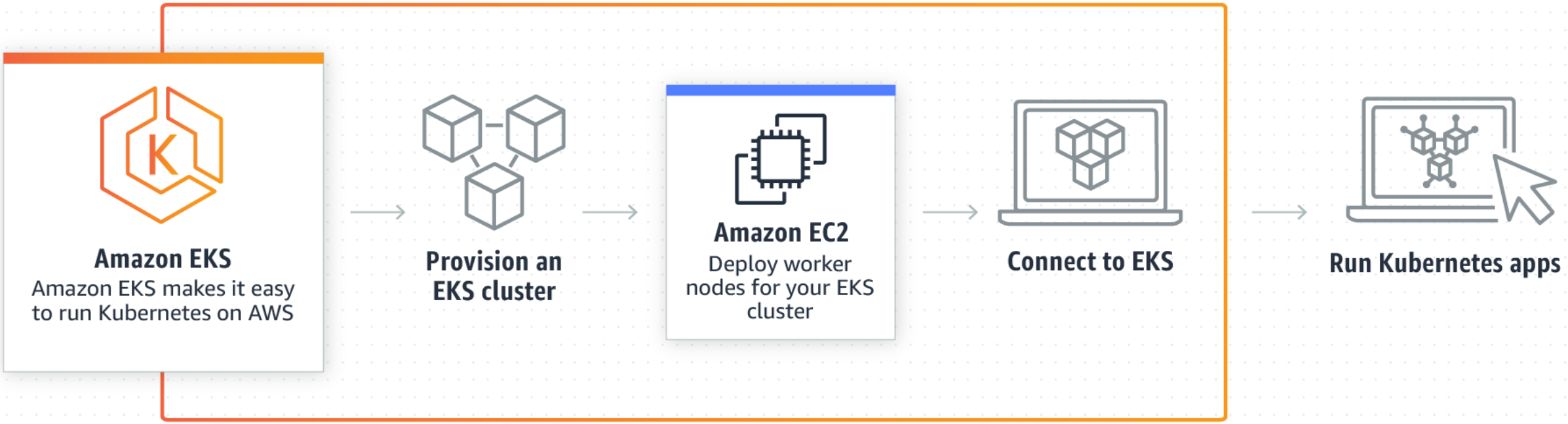
- Orekastracioni servis docker kontejnera
- Pokreće EC2 istance i upravlja docker kontejnerima
- Primena:
  - Mikroservisi
  - Paketno procesiranje
  - Mašinsko učenje

ECS - Elastic Container Service



EKS - Elastic Container Service for Kubernetes

- Orekastracioni servis za Kubernetes klaster
- AWS pokreće Kubernetes klaster preko nekoliko AZ
- Kompatibilan sa postojećim aplikacijama
- Nema potrebe za održavanjem



Lambda

- Izvršavanje koda bez servera
- Podržani svi programski jezici
- Reaguje na različite okidače
- Mikroservisna arhitektura
- Automatski skalira

Lambda

GoDaddy

Database layer

Database layer

- RDS - Relational Database Service
- DynamoDB
- ElastiCache
- Neptune
- Amazon Redshift
- Amazon DocumentDB

GoDaddy

RDS - Relational Database Service

- Relaciona baza kao servis
- Laka za održavanje
  - Automatski backup, patching,
- Omogućava redudansu i visoku dostupnost
  - Automatska detenkcija

GoDaddy

DynamoDB

- Key-value baza
- Dokument baza
- Multimaster baza
- Vreme odziva je jednocifreni broj milisekundi
- Serverless
- Velike performanse
  - DO 20 miliona upita po sekundi
- Primena
  - Gaming
  - Ad serving
  - IoT
  - Mobile

ElastiCache

- Memorijska keš baza
- Podržani sistemi
  - Redis
  - Memcache
- Skalabilna
- AWS održavana

GoDaddy

Storage layer

Storage layer

- S3
- S3 Glacier
- EFS
- FSx
- Storage Gateway
- AWS Backup

S3 - Simple Storage Service

- Object store
- REST API
- Trajnost podataka 99.999999999% (11 9’s)
- Jeftin
  - Nekoliko klasa cene prema nameni
- Primene
  - Disaster recovery
  - Backup
  - Arhive
  - Nativne cloud aplikacije

S3 Glacier

- Dugotrajno arhiviranje podataka
- REST API
- Trajnost podataka 99.999999999% (11 9’s)
- Vreme dohvatanja fajla 1-5 minuta
- Primena
  - Zamena za magnetne trake
  - Arhiviranje medicinskih podataka
  - Zakonska arhiviranja podataka
  - Digitalno očuvanje dokumenata

EFS – Elastic file system

- Mrežni disk za linux sisteme
- Paralelni pristup fajlovima sa vise mesta
- Protokol Network File System verzije 4
- Elastični kapacitet
  - Ne zakupljuje se unapred
- Mogućnost zakupa dodeljenih performansi (throughput)

FSx

- Servis za fajl sisteme trećih lica
- Podržani fajl sistemi
  - Windows File server
  - Lustre
- Primena
  - Windows-based storage
  - HPC
  - Mašinsko učenje

Storage Gateway

- Hibridni servis za kombinovanje cloud i on-premise storage Sistema
- Aplikacije koriste standardni protocol
  - NFS, SMB, iSCSI
- Gateway se konektuje na AWS servise kao što je S3, Clacier
- Fizički hardware ili virtualna mašina
- Mogućnost lokalnog keširanja

AWS Backup

- Centralni bekap servis
- Podržava EBS, Gatawey, RDS, DybamoDB..

GoDaddy

Security layer

Security layer

- IAM - Identity and access management
  - Roles, Policies, Users, Groups
- Secrets Manager
- AWS Single Sign-On
- Certificate Manager
- Key Management Service
- CloudHSM
- WAF & Shield

GoDaddy

GoDaddy

Live demo

Hvala na pažnji !
Pitanja ?