

# IAM

RAČUNARSTVO U OBLAKU  
FAKULTET TEHNIČKIH NAUKA  
UNIVERZITET U NOVOM SADU

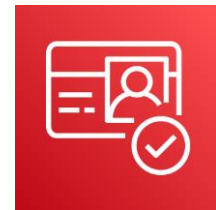


# Šta je IAM?

- IAM = Identity and Access Management
  - **Bezbednost**
  - Definiše korisnike i njihov pristup AWS resursima
  - Autentifikacija i autorizacija
  - Korisnici AWS platforme
    - **Ne rukovodi korisnicima aplikacije**
      - Moguće upotrebom **Cognito servisa**
  - Globalni servis
- Ko može da pristupi čemu

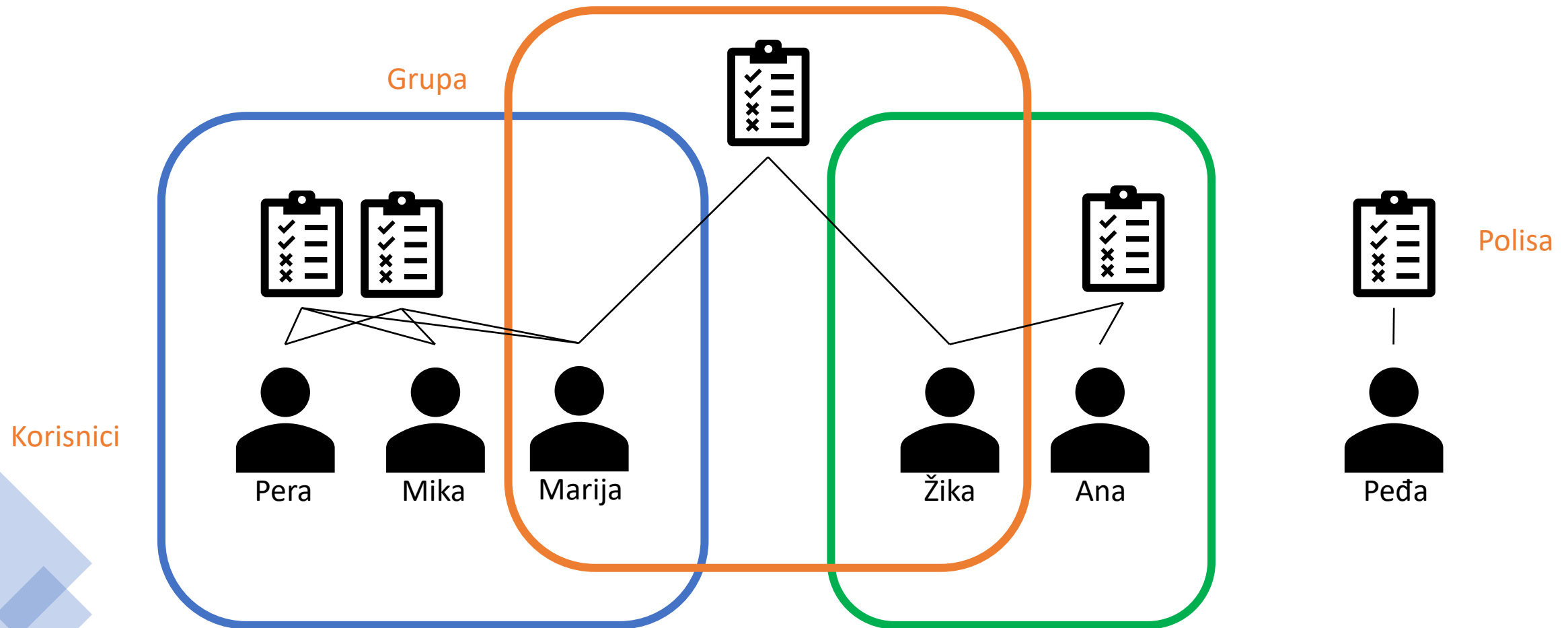


AWS Identity and Access Management  
(IAM)



Amazon Cognito

# Osnovni pojmovi



# Struktura polise

- Id – identifikator polise
- Verzija – verzija jezika za definisanje polisa (2012-10-17 najnovija)
- Statement – definisanje pristupa
  - Sid – statement ID (opciono)
  - **Effect** – dozvola ili zabrana akcije
  - **Action** – akcija nad resursom
  - Resource – **čemu** se pristupa (neophodno ako se polisa vezuje samo za subjekat)
  - Principal – **ko** pristupa (neophodno ako se polisa vezuje samo za objekat)
  - Condition – uslov pod kojim se pristupa (opciono)

```
{
  "Id": "Policy1",
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "1",
    "Effect": "Allow",
    "Principal": {"AWS":
["arn:aws:iam::account-id:root"]},
    "Action": "s3:*",
    "Resource": [
"arn:aws:s3:::mybucket",
"arn:aws:s3:::mybucket/*" ]
    "Condition": {"Bool":
{"aws:MultiFactorAuthPresent": "true"}}
  ]
}
```

# Tipovi polise

- Identity-based
  - **Čemu** identite može da pristupi
  - Vezuju se za **identitet** (korisnik, grupa, rola)
  - Neophodno navesti čemu se odobrava pristup
    - *Resource* obavezan
- Resource-based
  - **Ko** može čemu da pristupi
  - Mora se vezati za **resurs** (servis, bucket,...)
  - Neophodno navesti ko može da pristupi resursu
    - *Principal* obavezan
- Deny je jači od Allow

Account ID: 123456789012

## Identity-based policies

JohnSmith  
Can List, Read  
On Resource X

CarlosSalazar  
Can List, Read  
On Resource Y,Z

MaryMajor  
Can List, Read, Write  
On Resource X,Y,Z

ZhangWei  
No policy

## Resource-based policies

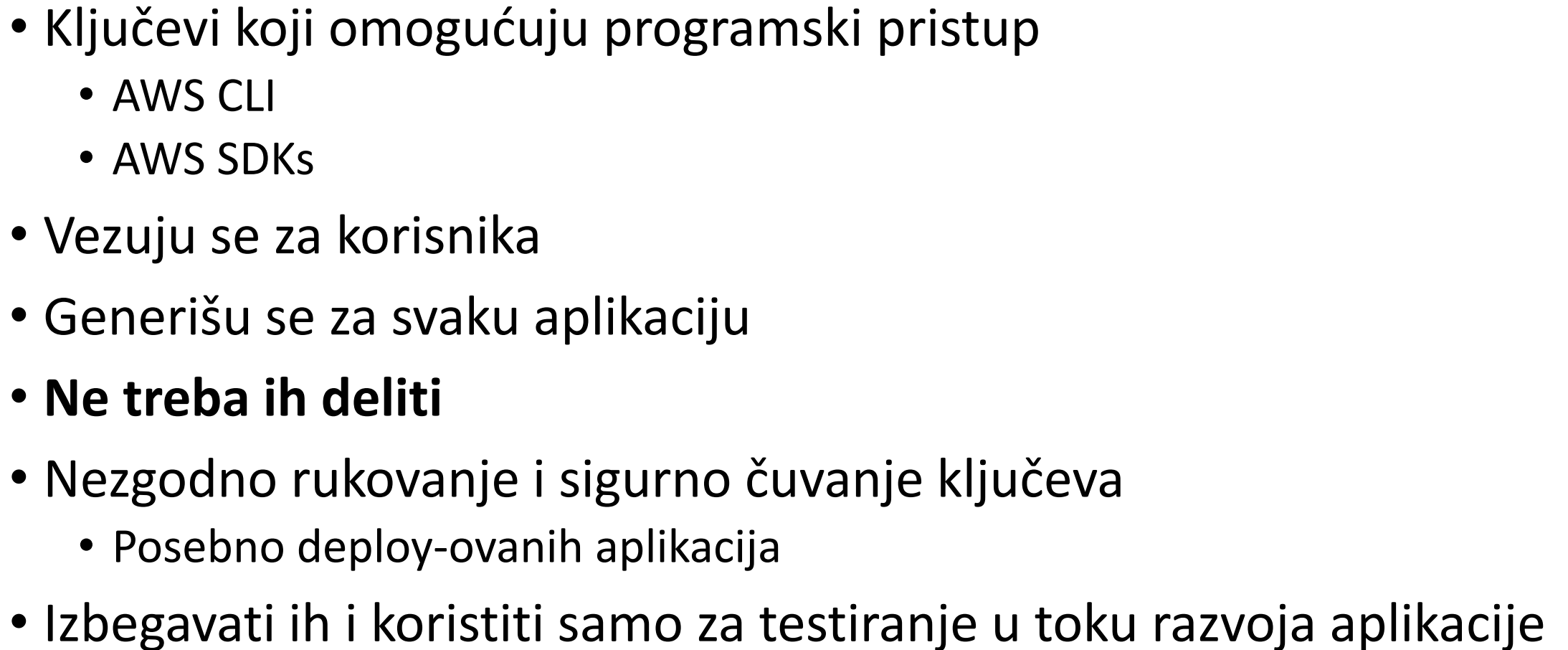
Resource X  
JohnSmith: Can List, Read  
MaryMajor: Can List, Read

Resource Y  
CarlosSalazar: Can List, Write  
ZhangWei: Can List, Read

Resource Z  
CarlosSalazar: Denied access  
ZhangWei: Allowed full access

# Access key



- Ključevi koji omogućuju programski pristup
    - AWS CLI
    - AWS SDKs
  - Vezuju se za korisnika
  - Generišu se za svaku aplikaciju
  - **Ne treba ih deliti**
  - Nezgodno rukovanje i sigurno čuvanje ključeva
    - Posebno deploy-ovanih aplikacija
  - Izbegavati ih i koristiti samo za testiranje u toku razvoja aplikacije
- 

# Rola

---

- Omogućava pristup servisima od strane drugih servisa i aplikacija
- Sastoji se iz polise koja definiše **ko** sme da preuzme rolu i polise koja definiše **šta** nosilac sme da uradi
  - **Ko** – Trust policy
  - **Šta** – Identity-based policy
- Rešava problem rukovanja ključevima – izbacuje ih
  - Rola se proverava direktno u okviru IAM-a u trenutku pozivanja
- Upotreba:
  - Pristup **jednog servisa drugom**
    - EC2 pristup S3, DynamoDB, RDS
    - Lambda pristup S3
  - Pristup od strane drugih AWS naloga
  - Pristup third-party aplikacija

# Primer Trust polise – KO



- Polisa koja daje prava EC2 instanci da preuzme rolu
  - Ako bi se prava dodeljivala drugom servisu, menjala bi se vrednost pod *Service* ključem
    - "Service": "lambda.amazonaws.com"

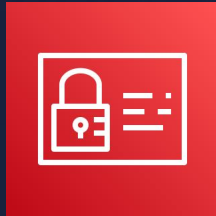
```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Principal": {
      "Service": "ec2.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  } ]
}
```



# Generalne smernice



- Ne koristiti root nalog
  - Koristiti MFA – Multifactor Authentication
  - 1 korisnik = 1 osoba
  - Okupiti korisnike u grupe i regulisati **permisije na nivou grupe**
  - **Uvek dodeljivati minimalna prava**
  - Kreirati jake politike lozinki
    - Barem 8 karaktera, veliko malo slovo, specijalni karakteri, pero albino pauna,...
  - Kreirati role za AWS servise koji treba da rade nešto na AWS platformi
    - **Lambde**
  - Generisati ključeve za programsko korišćenje AWS-a
- 
- 



AWS Identity and Access Management  
(IAM)



# IAM

# Zadaci



1. Kreirati korisnika
2. Kreirati grupu
3. Dodati korisnika u grupu i izlistati sve članove grupe
4. Dodeliti predefinisano *AmazonEC2FullAccess* polisu grupi
  - Oznaka polise: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`
5. Dodeliti predefinisano *AdministratorAccess* polisu korisniku
  - Oznaka polise: `arn:aws:iam::aws:policy/AdministratorAccess`
6. Kreirati Access Key za kreiranog korisnika za SDK potrebe primera *HelloS3*
7. Kreirati polisu koja omogućuje pristup DynamoDB tabeli
8. Kreirati rolu koja omogućava EC2 instanci pristup DynamoDB tabeli
  - Upotrebiti pređašnju polisu

\*[AWS Docs](#), [AWS CLI Docs](#), [LocalStack Docs](#)