

IAM

Identity and Access Management

- uopšteno
- ključni pojmovi
- AWS praktično

Šta je IAM?

Termin za procese, polise i tehnologije koje organizacijama omogućavaju upravljanje digitalnim identitetima.

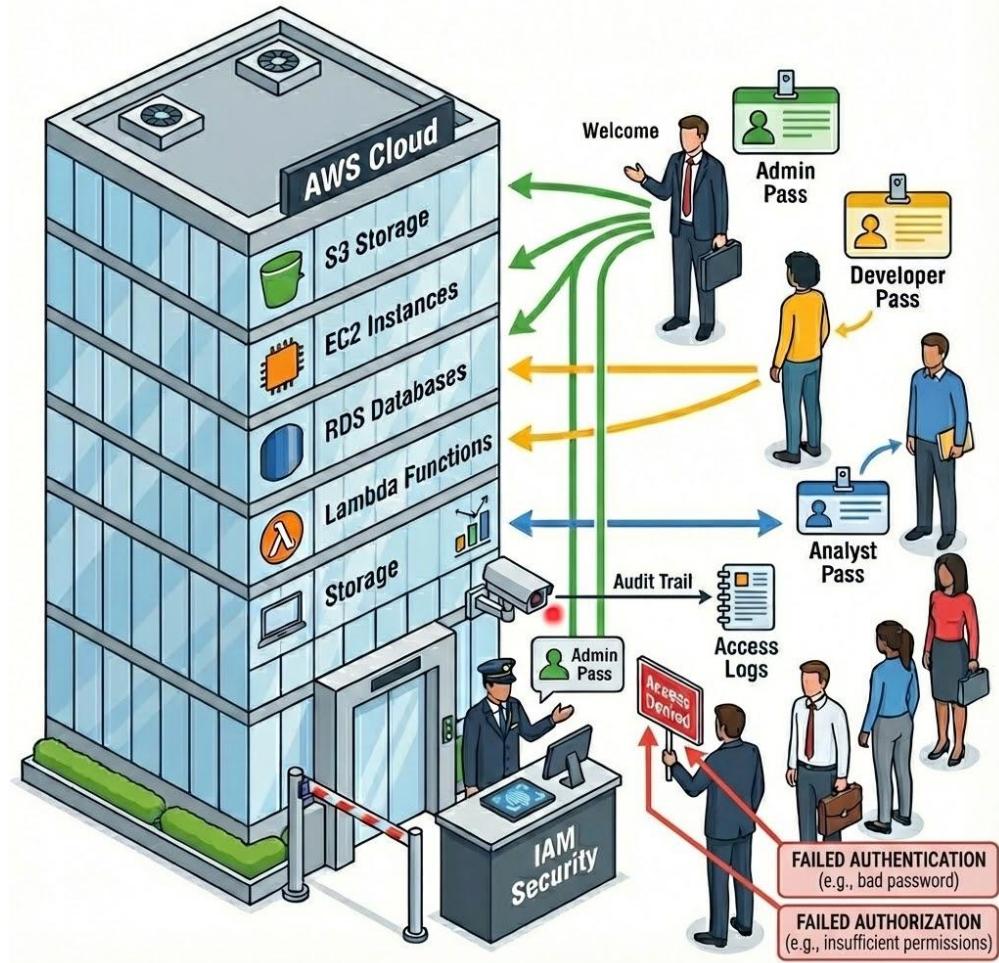
- okvir za upravljanje digitalnim identitetima
- nije samo username i password

→ adekvatni ljudi/identiteti
→ adekvatan pristup
→ adekvatnim resursima
→ u adekvatno vreme
→ iz adekvatnih razloga

- zaposleni, servisi, serveri...
- ciljevi: bezbednost i produktivnost

Analogija "zgrade"

- zgrada = AWS Cloud
- spratovi = AWS servisi
- portir = IAM servis
(stoji na ulazu i proverava)
- ID kartica = identitet
- tip kartice = permisije
- kamera = nadzor



AAAA model

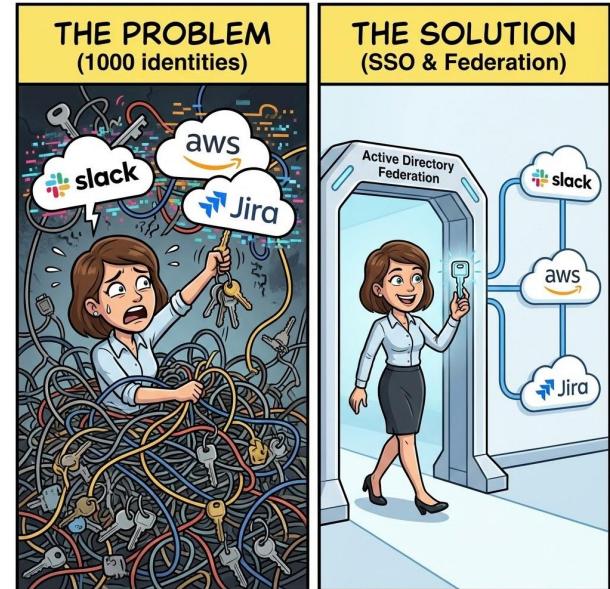


- Administration (Administracija)
 - kreiranje, upravljanje, brisanje **identiteta**
- Authentication (Autentikacija)
 - verifikacija identiteta (šifra, MFA)
- Authorization (Autorizacija)
 - verifikacija dozvola i polisa
- Audit (Revizija)
 - praćenje i beleženje aktivnosti
 - bezbednosni zahtevi organizacija

Gde žive identiteti u većim firmama?

Da li želimo da kreiramo za 1000 zaposlenih identitete za sve servise koji su im neophodni da bi radili posao (Slack, AWS, Jama, Jira, Gemini, Gmail...)?

- Directory Services (imenik identiteta)
→ Microsoft Active Directory
- Federation (federacija)
→ ugovori o poverenju između firme i spoljnih servisa
- SSO (Single Sign-On)
→ jedan nalog za sve



AWS servisi za ovu problematiku: Control Tower, Identity Center, IAM...

Principle of Least Privilege

- dodeljivanje samo minimalnih neophodnih dozvola korisniku/servisu za obavljanje zadataka
- smanjivanje rizika ako dođe do krađe identiteta
- smanjivanje rizika ako dođe do greške korisnika
→ ne želimo da obrišemo produkcionu bazu
- trudimo se da ne budemo lenji, samo da bi sve radilo

Činjenice (bezbednost):
<https://www.ibm.com/reports/data-breach>



IAM servis na AWS-u

Users, Groups, Roles

IAM servis na AWS-u

IAM User

- entitet koji kreiramo da bismo dali pristup konkretnoj osobi
- trajni kredencijali
- nije namenjen da se deli

Šta on može da radi kad se napravi?

Users (0) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age	Access key last use	ARN	Creation time	Consol

Access denied to iam:ListUsers
You don't have permission to `iam:ListUsers`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: arn:aws:iam::105859664880:user/marf-user
Action: iam:ListUsers
On resource(s): arn:aws:iam::105859664880:user/
Context: no identity-based policy allows the action

[Diagnose with Amazon Q](#)

IAM servis na AWS-u

IAM Group

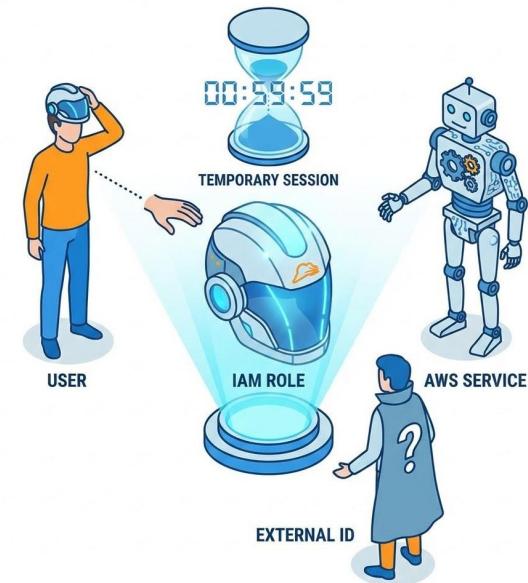
- kolekcija IAM korisnika
- koristi se kada više korisnika treba da ima iste “dozvole”
 - lakše upravljanje
- nasleđivanje dozvola

Kako se grupa razlikuje od korisnika?

IAM servis na AWS-u

IAM Role

- identitet sličan korisniku, ali nije vezan za jednu osobu/servis
 - kao prazna ID kartica koja se pozajmi
- nema lozinku ni trajne ključeve
- privremeni pristup nekim resursima (sesije do 12h)
- može da je koristi bilo ko naveden u “Trust Policy”
(u nastavku predavanja detaljnije)
- može da se zakači na više entiteta istovremeno
- AWS servis ne može da koristi drugi AWS servis bez pravilne autorizacije



Permissions/Policy

- Prolazimo kroz permisije (screenshot)
- Koncept policy-a kao dokumenta koji opisuje koje permisije su dozvoljene (json struktura)
- Statement definicija
 - Principal
 - Action
 - Effect
 - Resource
 - Sid....

IAM Policies Structure

- Consists of
 - Version: policy language version, always include "2012-10-17"
 - Id: an identifier for the policy (optional)
 - Statement: one or more individual statements (required)
- Statements consists of
 - Sid: an identifier for the statement (optional)
 - Effect: whether the statement allows or denies access (Allow, Deny)
 - Principal: account/user/role to which this policy applied to
 - Action: list of actions this policy allows or denies
 - Resource: list of resources to which the actions applied to
 - Condition: conditions for when this policy is in effect (optional)

```
{  
  "Version": "2012-10-17",  
  "Id": "S3-Account-Permissions",  
  "Statement": [  
    {  
      "Sid": "1",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": ["arn:aws:iam::123456789012:root"]  
      },  
      "Action": [  
        "s3:GetObject",  
        "s3:PutObject"  
      ],  
      "Resource": ["arn:aws:s3:::mybucket/*"]  
    }  
  ]  
}
```

© Stephane Maarek

@denimy

- Mogu da se zakače na servise/grupe/usere
- Dodaj graf gde 1 lambda ima 1 rolu, 1 rola ima više polisa

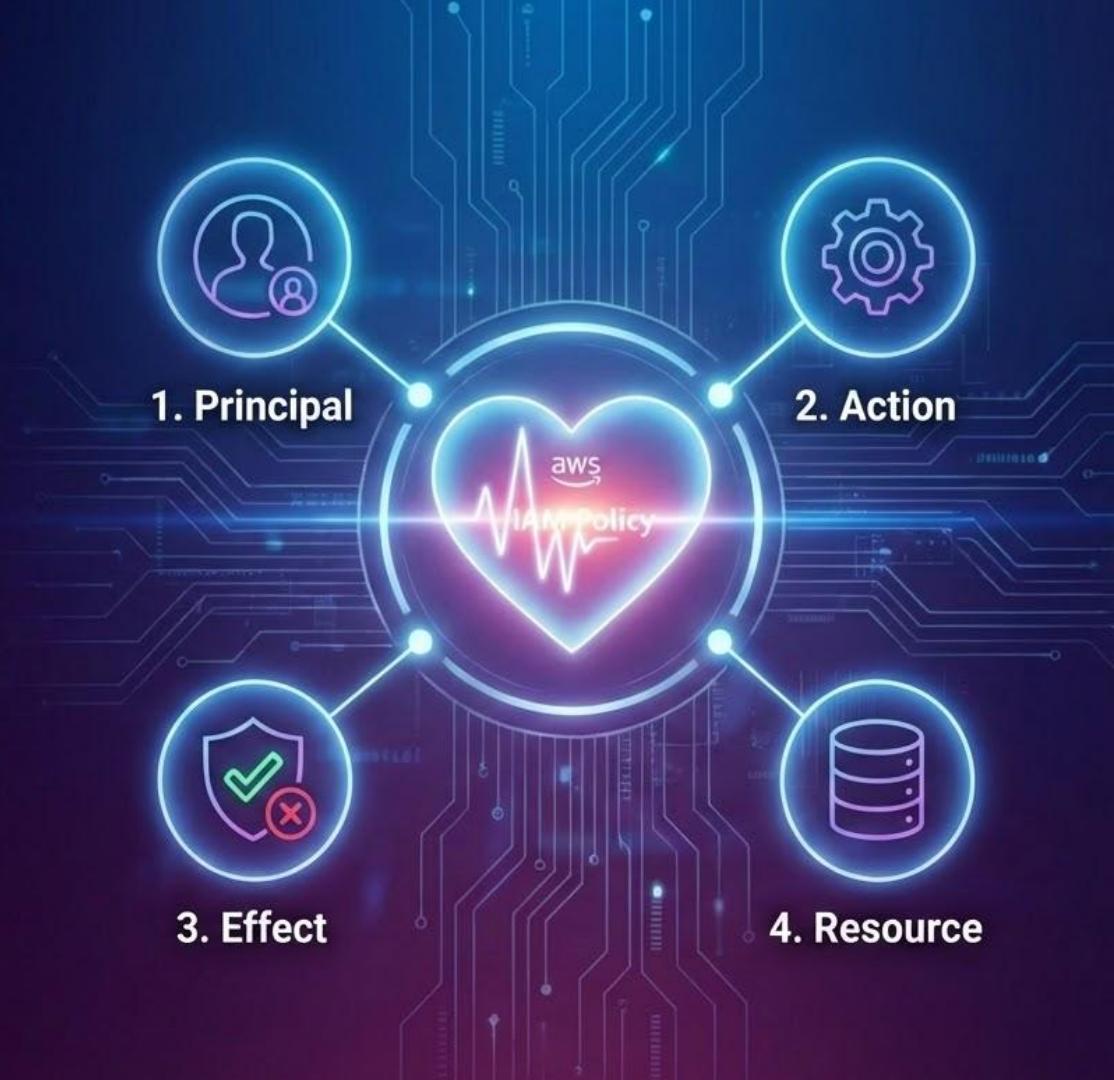
Permissions/Policy

Policy je JSON dokument koji opisuje permisije

Definiše šta je dozvoljeno ili zabranjeno određenom entitetu.

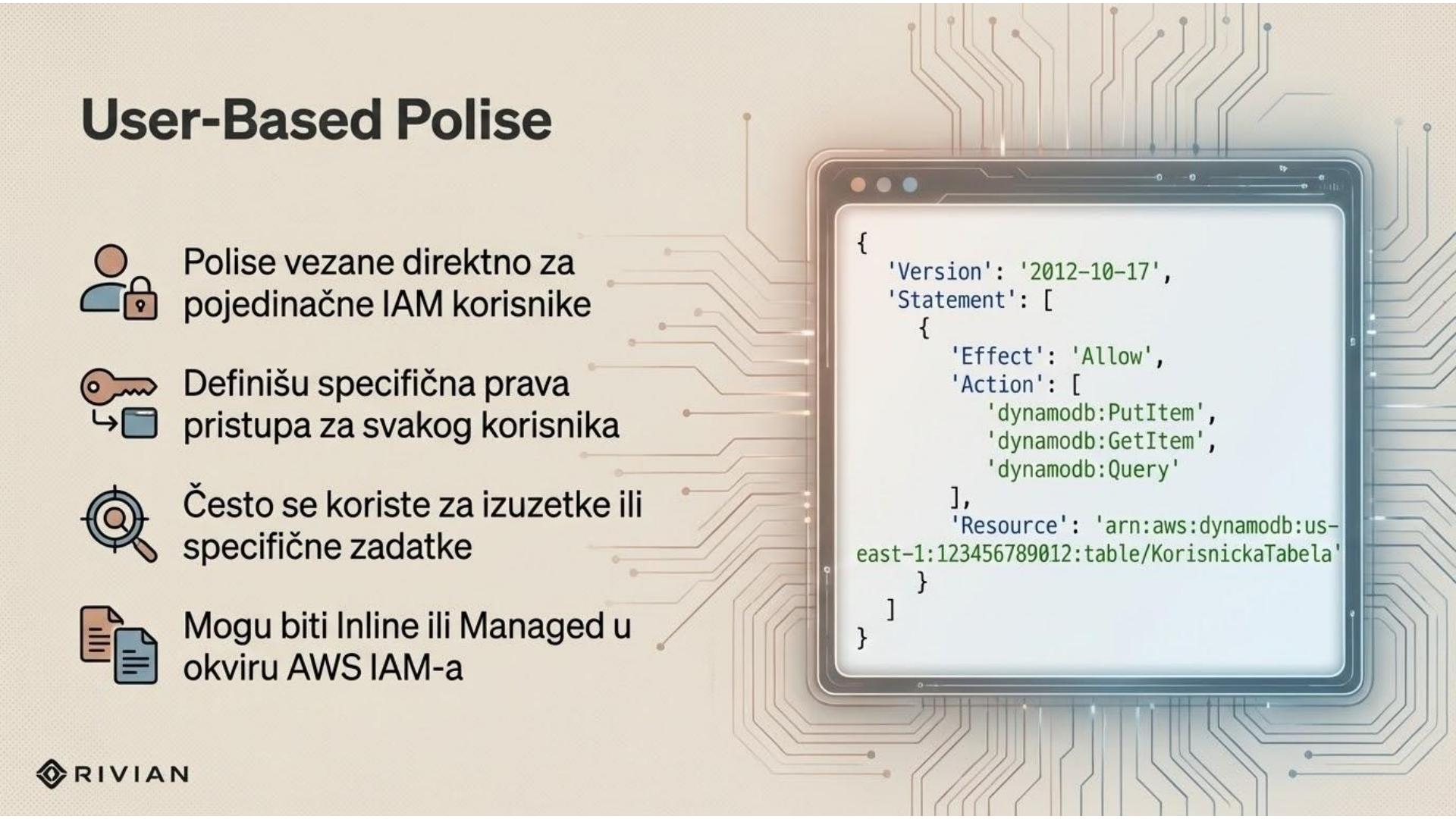
Ključni elementi:

1. Principal
2. Action
3. Effect
4. Resource.



User-Based Policies

-  Polise vezane direktno za pojedinačne IAM korisnike
-  Definišu specifična prava pristupa za svakog korisnika
-  Često se koriste za izuzetke ili specifične zadatke
-  Mogu biti Inline ili Managed u okviru AWS IAM-a



```
{  
    'Version': '2012-10-17',  
    'Statement': [  
        {  
            'Effect': 'Allow',  
            'Action': [  
                'dynamodb:PutItem',  
                'dynamodb:GetItem',  
                'dynamodb:Query'  
            ],  
            'Resource': 'arn:aws:dynamodb:us-east-1:123456789012:table/KorisnickaTabela'  
        }  
    ]  
}
```

Resource-Based Policies



Polise vezane direktno za pojedinačne resurse (npr. S3 bucket)



Definišu ko (principal) može pristupiti resursu i koje akcije su dozvoljene



Idealno za deljenje resursa između različitih AWS naloga

```
{  
  'Version': '2012-10-17',  
  'Statement': [  
    {  
      'Effect': 'Allow',  
      'Principal': '*',  
      'Action': [  
        's3:GetObject'  
      ],  
      'Resource': 'arn:aws:s3:::my-  
bucket/*'  
    }  
  ]  
}
```

Trust Policy u IAM-u

- Trust Policy definiše ko može da preuzme ulogu
- U suštini to je deo IAM Role definicije
- Određuje Principal-e koji su dozvoljeni za preuzimanje



Localstack

localhost.localstack.cloud:4566 ... Overview Status Resource Browser State IAM Policy Stream Chaos Engineering Extensions

Region: us-east-1 Account ID: 000000000000

Resource Browser

Which service are you looking for?

App Integration	Management/Governance	Security/Identity Compliance	Database
API Gateway	CloudFormation	Cognito	DynamoDB
SQS	CloudWatch Logs	Secrets Manager	RDS
SNS	CloudWatch	KMS	ElastiCache
Step Functions	Simple Systems Manager (SSM)	IAM	Timestream
EventBridge	CloudTrail	Certificate Manager	DocumentDB
Application Auto Scaling	Account	S3	Neptune
MWAA	Business Applications	Backup	Athena
MQ	Developer Tools	SageMaker	Kinesis
EventBridge Pipes	CodeCommit	Transcribe Service	Data Firehose
Compute	Front-end Web & Mobile	Machine Learning	Analytics
EC2	AppSync	SageMaker	Athena
Lambda	Amplify	Transcribe Service	Kinesis
ECS	Database Migration Service	Cost Explorer	Data Firehose
ECR			Kafka
EKS			Glue

Effective Unit Testing for AWS Step Functions

AWS recently introduced enhancements to the TestState API for unit testing...

Read More Dismiss

Ultimate trial expires 11 days

PITANJA

