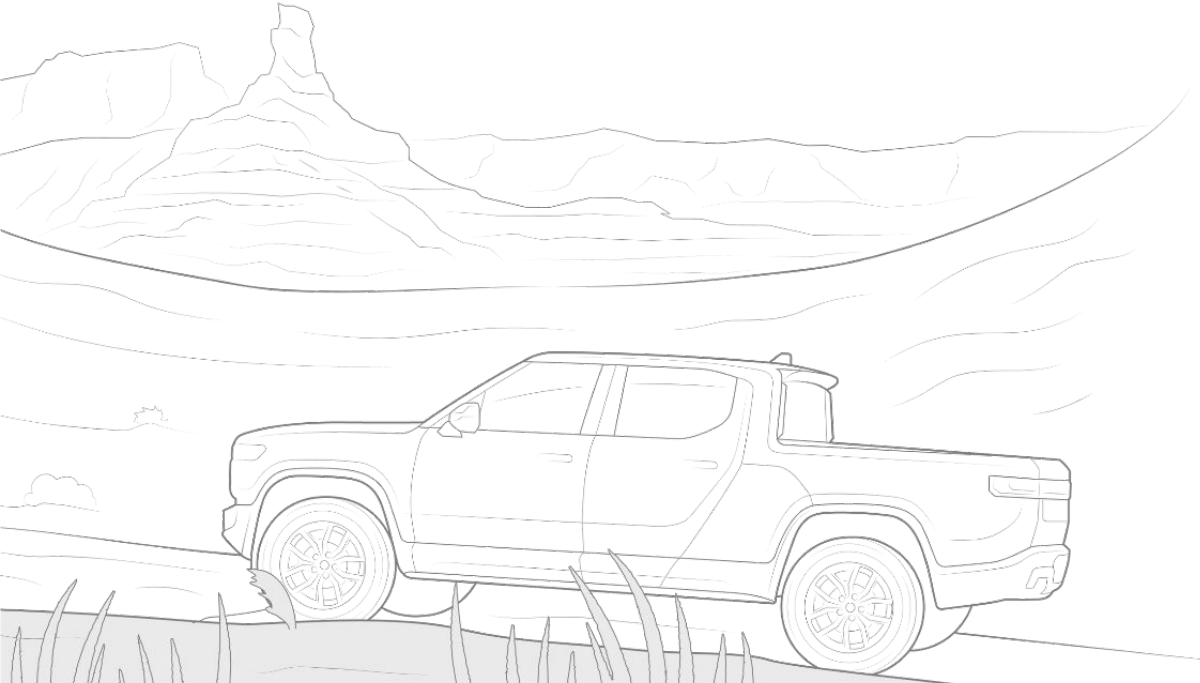


IAM

Identity and Access Management

- uopšteno
- ključni pojmovi
- AWS praktično

R|V TECH

Šta je IAM?

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

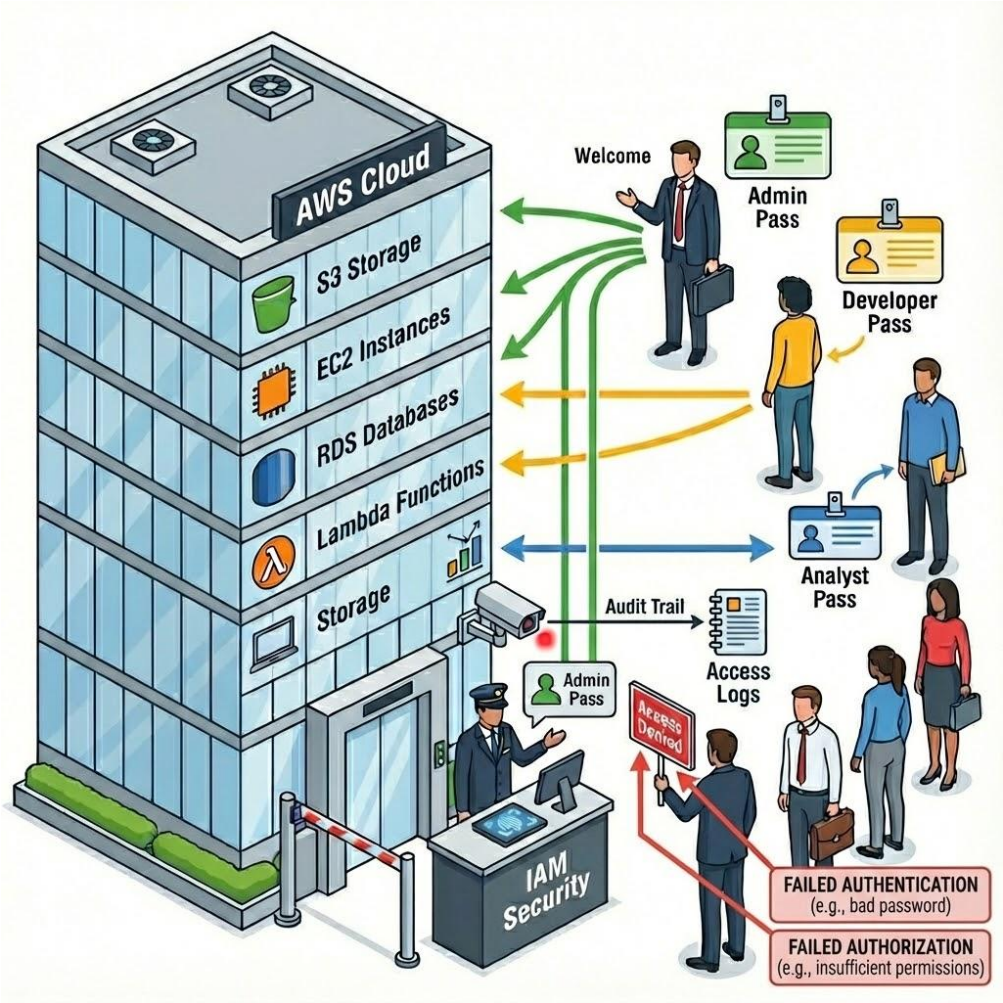
- okvir za upravljanje digitalnim identitetima
- nije samo username i password

→ 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



R|V TECH

AAAA model

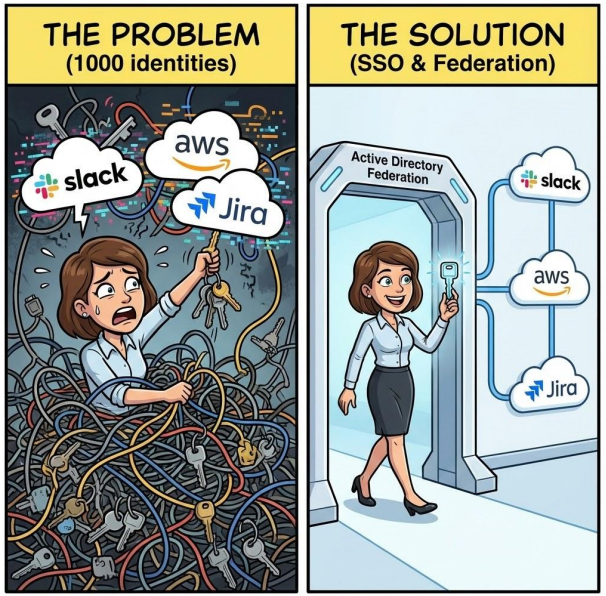
- Administration (Administracija)
  - kreiranje, upravljanje, brisanje ***identiteta***
- Authentication (Autentikacija)
  - verifikacija identiteta (šifra, MFA)
- Authorization (Autorizacija)
  - verifikacija dozvola i polisa
- Audit (Revizija)
  - praćenje i beleženje aktivnosti
  - bezbednosni zahtevi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

R|V TECH

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…

R|V TECH

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

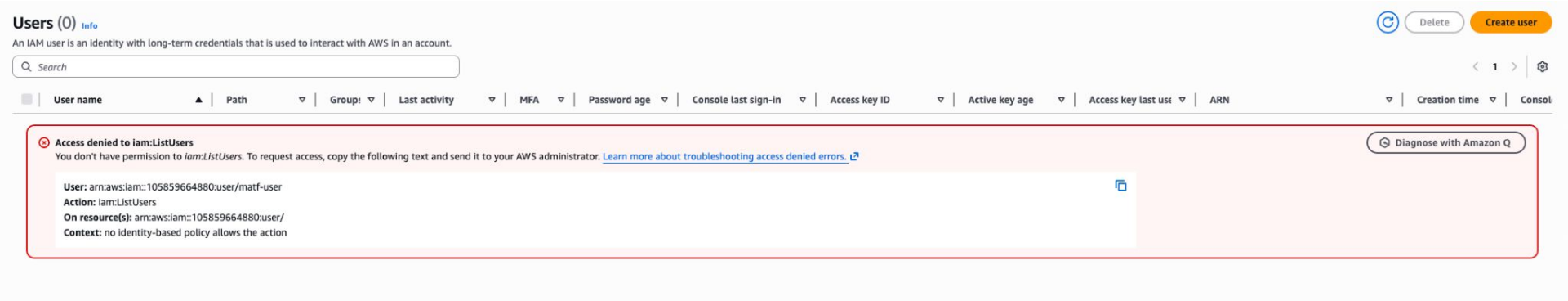
R|V
TECH

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?



R|V TECH

IAM servis na AWS-u

IAM Group

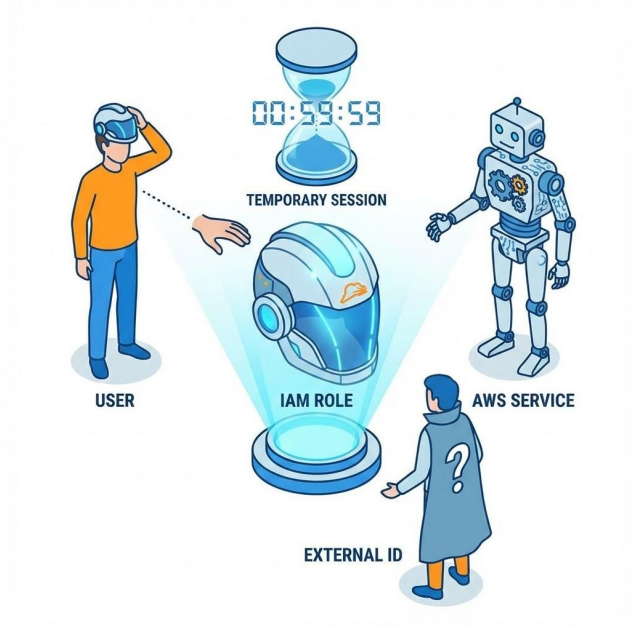
- kolekcija IAM korisnika
- koristi se kada više korisnika treba da ima iste “dozvole”
  → lakše upravljanje
- nasleđivanje dozvola

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

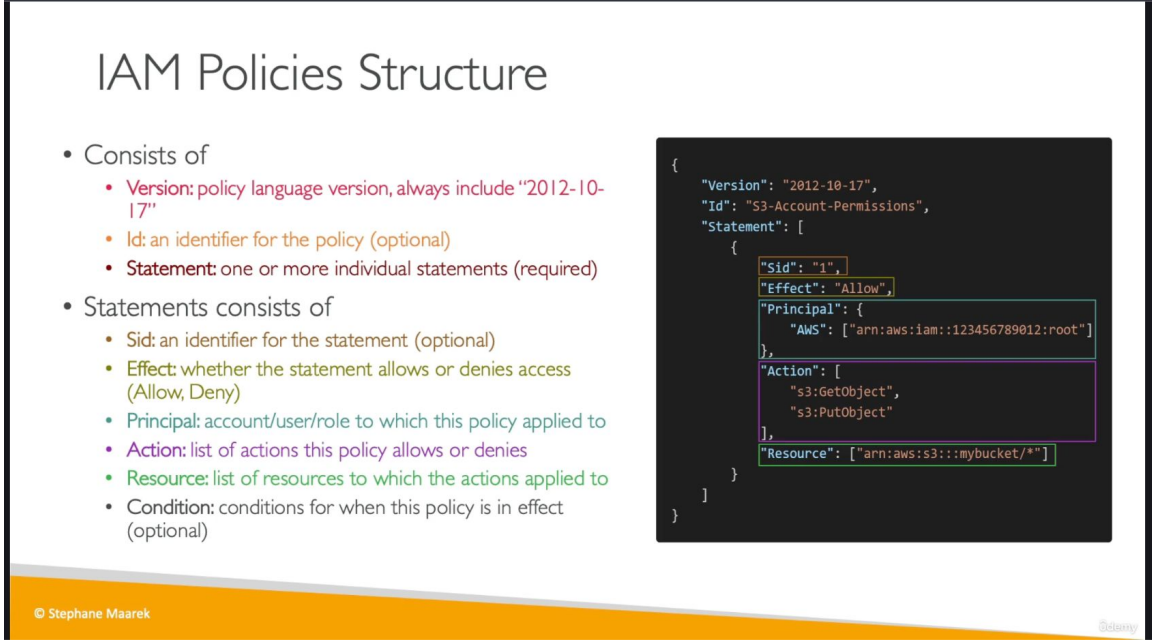


R|V TECH

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….



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

R|V TECH

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.

R|V TECH

User-Based Polise

- 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'
      }
   ]
}
```

RIVIAN

Resource-Based Polise

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/*'
      }
   ]
}
```

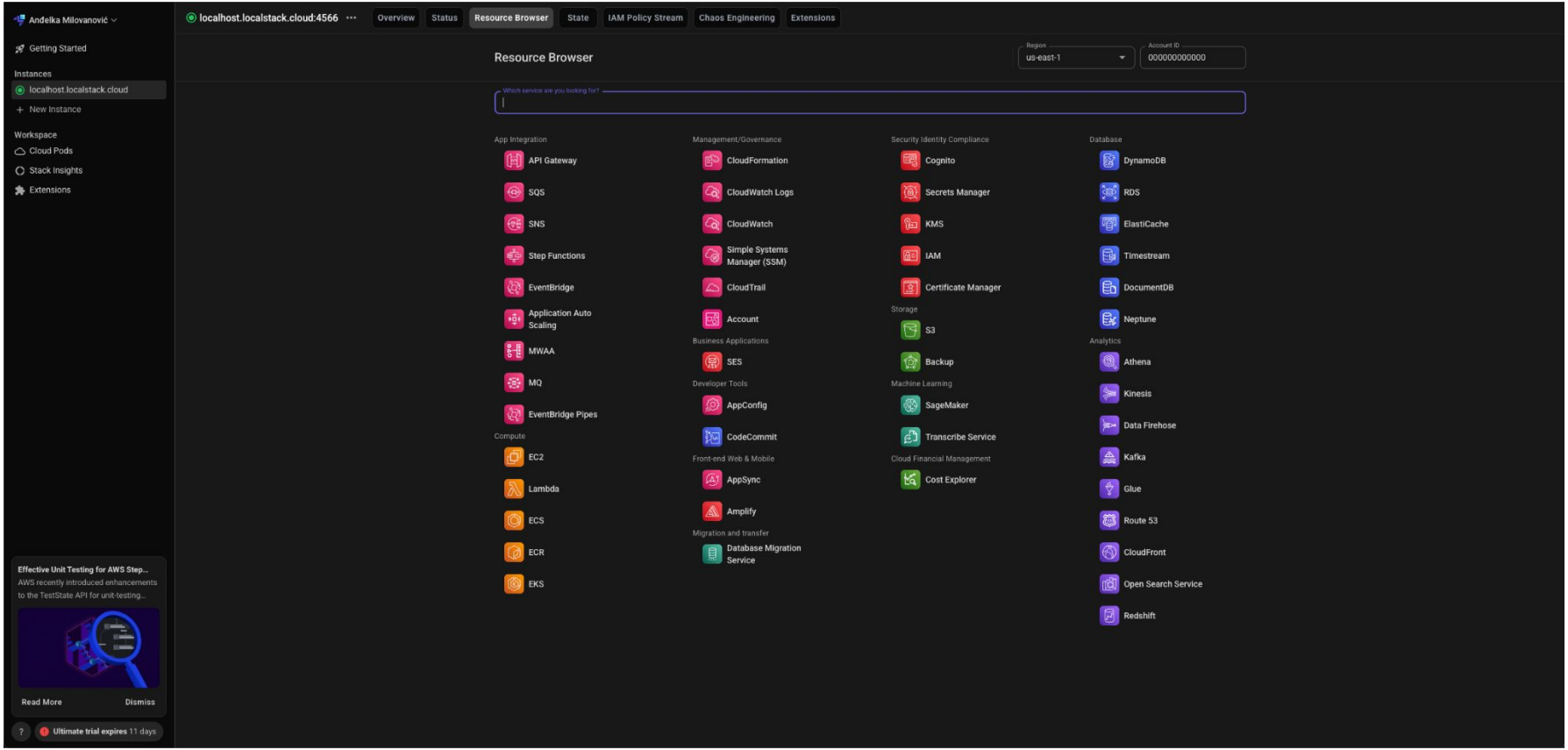
RIVIAN

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

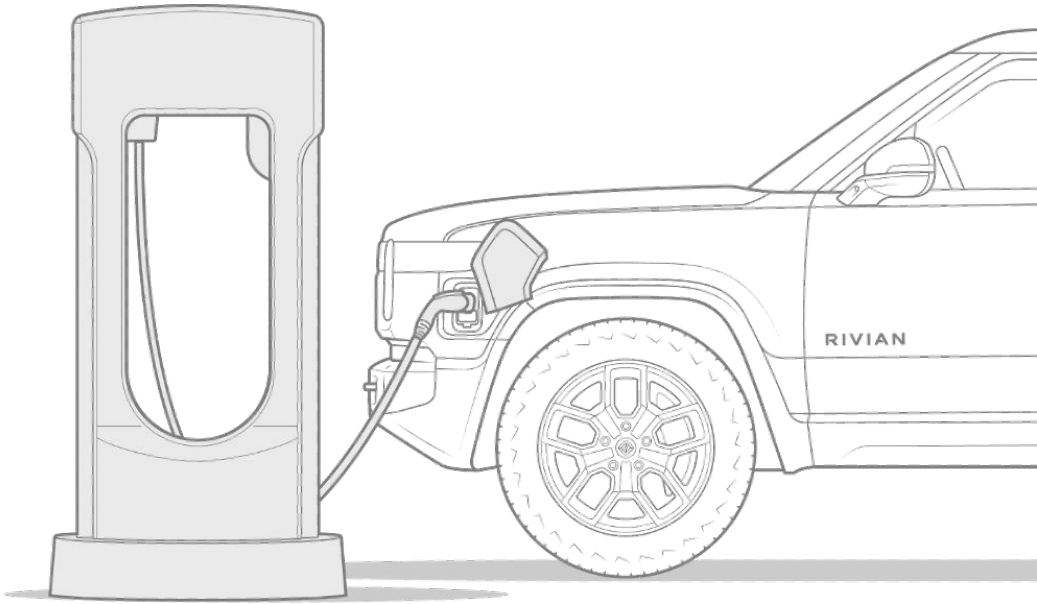
R|V TECH

Localstack



R|V TECH

PITANJA



R|V
TECH