Ralph Klos
PROJECTS & CONSULTANCY

HANDLEIDING

Werken met de IAM Builder

Least-privilege rollen, trust policies en rechten voor AWS IAM

VOOR
Ontwikkelaars, cloud- en platformteams

VAN
Ralph Klos Projects & Consultancy

VERSIE
IAM Builder 0.1

DATUM
6 oktober 2026

Inhoud

1. In het kort 3

2. Openen 3

3. Regio en accounts 3

4. Een rol in drie vragen 4

5. Uit code of uit logs 5

6. Alleen een policy 6

7. Het resultaat 6

8. Uitrollen 6

9. Projecten bewaren 7

10. Veiligheid en grenzen 7

1. In het kort

De IAM Builder maakt IAM-rollen met alleen de rechten die een toepassing echt nodig heeft. Per rol beantwoordt u drie vragen: wie gebruikt hem, wat mag hij doen en wat start hem. U krijgt de trust policy, de permissions policy en, over accounts heen, ook de policy aan de andere kant, als JSON of Terraform.

- **Het minimum dat werkt: lezen** of **lezen en schrijven** kiest de acties die samen nodig zijn, niet elke lees- of schrijfactie van de dienst. Meer vinkt u zelf aan.
- **Elke AWS-dienst:** met de acties, resourcetypes en ARN's uit de Service Authorization Reference van AWS.
- **Uit uw code of uit de logs:** plak code (boto3, JavaScript SDK, AWS CLI) of CloudTrail-events, en de acties die echt gebruikt worden staan erin.
- **Volledig in uw browser:** de pagina roept AWS niet aan, vraagt geen sleutels en stuurt niets weg, ook geplakte code en logs niet. Dat legt de pagina zelf vast in haar Content-Security-Policy.
- **Nederlands en Engels:** wissel met **NL / EN** bovenaan. Uw keuzes blijven in de browser bewaard.

> Bij elke regel in het resultaat staat waarom hij er staat. Zo kan een reviewer de policy nalezen zonder de builder te kennen.

2. Openen

- Online: **rkpc.be/tools/iam-builder/**. Er wordt niets geïnstalleerd en niets bewaard op de website.
- Of lokaal: open `index.html` van de map `rkpc-iam` in een recente browser (Edge, Chrome, Firefox, Safari). Ook zonder internet.
- De browser onthoudt de laatste stand. **Nieuw** maakt alles leeg, na een bevestiging in de pagina.

3. Regio en accounts

Vul de regio in en de accounts waarin de rollen en resources staan, elk met een naam en een account-ID van 12 cijfers. Zolang een ID ontbreekt, staat het voorbeeld 111122223333 van de AWS-documentatie in de policies en waarschuwt de pagina. Met meer dan één account kiest u per rol en per resource het account; zo maakt de builder ook toegang over accounts heen.

4. Een rol in drie vragen

Klik **+ Nieuwe rol**. Elke rol is een kaart met drie vragen. De naam vult zich in volgens wie de rol gebruikt; u kunt hem zelf wijzigen.

4.1 1. Wie gebruikt deze rol?

Dit wordt de trust policy. Kies uit één lijst:

KEUZE	WAT DE TRUST POLICY KRIJGT
EC2-server	`ec2.amazonaws.com`, een instance profile, en naar keuze Session Manager en de CloudWatch-agent
ECS-taak	Een taakrol en een execution role, met `aws:SourceAccount` en `aws:SourceArn`; ECR, logs en ECS Exec
Lambda-functie	`lambda.amazonaws.com`, logs alleen naar de eigen log group, naar keuze VPC en X-Ray
Een andere AWS-dienst	Meer dan 30 diensten (Backup, Glue, Step Functions, CodeBuild, EKS Pod Identity …) of een eigen service principal, met `aws:SourceAccount` en naar keuze `aws:SourceArn`
GitHub Actions	OIDC met `aud` en een `sub` voor uw organisatie, repository en branch of environment; nooit een kale *
Een ander account	Eén rol of het account, naar keuze met external ID en MFA
Externe identity provider	OIDC of SAML, met de voorwaarden op audience en subject

> `aws:SourceAccount` beschermt tegen het confused-deputy-probleem: alleen wanneer de dienst voor uw account werkt, mag hij de rol aannemen. Het voorbeeld bij `aws:SourceArn` volgt de dienst die u kiest.

4.2 2. Wat mag de rol doen?

Dit wordt de permissions policy. Klik **+ AWS-dienst** en kies uit de lijst: bovenaan de kant-en-klare resources, daaronder alle AWS-diensten.

SOORT	HOE HET WERKT
Kant-en-klaar	S3, DynamoDB, SQS, SNS, Secrets Manager, Parameter Store, ECR en Lambda. U vult de naam in en kiest het niveau (bv. lezen, schrijven, lezen en schrijven). De rij toont het minimum en de extra acties als vinkjes, elk met waarom u ze nodig zou hebben. Naar keuze de KMS-sleutel, alleen via die dienst.
Elke andere dienst	Kies een of meer resourcetypes en vul de delen van de ARN in. Klik dan **Minimum: lezen** of **lezen en schrijven**, of vink de acties zelf aan. De acties van de gekozen resourcetypes staan bovenaan.

Het minimum bevat de acties die samen nodig zijn: een update werkt niet als de code niet kan vinden of lezen wat ze bijwerkt. Voor Backup met een backup plan is dat `GetBackupPlan`, `ListBackupPlans`, `ListBackupPlanVersions` en `UpdateBackupPlan`. Voor ongeveer 50 veelgebruikte diensten komt het minimum uit een samengestelde lijst; voor de andere is het een schatting op basis van de resourcetypes. De pagina zegt welke van de twee.

Tagging zit altijd in het minimum

Tag en Untag van de resource zelf staan altijd in het minimum, op elk niveau: tagbeleid en scantools controleren of de tags van een resource bijgehouden worden. De builder neemt de eigen acties van de dienst (`sqs:TagQueue`, `ssm:AddTagsToResource`, `iam:TagRole`, `backup:TagResource` …), alleen op die ene resource en alleen in de policy van de rol. Kan een dienst het gekozen type niet taggen (een Glue-tabel), dan zegt de pagina dat.

Een actie die tot een resource beperkt kan worden, laat de builder nooit op `*` staan: dan vraagt hij het resourcetype. Acties die rechten kunnen wijzigen (privilege escalation) en `iam:PassRole` krijgen een waarschuwing of een fout.

4.3 3. Wat start het? (optioneel)

Voor ECS, Lambda en EC2: een Application Load Balancer, een EventBridge-regel of -Scheduler, een S3-gebeurtenis of een SQS-wachtrij. De builder maakt dan de toestemming die daarbij hoort: een `lambda:InvokeFunction`-permission met `SourceArn` en `SourceAccount`, een rol voor de Scheduler of de rechten om de wachtrij te lezen.

5. Uit code of uit logs

5.1 + Uit code halen

Voor een nieuw systeem is dit de exacte weg. Plak de code die AWS aanroept; de acties die ze gebruikt komen erbij, met hun resourcetype. De namen vult u zelf in.

- Python met boto3 (clients, resources en paginators)
- JavaScript SDK v3 (commands) en v2
- AWS CLI, ook `aws s3 cp` en `sync` met de buckets die ze noemen

De code kan ook aanroepen bevatten die nooit lopen. Kijk het resultaat dus na.

5.2 + Uit logs

Voor een systeem dat al draait. Plak CloudTrail-events van de rol (een logbestand met `Records`, de uitvoer van `aws cloudtrail lookup-events` of JSON-regels), of een policy die IAM Access Analyzer gegenereerd heeft. De acties komen erbij en de namen worden ingevuld uit de ARN's.

```
aws cloudtrail lookup-events --max-results 50 \
  --lookup-attributes AttributeKey=Username,AttributeValue=<sessie-van-de-rol> > events.json
```

Logs tonen alleen wat in die periode gelopen heeft. Een maandelijkse taak of een foutpad ontbreekt dan. Combineer de logs dus met de code.

6. Alleen een policy

Rechten nodig zonder een nieuwe rol, bv. voor een gebruiker, een groep, een bestaande rol of een IAM Identity Center permission set? Klik **+ Alleen een policy (zonder rol)**. U krijgt dan alleen vraag 2, en het resultaat is een customer managed policy (limiet 6.144 tekens).

7. Het resultaat

Rechts staat per rol wat u krijgt. De balk toont hoe vol een document zit ten opzichte van de limiet van IAM; fouten en waarschuwingen staan erboven.

DOCUMENT	WAARVOOR
Trust policy	Wie de rol mag aannemen (limiet 2.048 tekens)
Rechten	Wat de rol mag doen, als inline policy (limiet 10.240 tekens)
Andere kant	Over accounts heen: de bucket policy, queue policy, key policy of resource policy die de rol toelaat
Lambda-permission	Wie de functie mag starten (ALB, EventBridge, S3)
Identity provider	De OIDC- of SAML-provider, eenmaal per account

Wissel tussen **JSON** en **Terraform**. **Kopiëren** en **Downloaden** werken per document; **Alles (.tf)** geeft één Terraform-bestand met alle rollen en policies.

8. Uitrollen

Rol eerst uit in een testaccount en laat de toepassing een volledige cyclus draaien. Valideer de policies met IAM Access Analyzer.

```
aws accessanalyzer validate-policy --policy-type IDENTITY_POLICY \
  --policy-document file://mijn-rol-rechten.json
aws iam create-role --role-name mijn-rol \
  --assume-role-policy-document file://mijn-rol-trust.json
aws iam put-role-policy --role-name mijn-rol --policy-name mijn-rol \
  --policy-document file://mijn-rol-rechten.json
```

Of met Terraform:

```
terraform init
terraform plan
terraform apply
```

Krijgt de toepassing een `AccessDenied`, dan staat de ontbrekende actie in de foutmelding en in CloudTrail. Plak die events via **+ Uit logs** en de actie komt erbij.

9. Projecten bewaren

Geef het project een naam en klik **Bewaren**. U krijgt een leesbaar JSON-bestand met elke keuze. Zet het in Git naast de Terraform-code. Later klikt u **Openen…**, kiest u het bestand en staat alles weer zoals het was. Een bestand dat niet van de builder komt, wordt geweigerd; onbekende of verkeerde waarden worden genegeerd.

> Het projectbestand bevat account-ID's, rol- en resourcenamen. Bewaar het waar de code staat, niet in een publieke repository.

10. Veiligheid en grenzen

- **Geen AWS-toegang:** de builder vraagt geen sleutels, roept geen AWS-API aan en stuurt niets weg.
- **Openbare bronnen:** de acties, resourcetypes en ARN's komen uit de Service Authorization Reference van AWS; de voorwaarden volgen de IAM-gebruikersgids en de gidsen van elke dienst.
- **Het minimum is een startpunt:** de samengestelde lijsten dekken ongeveer 50 diensten; elders is het een schatting. Code en logs geven het exacte beeld.
- **Een startpunt, geen garantie:** kijk de rechten na, test in een testaccount en valideer met IAM Access Analyzer voor u uitrolt.

Vragen? Mail ralph@rkpc.be of kijk op rkpc.be.