Ralph Klos
PROJECTS & CONSULTANCY

HANDLEIDING

Werken met de SCP Builder

Guardrails kiezen, afbakenen en koppelen aan uw AWS-organisatie

VOOR
Cloud- en platformteams

VAN
Ralph Klos Projects & Consultancy

VERSIE
SCP Builder 0.4

DATUM
6 oktober 2026

Inhoud

1. In het kort . . . 3
2. Openen . . . 3
3. Werken met de builder . . . 4
4. Vertrouwde rollen . . . 4
5. Regio's . . . 5
6. Tagging afdwingen . . . 5
7. Vertrekpunten per OU . . . 6
8. Bestaande policies importeren . . . 6
9. Eigen statements . . . 6
10. Andere policytypes . . . 7
11. Samenvatting voor de klant . . . 8
12. Limieten . . . 8
13. Uitrollen . . . 8
14. Projecten en latere wijzigingen . . . 9
15. Veiligheid en grenzen . . . 10

1. In het kort

De SCP Builder stelt de service control policies (SCP's) samen die de meeste AWS-organisaties vandaag gebruiken. U kiest de guardrails, baakt elke guardrail af tot de rollen, accounts en regio's die u wilt, en krijgt policies die binnen de limieten van AWS passen, als JSON of Terraform.

- **Niets te installeren:** het is één webpagina die u opent vanaf uw schijf.
- **Volledig offline:** de pagina roept AWS niet aan, vraagt geen sleutels en stuurt niets weg. Dat legt de pagina zelf vast in haar Content-Security-Policy.
- **U koppelt zelf:** de builder maakt de policies; u bekijkt ze en zet ze in AWS Organizations.
- **Nederlands en Engels:** wissel met **NL / EN** bovenaan. Uw keuzes blijven in de browser bewaard.

> SCP's beperken alleen: ze geven nooit rechten. Ze gelden niet voor het management-account en niet voor service-linked roles. Wat de IAM-policies van een rol toestaan, wordt door de SCP afgetopt.

2. Openen

- Pak de map `rkpc-scp` uit, of kopieer ze, naar een plek naar keuze.
- Dubbelklik `index.html`. Elke recente browser werkt: Edge, Chrome, Firefox of Safari.
- De pagina werkt ook zonder internet, bv. op een afgeschermde beheerpc.
- De browser onthoudt de laatste stand; na het herladen meldt de pagina met welk project u verdergaat. **Nieuw project** en **Herstel** maken alles leeg, na een bevestiging in de pagina zelf.

BESTAND	INHOUD
`index.html`	De pagina
`scp.css`	De huisstijl, licht zoals rkpc.be
`catalog.js`	De guardrails, regio's, vrijstellingen en vertrekpunten per OU
`others.js`	De andere policytypes en het StackSet-template voor back-ups
`help.js`	De hulp per omgeving (knop **Hulp**)
`app.js`	De scope, het verdelen over policies, de uitvoer, projecten

> De knop **Hulp** rechtsboven legt per situatie uit hoe u uitrolt: AWS Organizations, Control Tower, één los account, als code, en later wijzigen.

3. Werken met de builder

	STAP	WAT U DOET
1	**Vertrouwde rollen**	Vink de rollen aan die altijd moeten blijven werken, en voeg uw eigen rollen toe.
2	**Guardrails kiezen**	Kies een **vertrekpunt per OU** of **Meest gebruikt**. Zet daarna aan of uit wat u wilt; filter op categorie of zoek.
3	**Afbakenen**	Open **Opties en scope** per guardrail: instellingen, vrijstelling, accounts en regio's.
4	**Nakijken**	Het resultaat rechts toont het aantal policies, de grootte en de plaatsen op het doel.
5	**Exporteren**	Kies JSON, Terraform of Andere policies en klik **Download** of **Kopieer**. **Samenvatting** bovenaan geeft het overzicht voor de klant.

Per guardrail kunt u de scope zo beperken:

KEUZE	WAT HET IN DE POLICY ZET
Vertrouwde rollen vrijstellen	`ArnNotLike` op `aws:PrincipalArn`: de rollen uit stap 1 vallen erbuiten.
Alleen deze accounts	`StringEquals` op `aws:PrincipalAccount`.
Alle behalve deze	`StringNotEquals` op `aws:PrincipalAccount`.
Alleen in sommige regio's	`StringEquals` op `aws:RequestedRegion`.

> Voorwaarden binnen één statement gelden samen. Een guardrail weigert dus alleen wie geen vertrouwde rol is, in een gekozen account, in een gekozen regio.

4. Vertrouwde rollen

Guardrails slaan vertrouwde rollen over, zodat Control Tower, StackSets, uw pipelines en de break-glass-toegang blijven werken. Dat geldt ook voor de tagging-guardrail: een pipelinerol die resources zonder tags aanmaakt, wordt dan niet geblokkeerd. Per guardrail zet u de vrijstelling uit.

- **Vaste rollen:** Control Tower, StackSets, de Organizations-toegangsrol en een break-glass-rol, met één klik.
- **Eigen rollen:** één ARN per regel; `*` mag, bv. `arn:aws:iam::*:role/pipeline-*`.
- **Vertrouwen via tag:** rollen met bv. `rkpc:trusted = true` zijn ook vrijgesteld. Handig als u veel rollen hebt die u niet allemaal bij naam wilt opsommen.
- **De root-gebruiker** krijgt nooit een vrijstelling: die guardrail geldt voor iedereen.

> Vertrouwen via tag is alleen veilig als niemand de tag zelf kan zetten. Daarom voegt de builder de regel `ProtectTrustTag` toe: alleen de vertrouwde rollen bij naam mogen die tag op een rol, gebruiker of sessie zetten of weghalen. Zonder vertrouwde rol bij naam kan niemand de tag nog zetten; de builder waarschuwt daarvoor.

5. Regio's

Alleen goedgekeurde regio's weigert elke oproep buiten de regio's die u kiest. Globale diensten zoals IAM, Route 53, CloudFront, billing en support draaien vanuit us-east-1 en staan daarom in een uitzonderingslijst (`NotAction`).

De gekozen regio's staan als labels bovenaan; met het kruisje haalt u er een weg. Een regio voegt u toe door de code te typen (de lijst stelt alle commerciële regio's voor, met naam), met Enter of **Toevoegen**, of met een klik op een Europese regio onder **Snel toevoegen**. Meerdere codes met komma's mag ook. Een geldige code die niet in de lijst staat, bv. een nieuwe regio, wordt aanvaard en gemarkeerd met "niet in de lijst": controleer die zelf.

Sommige diensten werken bewust over regio's heen. Die vinkt u aan als u ze toelaat:

DIENST	WAAROM
Bedrock cross-region inference	Inference profiles sturen een oproep naar een andere regio als de eigen regio vol zit.
Amazon Q Developer	Draait vanuit us-east-1.
S3-replicatie	De replicatierol schrijft in de doelregio, bv. voor disaster recovery.
AWS Backup-kopieën	Een copy job schrijft in de vault van de doelregio.
Amazon Q in chat-apps	Een globale dienst.

> Een aangevinkte dienst werkt daarna in elke regio, niet alleen voor het doorsturen. AWS voegt geregeld globale diensten toe: vergelijk de lijst met het actuele voorbeeld van AWS voor u koppelt.

6. Tagging afdwingen

Tags verplichten bij het aanmaken blokkeert nieuwe resources zonder de tags die u opgeeft. De tagnamen kiest u zelf; toegestane waarden zijn optioneel.

INSTELLING	EFFECT
Tagnaam, geen waarden	De tag moet er zijn, met elke waarde. `Null` op `aws:RequestTag/<naam>`.
Tagnaam met waarden	De tag moet er zijn, met een van de waarden. Extra `StringNotEquals`.
Diensten	16 diensten, met **Alles** of **Niets** in één klik: EC2, RDS en Aurora, CloudFormation, Lambda, ECS, EKS, ECR, DynamoDB, EFS, KMS, Secrets Manager, SNS, SQS, CloudWatch Logs, Step Functions en Kinesis.
Beschermen	Niemand haalt de tags weg of zet later een andere waarde.

Onder **Tag policy** krijgt u de bijhorende tag policy. Die legt de schrijfwijze en de waarden vast en toont afwijkingen in de Tag Editor; de SCP doet het blokkeren. Zet tag policies eerst aan in AWS Organizations.

> Waarom niet gewoon "alle diensten"? Een SCP kan een tag alleen eisen bij een aanmaakoproep die tags meekrijgt (`aws:RequestTag`). Een Deny op alle acties zonder tag zou ook elke lees- en lijstoproep blokkeren. De builder dekt daarom de diensten waar het kan; de rest volgt u op met de tag policy en de Tag Editor. CloudWatch Logs staat standaard uit: Lambda en andere diensten maken loggroepen zonder tags aan. CloudFormation aan betekent dat ook CDK- en StackSet-deploys tags nodig hebben.

> Hoofdletters tellen: `CostCenter` is niet `costcenter`. Tag een EC2-instance en zijn volumes in dezelfde launch (`TagSpecifications`), anders weigert de guardrail de launch.

7. Vertrekpunten per OU

Elke OU vraagt iets anders. Kies bovenaan de lijst een vertrekpunt en klik **Toepassen**: de guardrails en de andere policies voor die OU staan dan aan. Daarna stelt u bij zoals altijd.

VERTREKPUNT	WAARVOOR
Root	Wat elk account erft, plus de AI opt-out. Klein houden: elke OU eronder telt deze SCP mee.
Security	Log archive en audit: zo weinig mogelijk wijzigingen.
Infrastructuur	Het netwerkaccount beheert internet gateways en VPN; daarom die guardrails niet.
Workloads productie	Strikt: versleuteling, centraal netwerk, tags, geen IAM-gebruikers; met de declaratieve EC2-policy en de backup policy.
Workloads test en ontwikkeling	Dezelfde basis met meer vrijheid in het netwerk en een rem op dure instancetypes.
Sandbox	Vrij experimenteren binnen een hek: regio's, kosten, AI-modellen, geen verbindingen naar buiten.
Opgeschort	Alles dicht behalve voor de vertrouwde rollen, voor accounts die worden afgesloten.

8. Bestaande policies importeren

Met **Bestaande policies importeren** leest de builder SCP's die al gekoppeld zijn: één bestand, een lijst policies of het `findings.json` van de RKPC Toolkit. Statements die de builder herkent, worden weer guardrails met hun instellingen. Al de rest komt woord voor woord bij de eigen statements: er gaat niets verloren.

> De toolkit bewaart elke SCP met de OU's en accounts waaraan ze hangt. Importeer `findings.json` en u ziet meteen waar u op verder bouwt.

9. Eigen statements

Iets wat niet in de catalogus staat? Plak het onder **Eigen statements**: één statement, een lijst of een volledige policy. Het komt in dezelfde SCP's, de Terraform en het projectbestand. Vink aan of de vertrouwde rollen ook daar vrijgesteld zijn. De kaart staat onder elk filter.

10. Andere policytypes

Naast SCP's kent AWS Organizations andere policies. Elk type zet u eenmalig aan in de root (`aws organizations enable-policy-type`); de knop **Hulp** geeft de commando's.

POLICY	WAT ZE DOET
Resource control policy	Een dataperimeter op uw buckets, sleutels, queues en secrets: alleen via TLS, alleen uw organisatie, AWS-diensten alleen namens u.
Declaratieve EC2-policy	AWS zet de instelling zelf vast: geen publieke AMI's of snapshots, IMDSv2, geen serial console.
AI opt-out	AI-diensten van AWS gebruiken uw inhoud niet om te verbeteren.
Backup policy	Hetzelfde back-upplan in elk account, op basis van een tag.

De backup policy verwijst naar een vault en een rol die in elk account moeten bestaan. Onder **Andere policies** staat daarom ook een **StackSet-template** (CloudFormation) dat ze aanmaakt: de vault in elke regio, de rol één keer per account. Bij het uitrollen vult u de ARN van uw KMS-sleutel in en eventueel het organisatie-ID voor een centraal back-upaccount.

```
aws cloudformation create-stack-set --stack-set-name rkpc-backup \
  --template-body file://rkpc-backup-stackset.json --capabilities CAPABILITY_NAMED_IAM \
  --permission-model SERVICE_MANAGED --auto-deployment
Enabled=true,RetainStacksOnAccountRemoval=false \
  --parameters ParameterKey=KmsKeyArn,ParameterValue=arn:aws:kms:eu-west-1:111122223333:key/...
aws cloudformation create-stack-instances --stack-set-name rkpc-backup \
  --deployment-targets OrganizationalUnitIds=ou-xxxx-xxxxxxxx --regions eu-west-1 eu-central-1
```

> Een KMS-sleutel is per regio: met één sleutel-ARN voor alle regio's gebruikt u een multi-region key, of laat u het veld leeg voor de AWS-sleutel van Backup. De syntaxis van deze policytypes is op 2 oktober 2026 nagekeken tegen de AWS-documentatie; kijk ze opnieuw na als die datum ver achter u ligt.

11. Samenvatting voor de klant

Samenvatting bovenaan maakt een overzicht met de RKPC-hoofding: klant, doel, datum en referentie, wat aan staat en hoe ver het reikt, de vertrouwde rollen, de bestanden, wat nog op te lossen is en de volgende stappen. Het venster toont meteen de A4-pagina's zoals ze op papier komen, met kop- en voetregel en paginanummers; een lange tabel loopt door met de kolomkoppen bovenaan de volgende pagina. **Afdrukken of PDF** (of Ctrl+P) drukt precies die pagina's af, ongeacht de marges in het afdrukvenster. Zet daar enkel **Kop- en voetteksten** uit; de browser stelt de referentie voor als bestandsnaam.

12. Limieten

- **10.240 tekens per SCP.** De builder verdeelt de statements over zo weinig policies als passen. De meter per policy telt de compacte JSON.
- **10 SCP's per doel**, FullAWSAccess inbegrepen. Bij meer waarschuwt de builder: koppel dan een deel aan een bovenliggende OU, die worden geërfd.
- **Andere types:** een RCP 5.120 tekens en 5 per doel (RCPFullAWSAccess inbegrepen); declaratieve, backup- en tagpolicies 10.000 tekens; een AI-opt-outpolicy 2.500 tekens. Zo staat het in de AWS-quota van 2 oktober 2026; AWS verhoogt die soms, kijk bij twijfel op de pagina "Quotas and service limits".
- **Opgemaakt of compact:** downloaden geeft leesbare JSON. De console en de Terraform-uitvoer halen de witruimte zelf weg. Voor de CLI of de API vinkt u **Compact** aan, want daar telt elke spatie mee.

13. Uitrollen

Koppel altijd eerst aan een sandbox-OU. Volg een paar dagen `AccessDenied` in CloudTrail en ga pas daarna naar test en productie.

13.1 In de console

AWS Organizations, **Policies**, **Service control policies**, **Create policy**. Plak de JSON, bewaar, en koppel de policy onder **Targets** aan de OU.

13.2 Met de CLI (vink Compact aan)

Vanuit het management-account, met uw eigen profiel:

```
aws organizations create-policy --type SERVICE_CONTROL_POLICY \
  --name rkpc-guardrails-1 --description "RKPC guardrails" \
  --content file://rkpc-guardrails-1.json
aws organizations attach-policy --policy-id p-xxxxxxxx --target-id ou-xxxx-xxxxxxxx
```

13.3 Met Terraform

Kies **Terraform** en klik **Download**: u krijgt `rkpc-guardrails.tf` en de JSON-bestanden ernaast. Zet ze in één map en geef het doel mee:

```
terraform init
terraform plan -var target_id=ou-xxxx-xxxxxxxx
```

13.4 Testen in de sandbox-OU

- **Wat geweigerd moet worden:** probeer in een sandbox-account, met een gewone rol, een paar acties die een guardrail verbiedt, bv. iets starten in een regio buiten uw lijst. De fout noemt dan "an explicit deny in a service control policy".
- **Wat moet blijven werken:** herhaal het met een vertrouwde rol (break-glass, uw pipeline) en draai uw gewone deployment. Een `AccessDenied` die u niet verwacht, vindt u in CloudTrail.
- **Andere policytypes:** bekijk vanuit het management-account wat een account echt krijgt:

```
aws organizations describe-effective-policy --policy-type TAG_POLICY --target-id 111122223333
aws organizations describe-effective-policy --policy-type BACKUP_POLICY --target-id 111122223333
```

- Hetzelfde met `AISERVICES_OPT_OUT_POLICY` en `DECLARATIVE_POLICY_EC2`. Rol de StackSet uit vóór u de backup policy koppelt, anders mist de vault of de rol.
- **Terug:** loopt iets vast, koppel de policy los met `aws organizations detach-policy`; dat werkt meteen. Laat FullAWSAccess altijd gekoppeld.

13.5 Eén account zonder Organizations

SCP's bestaan alleen in AWS Organizations, en gelden niet voor het management-account. Maak dus een nieuw, leeg management-account en nodig het bestaande account uit als member. Tijdelijk kan de JSON ook als IAM-policy op uw rollen, maar die is los te koppelen en dekt de root-gebruiker niet.

14. Projecten en latere wijzigingen

Geef het project een naam en klik **Project opslaan**. U krijgt een leesbaar JSON-bestand met elke instelling: guardrails, scope, regio's, tags, vrijstellingen en de vertrouwde tag. De Terraform-download bevat het ook. Zet het in Git naast de policies.

- Vraagt de klant een wijziging, klik **Project openen** en kies het bestand.
- Alle schermen staan weer zoals bij het opslaan. Wijzig wat nodig is.
- Sla het project opnieuw op en laat het verschil reviewen (`git diff`) voor u koppelt.

Het bestand bewaart ook de policies zoals ze toen gebouwd zijn. Maakt een nieuwere versie van de builder iets anders, dan waarschuwt de pagina bij het openen: vergelijk dan met wat gekoppeld is. Een bestand dat niet van de builder komt, wordt geweigerd; onbekende of verkeerde waarden worden genegeerd.

> Het projectbestand bevat account-ID's en rolnamen van de klant. Bewaar het waar de policies staan, niet in een publieke repository.

15. Veiligheid en grenzen

- **Geen AWS-toegang:** de builder vraagt geen sleutels, roept geen AWS-API aan en stuurt niets weg.
- **Openbare bronnen:** de guardrails volgen de voorbeelden in de AWS Organizations-gebruikersgids en de AWS Security Reference Architecture.
- **Een startpunt, geen garantie:** elke organisatie is anders. Test in een sandbox-OU en lees de policy na voor u ze koppelt.
- **Het management-account** valt nooit onder een SCP. Houd er geen workloads in.

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