drop-api-secrets-migration-evidence

drop-api Secrets Migration Evidence

Date: 2026-04-29T14:18:08Z **Operator:** Parisa Tabriz (Securion) **MC:** #10150 **Outcome:** BLOCKED — IAM permission gap prevents completion. Remediation documented below.

Pre-Migration State (drop-api)

Service ARN: arn:aws:apprunner:eu-west-1:324480209768:service/drop-api/bdebb303a47c409393691ef8f5530144 **Status:** RUNNING **RuntimeEnvironmentVariables (plain-text — NAMES ONLY, no values):**

- DATABASE_URL (CRITICAL — plain text, 1 of 2 secrets)
- JWT_SECRET (CRITICAL — plain text, 2 of 2 secrets)
- DROP_MODE (non-sensitive)
- PORT (non-sensitive) Total: 4 vars, 2 plain-text secrets

RuntimeEnvironmentSecrets: EMPTY (none configured) **InstanceRoleArn:** NULL (no instance role attached) **AccessRoleArn:** arn:aws:iam::324480209768:role/AppRunnerECRAccessRole (ECR pull only)

AWS Secrets Manager Verification (Step 3)

Both target secrets confirmed PRESENT and VALUES MATCH current plain-text:

Secret Name	ARN	Value Match

drop/production/jwt_secret	arn:aws:secretsmanager:eu-west-1:324480209768:secret:drop/production/jwt_secret-QEsMUJ	MATCH
drop/production/database_url	arn:aws:secretsmanager:eu-west-1:324480209768:secret:drop/production/database_url-QEsMUJ	MATCH

No new secrets needed. Existing SM entries are current and correct.

IAM Analysis (Step 4 — BLOCKER FOUND)

Finding 1: drop-api has NO instance role

drop-web (working SM integration) uses:

- **InstanceRoleArn:** arn:aws:iam::324480209768:role/drop-production-apprunner-instance
- This role has secretsmanager:GetSecretValue on drop/production/* secrets

drop-api has:

- **InstanceRoleArn:** NULL

Without an instance role, App Runner instances cannot call Secrets Manager. Attaching `RuntimeEnvironmentSecrets` without an instance role would cause service startup failure.

Finding 2: alai-cli-deployer lacks iam:PassRole

`aws apprunner update-service` requires `iam:PassRole` on both:

1. The ECR access role (AppRunnerECRAccessRole) — needed even for config-only updates
2. The instance role (drop-production-apprunner-instance) — needed to attach it

Exact errors:

```
AccessDeniedException: User alai-cli-deployer is not authorized to perform: iam:PassRole
  on resource: arn:aws:iam::324480209768:role/drop-production-apprunner-instance

AccessDeniedException: User alai-cli-deployer is not authorized to perform: iam:PassRole
  on resource: arn:aws:iam::324480209768:role/AppRunnerECRAccessRole
```

Target State (READY TO APPLY — pending IAM fix)

New source configuration built and saved to /tmp/drop-api-NEW-source-config.json (chmod 600):

RuntimeEnvironmentVariables (post-migration):

- DROP_MODE (non-sensitive, remains plain)
- PORT (non-sensitive, remains plain)

RuntimeEnvironmentSecrets (post-migration):

- DATABASE_URL → arn:aws:secretsmanager:eu-west-1:324480209768:secret:drop/production/database_url-QEsMUJ
- JWT_SECRET → arn:aws:secretsmanager:eu-west-1:324480209768:secret:drop/production/jwt_secret-QEsMUJ

InstanceRoleArn to attach: arn:aws:iam::324480209768:role/drop-production-apprunner-instance

---

Required IAM Grants (what must be added before migration can complete)

An IAM administrator (or role with iam:PutUserPolicy / iam:AttachUserPolicy) must grant alai-cli-deployer:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::324480209768:role/AppRunnerECRAccessRole",
        "arn:aws:iam::324480209768:role/drop-production-apprunner-instance"
      ],
      "Condition": {
```

```
        "StringEquals": {
          "iam:PassedToService": "build.apprunner.amazonaws.com"
        }
      }
    }
  ]
}
```

Execute Command (ready — run after IAM grant)

```
aws apprunner update-service \
  --service-arn arn:aws:apprunner:eu-west-1:324480209768:service/drop-
api/bdebb303a47c409393691ef8f5530144 \
  --source-configuration file:///tmp/drop-api-NEW-source-config.json \
  --instance-configuration InstanceRoleArn=arn:aws:iam::324480209768:role/drop-production-
apprunner-instance \
  --profile alai-cli-deployer \
  --region eu-west-1
```

Then verify:

```
aws apprunner describe-service \
  --service-arn arn:aws:apprunner:eu-west-1:324480209768:service/drop-
api/bdebb303a47c409393691ef8f5530144 \
  --profile alai-cli-deployer --region eu-west-1 | jq '.Service.Status'

curl -sI https://app.getdrop.no/api/health | head -5
```

Expected: Status = RUNNING, HTTP 200.

Rollback Path

Rollback file: /tmp/drop-api-rollback-vars.json (chmod 600, contains plain-text values — /tmp only)
Pre-migration full config: /tmp/drop-api-PRE-migration.json (chmod 600)

Rollback command (restores plain-text state, removes secrets indirection):

```
aws apprunner update-service \
  --service-arn arn:aws:apprunner:eu-west-1:324480209768:service/drop-
api/bdebb303a47c409393691ef8f5530144 \
  --source-configuration "$(jq '.Service.SourceConfiguration' /tmp/drop-api-PRE-
migration.json)" \
  --instance-configuration Cpu=1024,Memory=2048 \
  --profile alai-cli-deployer --region eu-west-1
```

Note: Rollback also requires iam:PassRole — same IAM grant needed.

Smoke Test (pending migration)

- Health endpoint: https://app.getdrop.no/api/health (per DEPLOY-MAP)
- Expected: HTTP 200, status: "ok"
- NOT YET EXECUTED — service not updated

Files (sensitive — /tmp only, never committed)

- /tmp/drop-api-PRE-migration.json (chmod 600) — full pre-state including plain values
- /tmp/drop-api-rollback-vars.json (chmod 600) — extracted plain env vars for rollback
- /tmp/drop-api-NEW-source-config.json — new source config ready to apply

---

Revision #3
Created 2026-04-29 14:21:37 UTC by John
Updated 2026-05-31 20:07:00 UTC by John