AWS Auth Runbook — alai-cli-deployer IAM key (MC #9523)

AWS Auth Runbook (post-MC #9523)

Status

Active as of 2026-04-27. IAM access key created, activated, verified.

Primary auth

- **IAM User:** alai-cli-deployer
- **UserId:** AIDAUXDEHCNUHSS72WSYC
- **Arn:** arn:aws:iam::324480209768:user/alai-cli-deployer
- **Access Key ID:** AKIAUXDEHCNUBIP6OGV5
- **Credentials file:** ~/.aws/credentials profile [alai-cli-deployer] (mode 0600)
- **Bitwarden item:** "AWS IAM Access Key — alai-cli-deployer" (ID: 0605acce-fb80-4a36-ac11-3b55ffe66a3e)
- **Primary region:** eu-west-1 (Drop App Runner + ECR)
- **Secondary region:** eu-north-1

Shell activation

AWS_PROFILE=alai-cli-deployer is exported in ~/.zshrc (added MC #9523, 2026-04-27). No interactive login needed. All aws commands use this profile by default.

Override for a single command: AWS_PROFILE=alai-cli-deployer aws

Daily use

No login needed. All aws CLI commands authenticate via the access key in ~/.aws/credentials.

Verification at any time: aws sts get-caller-identity Expected: UserId AIDAUXDEHCNUHSS72WSYC, Arn arn:aws:iam::324480209768:user/alai-cli-deployer

aws apprunner list-services --region eu-west-1 aws ecr describe-repositories --region eu-west-1

IAM Policies (as of MC #9523, 2026-04-27)

Policy | Rationale AWSAppRunnerFullAccess | Drop deploy - create/update/start App Runner services AmazonEC2ContainerRegistryFullAccess | Push/pull Docker images to ECR (Drop API + Web) SecretsManagerReadWrite | Read/write Drop secrets (DB, API keys) AmazonS3FullAccess | Build artifacts, CodeBuild source/output buckets CloudWatchLogsFullAccess | App Runner + CodeBuild runtime logs AWSCodeBuildAdminAccess | MC #9540 Drop CodeBuild (future)

Key rotation (every 90 days - next due 2026-07-26)

1. Create new access key: aws iam create-access-key --user-name alai-cli-deployer > /tmp/new-key.json
2. Update credentials file (use Python, do NOT print secret to terminal): python3 -c " import os, json, configparser new = json.load(open('/tmp/new-key.json'))['AccessKey'] cfg_path = os.path.expanduser('~/.aws/credentials') config = configparser.ConfigParser() config.read(cfg_path) config['alai-cli-deployer']['aws_access_key_id'] = new['AccessKeyId'] config['alai-cli-deployer']['aws_secret_access_key'] = new['SecretAccessKey'] with open(cfg_path, 'w') as f: config.write(f) os.chmod(cfg_path, 0o600) print('Updated:', new['AccessKeyId']) "
3. Verify: AWS_PROFILE=alai-cli-deployer aws sts get-caller-identity
4. Delete old key: aws iam delete-access-key --user-name alai-cli-deployer --access-key-id OLD_KEY_ID
5. Update Bitwarden item 0605acce-fb80-4a36-ac11-3b55ffe66a3e with new key values
6. Shred temp file: shred -u /tmp/new-key.json

Recovery (if credentials file lost)

1. Retrieve key from Bitwarden: SESSION=0L9KMqYMX1/HfMdDBLJ3MsNZwATGz5Bv++fCFat2uT1RPCrvy1mCrcsNiL0uGxei

yTIJXKWkWV28W0vjZEjq4A== BW_SESSION= bw --nointeraction get item 0605acce-fb80-4a36-ac11-3b55ffe66a3e | jq -r '.login.username, .login.password'

2. Re-create ~/.aws/credentials profile with recovered values (mode 0600)
3. Verify: AWS_PROFILE=alai-cli-deployer aws sts get-caller-identity

Recovery (if Bitwarden unavailable - last resort)

1. Authenticate as a user with IAM admin access
2. Create new access key: aws iam create-access-key --user-name alai-cli-deployer
3. Update credentials file + Bitwarden
4. Delete old key after verification

Security notes

- Credentials file at ~/.aws/credentials is local convenience copy (mode 0600)
- Bitwarden (vault.basicconsulting.no) is source of truth for recovery
- DO NOT print SecretAccessKey to terminal - always write directly to file via Python
- DO NOT commit credentials to any git repo
- AWS account: 324480209768 (ALAI)
- IAM user has NO console access (programmatic only)

Services accessible with this profile

- App Runner: drop-api (RUNNING), drop-web (RUNNING) - eu-west-1
- ECR: drop-api, drop-web repositories - eu-west-1
- Secrets Manager: all secrets in account
- S3: all buckets
- CloudWatch Logs: all log groups
- CodeBuild: all projects (for MC #9540)

Revision #2
Created 2026-04-27 19:29:56 UTC by John
Updated 2026-05-31 20:06:36 UTC by John