AWS access documentation

This document gives the access that Fingoweb needs in your AWS account. It also tells you how to make, use and remove this access.
This document is for these Fingoweb services in AWS Marketplace:

- Container Optimization for Amazon ECS
- Autoscaling GitLab CI Runners on AWS

Assessment

For the assessment, you make one IAM role in each AWS account that we examine. The role has these parts:

- **Trust policy.** Only the Fingoweb AWS account can assume the role. Fingoweb must also give the external ID that we send to your company.
- **AWS managed policies `ViewOnlyAccess` and `SecurityAudit`.** These policies let us read the configuration and the metrics of your resources. They do not let us read the objects in your S3 buckets.
- **Inline policy.** This policy lets us read your cost data and your optimization data.

Make the role

1. Make an IAM role with the trust policy in this document.
2. In the trust policy, put the account ID and the external ID that we send you.
3. Attach the AWS managed policies `ViewOnlyAccess` and `SecurityAudit` to the role.
4. Add the inline policy in this document to the role.
5. Send the ARN of the role to Fingoweb.

Remove the role

1. After you get the assessment report, delete the role.

Trust policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<058264220596>:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "<EXTERNAL_ID>"
        }
      }
    }
  ]
```

```
}
```

Inline policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ce:Describe*",
        "ce:Get*",
        "ce:List*",
        "cost-optimization-hub:Get*",
        "cost-optimization-hub:List*",
        "compute-optimizer:Describe*",
        "compute-optimizer:Get*",
        "savingsplans:Describe*",
        "budgets:ViewBudget"
      ],
      "Resource": "*"
    }
  ]
}
```

Implementation

Normally, we do not need write access to your AWS account. We send the changes to the infrastructure code and to the application code as merge requests. Your pipeline deploys the changes with your deployment role.
Sometimes we need direct access, for example if you do not have a deployment pipeline. In that case:

- The implementation plan gives the exact IAM policy.
- The policy gives access only to the services in the plan.
- You examine the policy before you make the role.
- At the end of the work, you delete the role.

Contact

If you have questions about access, send an email to contact@fingoweb.com.