Retrieve Accounts info from an Organization Unit

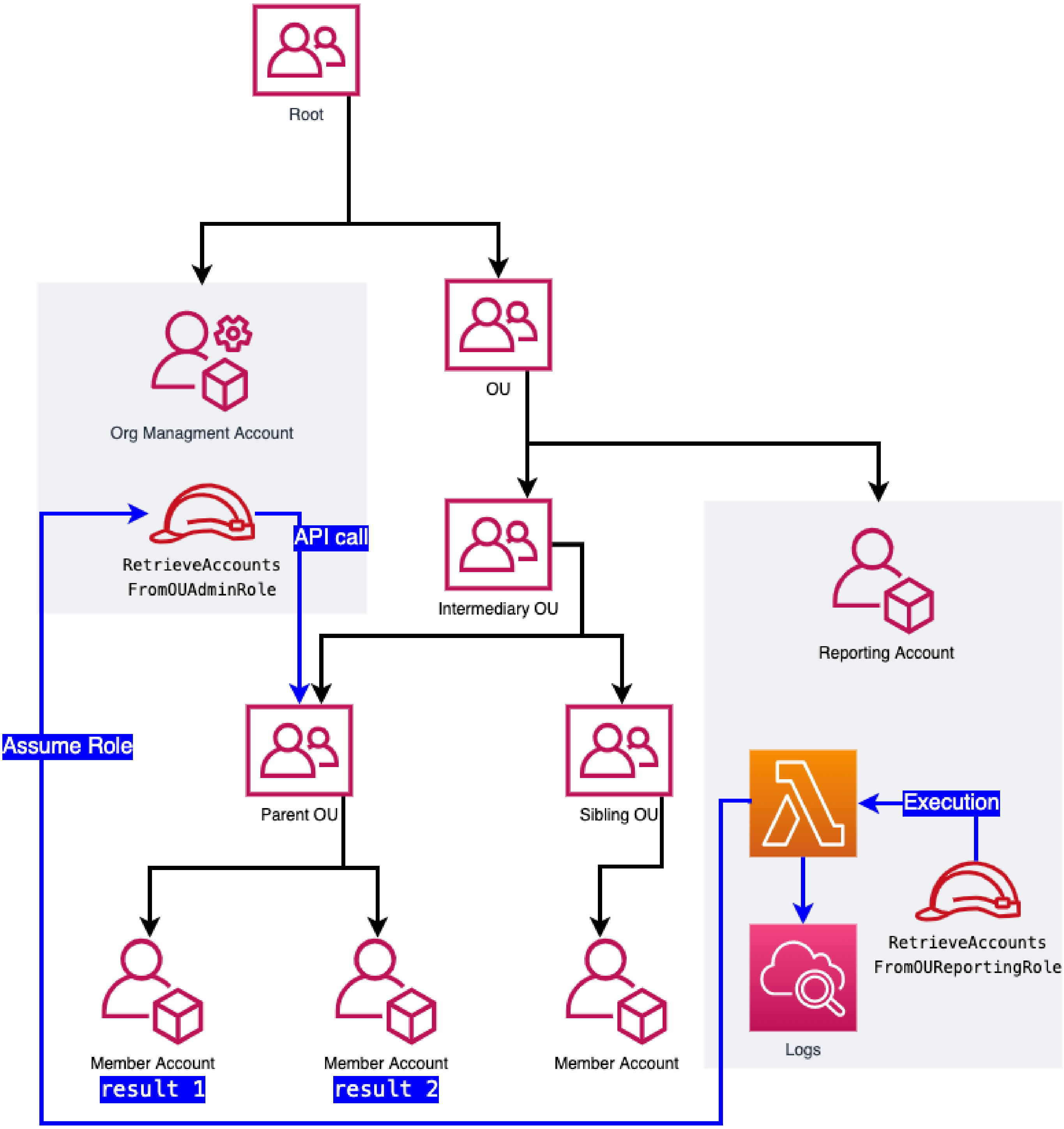
This is an educational code sample.
Latest code version is available at: https://github.com/aws-samples/retrieve-accounts-from-organization-unit

Scenario

In our company all the `AWS Accounts` belong to an `AWS Organization` managed by "Central-IT" sysop team.
We are managing a business department which has an `AWS Organization Unit` containing all our member `AWS Accounts`.
We want to get the list and details of the `AWS Accounts` of our `Organization Unit`.

We can use the `AWS Organization` API ListAccountsForParent.
But, this API can be invoked only from the organization's management account or by a member account that is a delegated administrator for an AWS service.
Also, for confidentiality reason, we should have access only to resources related to our business department.
So, we ask the administrator of the Organization to create a new `Role` in the `management account` with query capability limited to only our `Organization Unit`.

We can then create a reporting app to query for the information.
This app will asssume the created `Role` to be allowed to invoke the API.
We will create in this code-sample a simple illustrative `AWS Lambda Function` that log the results in `AWS CloudWatch`.



Deploying this solution

This CDK project contains two stacks:

- One deployed on the Organization managment account: create the `IAM Role` to invoke the `AWS Organization` API
- One deployed on the reporting account: `AWS Lambda Function` to query and log the account info.

Prerequisites

- AWS CDK installed. Follow the installation guide here.
- The principal used for CDK deployment has access to `CloudFormation` and can create and write to a new `S3 Bucket`

- AWS Accounts:
    - An AWS account root of an `AWS Organization` and credentials to deploy on this account.
    - Few illustrative AWS Accounts below an `Organisation Unit` in the same `AWS Organization`.
    - An AWS account in the same `AWS Organization` to run this solution, and credentials to deploy on this account.

1. Initalize dependencies (do only once)

If you are on MacOS and Linux:

```
python3 -m venv .venv
source .venv/bin/activate
pip install -r requirements.txt
```

If you are on Windows:

```
python3 -m venv .venv
.venv\Scripts\activate.bat
pip install -r requirements.txt
```

2. Deploy on the reporting account

First target the account that will query and report the OU accounts info. Then deploy the CDK stack:

```
cdk bootstrap aws://unknown-account/unknown-region
cdk deploy ReportingAppStack  \
    --parameters managmentAccountId=<AWS Organisation managment account
id, ie: 1234567890>  \
    --parameters organizationUnitId=<Organization Unit id, ie: ou-abcd-
abcde1234>
```

3. Deploy on the Organization managment account

First target the `AWS Organization` `managment account`. Then deploy the CDK stack:

```
cdk deploy ManagmentAccountRoleStack \
    --parameters reportingAccountId=<Account id where will run the
reporting app, ie: 1112223335> \
    --parameters organizationId=<Organization id, ie: o-abcdefg123> \
    --parameters organizationUnitId=<Organization Unit id, ou-abcd-
abcde1234>
```

4. Invoke Lambda Function and see output

You can execute the `Lambda function` directly in the `console` and then check the logs in `AWS CLoudWatch Logs`

or you can do the same via `AWS CLI`:

First target the reporting account. Then:

```
aws lambda invoke --function-name log-organization-unit-accounts-id
response.json
```

finally display the logs

```
export latestLogStreamName=`aws logs describe-log-streams --log-group-name
'/aws/lambda/log-organization-unit-accounts-id' --query
logStreams[-1].logStreamName --output text`
echo "log Stream name is: $latestLogStreamName"
AWS_PAGER="" aws logs get-log-events --log-group-name '/aws/lambda/log-
organization-unit-accounts-id' --log-stream-name "$latestLogStreamName"
```

5. Clean Up

First Target the `AWS Organization managment account`. Then:

```
cdk destroy managment_account_role
```

First Target the reporting account. Then:

```
cdk destroy reporting_app
```

Security

See CONTRIBUTING for more information.

License

This library is licensed under the MIT-0 License. See the LICENSE file.