Set up the enviornment account connection

Proton alleviates complicated cross-account policies by using a secure `environment account connection` feature. With environment account connections, platform administrators can give Proton permissions to provision infrastructure in other accounts. They create an IAM role and specify a set of permissions in the target account. This enables Proton to assume the role from the management account to build resources in the target accounts.

> You will use the account we used for provisioning the `multi-svc-beta` environment account as a management account as well. In a real world scenario, the management accounts and environment accounts should stay separated.

Let's imagine tha we, as platform administrators, need to create a production environment to run the microservices application, and we intend to do so in a separate account following best practices.

First things first. As mentioned before, we need to create a Proton service role that's scoped down to only the permissions that are needed for provisioning the environment infrastructure resources.

If you are at an AWS event, it is time to buddy up to use each other's accounts. Your buddy's account will serve as a secondary (production) environment account during the rest of this module. Exchange AWS Account IDs to continue:

```
export SECONDARY_ENV_ACCOUNT_ID="<secondary_env_account_id>"
echo "export SECONDARY_ENV_ACCOUNT_ID=${SECONDARY_ENV_ACCOUNT_ID}" | tee -a ~/.bash_profile
source  ~/.bash_profile
```

Create the scoped IAM service roles in your account to let your buddy provision infrastructure in your account and log in to request a connection. Ask your buddy to do the same in his account:

```
wget -O ~/environment/proton-account-connection-roles.yaml "https://static.us-east-1.prod.workshops.
cd  ~environment
aws cloudformation deploy \
  --template-file proton-account-connection-roles.yaml \
  --stack-name AWSProtonWorkshop-AccountConnectionRoles \
  --parameter-overrides "EnvironmentAccountId=${SECONDARY_ENV_ACCOUNT_ID}" \
  --capabilities "CAPABILITY_IAM" "CAPABILITY_NAMED_IAM"
```

We are now ready to send a request to connect to your management account. Copy & paste the output of `AWSProtonWorkshop-AccountConnectionRoles` stack in your browser. This URL will let you login to your buddy's account.

```
aws cloudformation describe-stacks --stack-name AWSProtonWorkshop-AccountConnectionRoles | \
  jq -r '.Stacks[0].Outputs[0].OutputValue'
```

Naviagate to Proton's Console and click **Environment Account Connections** from the navigation pane (expand if collapsed). Then click **Request to Connect** in "Sent requests to connect to a management account". Complete the request with the following values:

> Find out your account ID executing `echo  $AWS_ACCOUNT_ID` in Cloud9

1. For "Management account ID", use your original account ID.
2. For "Environmet name", type "multi-svc-<your_account_id>". Replace accountId with your account ID.

4. For "Service Role", select the role that starts with "EnvironmentAccountProtonRole"
5. Click "Request to Connect"

Now click **"Switch back"** from the top-right dropdown (the one in color that indicates the role and account you are actually using). You should have a new environment account connection request now. Go ahead and accept it!

Previous Next