Introduction

Welcome to Serverless Workshop! Based on my experiences of the ServerlessConf in Paris this year and my current interests, I have decided to host a Bits & Bites session in a workshop format on Serverless, more specifically: on the Amazon WebServices Serverless Platform, AWS Lambda.

All information contained in this and subsequent tutorials is caveat emptor-ware, e.g. best effort at providing correct information, but you – the proud holder of the AWS account – will be ultimately responsible for handling your account and seeing to it that you do not exceed the limits of the free tier services.

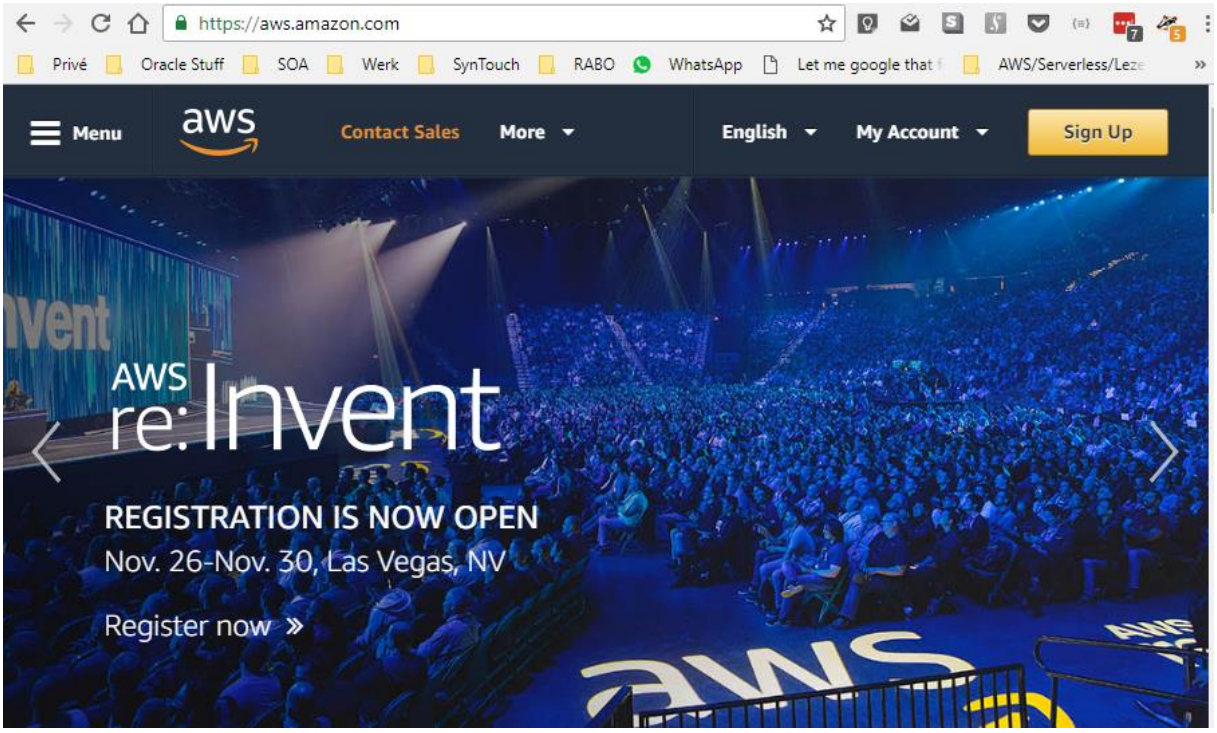
This first tutorial will guide you how to create and setup your account.

Registration

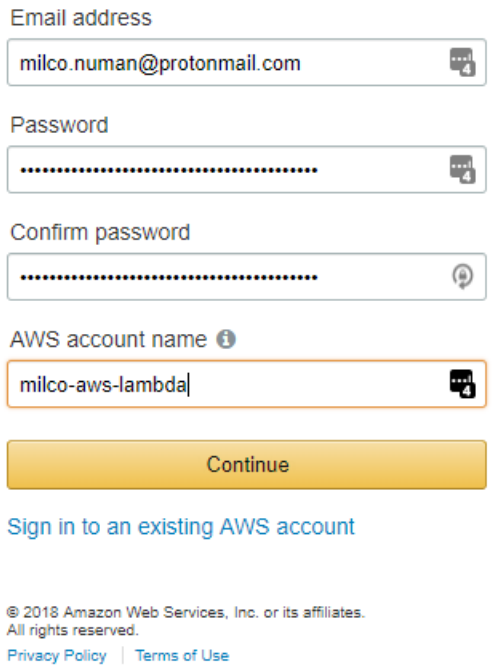
Registration for an AWS account is easy, but it does require you to supply your credit card details (you should incur any charges from the activities in the workshop).

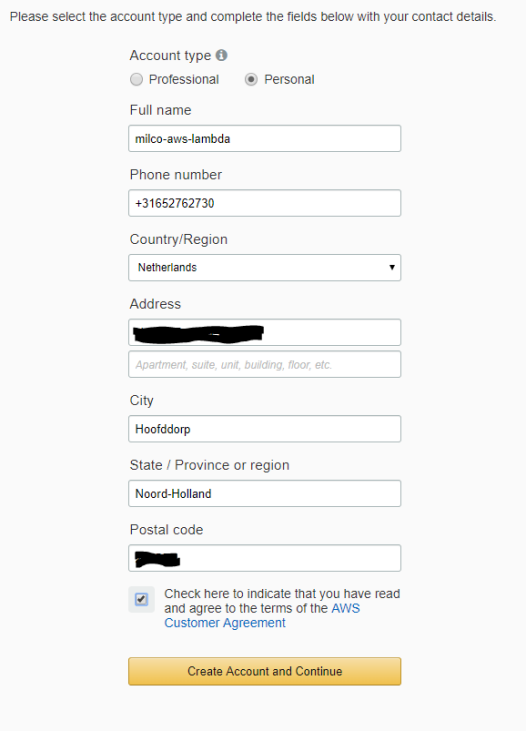
Create your account

Navigate to the AWS site (aws.amazon.com), in the top right there is a “Sign Up” button:

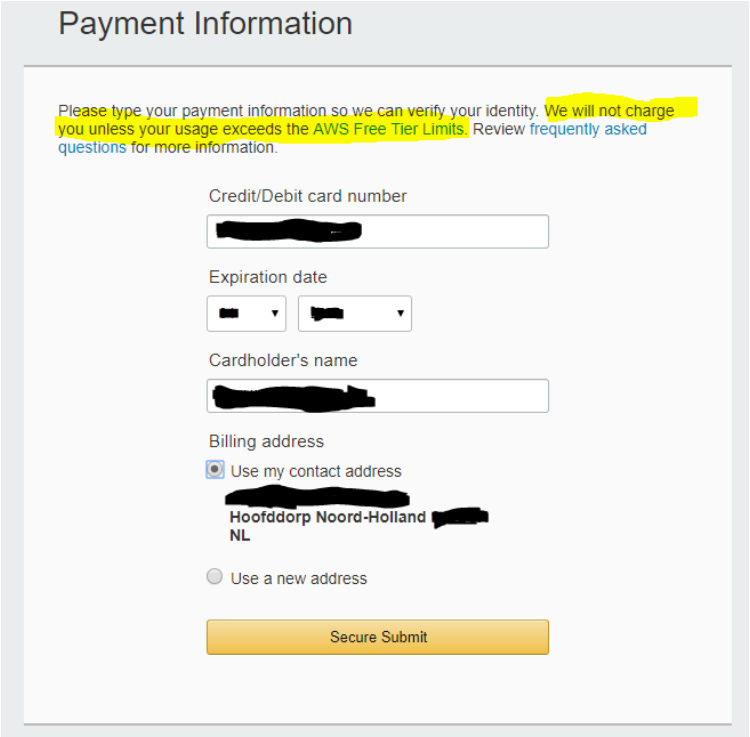


In the next dialogue, provide the requested information; we’ll setup your account to use the AWS account name in your sign-in URL. Register a personal account and provide personal details including your mobile phone number as you will receive a confirmation code for the completion of the registration:



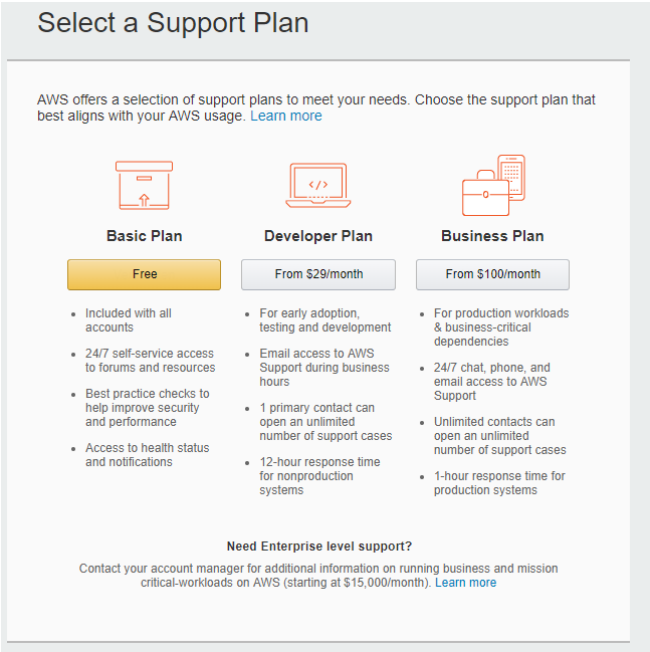


Continue to provide your credit card details for billing:

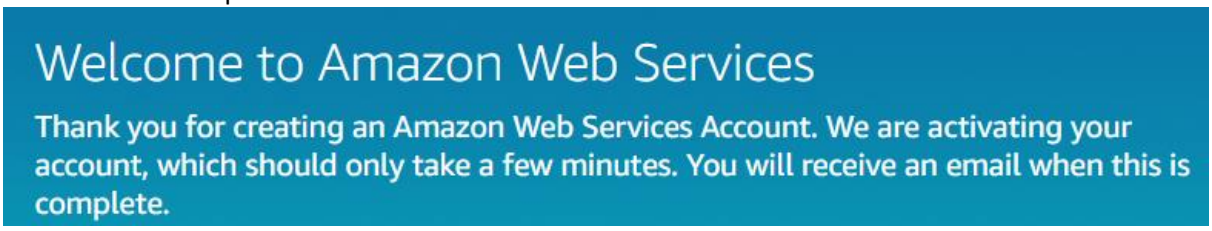


You will be asked to confirm your telephone number and AWS will call you, instructing you to enter the code shown on the web page to confirm your identity.

Choose the **Basic Support** plan that is marked Free:



This is the final step:



Wait for the email to arrive ….

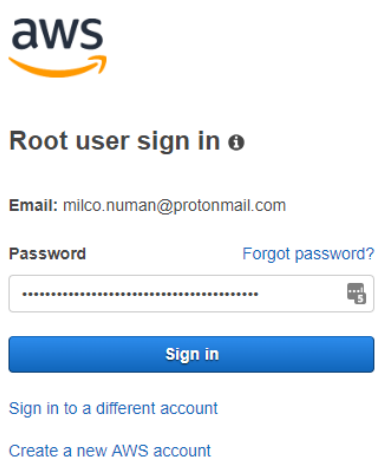
You have created the **ROOT** user, which means that this user has *unlimited administrative access* to the account, including billing information. As in UNIX, this is not a good user for day-to-day operations, so as soon as we're able to login we will need to create a restricted user and optionally secure access to the root account.

Regions

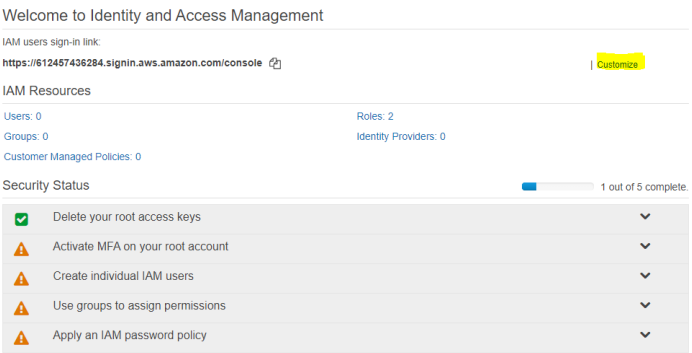
As soon as we login, you should take notice of the region you're working in – this will be shown on the top of the page. Although AWS has multiple regions in EMEA, not all services are already available in all of these regions. Whenever creating resources, these will be created in your current region. As we want to use the Cloud9 development environment, make sure that your region is set to Ireland (this is currently the only EMEA region that supports this service).

Account Setup

As soon as you have received the email that registration is completed, log into your root account:

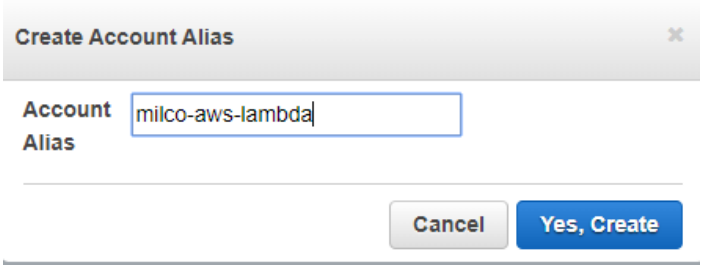


When logging in for the first time, you should be automatically directed to the IAM (Identity and Access Management) Module, where a number of items that require your attention will be marked by exclamation mark icons:



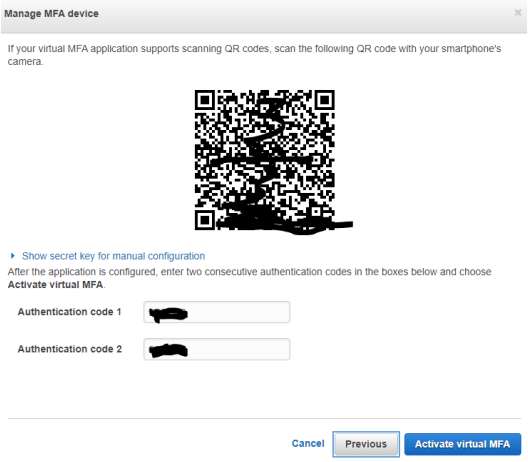
Account sign-in link

Setup your account sign-in link to be more descriptive than the default https://your-account-id-here.signin.aws.amazon.com/console by overwriting the numeric account id with a more descriptive account alias.



MFA

MFA stands for Multi Factor Authentication and is the mechanism to require multiple proofs of identity before granting access. Usually, the identification tokens consist of something you know (password) and something you have (authentication token generator) or are (biometric characteristics like finger print reader). It is always a good practice to protect your account with MFA!

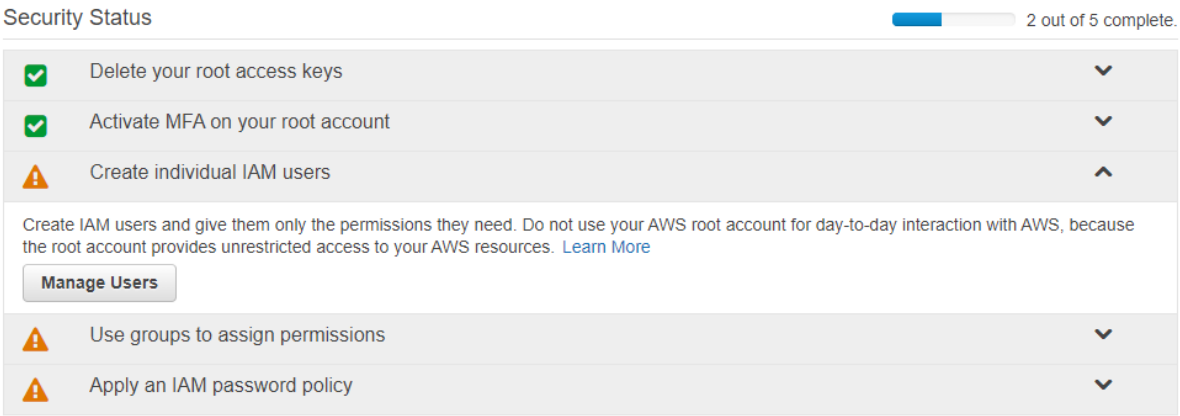


Set Multi-Factor Authentication on your root account; for this to work, you will need to have an app like **Google Authenticator** or **Authy** running on your smartphone. AWS also supports miscellaneous hardware devices.

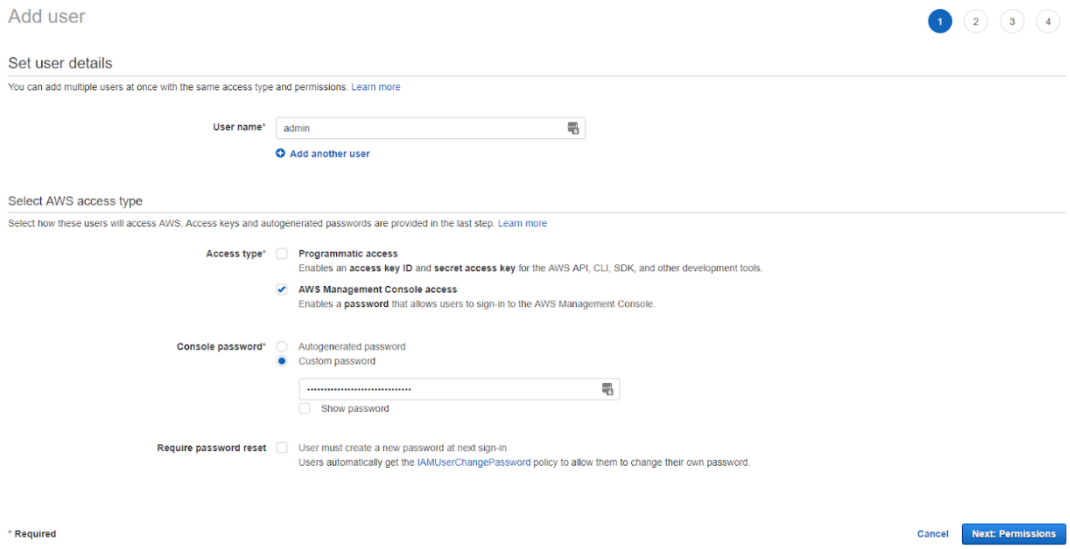
Scan the QR-code using your virtual MFA and follow instructions to require MFA for your account.

Create user and group

Next up, creating a non-root access user for day-to-day operations (administrator and development). This user will be granted elevated privileges (administrator rights for all services) that in a corporate scenario you typically would not have, but this makes development and administration easier for the workshop. Use the Manager Users button to start:

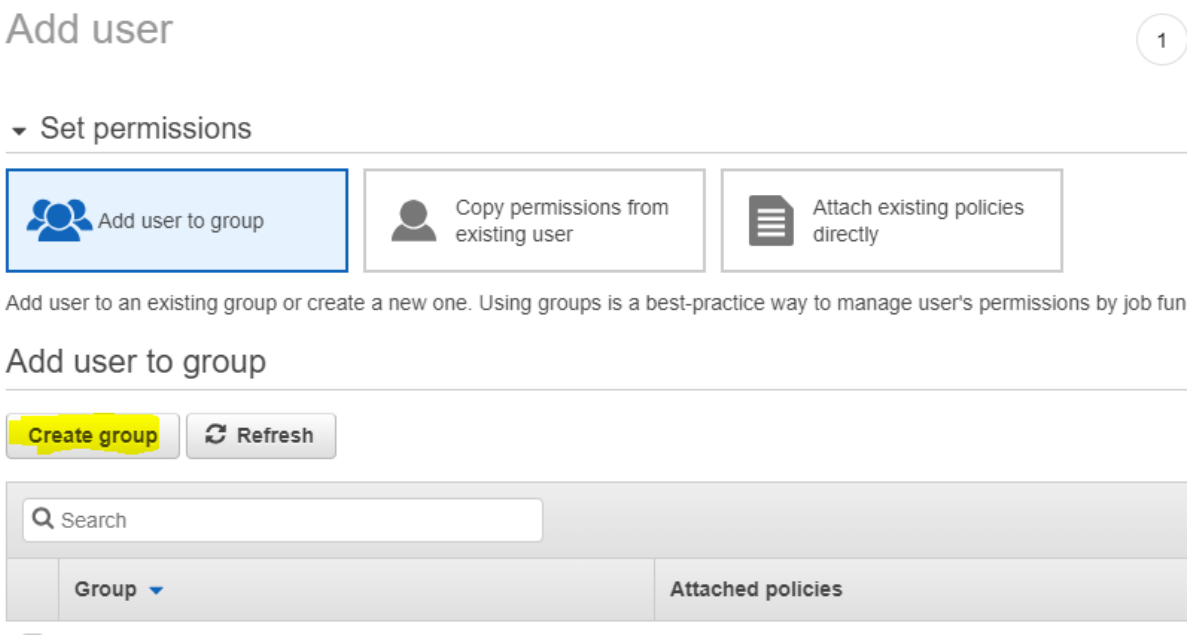


Create an admin user of your choice, enable for console accessset your password manually:

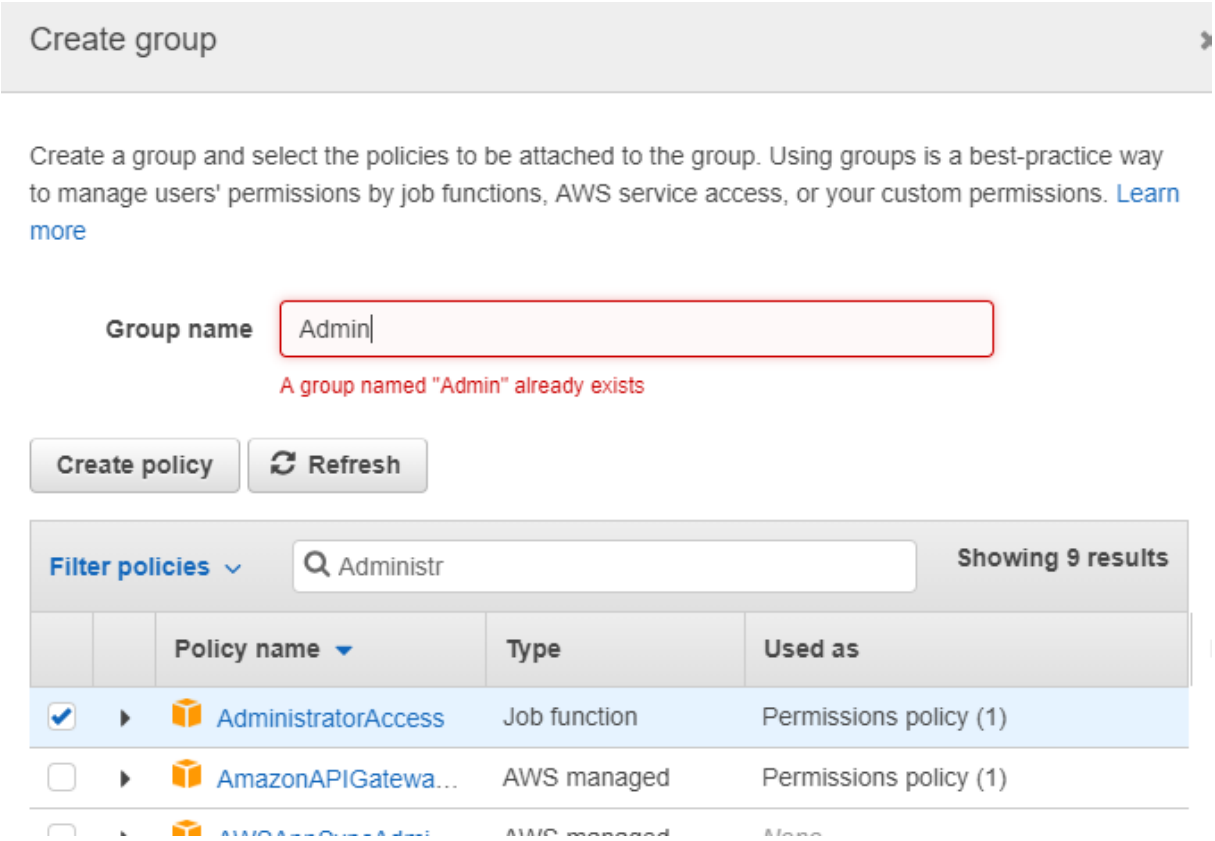


(Console access is for interactive users, programmatic access generates a new set of key and secret for command line access using the CLI and APIs).

On the next screen, Permissions, add the user to a new group you will create by using the “Create Group” button:



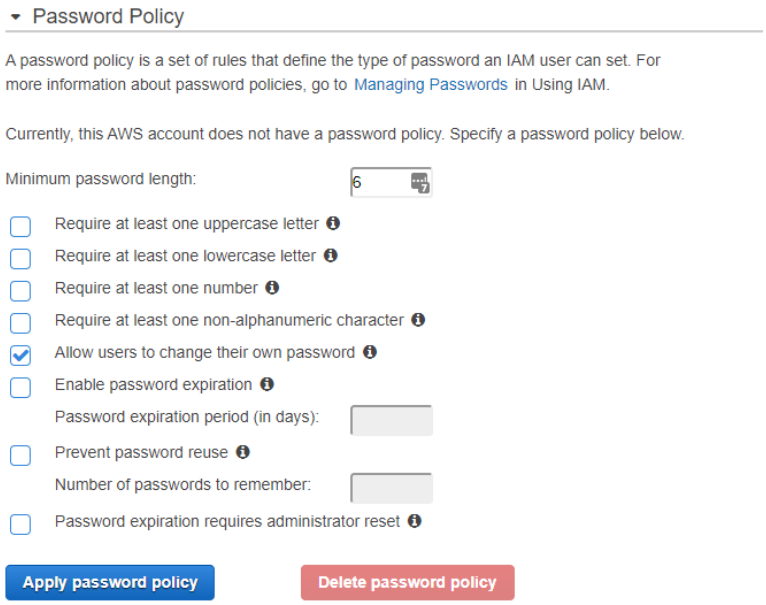
Create an admin group, selecting the AdministratorAccess policy from the list:



On returning, make sure the newly created Admin group is selected for the user, Review and Create.

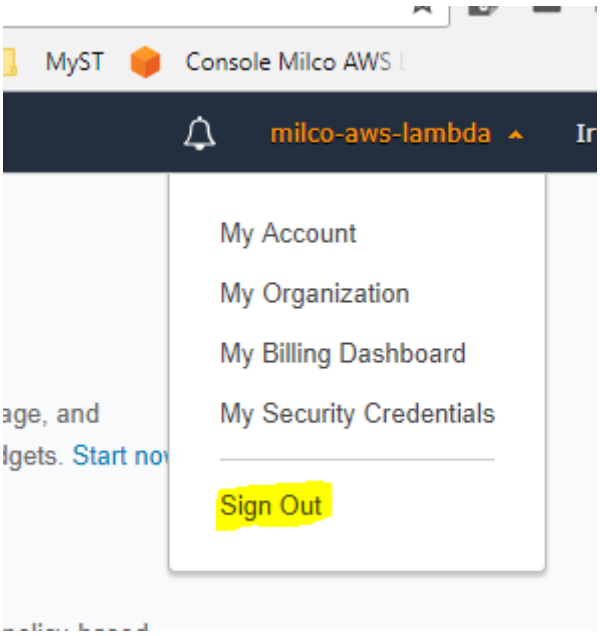
Password policies

In a real life scenario, password policies may also be applied, requiring you to generate “strong” passwords by requiring minimum length and certain other characteristics. If you feel like it, you can apply such a policy but as I am in the habit of generating strong passwords using LastPass, I will not apply a password policy on top of that:

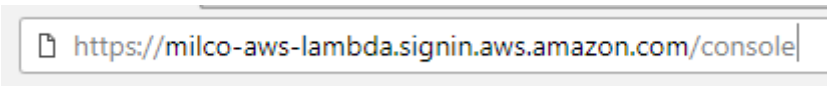


Test your user

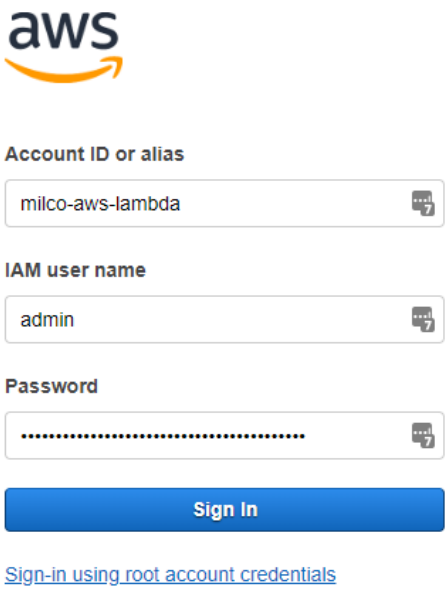
Your still working using your root account credentials, so it is time to logout and log back in again with your newly created user:



Login at your new account alias URL:



Now provide your admin user credentials to login (so not your root account!):



Next up: Cloud9