AWS Organizations with SSO, uniform cloudTrail and billing, Admin role that can assume role in other account. - GL

Creating separate AWS accounts to make one organization. Within this Organization we would like one consolidated billing receipt, more uniformed permissions and logs. Create IAM Admin with MFA to use instead of the Root account due to unrestricted power. An Admin in one account will be able to assume a role and act as an admin in another account to provide support for that department in case their Admin cannot be reached or is out of town. Billing alarms for when account reaches threshold in price limit and create notifications to allow user to decide what action to take.

For more organizational access permission sets will be used with SSO to create a user portal with access to all accounts but with limited permissions.

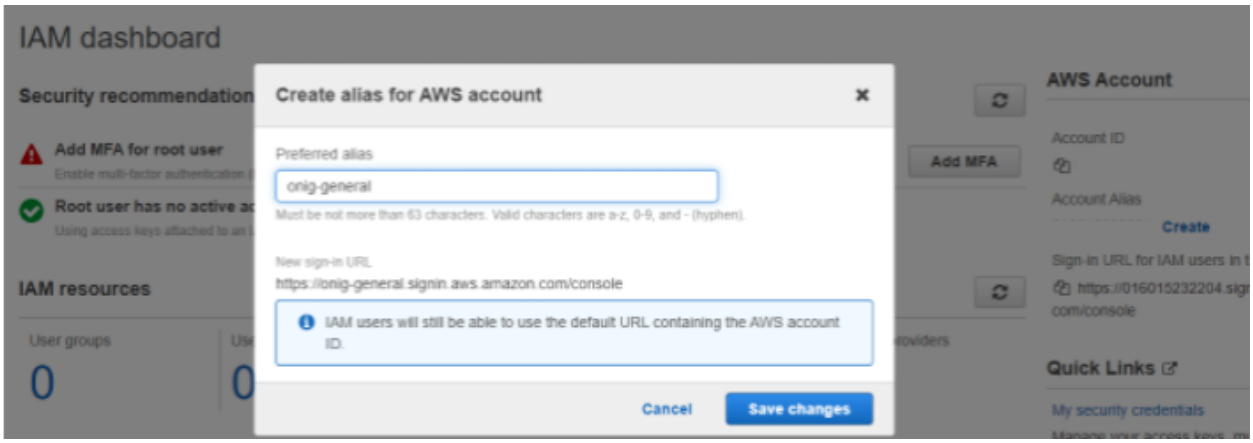
Congratulations!

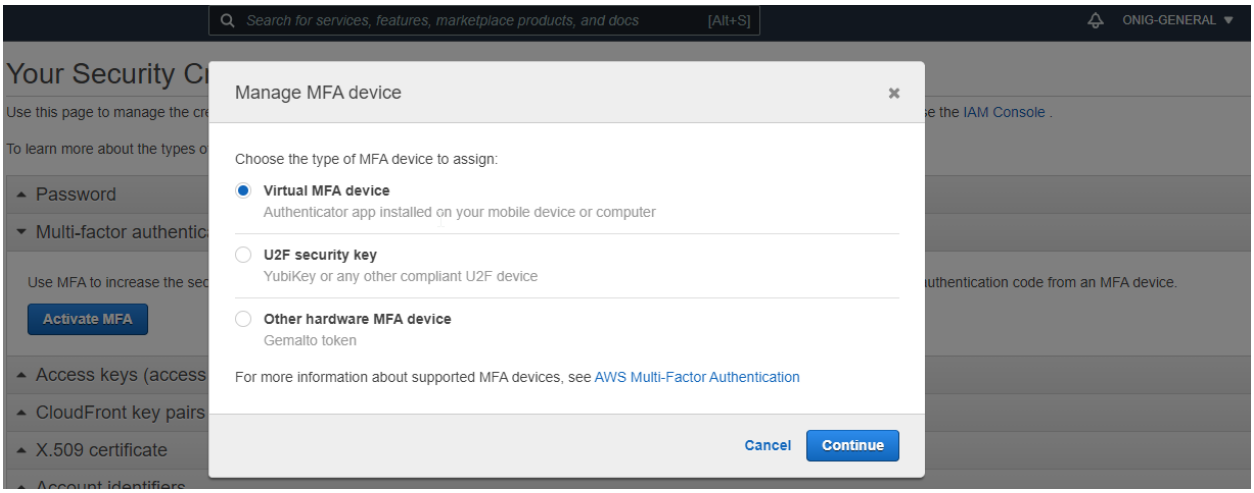
Thank you for signing up with AWS.

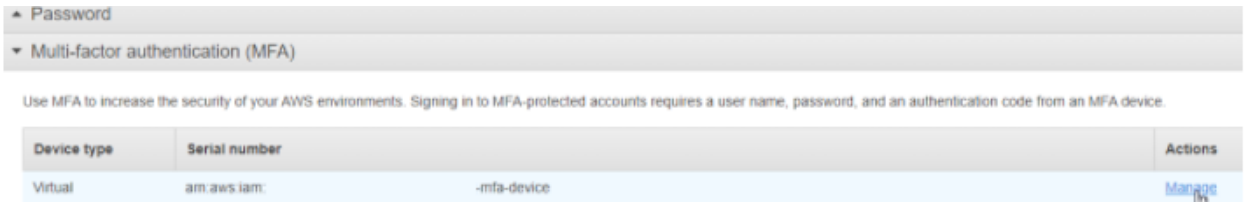
We are activating your account, which should take a few minutes. You will receive an email when this is complete.

Go to the AWS Management Console

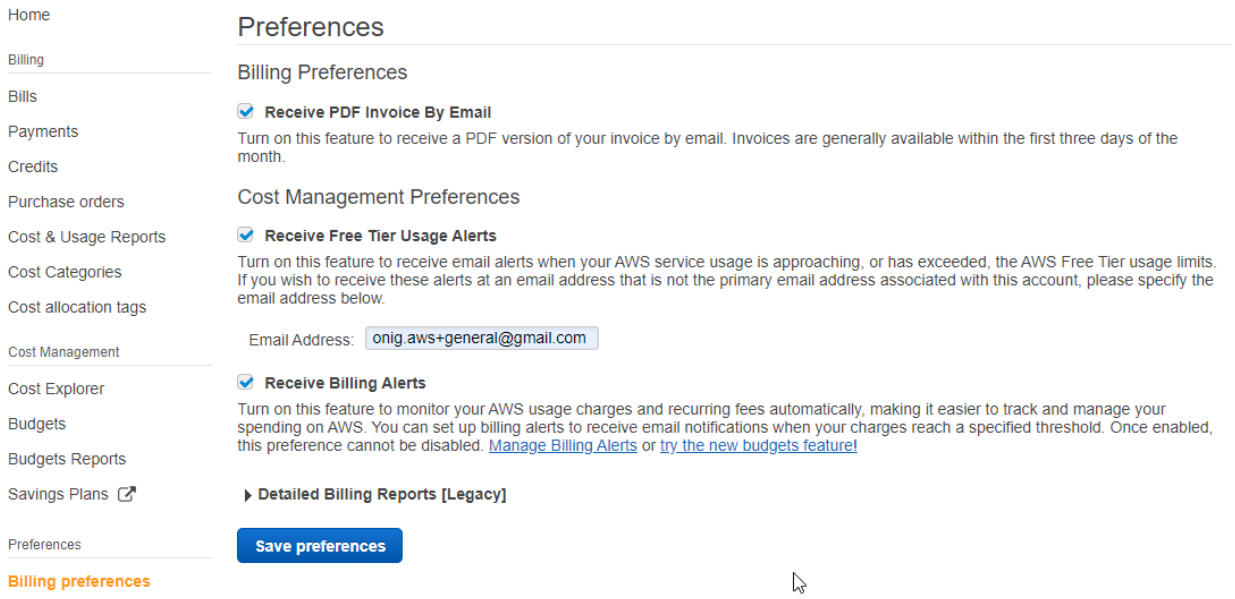
- We can also create an alias for the account for a more readable URL for users. Since it is on the same screen.
- Next step is to secure the account. We need MFA for a second authentication factor in case somebody gets hold of username and password. MFA generates a new code every 30 seconds making it hard to obtain.



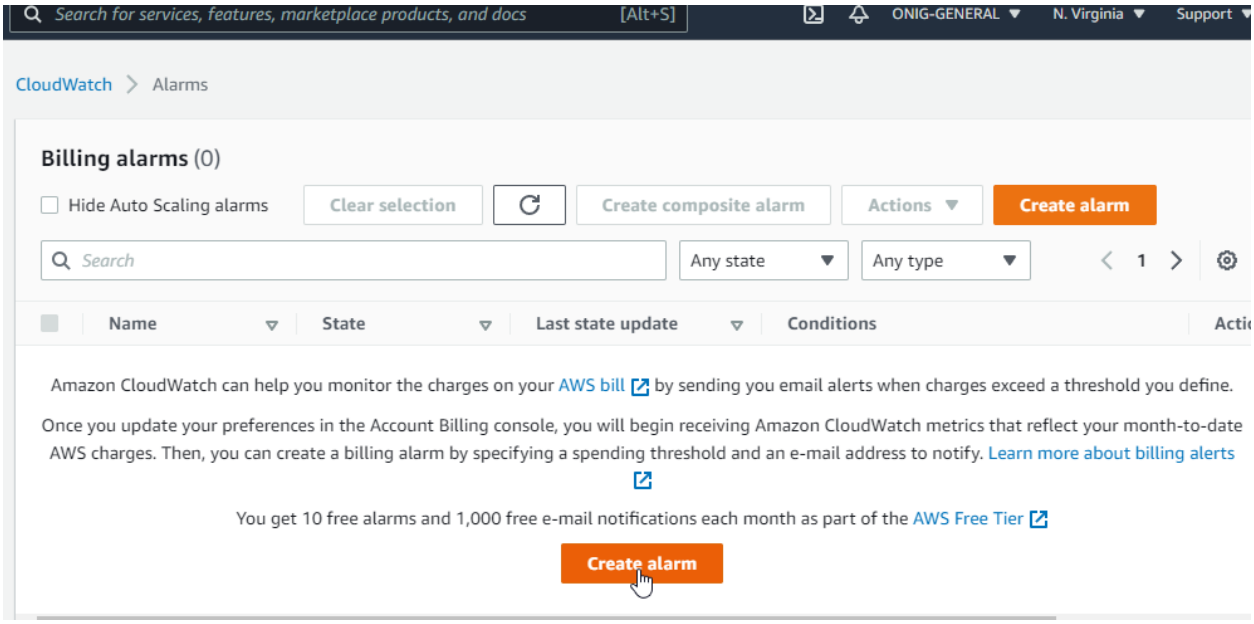




- To make sure we do not go over AWS service usage an alert needs to be made. By default all the boxes are unchecked. We also need this checked to allow cloudWatch Alarms to monitor it



- Now we need to make an actual alarm, this will monitor certain metrics and change state based on a condition. In this case, when we exceed free tier we want the alarm to go from OK to ALARM.
- By default we have no alarms.



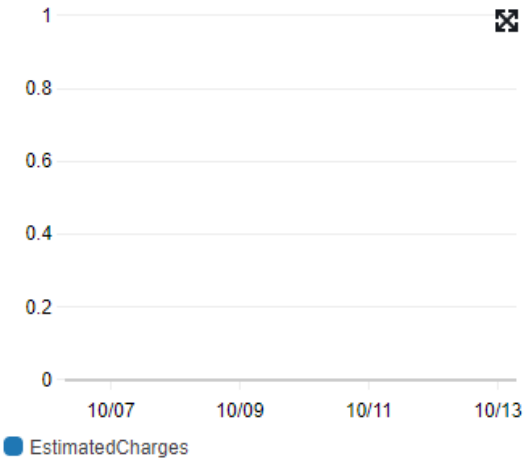
- This alarm will track the following metric named EstimatedCharges. Specifically, It'll track every 6 hours and if the charge for the account reaches a $10 quota for the month.

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.



Namespace

AWS/Billing

Metric name

EstimatedCharges

Currency

USD

Statistic

Maximum

Period

6 hours

Conditions

Threshold type

- Static — Use a value as a threshold
- Anomaly detection — Use a band as a threshold

Whenever EstimatedCharges is...

Define the alarm condition.

- Greater — > threshold
- Greater/Equal — >= threshold
- Lower/Equal — <= threshold
- Lower — < threshold

than...

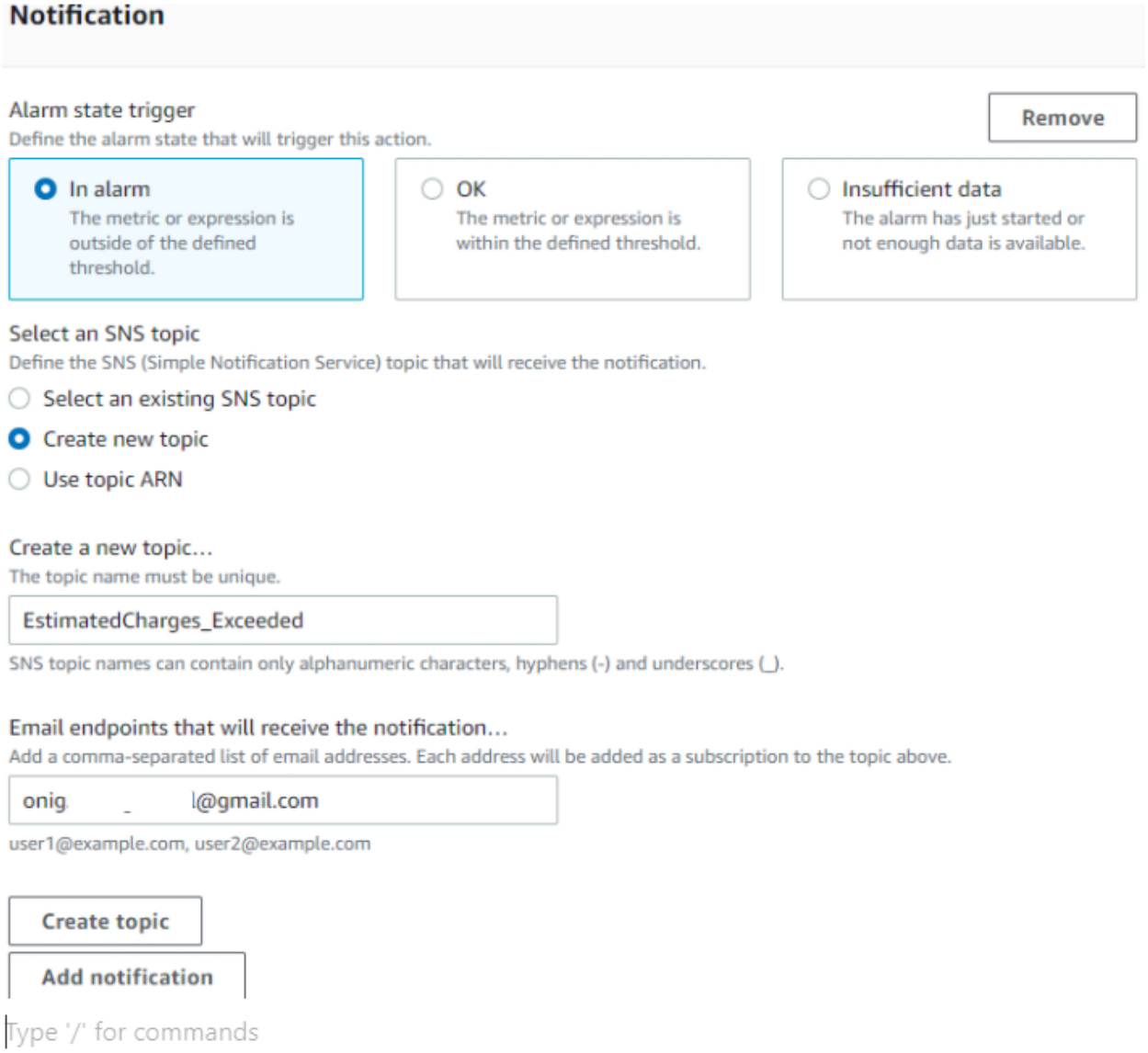
Define the threshold value.

10 USD

Must be a number

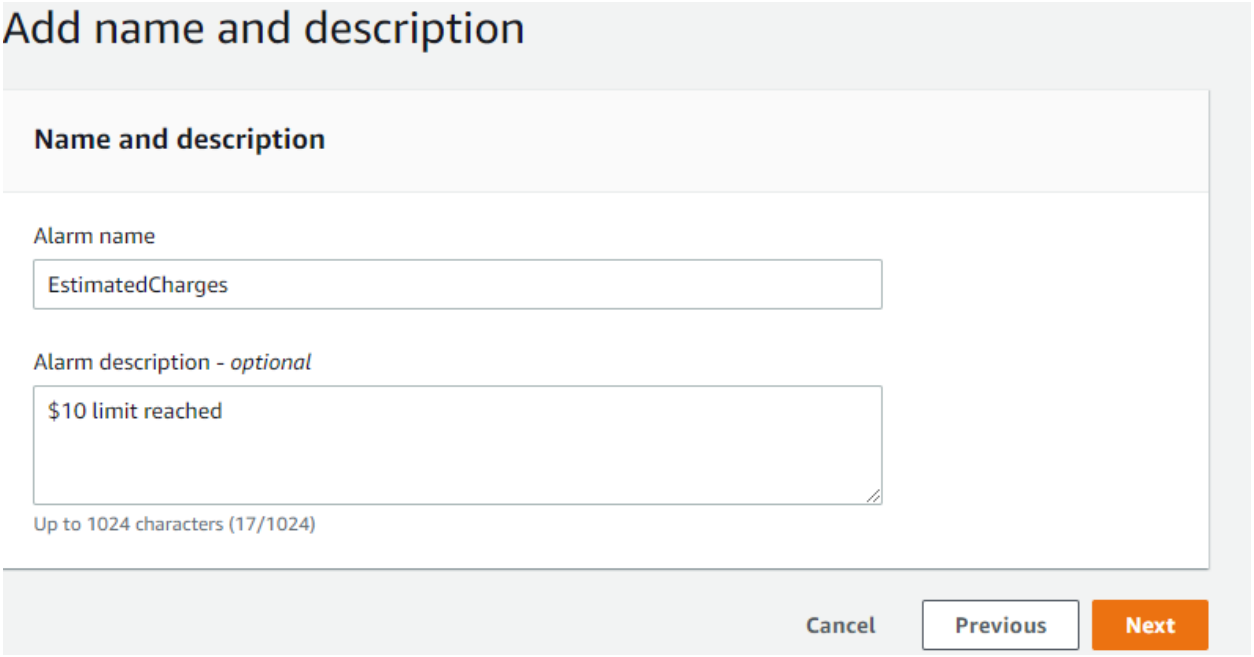
▶ Additional configuration

Cancel Next

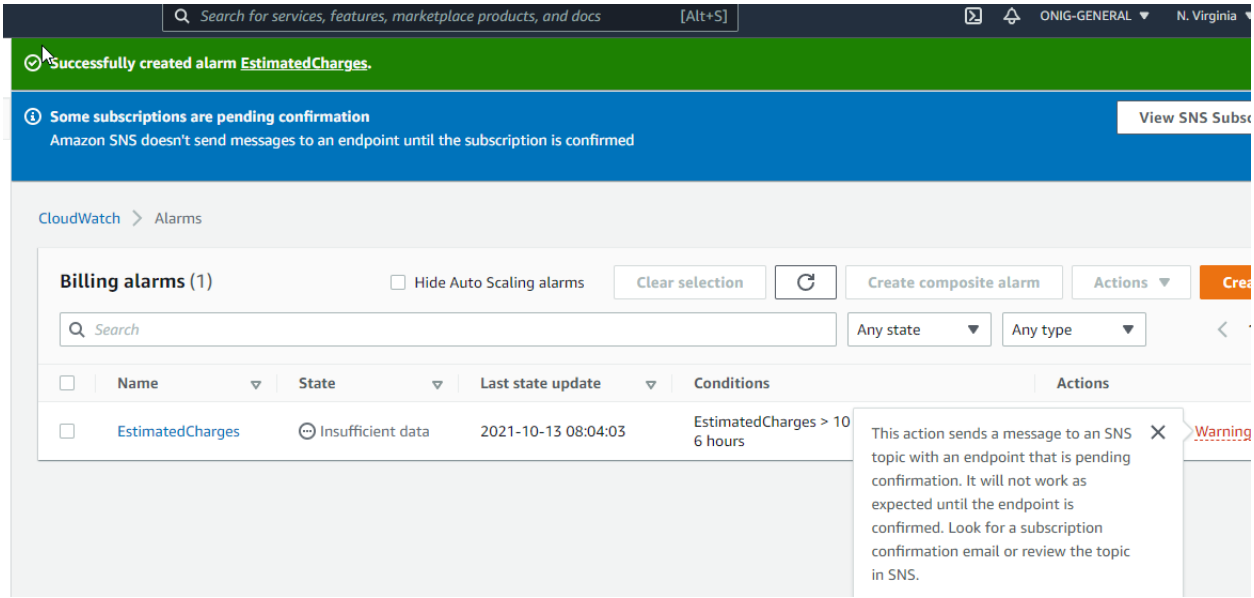


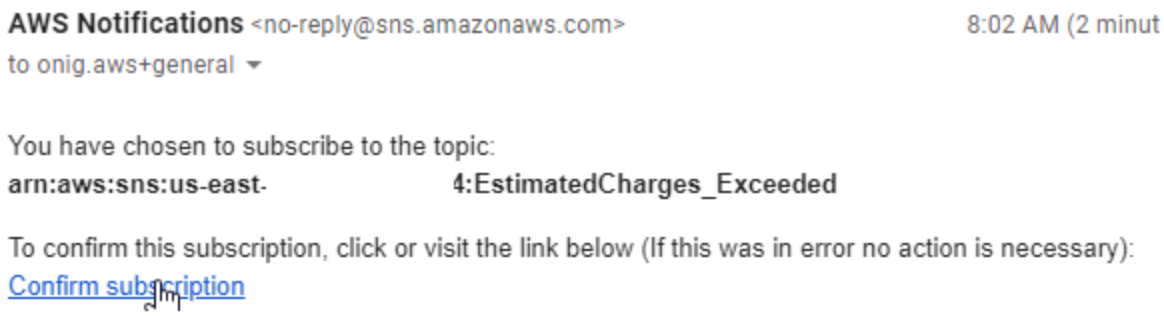
- We then need to define an alarm state for when the metric is met. In this case below, state will be in ALARM, and we want to notify the owner via email. An SNS topic needs to be made which is a subject or communication channel. Whoever is subscribed to this channel may receive the alert.

- Finally add a name and description to the alarm

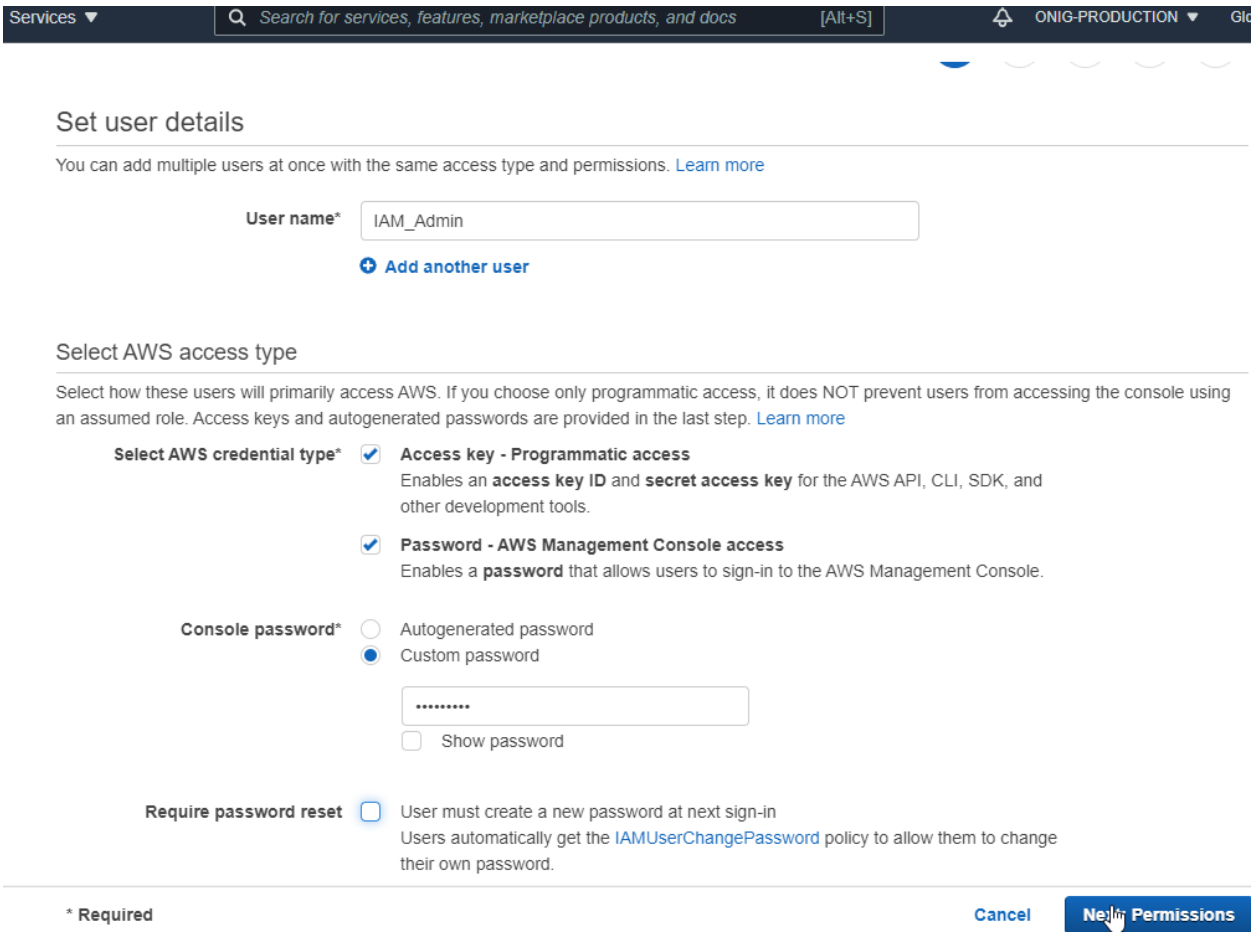


- A subscriber must confirm they would like to be added to the channel otherwise they will never receive it.

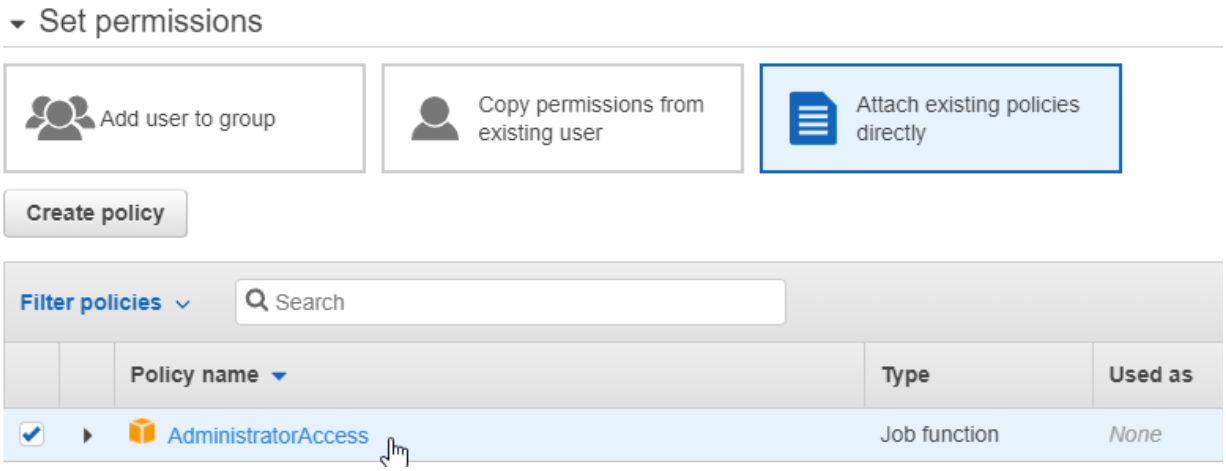




- Do this for second account*
- The AWS accounts now just need an IAM admin because we do not want to use the Root for safety reasons.
- Create an IAM Admin to act as the account administrator. Since I am going to use the user I will create a password to keep otherwise if assigning may want to autogenerate and allow the target user to generate a new one on fist sign-on.



- We want to then add a policy with authorizes the users access to services. In this case administrator privilege's.



- The policy is written in JSON. In this case it is allowing any action on any resource. By default everything is denied, you must give allow privileges.

- Now we can logout of root and use the admin account from now on. Sign in using the console URL created when we made an account alias. You can check if you're logged into an IAM USER by clicking you username dropdown menu.

Sign in as IAM user

Account ID (12 digits) or account alias

onig-general

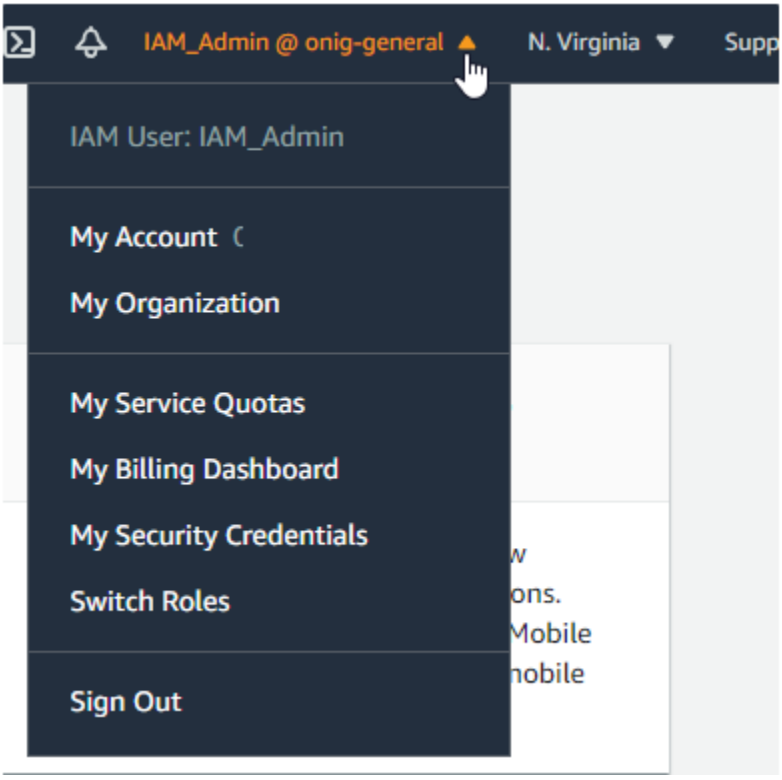
IAM user name

Password

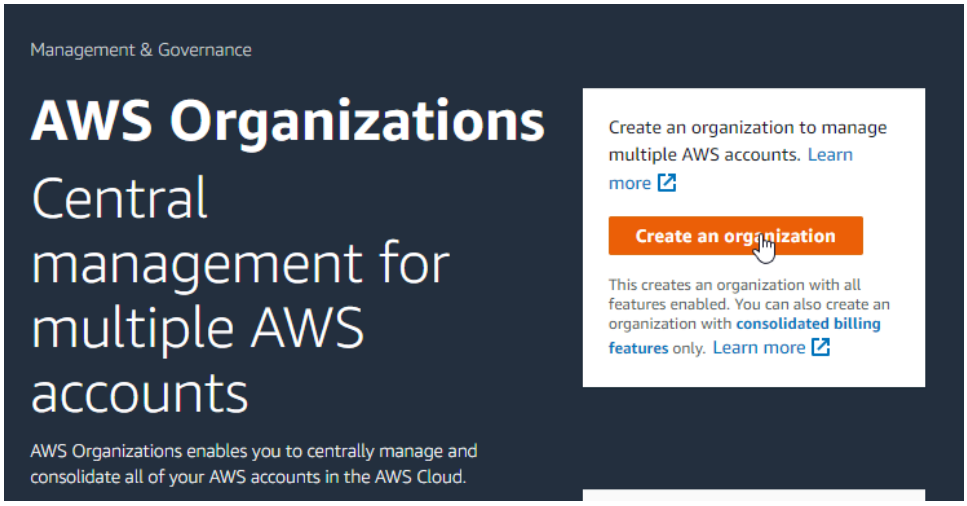
Sign in

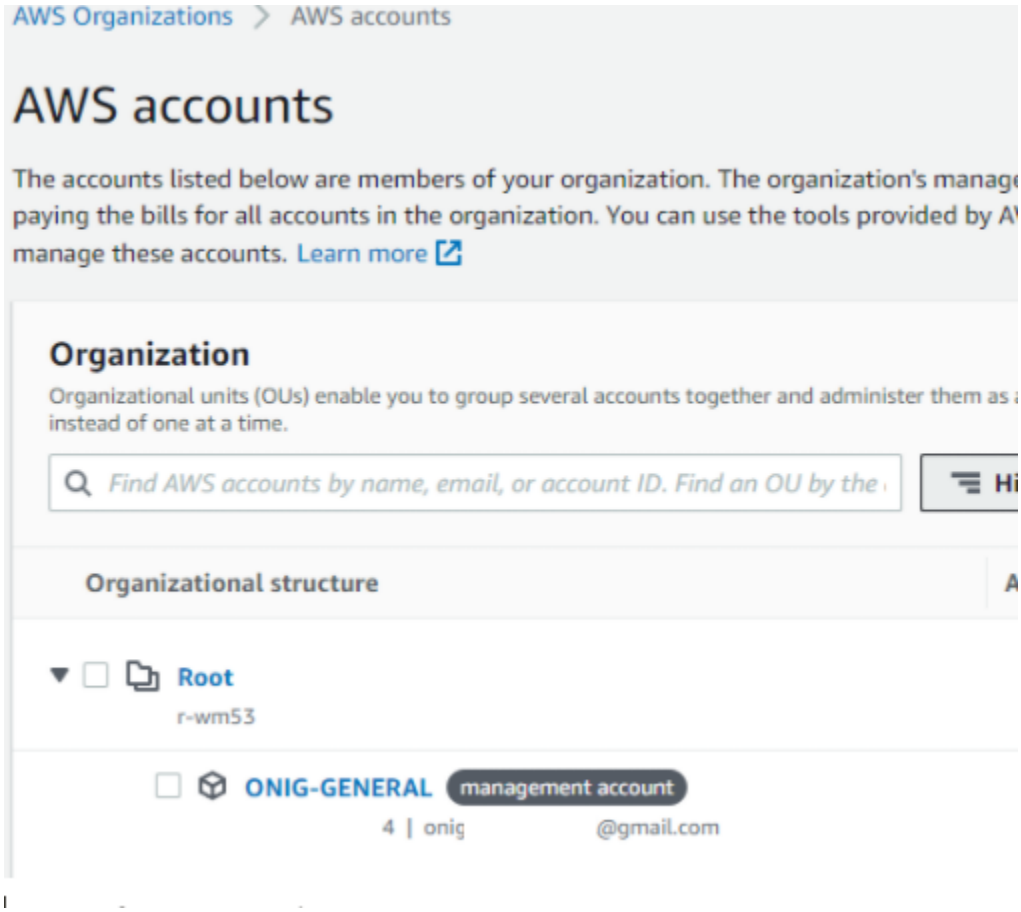
Sign in using root user email

Forgot password?

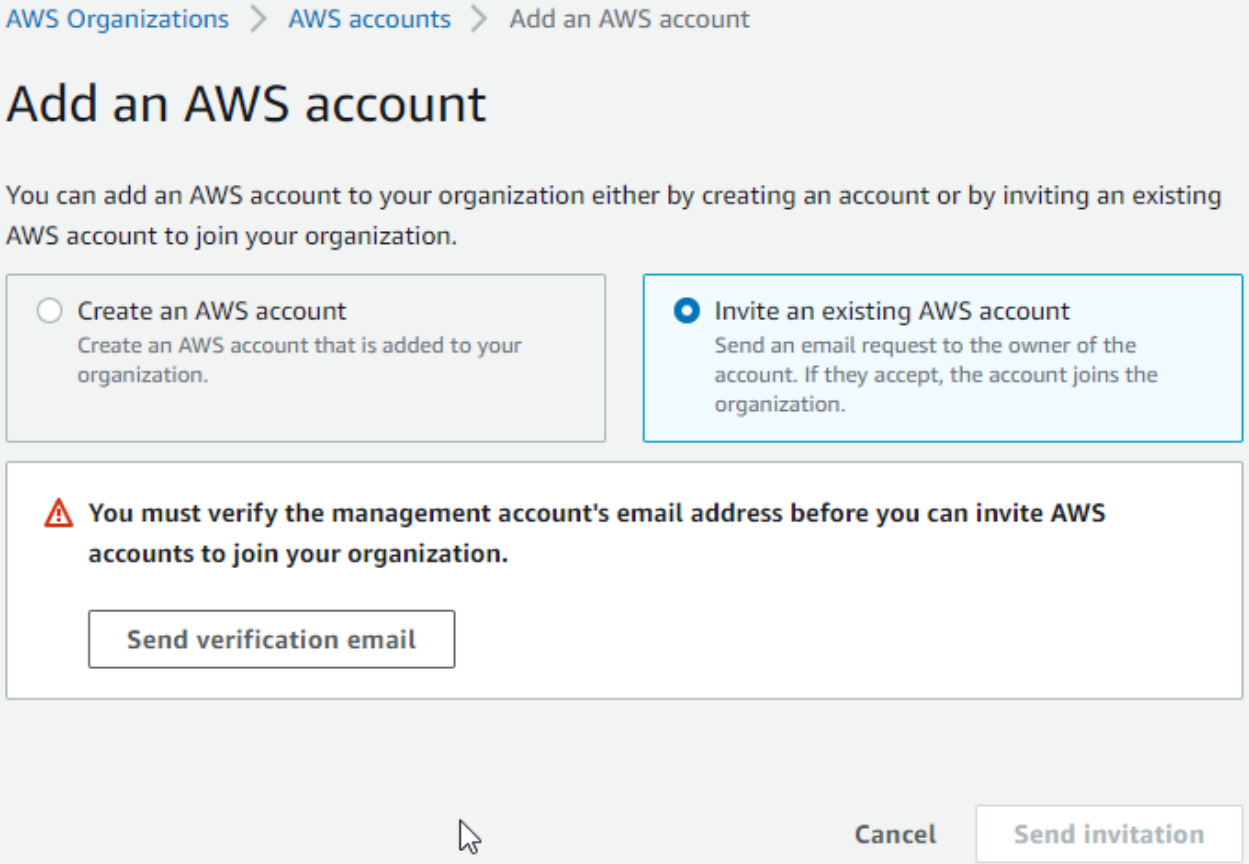


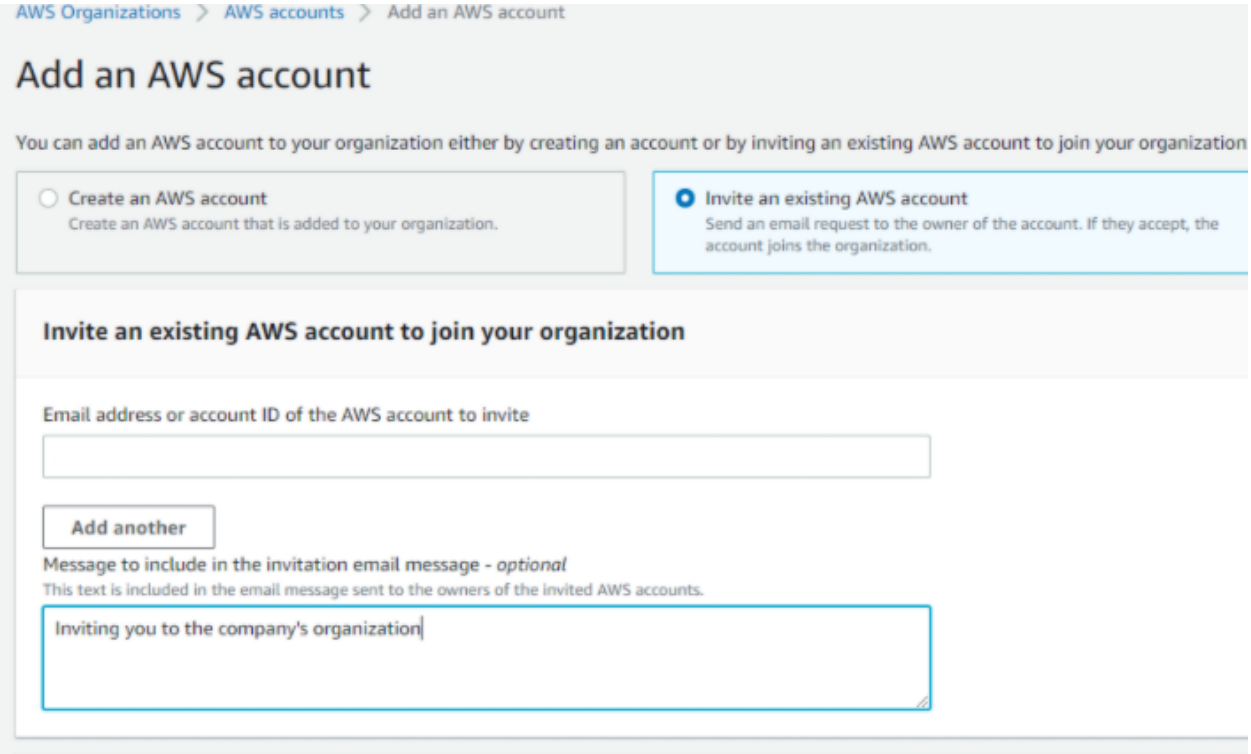
- Now we can create an AWS organizations, this way we can merge accounts and have one consolidated bill. Click create and you're all set, this will then be the root account in the organization



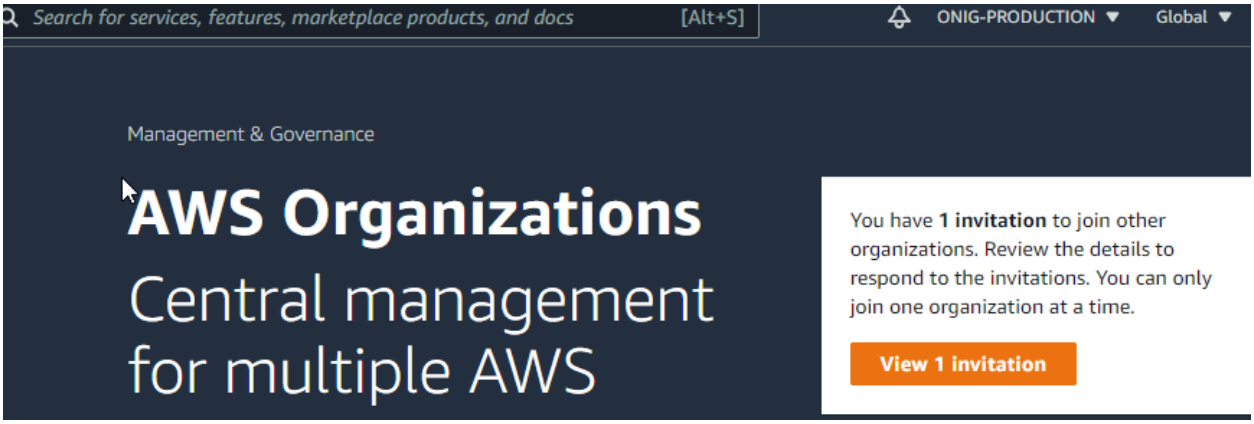


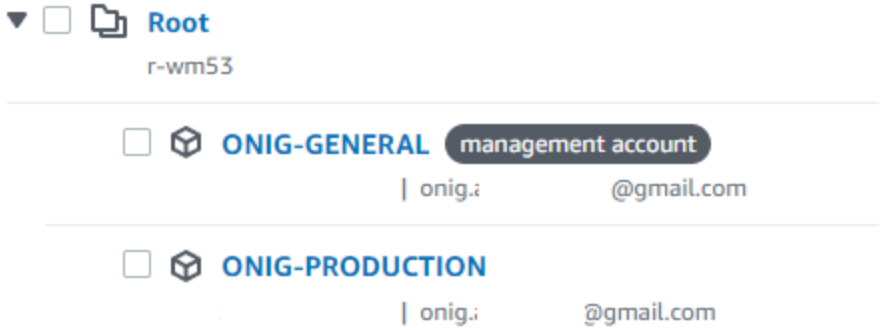
- We can invite existing accounts to this organization or create accounts from within. If inviting existing you must verify the "management account's" email


AWS Organizations > AWS accounts > Add an AWS account
Add an AWS account
You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.
Create an AWS account
Create an AWS account that is added to your organization.
Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.
You must verify the management account's email address before you can invite AWS accounts to join your organization.
Send verification email
Cancel
Send invitation

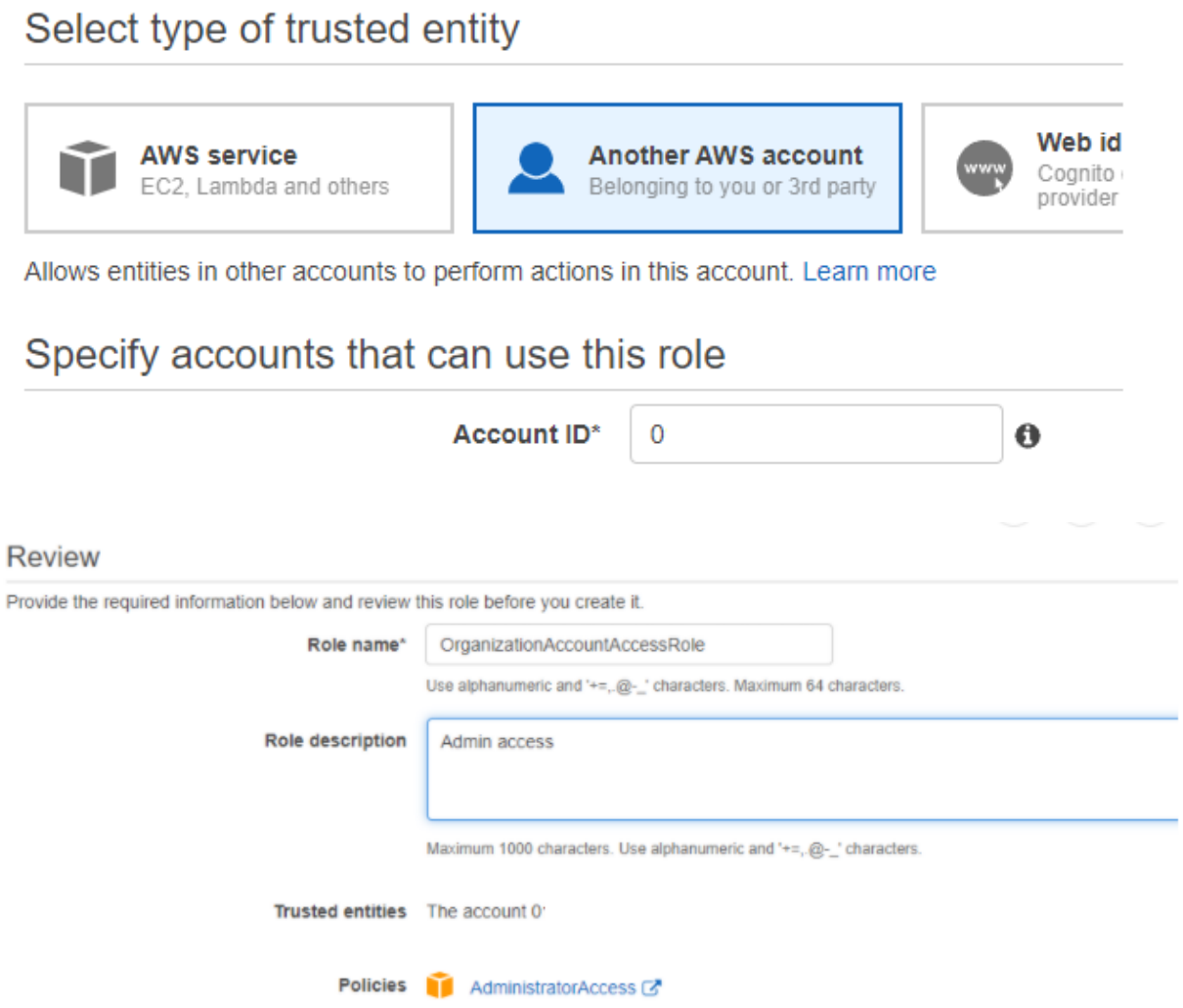

AWS Organizations > AWS accounts > Add an AWS account
Add an AWS account
You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization
Create an AWS account
Create an AWS account that is added to your organization.
Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.
Invite an existing AWS account to join your organization
Email address or account ID of the AWS account to invite
Add another
Message to include in the invitation email message - optional
This text is included in the email message sent to the owners of the invited AWS accounts.
Inviting you to the company's organization

- Accept invitation from the other account in AWS Organizations tab

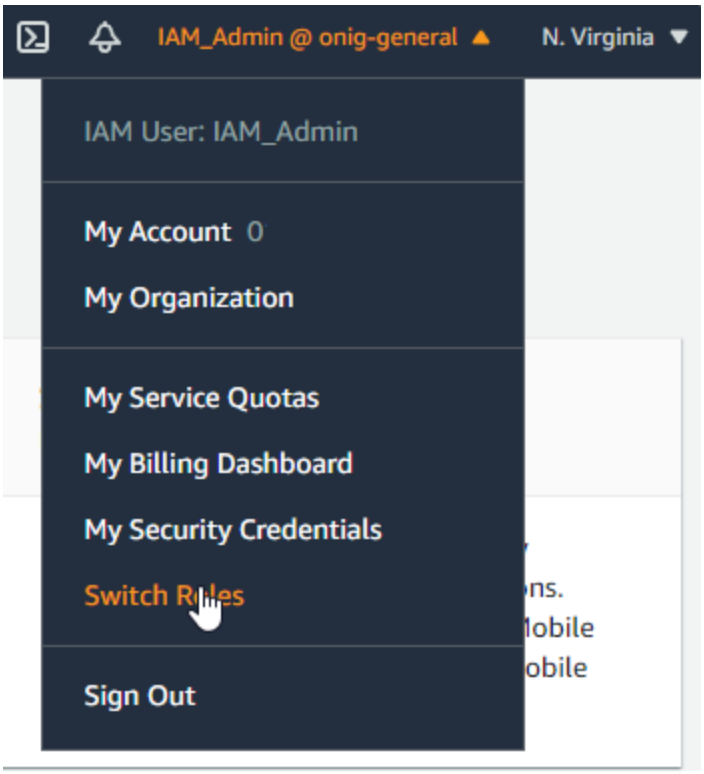


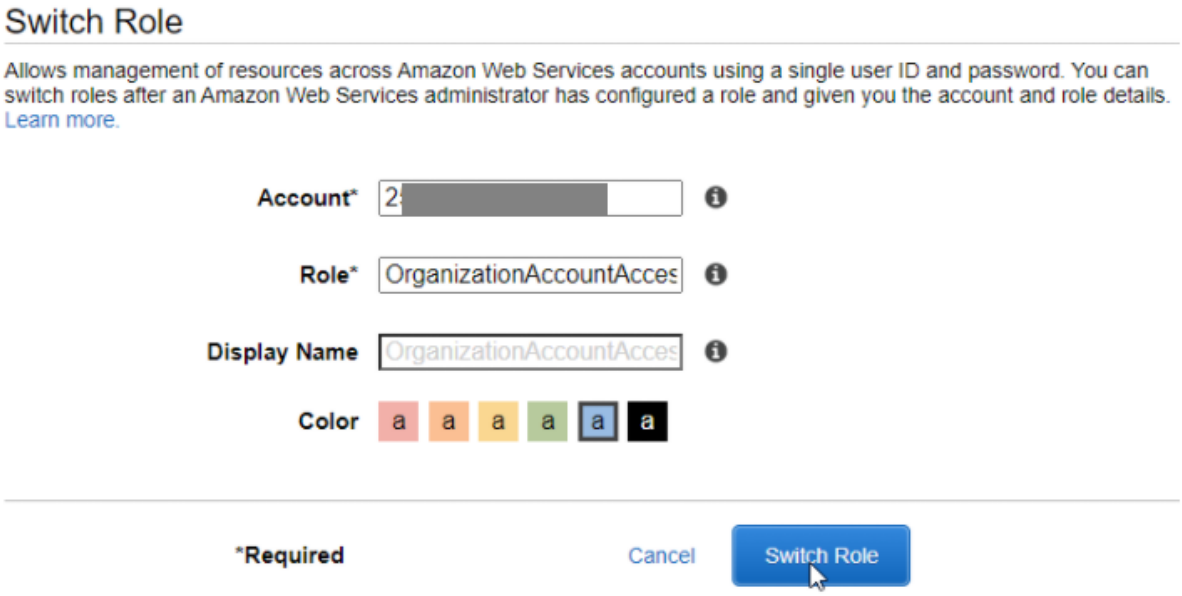


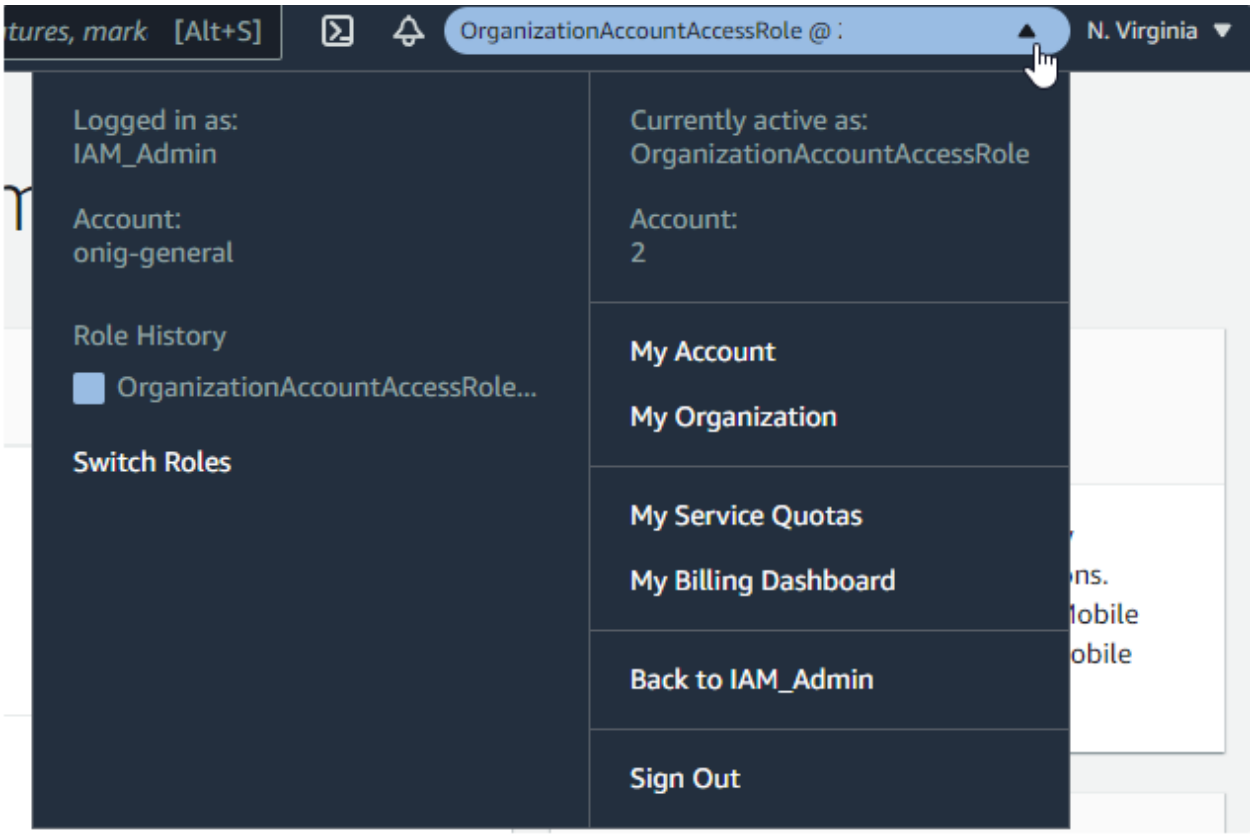
- Because we invited an AWS account this means we need to create a role switching role in order to go into it from another account. If you create an account within the organization then it automatically creates this. All you need is create a role in the invited account (prod), specify another AWS account (general) and input the ID.



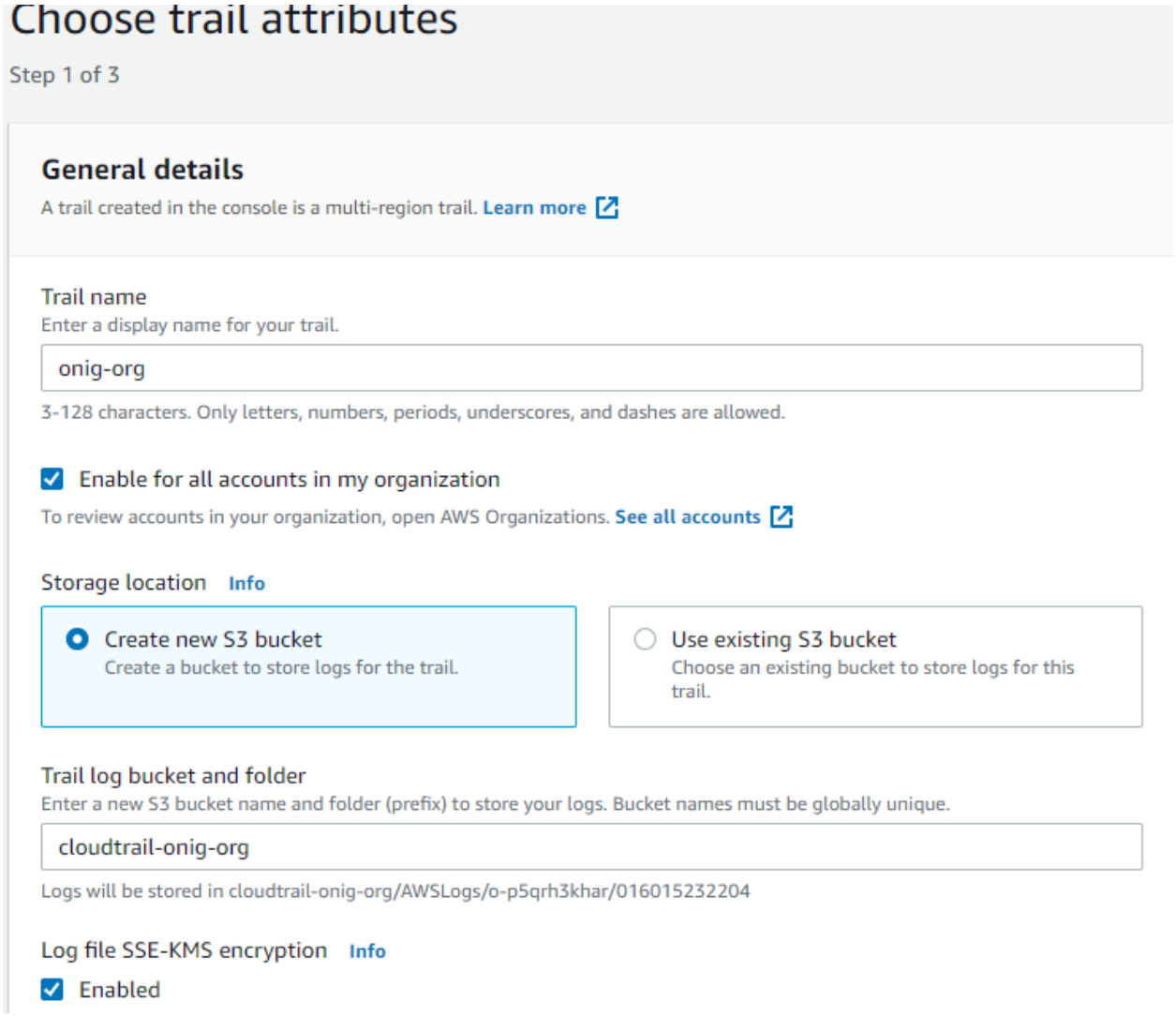
- So now we can assume a role from the general management account into the prod account. Just need the account ID you want to switch to as well as the name of the role.


IAM_Admin @ onig-general
N. Virginia
IAM User: IAM_Admin
My Account
My Organization
My Service Quotas
My Billing Dashboard
My Security Credentials
Switch Roles
Sign Out

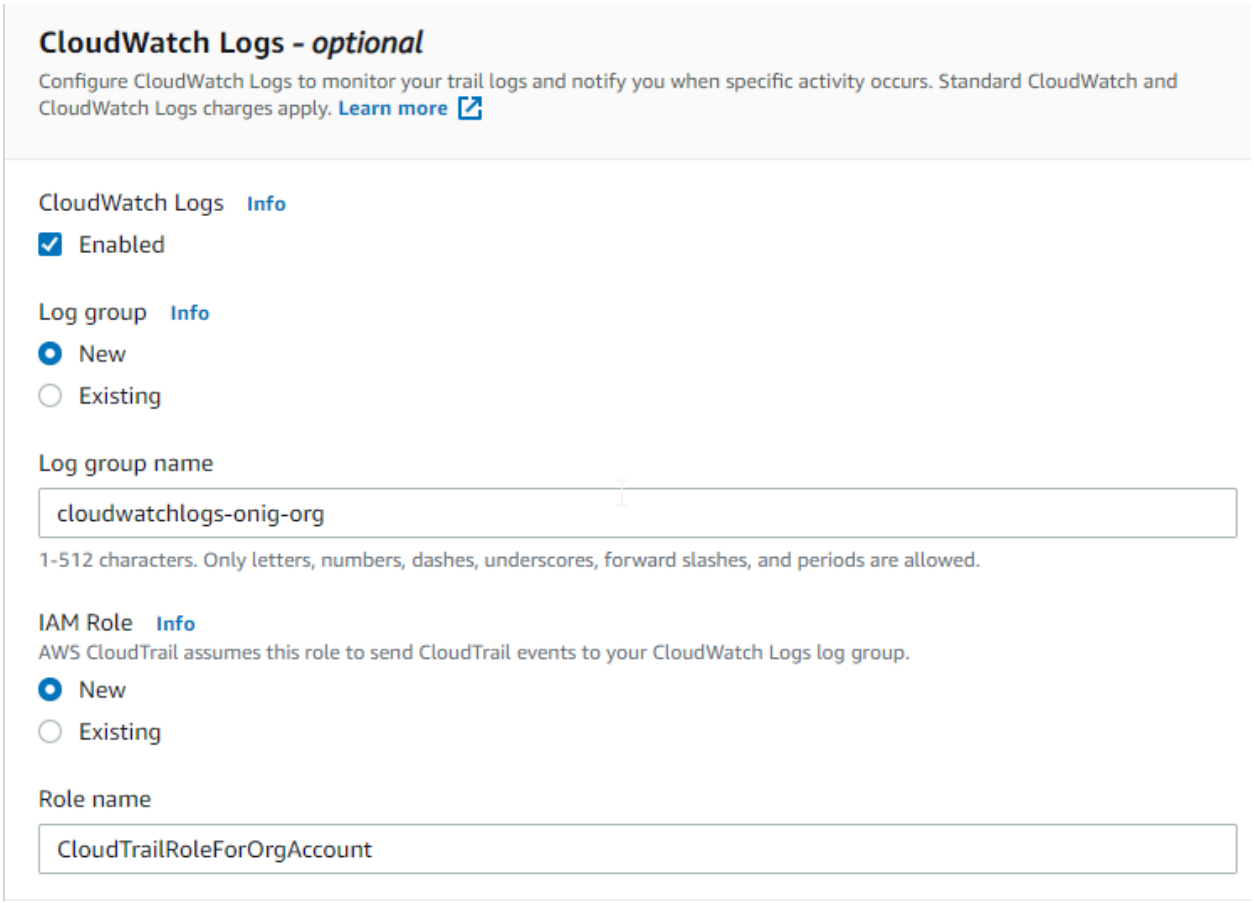

Switch Role
Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details.
Learn more.
Account*
Role*
OrganizationAccountAcces
Display Name
OrganizationAccountAcces
Color
*Required
Cancel
Switch Role



- So we are not going to implement organizational level cloudTrail which will log all the API calls within all the AWS accounts. This way it is located in one S3 bucket making it easy to analyze,
- A trail is a configuration about the logs we want to deliver to the S3 bucket to store for later. Organization trails allows us to use a configuration for all member accounts of a management account in an AWS organization. Therefore we have one unified logging system for a whole account. We can also integrate with cloudWatch logs so we have the ability to to monitor trail logs and notify via alarms when an activity occurs.
- 3 types of trails are captured: insight events (unusual volumes of API calls), data events ('GET' to S3 objects) and management events (default, EC2 restarted, who logged in)



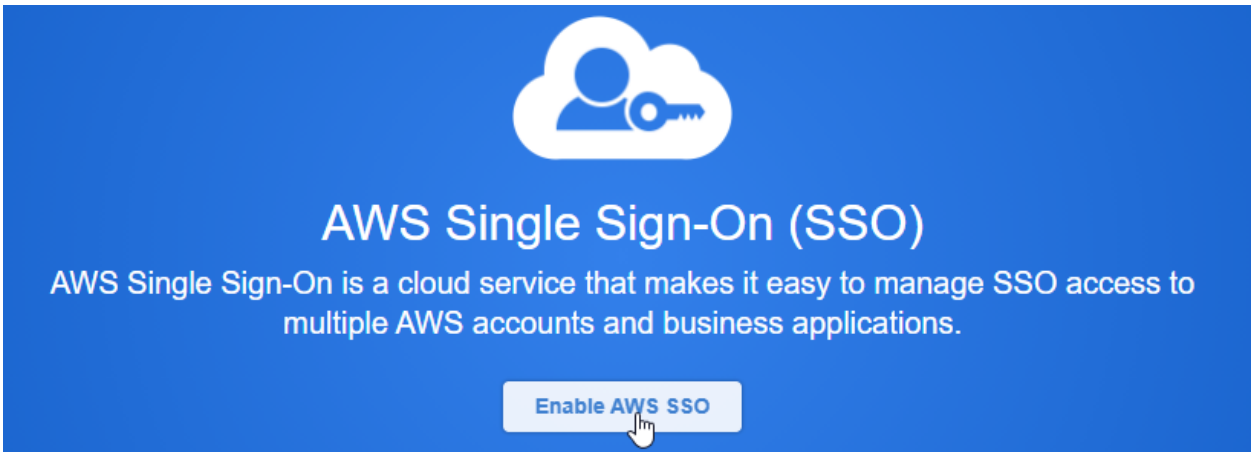
- Enable cloudWatch logs and a log group, needs an IAM role to give permission.



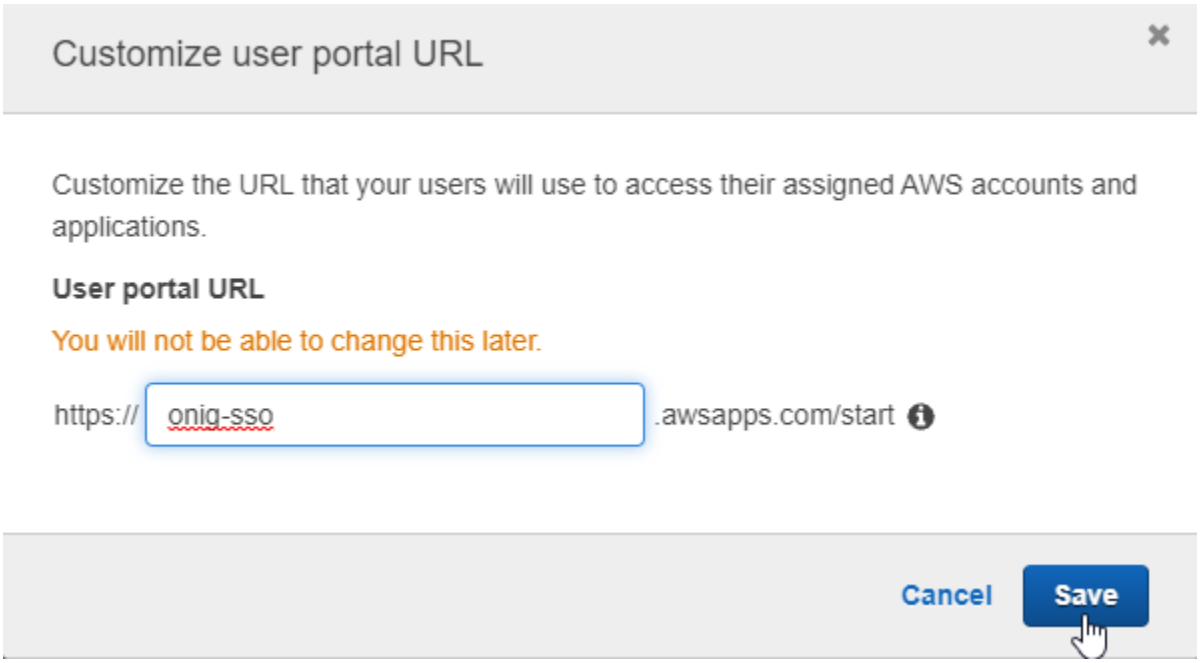
- CloudTrail can be applied to all regions!

Enabling SSO

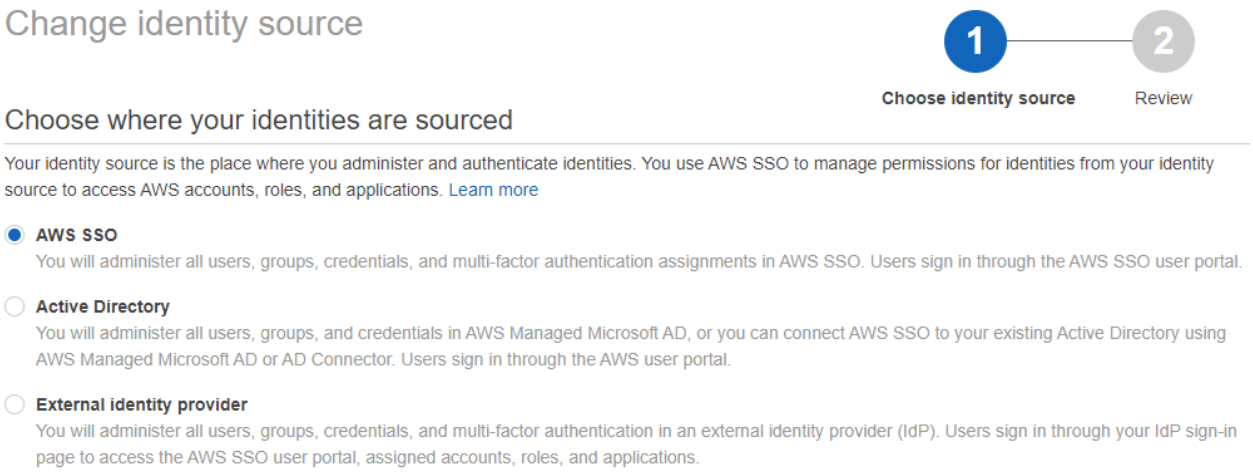
- We can establish permission sets for groups and users in SSO. This way we can give admin, billing or read only permissions easily for multiple accounts in one organization. We can also give a session duration before it has to be renewed.



- Change the user portal for SSO for a more human readable domain

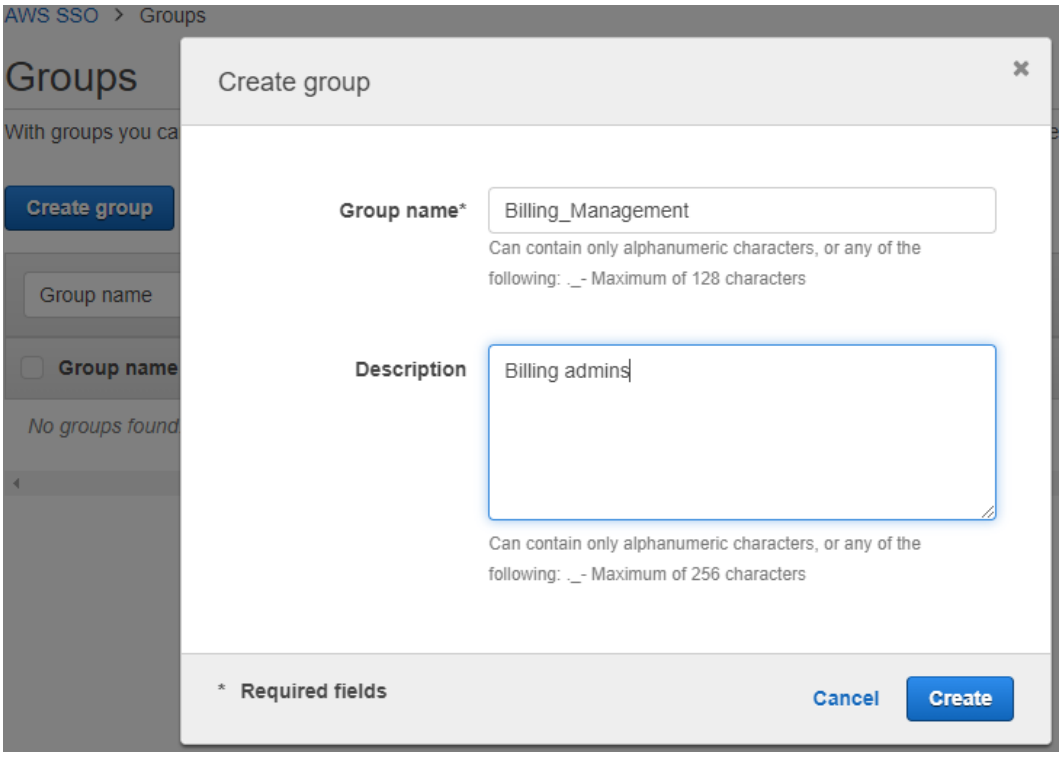


- We can select the source for our identities, SSO (you administer), Microsoft AD, external IdP (we administer via external IdP)

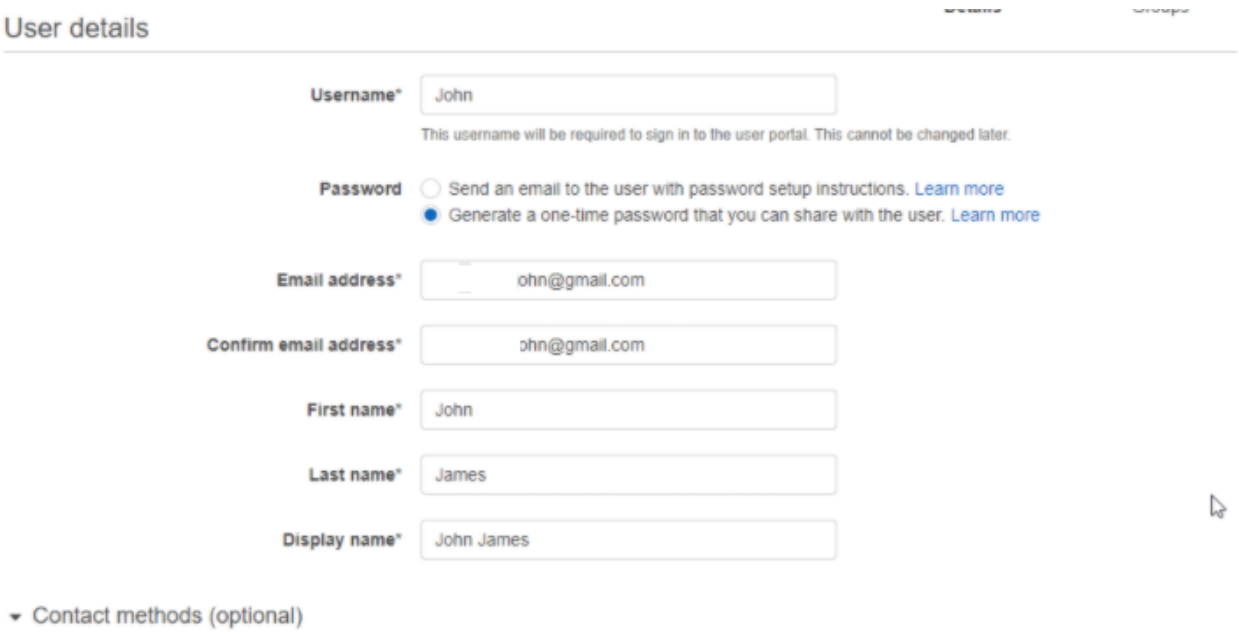


- Change multi-factor options if needed. Can prompt it on every login, what device MFA is allowed on etc.

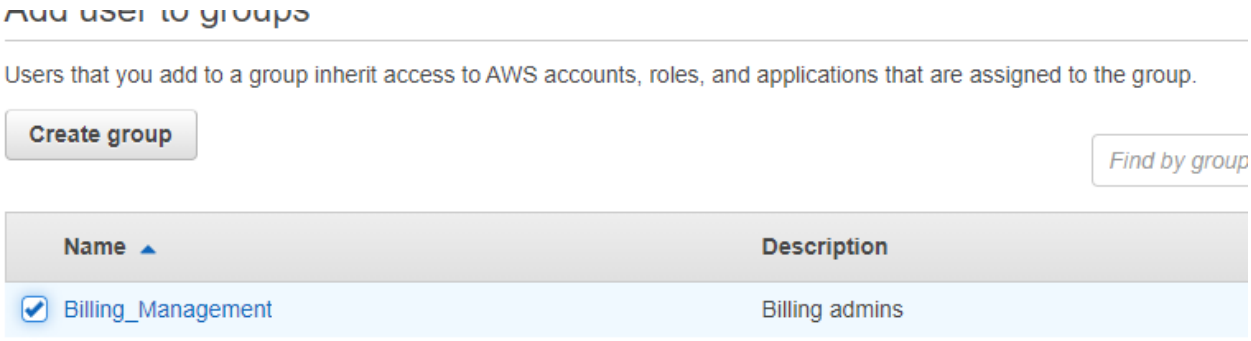
- We want to create an SSO group called billing, and with this we can add users who will be in charge of billing alarms and alerts to have the necessary permissions. We use permission sets which define access levels for the user or group it is assigned to within SSO. This is different to normal IAM because this applies to all the accounts rather than just one. All a user has to do is log into the SSO portal and their credentials are assigned a set of permissions.



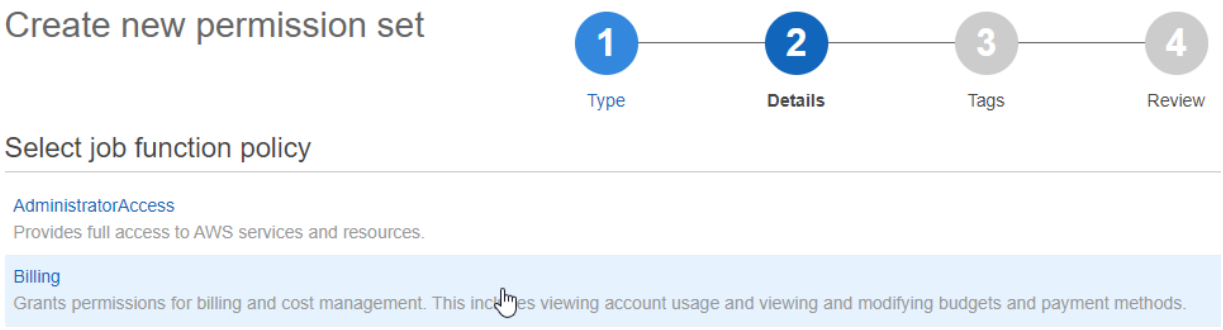
- Once we have a group we can make the user. SSO gives us additional information like contact methods, job info etc.



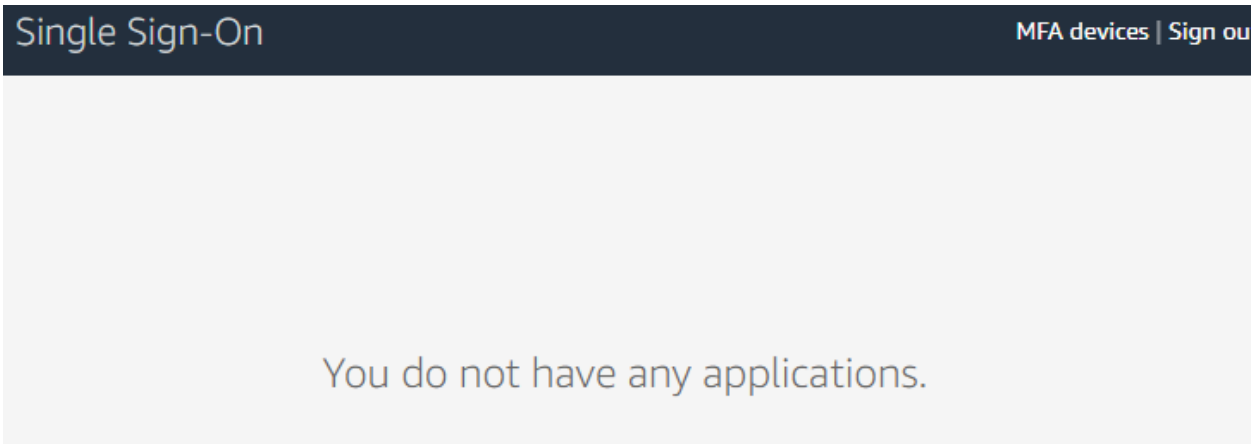
- Add the user to our billing group



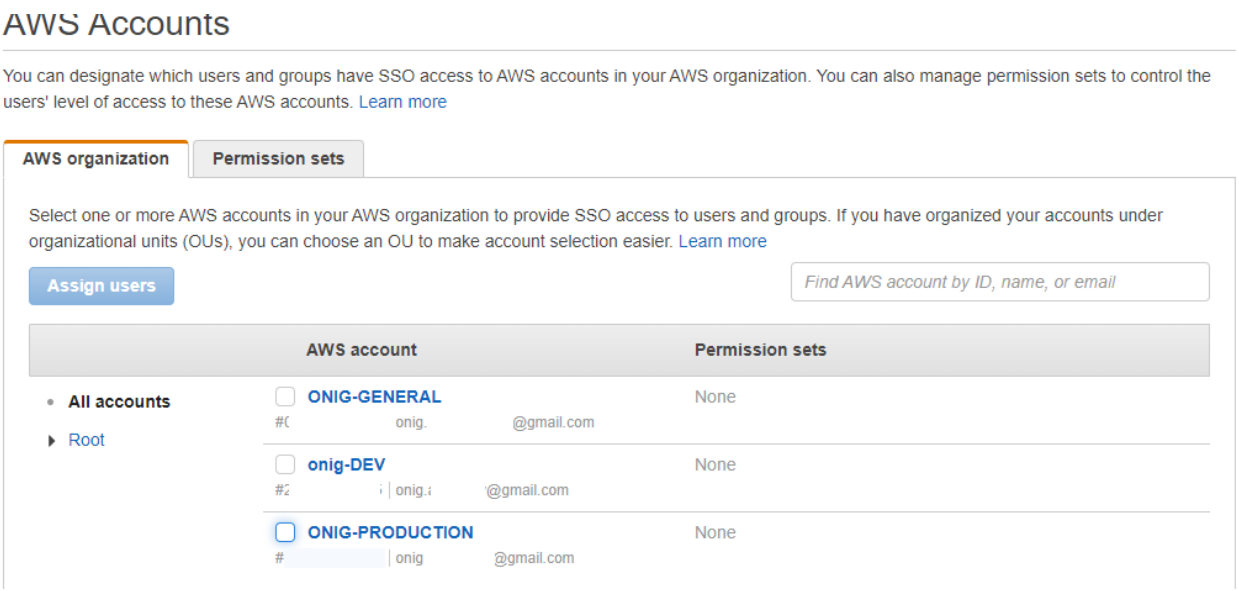
- We need to attach some permissions to the group/ user as we cannot do anything at the moment.
- We will create a permission set which can be attached to the SSO group/ user to give permission to the orgnization
- We will select the billing set



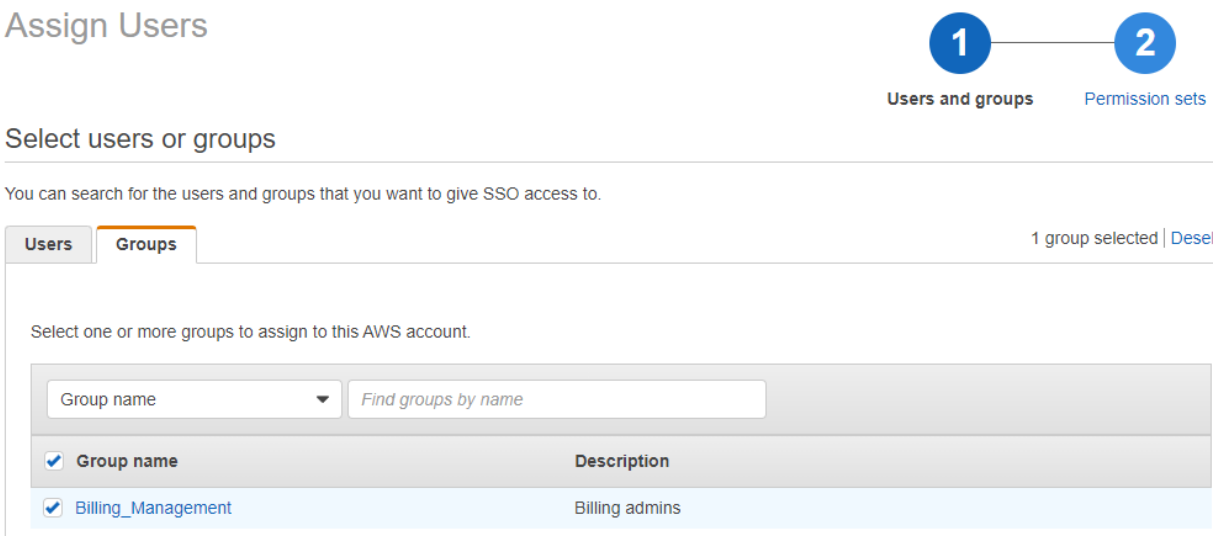
- When you sign into the user you made via SSO portal you will see everything you have access to
- In this case, we see nothing. And that is because we did not attach the permission sets to the designated accounts. The user John and it's billing group has the permission set but the accounts do not.



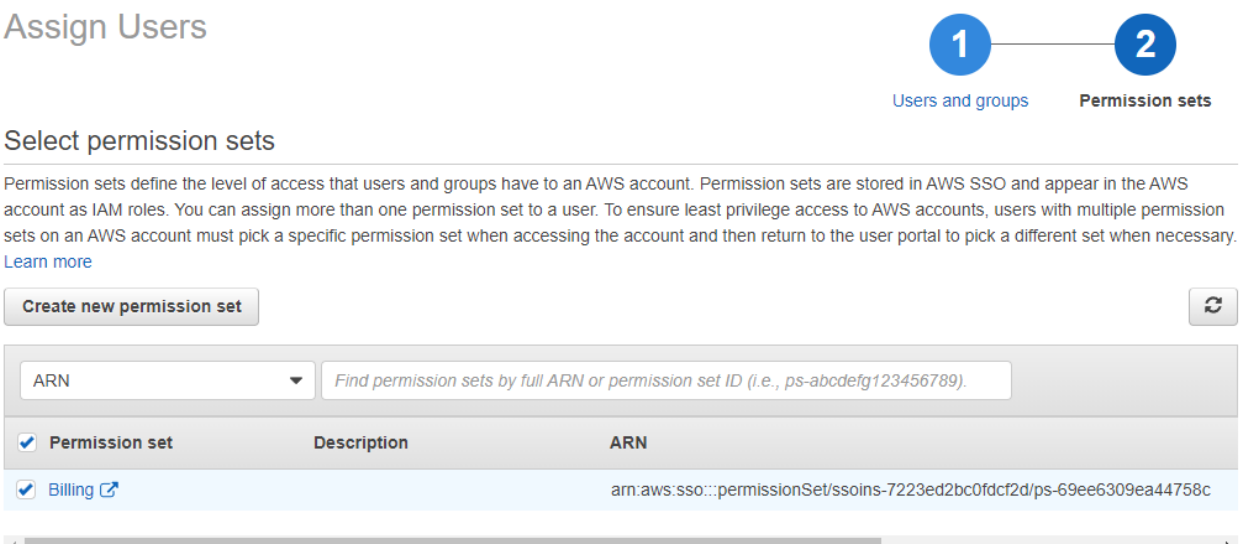
- We can go back into SSO and view our AWS Accounts and confirm, no accounts have SSO users or groups attached to them.



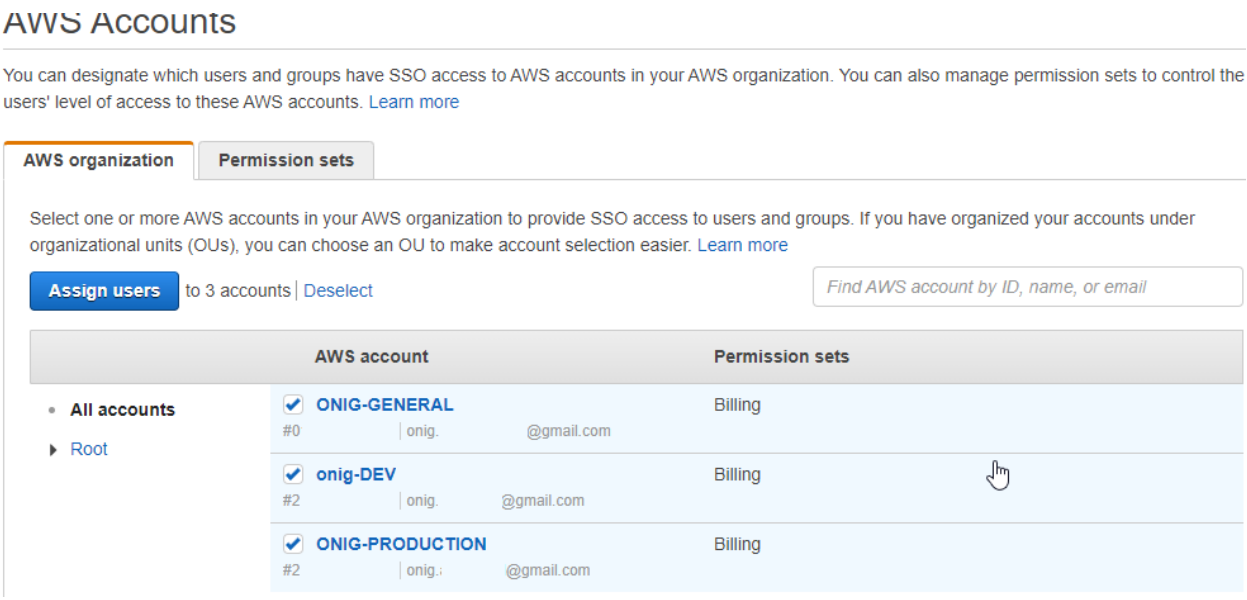
- Add group in this case to all the accounts



- Add permission set to the SSO group



- Now you should see permission sets attached to the accounts



- Now log back into the SSO console via John