**Cloud Computing**

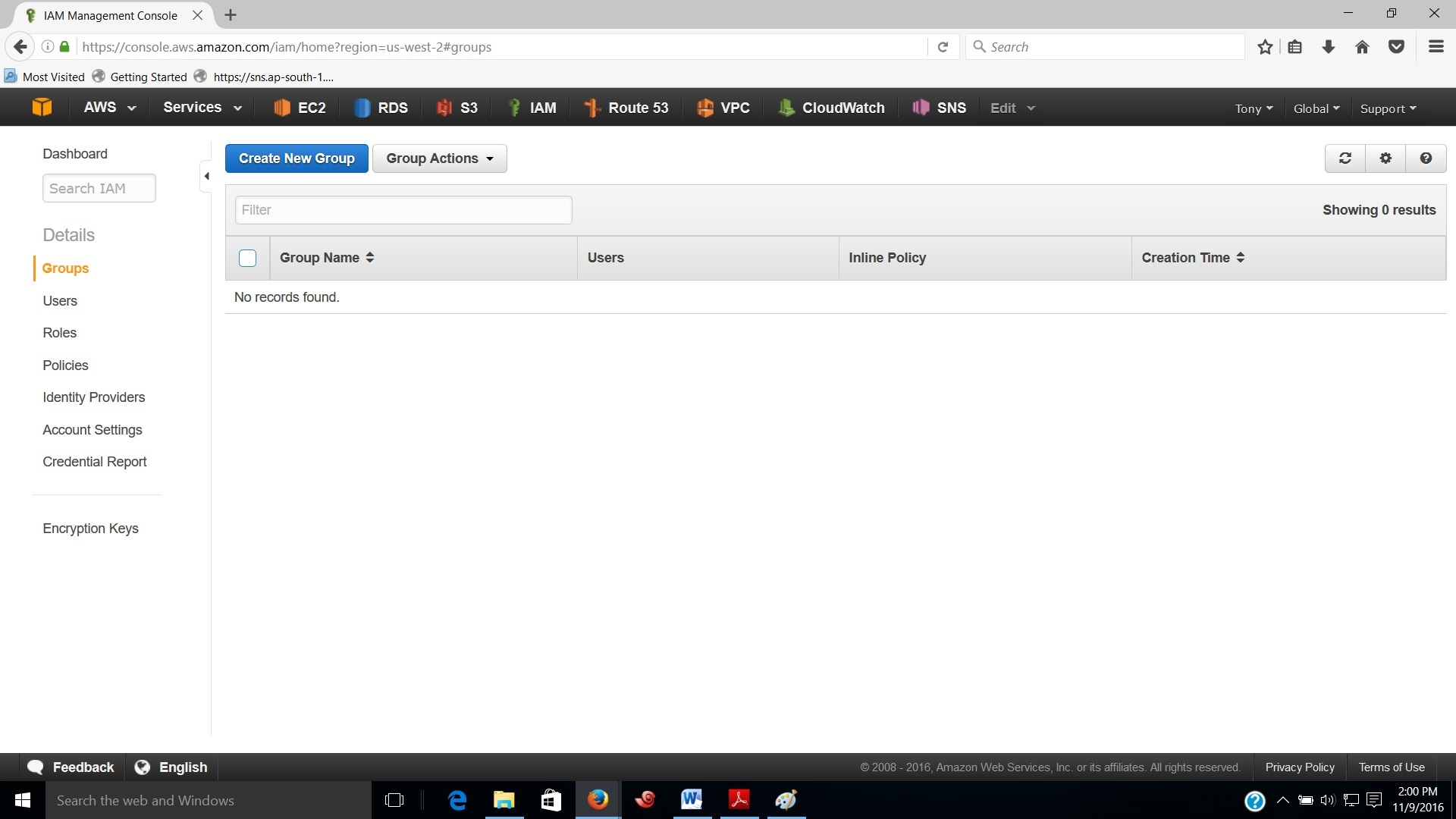
Session 7 : Identity and Access Management

Assignment 1: IAM Accounts

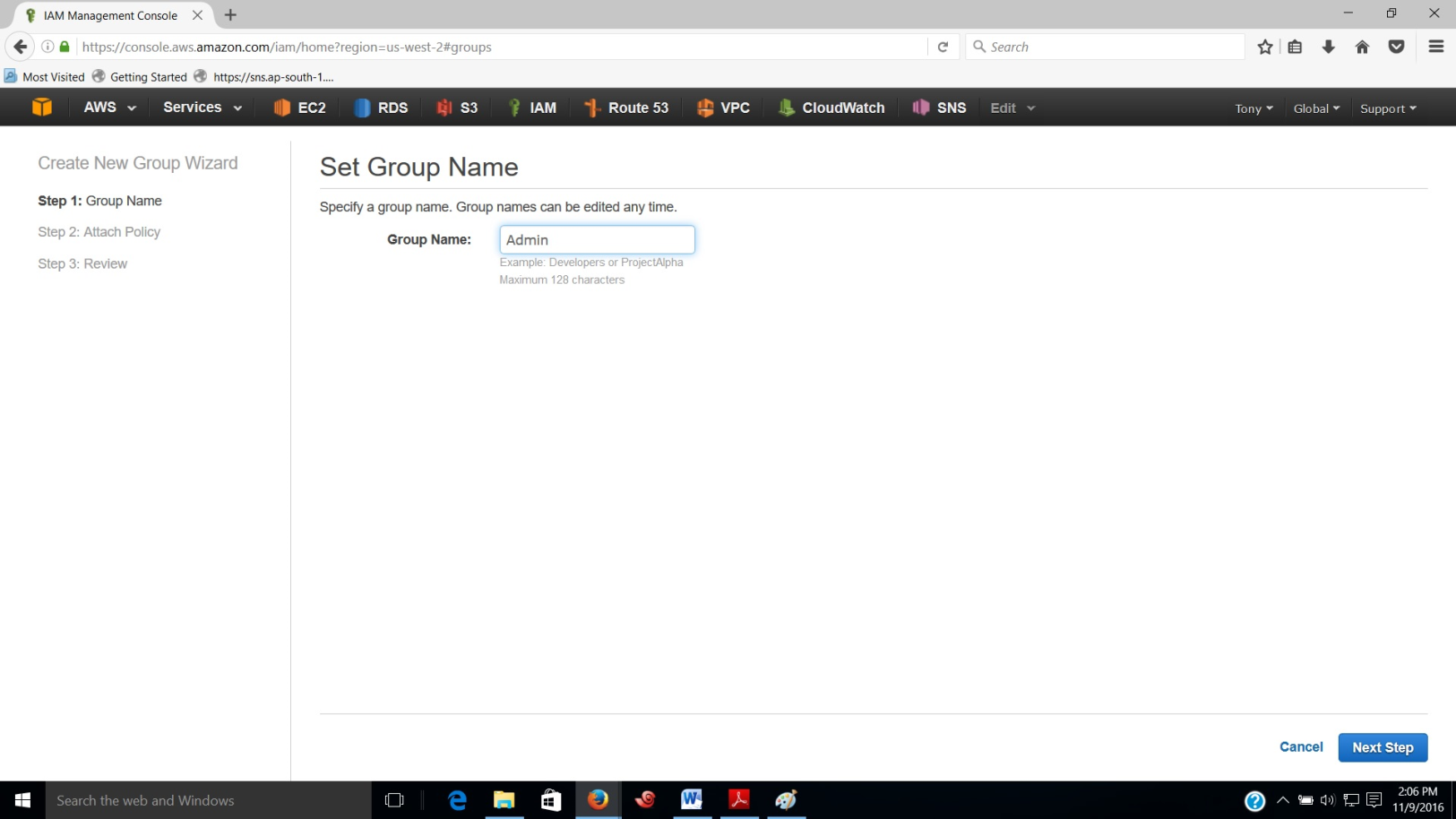
* Creating a Administrator Group

An IAM Group is a collection of IAM users. We are used to provide permissions for a collection of users. With IAM Group it is easier to manage permissions for those users. It is the way to attach policies to multiple users at one time.

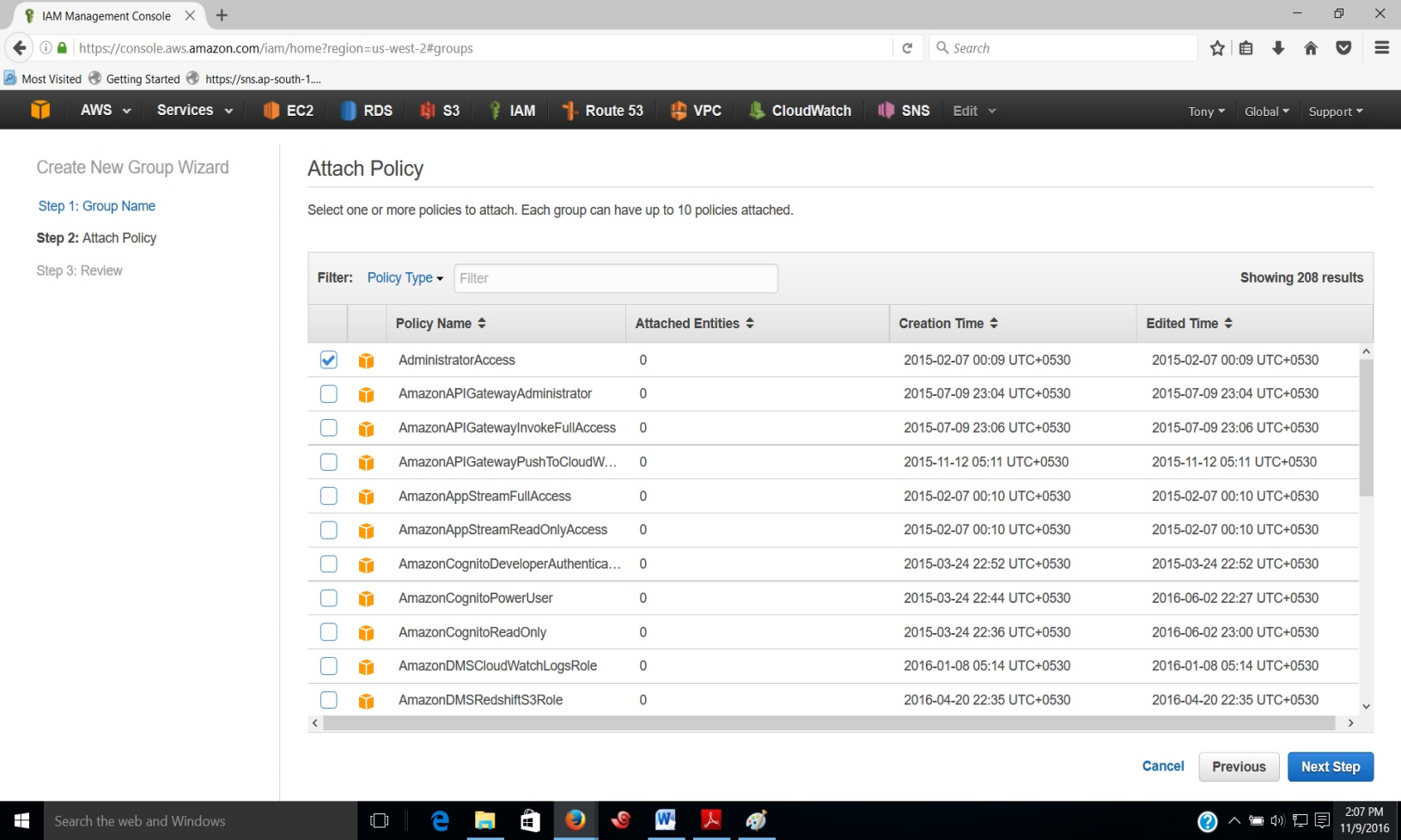
1. Sign in to the Identity and Access Management (IAM) console.
2. Click on the Groups tab of the IAM Dashboard.
3. Click on Create New Group.



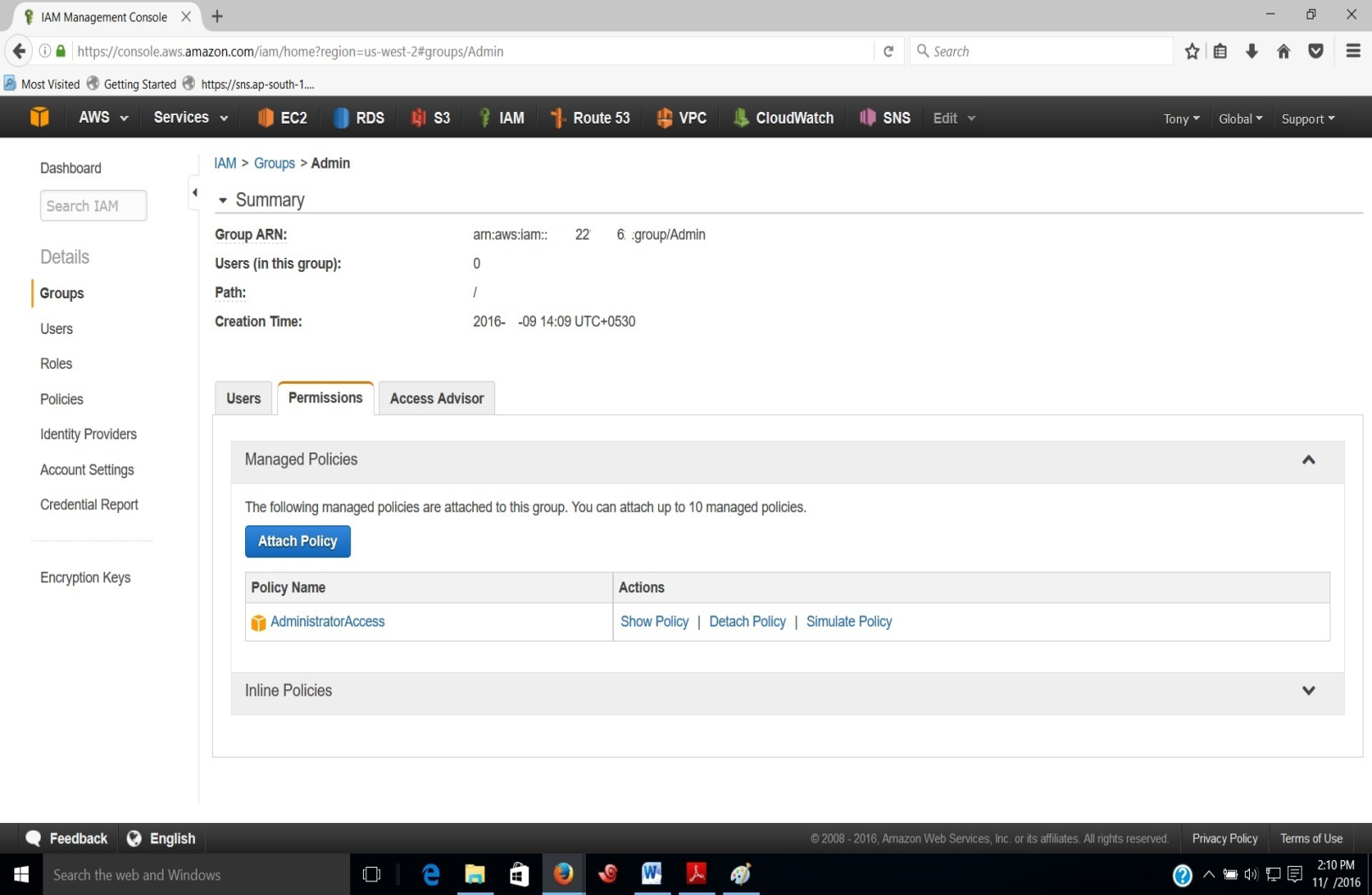
1. Give name for the Administrator Group and Click on Next Step.



1. In the Attach Policy page select AdministratorAccess policy to grant full permissions for all AWS Resources. Use the Filter drop-down menu and Filter box to search for a specific policy you need.



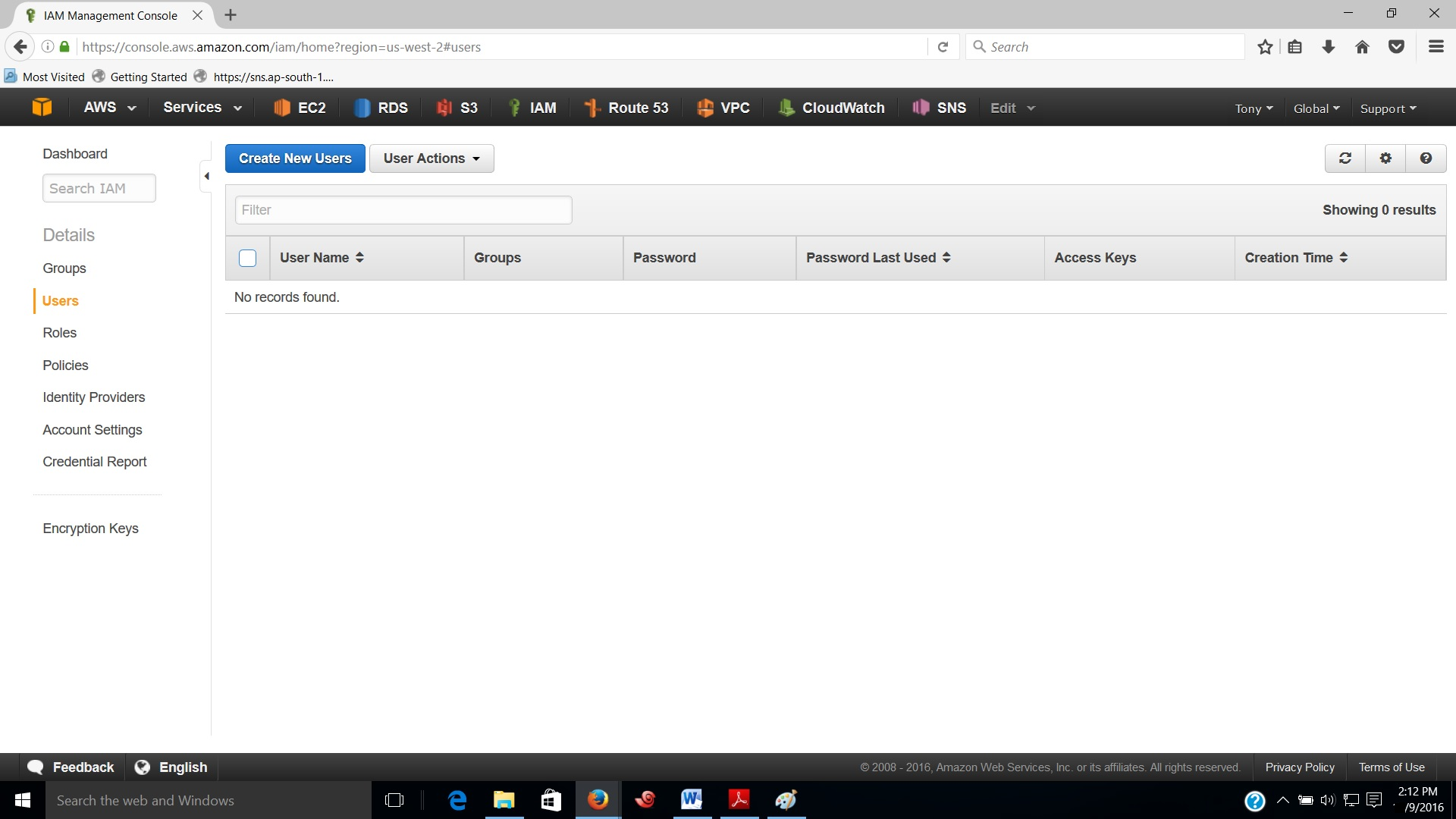
1. Click on Next Step, Review the details and then choose Create Group. New group will be listed under Group Name. Click on newly created group to see the details.



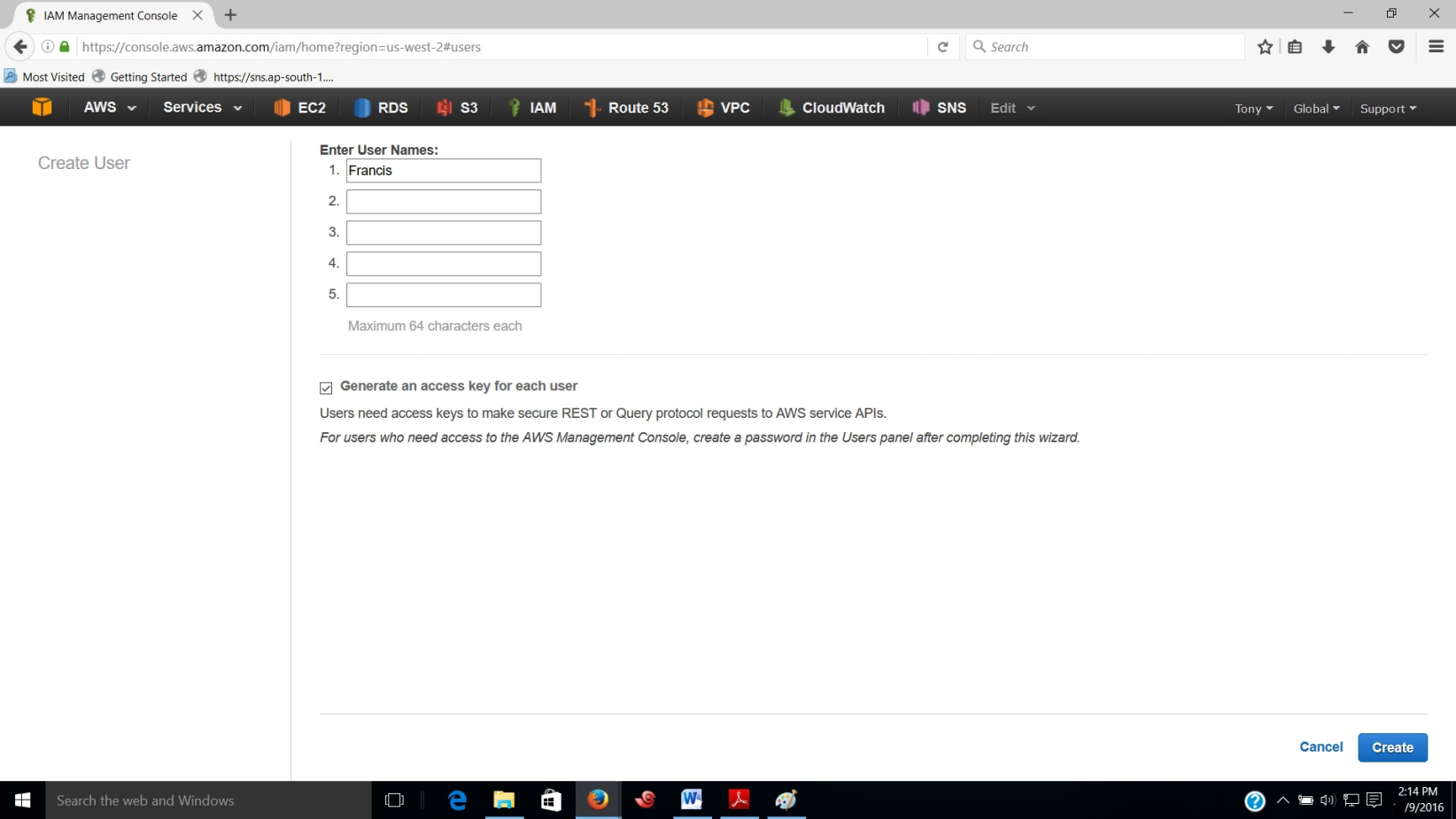
* Creating a User to add to the Administrator Group

An IAM User is an entity that we create in AWS and it represents the person who uses the IAM user to interact with AWS. IAM users enables a person to sign in to the AWS Management Console for interactive tasks and to make programmatic requests to AWS services using the CLI or API. A user in AWS consists of a name, a password to sign into the Management Console, and up to two access keys to use for API or CLI access.

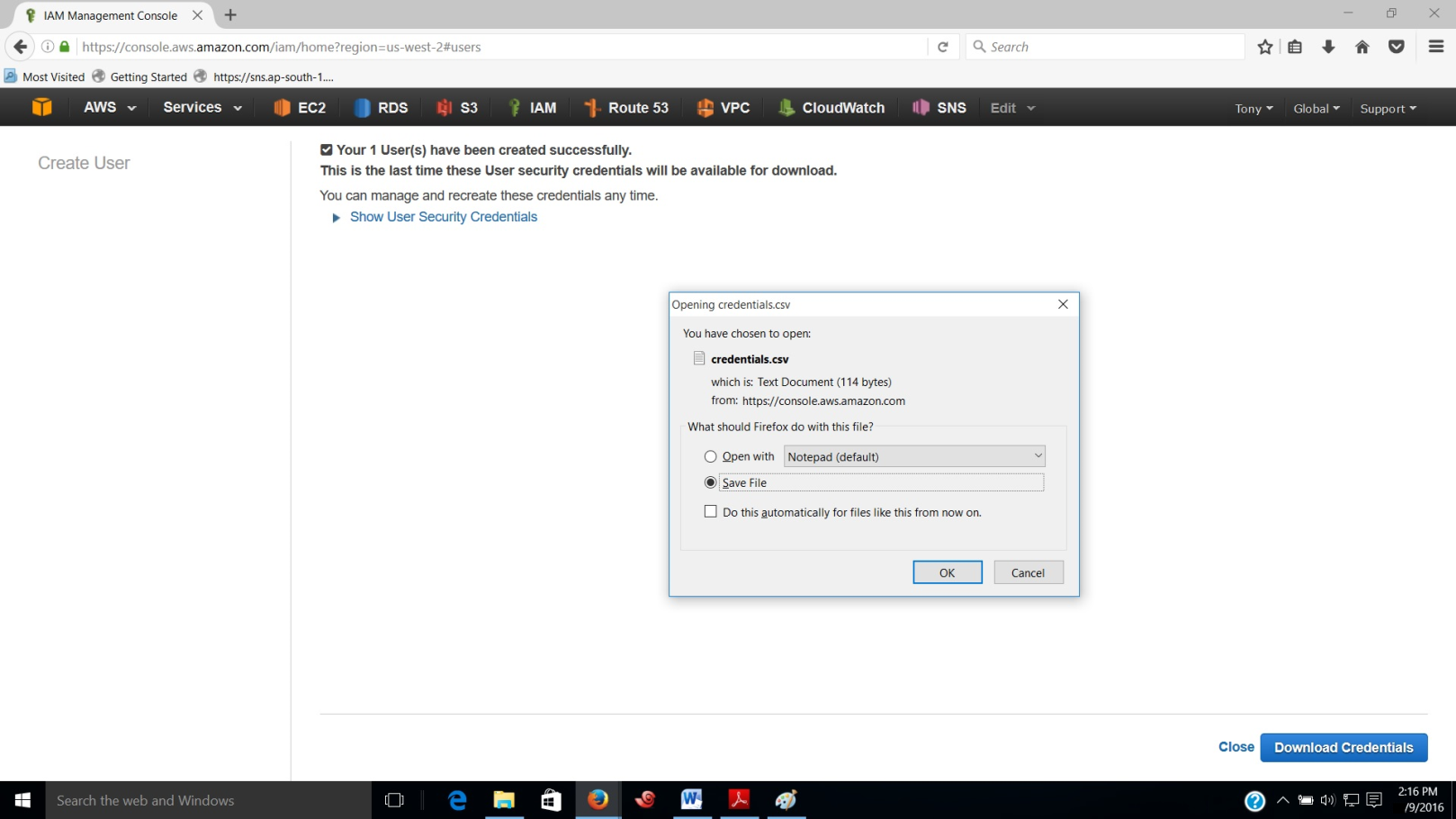
1. In the navigation pane, select Users, and then choose Create New Users.



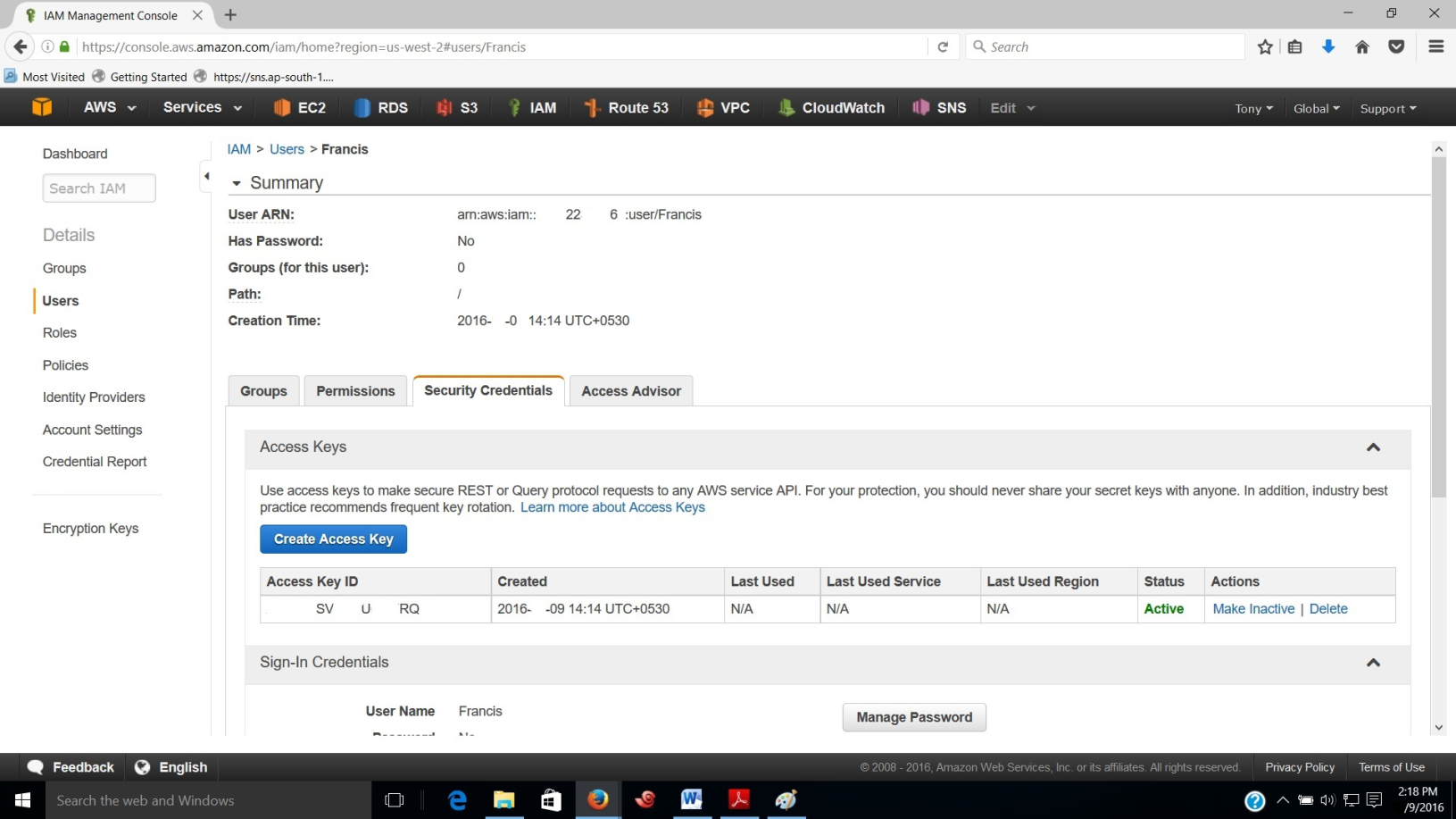
1. Give a name for the User and select the checkbox next to Generate an Access key for each user.
2. Click on Create button.



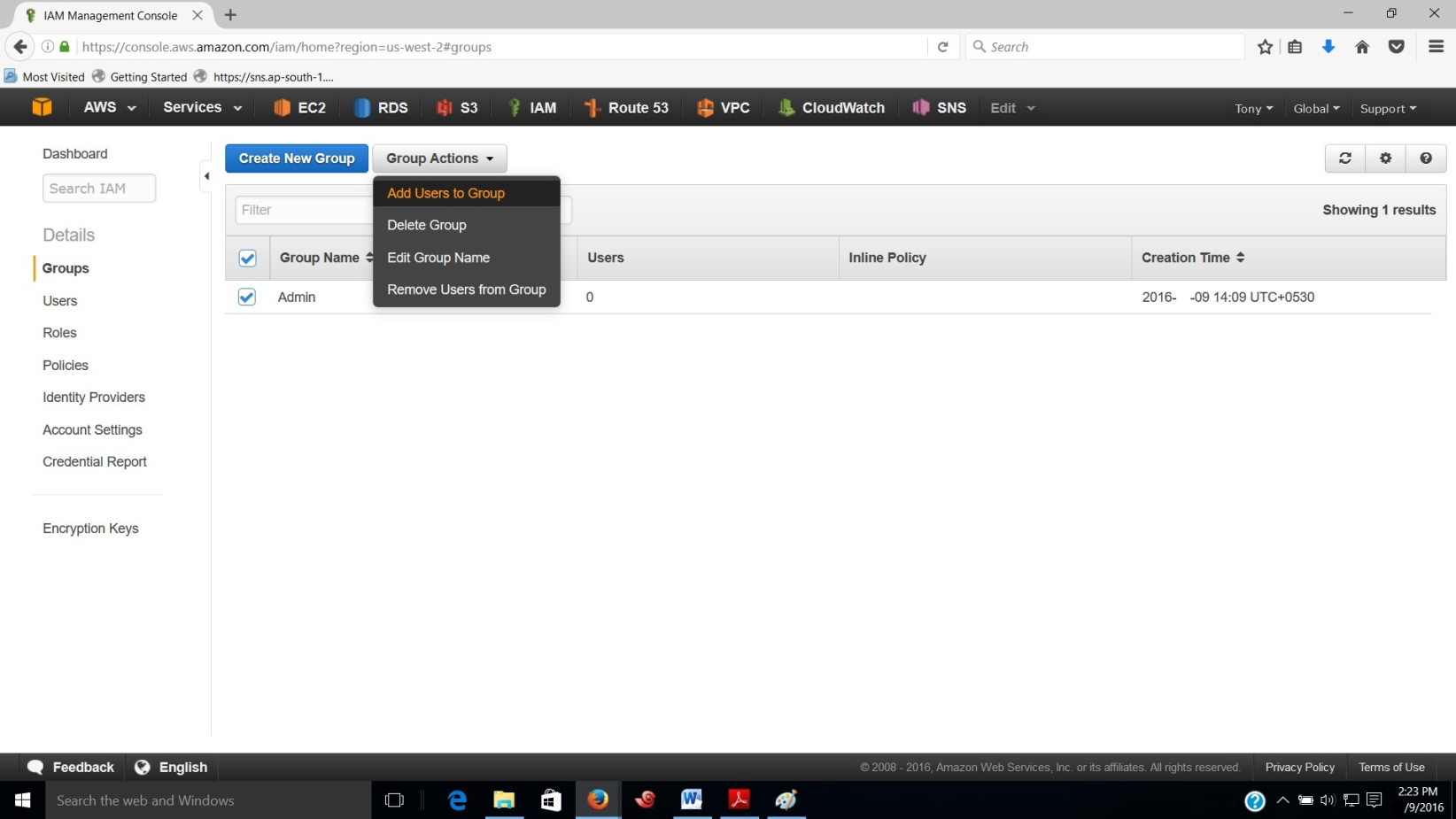
1. An IAM User will be created with specific credentials such as user access key and key id. These credentials can be used to access AWS resources through Command Line Interface.
2. Click on Download Credentials to download and save user access key.



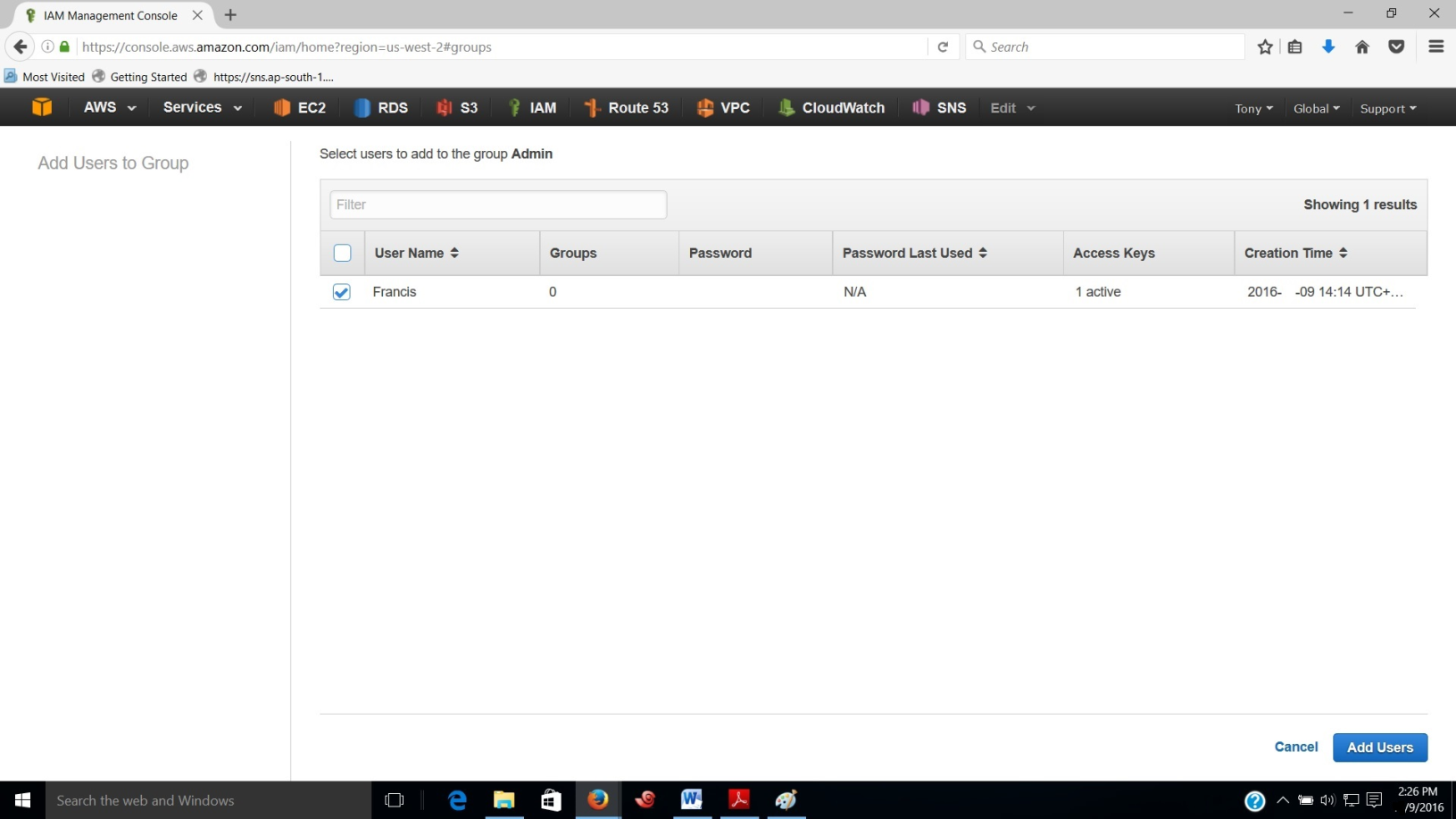
1. Click on the newly created user to see the details. We can see ARN, date and time of user creation, access key id and status of access key etc.



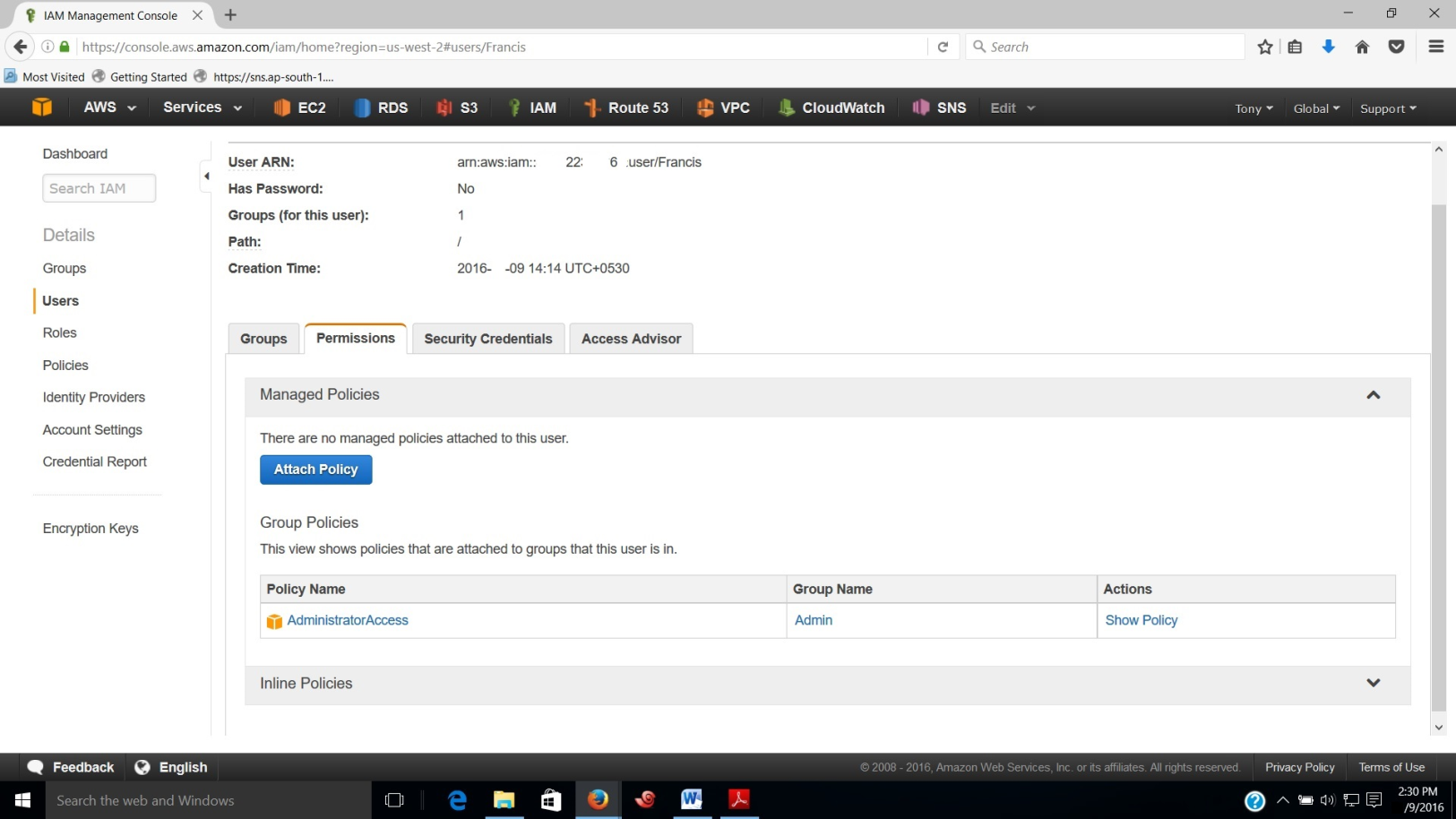
1. In order to get Administrative privileges user must be added to Administrator Group.
2. Choose the Groups tab, select Administrator Group and Click on Group Actions.
3. Then select Add Users to Group.



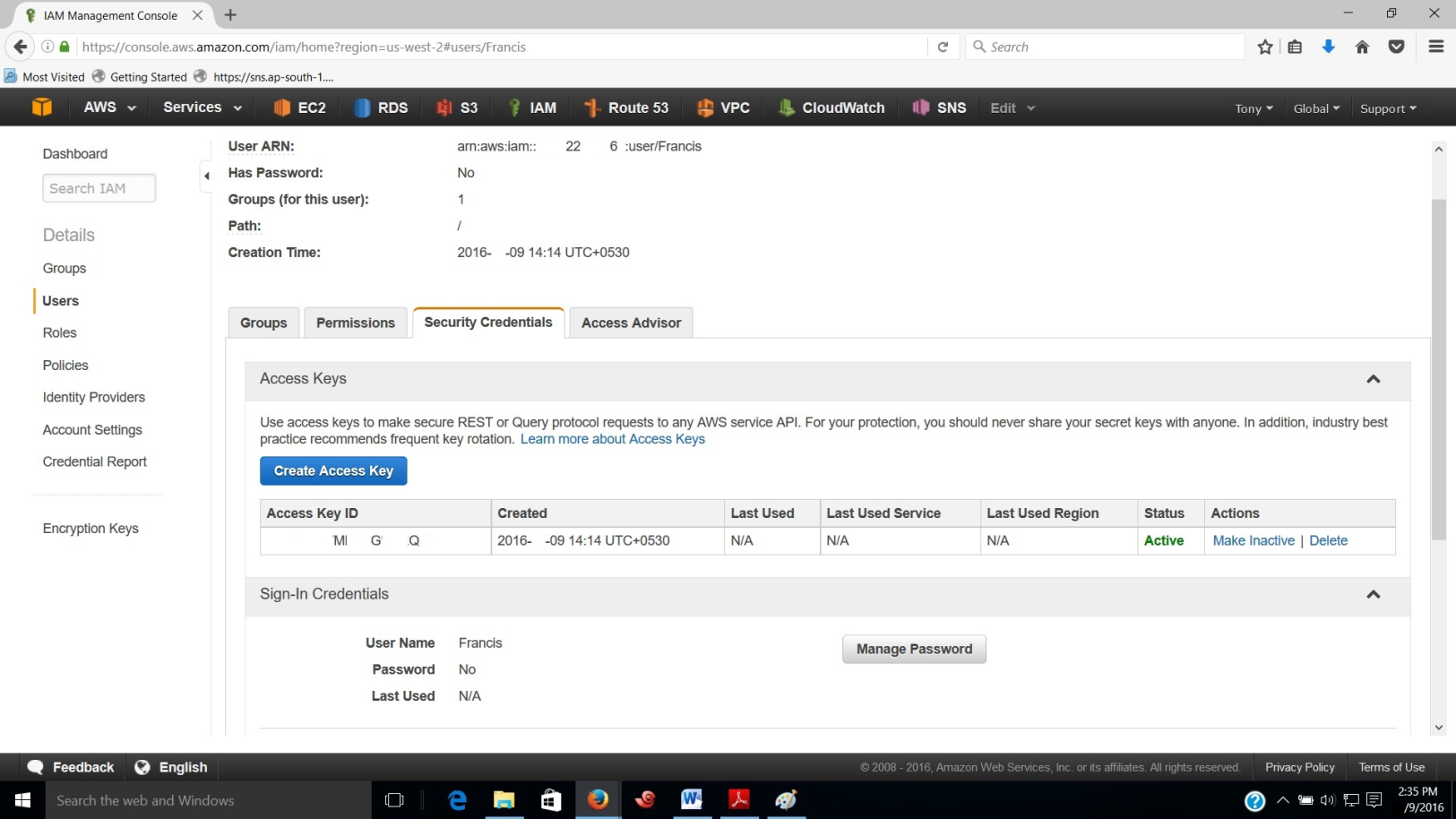
1. On the Add users to group page, select the users you want to add to Administrator group.
2. Click on Add Users.



1. Click on the users tab on the IAM navigation pane and select new user to see the details.
2. Click on the Permissions tab to see the access rights of the user. We can see that under group policies AdministratorAccess policy is allocated to the user.



1. To protect from unauthorized access we need to give password for the Administrator user.
2. Click on the Security Credential tab. Click on Manage Password below Sign-in Credentials to set password for the Administrator user.



1. On the Manage password page select the option Assign a Custom password and fill the required password to the fields. Click on apply to set the given password.

