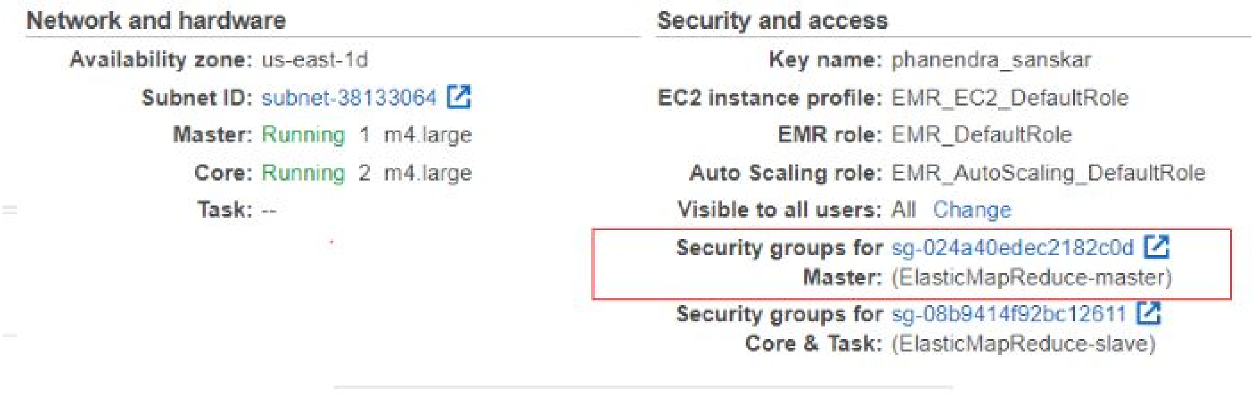
I am not able to perform SSH to the master node?

1. Under the cluster information page click on the security groups of the master node



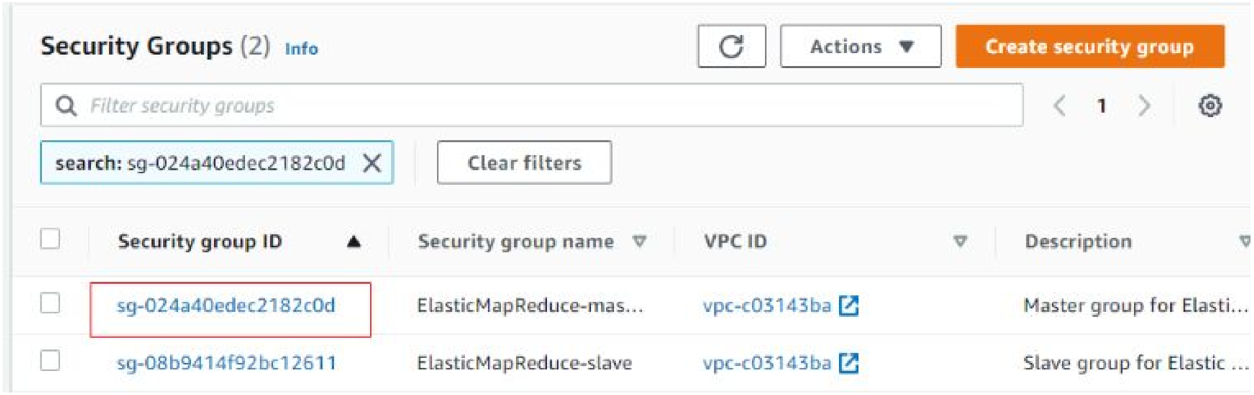
Network and hardware

Availability zone: us-east-1d
Subnet ID: subnet-38133064
Master: Running 1 m4.large
Core: Running 2 m4.large
Task: --

Security and access

Key name: phanendra_sanskar
EC2 instance profile: EMR_EC2_DefaultRole
EMR role: EMR_DefaultRole
Auto Scaling role: EMR_AutoScaling_DefaultRole
Visible to all users: All Change
Security groups for Master: sg-024a40edec2182c0d (ElasticMapReduce-master)
Security groups for Core & Task: sg-08b9414f92bc12611 (ElasticMapReduce-slave)

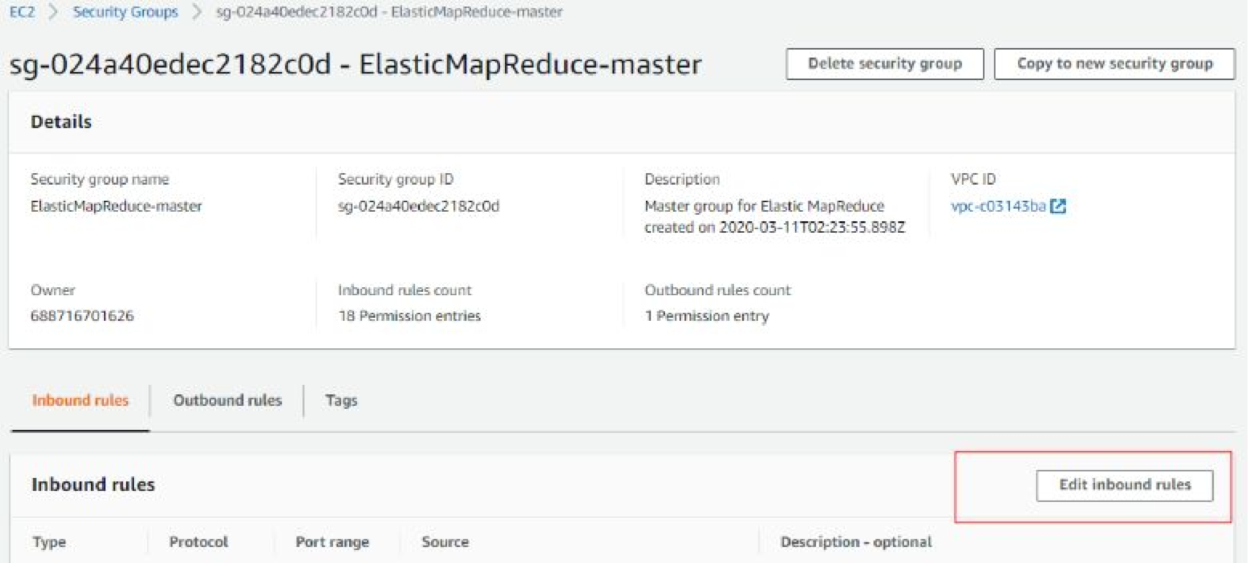
2. Clicking on the security group and you will land on a similar page. Here click on the security group of the Elastic Mapreduce-master node as highlighted in the image.



search: sg-024a40edec2182c0d

	Security group ID	Security group name	VPC ID	Description
□	sg-024a40edec2182c0d	ElasticMapReduce-mas...	vpc-c03143ba	Master group for Elasti...
□	sg-08b9414f92bc12611	ElasticMapReduce-slave	vpc-c03143ba	Slave group for Elastic ...

3. Clicking on the security group will land you on the corresponding security information page. Click on edit inbound rules to add a new rule


EC2 > Security Groups > sg-024a40edec2182c0d - ElasticMapReduce-master
Delete security group
Copy to new security group
Inbound rules
Outbound rules
Tags
Edit inbound rules

sg-024a40edec2182c0d - ElasticMapReduce-master

Details

Security group name: ElasticMapReduce-master

Security group ID: sg-024a40edec2182c0d

Description: Master group for Elastic MapReduce created on 2020-03-11T02:23:55.898Z

VPC ID: vpc-c03143ba

Owner: 688716701626

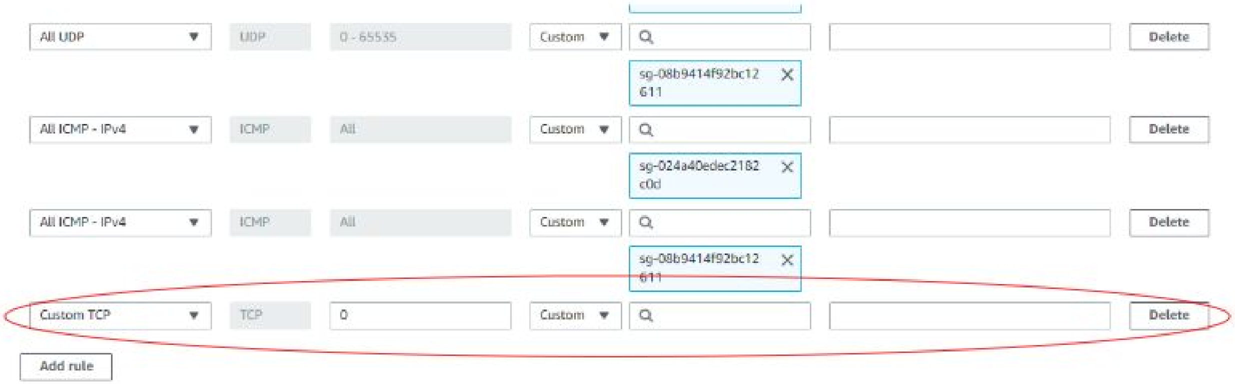
Inbound rules count: 18 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules

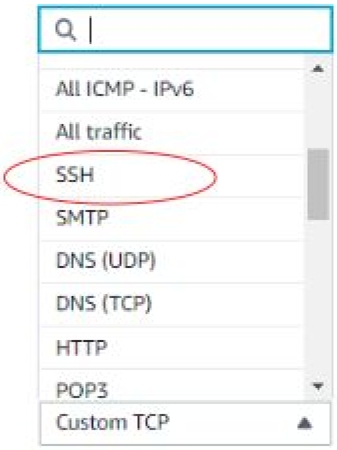
Type	Protocol	Port range	Source	Description - optional

4. This will take you list of existing rules where you have the option to delete the existing rules [Clicking on delete on the extreme right-hand side] or add a new rule by clicking on **Add rule** towards the bottom of all the rules. Clicking on add rule will add a new row as shown in the figure below

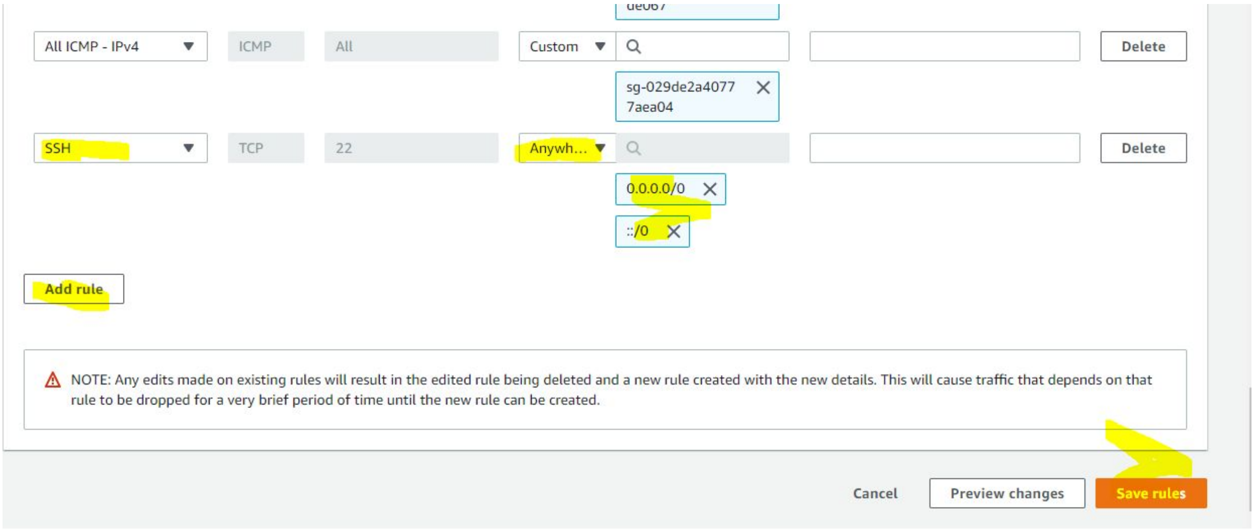


All UDP	UDP	0 - 65535	Custom	sg-08b9414f92bc12611	
All ICMP - IPv4	ICMP	All	Custom	sg-024a40edec2182c0d	
All ICMP - IPv4	ICMP	All	Custom	sg-08b9414f92bc12611	
Custom TCP	TCP	0	Custom		

a. Under the type field of the newly added row select **SSH**



b. Choose **Anywhere** under the source field. This will automatically 0.0.0.0/0 and ::/0 in the adjacent blank column.



All ICMP - IPv4	ICMP	All	Custom	sg-029de2a40777aea04		Delete
SSH	TCP	22	Anywh...	0.0.0.0/0 ::/0		Delete

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

c. On addition of the rule and choosing the appropriate options as shown below, click on save rule [at the bottom of the screen] to successfully add the rule

On adding this rule it enables you to perform an SSH to the master node of the cluster.

I cloned an existing cluster and it terminated with errors? or
I restarted the laptop and not able to connect to the EMR cluster

You get this error when you choose **My IP** under the source field section at the time of adding the SSH rule. To avoid this you either update the rule by changing it to **anywhere** instead of **My IP**

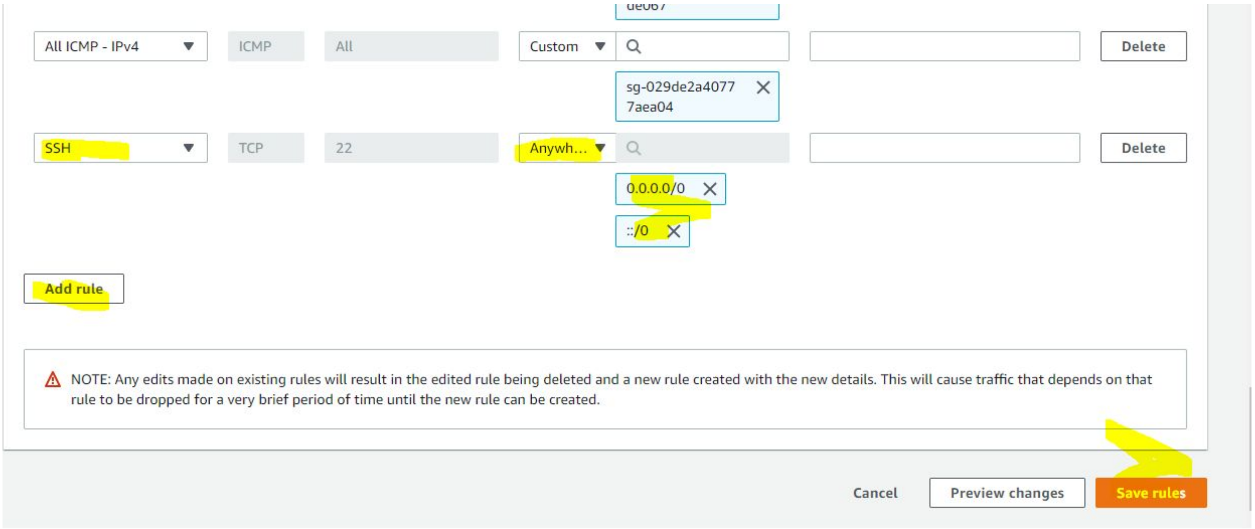
OR

[Less Recommended]
Every time while cloning the cluster or connecting to the cluster, you need to edit the security groups and give your current IP address in the earlier created rule for SSH [In case you chose My IP instead of Anywhere]

This will ensure you to do a successful SSH or successfully cloning to a new cluster.

Important - General Practice

To avoid this hassle every time you clone a cluster or every time you restart the laptop a common practice followed while studying/ or internal testing is choosing the option **anywhere** instead of custom or **My IP.** In the actual development environment, this should be avoided because it leaves the cluster vulnerable and any IP address can access the cluster.



All ICMP - IPv4 | ICMP | All | Custom | sg-029de2a4077 7aea04 | Delete

SSH | TCP | 22 | Anywh... | 0.0.0.0/0 | ::/0 | Delete

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

The "**Type**" field will be **SSH**", and the **Source** will be "**Anywhere**" for this rule. For frequent testing, you can avoid using My IP address and choose "Anywhere" while adding rules in the Security Group.

After adding the rule do not forget to click **save rules** at the bottom of the window