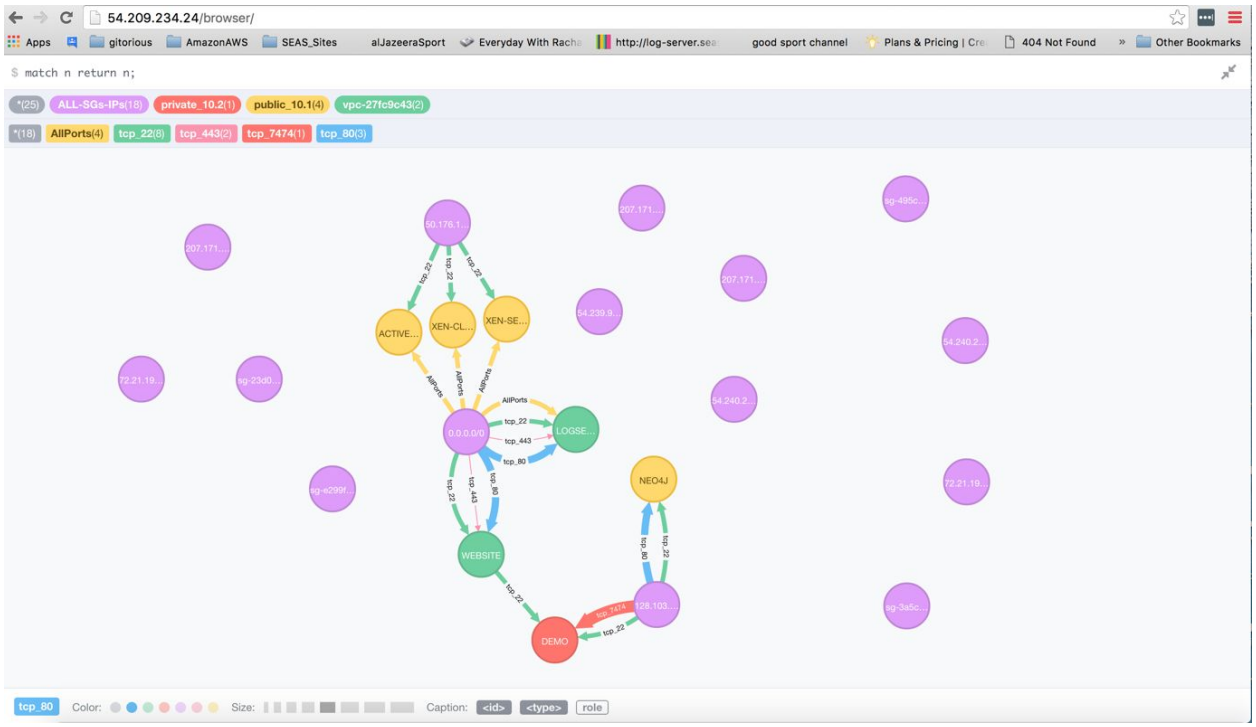
Using the aws_neo4jv01 AMI for AWS EC2s connections

How to

1) Create a role with read access to your environment.
2) Create instance from the aws_neo4jv01 with that role.
3) Copy paste the IP of the instance to your browser.
4) Use the neo4j sql command to reveal the graph

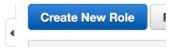
   Match (n) return n;
5) Example:

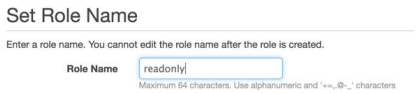


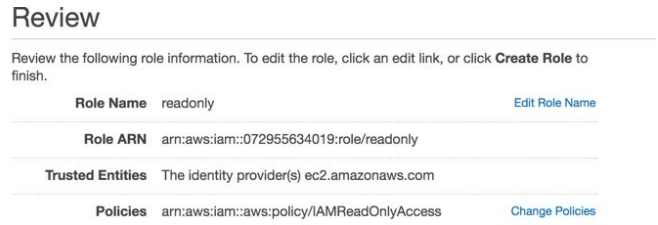
Create Role:

Create a “ReadOnlyRole” for Amazon EC2 instance.
This role will be used by the neo4j instance for the Python code to be able to access the environment to collect/analyse the nodes relation and send it to neo4j.
Note: For later development this role might need to have write access so neo4j be able to add or remove EC2/securityGroup IPs.

Steps:
IAM -> Roles -> Create New Role -> “set role name” - > Amazon EC2 -> ReadOnlyAccess -> Create Role.





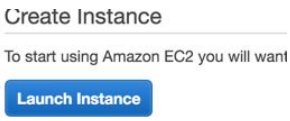


Create Instance:

B) Run the instance with the ReadOnlyRole.

It is the same create EC2 instance steps.Add the ReadOnlyRole to the instance and open port 22 and 80 for the security group.

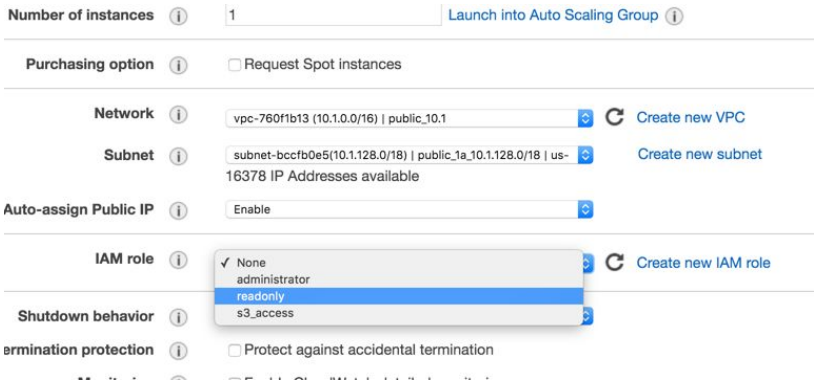
1)



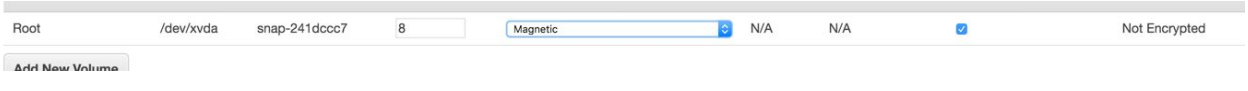
2) Choose AMI: select “aws_neo4jv01”

3) Instance type(Micro is ok)

4) Make sure to choose the “readonly” role you created earlier.

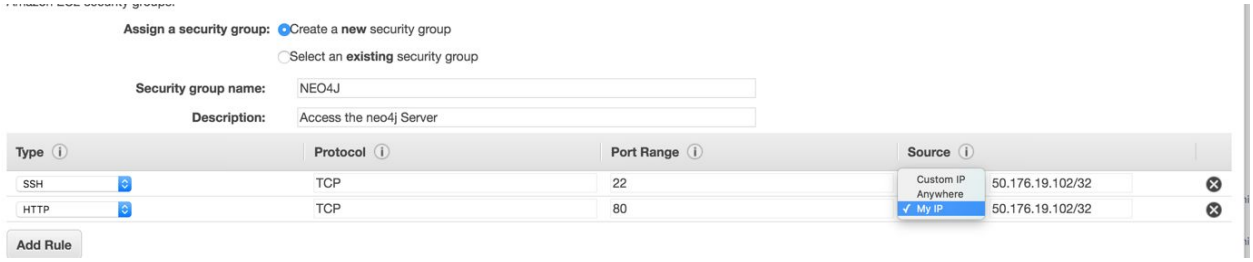


5) Volume Type(magnetic is ok)

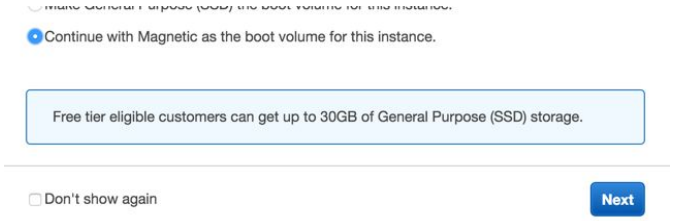


6) Better to tag the instance

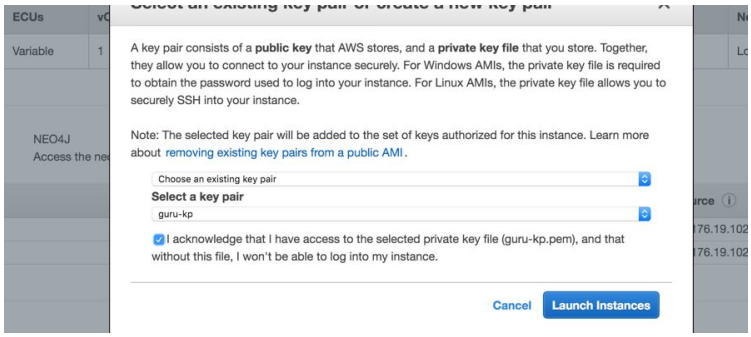
7) Create a security group. Make sure to protect this instance.



8) Continue with magnetic



9) Choose your keys

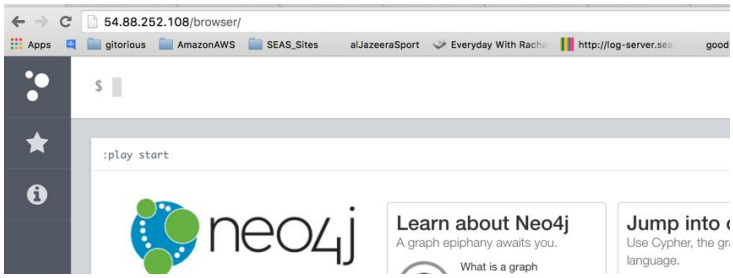


C) Check the instance

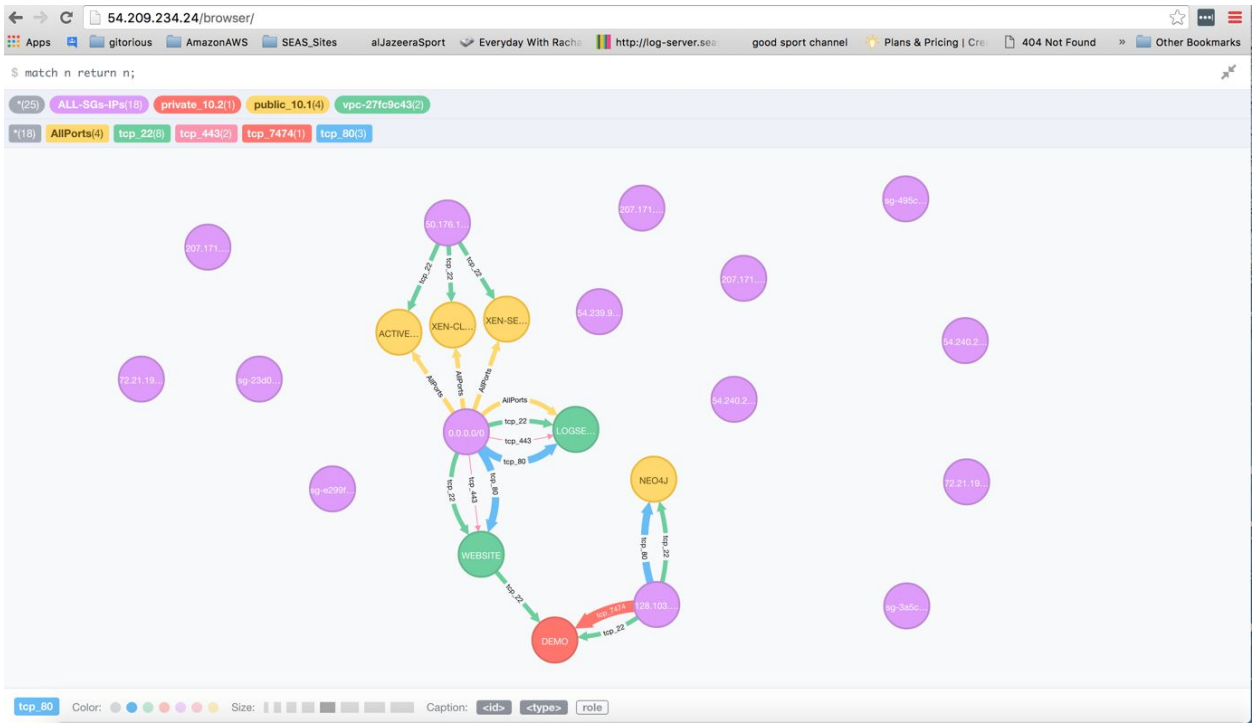
NEO4J URL:

When the instance finishes initialize, stick the instance Public IP to your machine browser (for whom you opened the security Group)

My instance IP is 54.88.252.108, check it on the browser



Reveal the graph using the SQL like command (MATCH (n) RETURN n)



What does the graph tell us ?

1) VPCs : I have 3 VPCs in my environment
    a) Private VPC have one instance
    b) Public VPC with 4 instances
    c) VPC-######## (VPC with no name tag) with 2 instances
2) ALL-SGs-IPs : I have 18 IPs in my security groups. Some of the security group might have embedded security group that is dealt as an IP.
3) I have 18 kinds of ports are open in my Security group
    a) 4 instances open all ports to the internet (0.0.0.0/0)
    b) Port 22 is opened to 8 IPs

    c) Port 7474 opened to one IP
    d) Port 80 opened to 3 IPs
4) Many IPs are in my security group but they never used , why ?
5) Some nodes have the title start with sg-???? Which means that they are a security groups that embedded inside other security groups.

Whats Nex:

1. Subnet Graph
2. VPC peering graph
3. Active connection graph.
4. Node size based on AWS instance type.
5. Stop vs running nodes.
6. Many others.