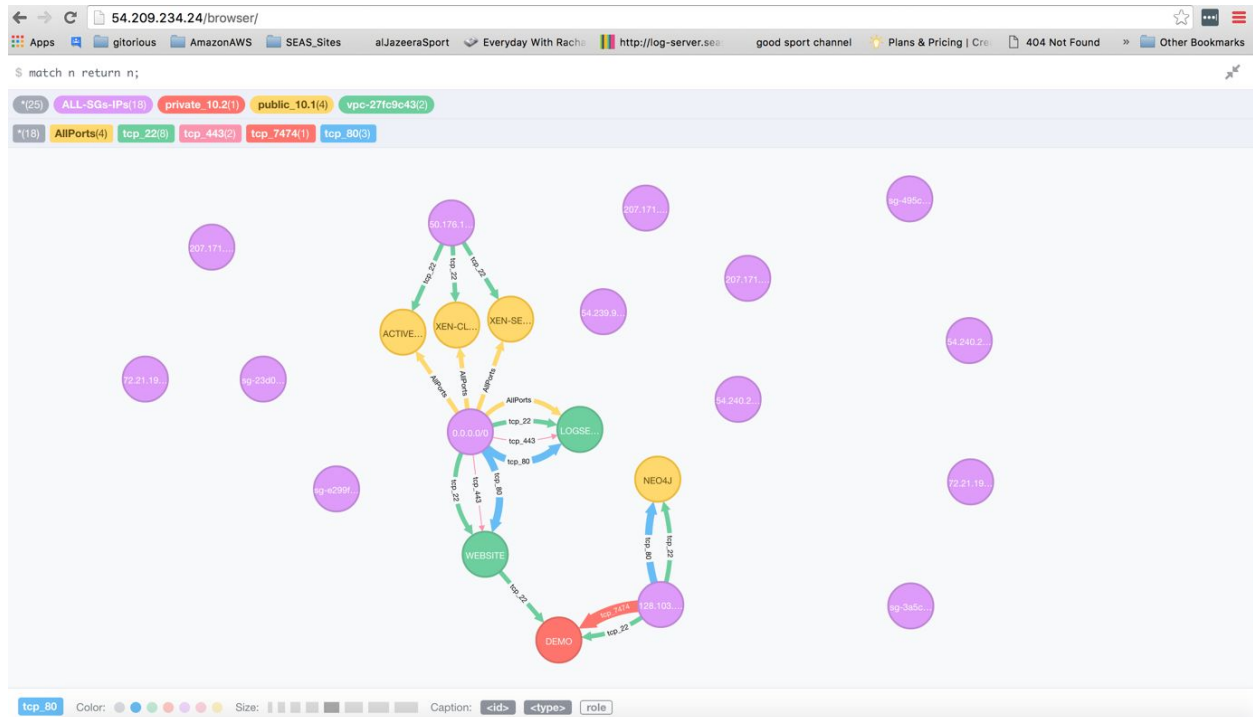


## Using the aws\_neo4jv01 AMI for AWS EC2s connections

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.

## Security & Identity



### Identity & Access Management

Manage User Access and Encryption Keys

Directory Service

Users

**Roles**

Policies

☐ administrator

☐ s3\_access

Create New Role

### Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name

Maximum 64 characters. Use alphanumeric and '+', '@', '-' characters

### Select Role Type

#### AWS Service Roles

##### Amazon EC2

Allows EC2 instances to call AWS services on your behalf.

Select



ReadOnlyAccess

0

2015-02-06 13:39 EDT

2016-05-12 17:16 EDT

## Review

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

Role Name	readonly	<a href="#">Edit Role Name</a>
Role ARN	arn:aws:iam::072955634019:role/readonly	
Trusted Entities	The identity provider(s) ec2.amazonaws.com	
Policies	arn:aws:iam::aws:policy/IAMReadOnlyAccess	<a href="#">Change Policies</a>

Cancel

Previous

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)

## Create Instance

To start using Amazon EC2 you will want

[Launch Instance](#)

### 2) Choose AMI: select “aws\_neo4jv01”

**Community AMIs**  
**Operating system**

- ☐ Amazon Linux
- ☐ Cent OS
- ☐ Debian
- ☐ Fedora
- ☐ Gentoo

Graph for AWS environment connection

Root device type: ebs    Virtualization type: hvm

64-bit

 **aws\_neo4j\_v01** - ami-ec6b8281

Create neo4j graph for EC2 relations among themselves and the SGs IPs

Root device type: ebs    Virtualization type: hvm

64-bit

[Select](#)

### 3) Instance type(Micro is ok)

<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	1
-------------------------------------	-----------------	--------------------------------	---	---	---

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

Number of instances  [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)

Auto-assign Public IP

IAM role ☒ None administrator ☒ readonly ☐ s3\_access [Create new IAM role](#)

Shutdown behavior

Termination protection ☐ Protect against accidental termination

### 5) Volume Type(magnetic is ok)

Root	/dev/xvda	snap-241dccc7	8	Magnetic	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted
<a href="#">Add New Volume</a>								

### 6) Better to tag the instance

Key (127 characters maximum)	Value (255 characters maximum)
Name	NEO4J
<a href="#">Create Tag</a> (Up to 10 tags maximum)	

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

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom IP Anywhere 50.176.19.102/32
HTTP	TCP	80	My IP 50.176.19.102/32

Add Rule

## 8) Continue with magnetic

Make sure that you have selected the correct volume for this instance.

☒ Continue with Magnetic as the boot volume for this instance.

Free tier eligible customers can get up to 30GB of General Purpose (SSD) storage.

☐ Don't show again

Next

## 9) Choose your keys

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

☒ I acknowledge that I have access to the selected private key file (guru-kp.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

## C) Check the instance

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
NEO4J	i-000bc37b8ac42287d	t2.micro	us-east-1a	running	Initializing	None	

Instance: **i-000bc37b8ac42287d (NEO4J)** Public IP: 54.88.252.108

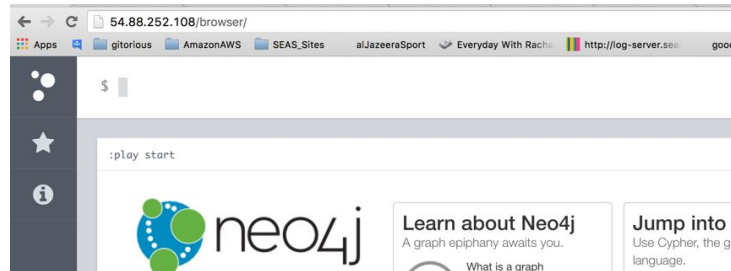
Description Status Checks Monitoring Tags

Instance ID	i-000bc37b8ac42287d	Public DNS	-
Instance state	running	Public IP	54.88.252.108

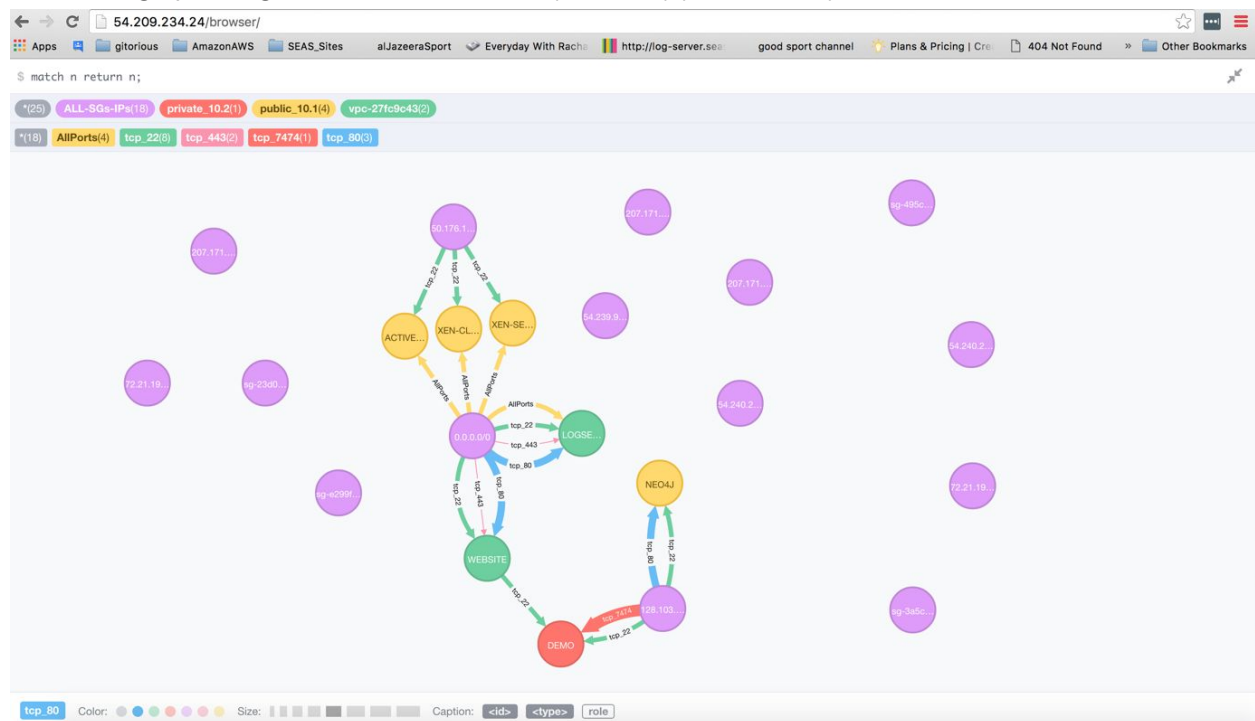
NEO4J URL:

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.