INSTALL GRAPH DATABASE NEO4J (for validation purpose only)

Currently only on MacOS

ADSynth generates Active Directory attack graphs and export them into the format of JSON. These JSON files can be directly imported in any algorithms.

Neo4J is a graph database, providing a wide range of queries for analyzing the attack graphs. However, due to the latency in Neo4J data transaction, we only take advantages of Neo4J to run the experiments. ADSynth utilizes its own local graph database for the attack graph generation process.

We provide the instructions to install Neo4J.

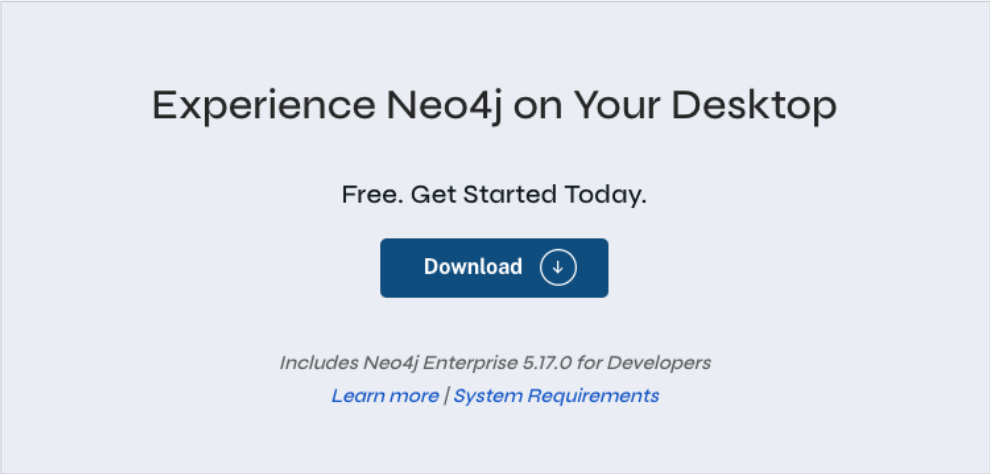
I. Installation

1. Oracle Java 17 (10 mins)

- The instruction to install Java 17 can be found here: https://docs.oracle.com/en/java/javase/21/install/installation-jdk-macos.html#GUID-F575EB4A-70D3-4AB4-A20E-DBE95171AB5F
- Please read the section *JDK Installation Instruction Notation for macOS* and then follow steps in section *Installing the JDK on macOS* to install Java.

2. Neo4J Desktop installation on MacOS (10 mins)

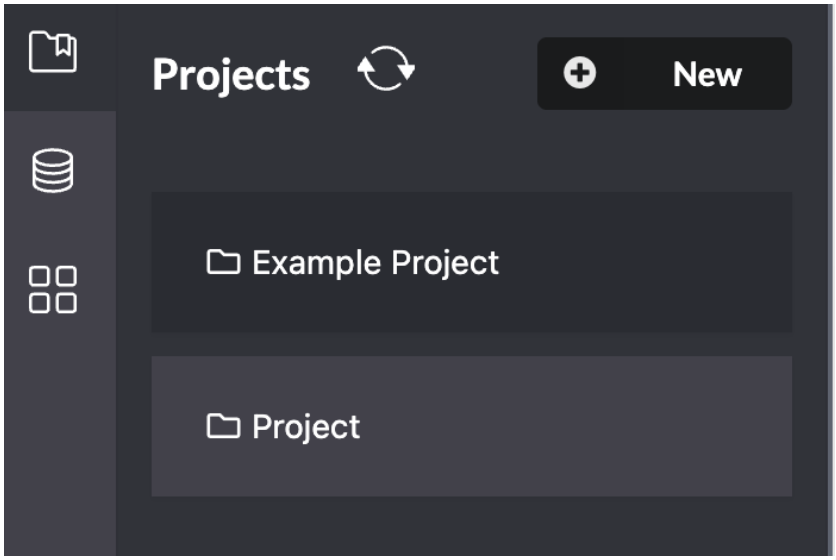
- Head to the Neo4J web page



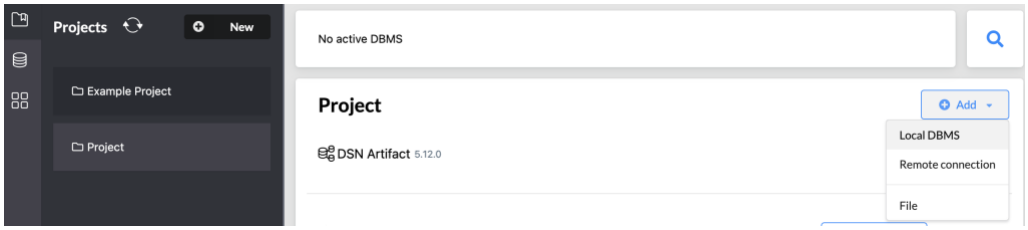
- Click on the button Download. You will be asked to provide some basic information. After that, the package wil be downloaded and you will be directed to the page containing an Activation key and an installation video. Please follow that.

3. Setup Neo4J

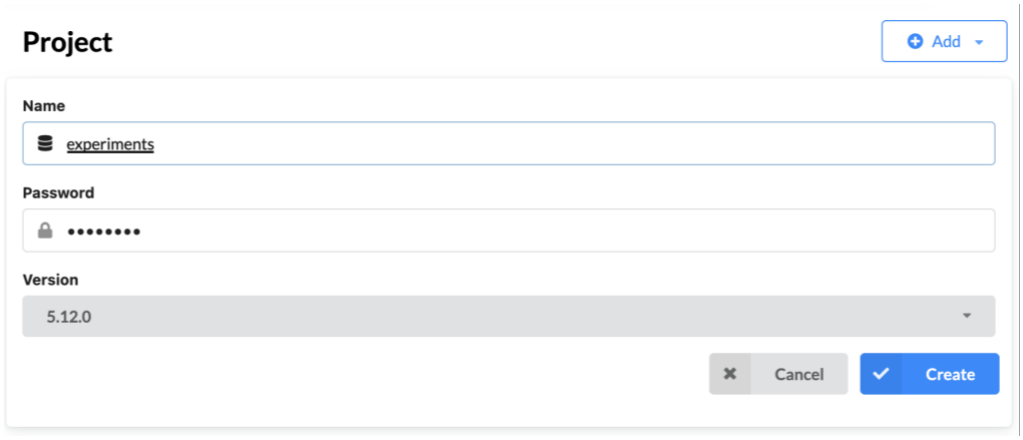
- Upon successful installation, please open Neo4J.
- On the top left corner, create a new project by clicking on the New button



- In the newly created project, on the top right corner, click the button Add and choose *Local DBMS* to create an environment for our experiment.



- Subsequently, type in the name and the password for the environment, then click Create. For simplicity, please set the user name to *neo4j* and password to *password*.



- After a few seconds, the environment will be created.

4. Installing required packages

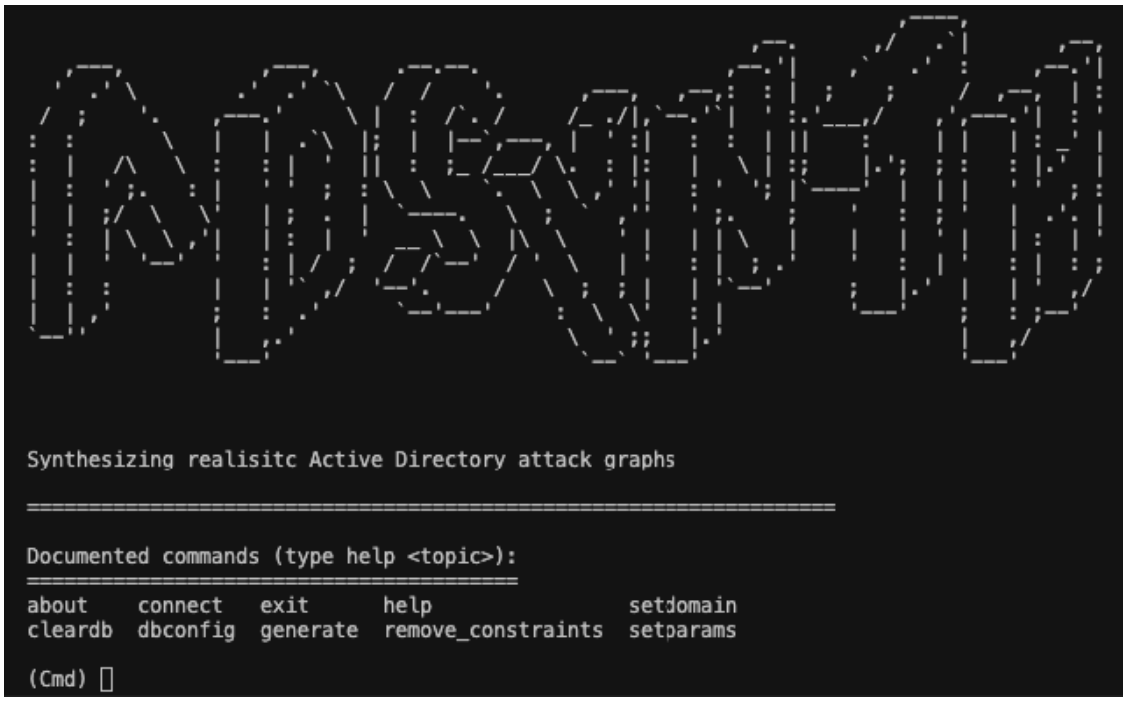
- Install neo4j-driver: *pip install neo4j* or *pip3 install neo4j*
- Install tabulate: *pip install tabulate* or *pip3 install tabulate*

5. **Starting Neo4J**

   To start Neo4J, click button Start next to the environment's name. Starting Neo4J is the first step before running ADSynth.

II. Running ADSynth

- In VSCode, head to the folder of the tool ADSynth.
- In the terminal, execute the below command to run ADSynth
  PYTHONPATH="/Users/Downloads/ADSynth/adsynth" python3 -m adsynth
  Replace the path in PYTHONPATH with your own path to the folder ADSynth. The *adsynth* (lowercase) is the main module



- **Step 1:** *dbconfig* - set up connection with Neo4J (required community preferences, though not related to the attack graph generation of ADSynth). For *level of security,* please leave it by default – Customized (1).
- **Step 2:** *setparams* – set up parameters in AD systems, such as numbers of users, computers, level of misconfigurations. A detailed list of descriptions for all parameters can be found in the attached Excel file.

  The parameter file is a JSON file. For the parameters we used to conduct experiments, we included them in JSON files in folder *experiment_params*. For each experiment, please copy and paste **the full path** of the JSON file, as shown below.

```
(Cmd) setparams
Parameters JSON file [DEFAULT] /Users/Downloads/ADSynth/adsynth/experiment_params/secure_5k.json
```

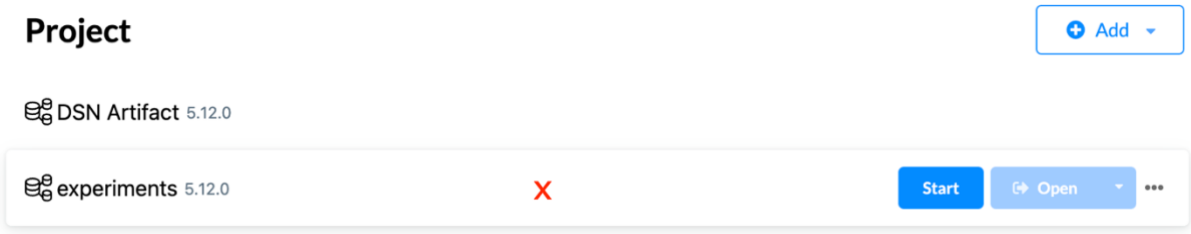
- **Step 3:** *generate* – the generation process is started. The generated attack graph is in the JSON format and can be found in folder *generated_datasets*. The name of the JSON file is *Year-Month-Day_Hour-Minute-Second-Microseconds.json*

III. Uploading JSON files to Neo4J

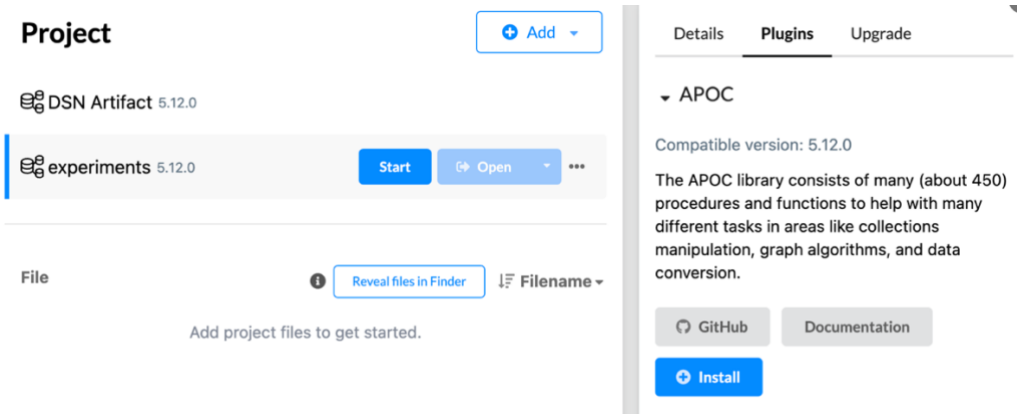
The generated JSON files containing ADSynth attack graphs can be directly used in AD algorithms. If you want to analyze the graphs using Neo4J, please follow the instructions.

a) Plugins installation

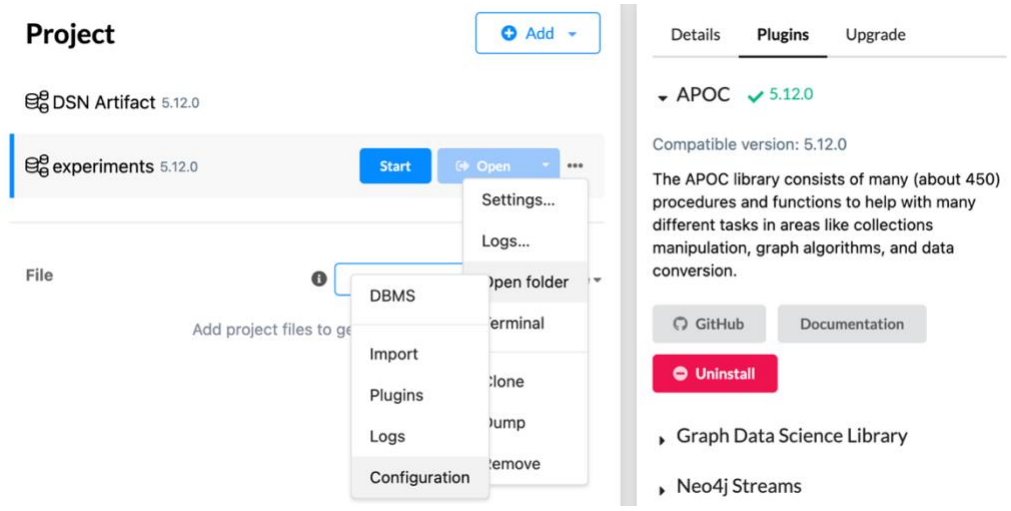
- Hover your mouse over your environment, click on the white space (at the X marker in the snapshot)



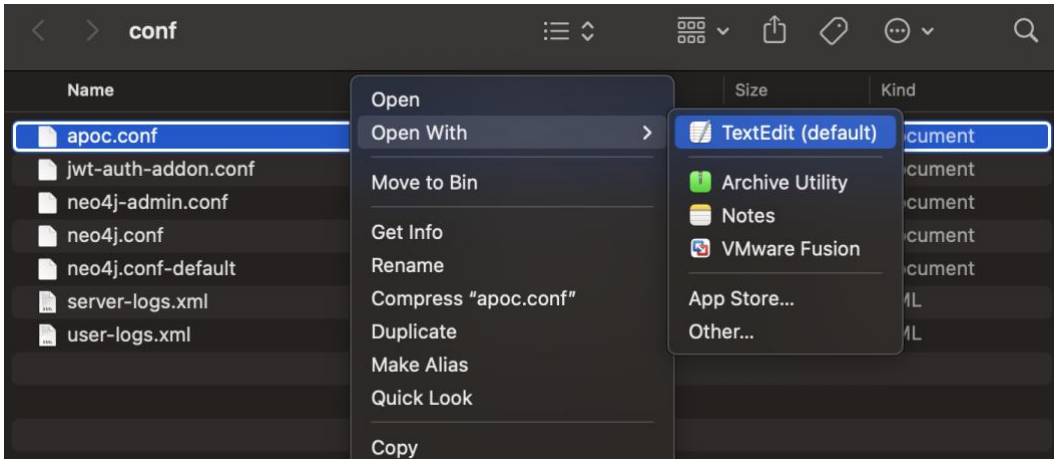
- A bar will appear on the right of the screen, please choose tab *Plugins, then APOC*. Click Install to install APOC. This is the library we used to run experiments.



- To complete the setup for library APOC, hover your mouse over the 3 dot button, choose Open folder > Configuration



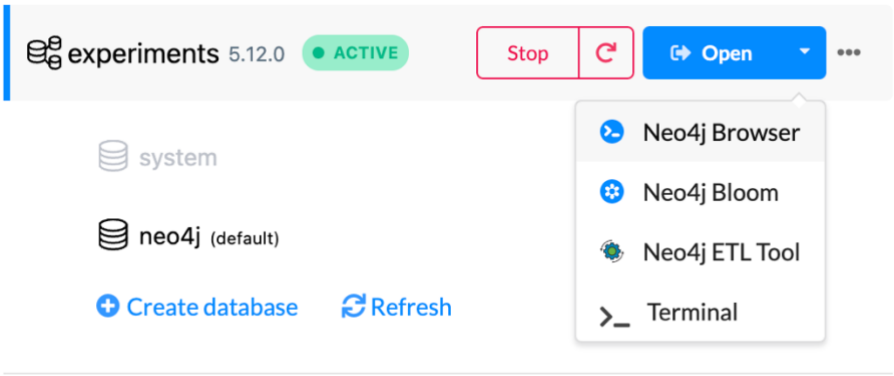
- A window will be opened. Please find a file called *apoc.conf*. If not found, please create a file with the same name *apoc.conf*. Open the file using TextEdit



Within the *apoc.conf*, add these two lines:
apoc.import.file.enabled=true
apoc.import.file.use_neo4j_config=false
Upon saving the file close the window, and the installation for APOC is completed.

b) Uploading JSON to Neo4J

Step 1: Open Neo4J browser as shown in the figure



Step 2: Importing the data into Neo4J

CALL apoc.import.json("/Users/Downloads/ADSynth/DB_STORAGE.json")

Replace the **full path** to the JSON file you want to test. The generated attack graphs (JSON files) are located in the folder *generated_datasets* above. Please check the name of the dataset carefully before conducting any experiment.