Nightfall Truffle Box¶

The easiest way to get started onNightfall .

Supported hardware & prerequisites¶

Mac and Linux machines with at least 16GB of memory and 10GB of disk space are supported.

Nightfall requires the following software to run:

- Docker
- Launch Docker Desktop (on Mac, it is on the menu bar) and set memory to 8GB with 4GB of swap space (minimum - 12GB memory is better) or 16GB of memory with 512MB of swap.The default values for Docker Desktop will NOT work. No, they really won't
- .
- Node
- (tested with 10.15.3) with npm and node-gyp
- If running macOS, install Xcode then runxcode-select —install
- to install command line tools.
- Note: Currently will not work with node v12. To check the node version, runnode --version
- . If using mac/brew, then you may need to runbrew install node@10
- andbrew link --overwrite node@10 --force
- Python
- Be sure npm is setup to use v2.7 of python, not python3. To check the python version, runpython --version
- You may need to runnpm config set python /usr/bin/python2.7
- (or wherever your python 2 location is)

Installation¶

First ensure you are in a new and empty directory.

1. Run theunbox
2. command vianpx
3. and skip to step 3. This will install all necessary dependencies.
4. npx
5. truffle
6. unbox
7. nightfall
8. Alternatively, you can install Truffle globally and run theunbox
9. command.
10. npm
11. install
12. -
13. g
14. truffle
15. truffle
16. unbox
17. nightfall
18. Start Docker.
19. In the root project directory, we generate the keys and constraint files for ourZero Knowledge Proofs
20. . This is about 7GB and depends on randomness for security.This step can take a while, depending on your hardware (1-3 hours)
21. . Before you begin, check once more you have provisioned enough memory for Docker.
22. npm
23. run
24. setup
25. Alternatively, you can generate specific verification keys and constraint files one at time using a prompt.
26. npm
27. run
28. setup
29. -
30. prompt
31. Now, run the development console.
32. truffle
33. develop
34. Compile and migrate the smart contracts. Note inside the development console we don't preface commands withtruffle
35. .

36. compile
37. migrate
38. Execute the script provided for registering Zero Knowledge Proof verification keys on-chain. Note inside the development console we don't preface commands withtruffle
39. .
40. exec
41. scripts
42. /
43. registerVks
44. .
45. js
46. Truffle can run tests written in Solidity or JavaScript against your smart contracts. Note the command varies slightly if you're in or outside of the development console.
47. // inside the development console.
48. test
49. // outside the development console..
50. truffle
51. test

FAQ¶

- How do I use this with Ganache-CLI?
- It's as easy as modifying the config file
- .
- Where can I find more documentation?
- This box is a marriage ofTruffle
- ,Nightfall
- , andZoKrates
- . Any of them would be a great place to start!

Acknowledgements¶

This software usesZoKrates which islicensed underLGPL3 .