enclaive/nginx-sgx ☆

By **enclaive** • Updated 14 days ago

SGX-ready Enclaive Docker Image for Nginx

Container

NGINX-SGX: SGX-ready NGINX open source server

packed by enclaive

#intelsgx # confidentialcompute #dont-trust-a-cloud
Contribute · Report Bug · Request Feature

What is NGINX and SGX?

> NGINX Open Source is a web server that can be also used as a reverse proxy, load balancer, and HTTP cache. Recommended for high-demanding sites due to its ability to provide faster content.

Overview of NGINX

> Intel Security Guard Extension (SGX) delivers advanced hardware and RAM security encryption features, so called enclaves, in order to isolate code and data that are specific to each application. When data and application code run in an enclave

additional security, privacy and trust guarantees are given, making the container an ideal choice for (untrusted) cloud environments.

Overview of Intel SGX

Application code executing within an Intel SGX enclave:

- Remains protected even when the BIOS, VMM, OS, and drivers are compromised, implying that an attacker with full execution control over the platform can be kept at bay
- Benefits from memory protections that thwart memory bus snooping, memory tampering and “cold boot” attacks on images retained in RAM
- At no moment in time data, program code and protocol messages are leaked or de-anonymized
- Reduces the trusted computing base of its parent application to the smallest possible footprint

Why use NGINX-SGX (instead of "vanilla" NGINX) images?

Following benefits come for free with NGINX-SGX :

- "Small step for a dev, giant leap for a zero-trust infrastructure"
- All business benefits from the migration to a (public) cloud without sacraficing on-premise infrastructure trust
- Hardened security against kernel-space exploits, malicious and accidental privilege insider attacks, UEFI firmware exploits and other "root" attacks using the corruption of the application to infiltrate your network and system
- Run on any hosting environment irrespectivably of geo-location and comply with privacy export regulation, such as Schrem-II
- GDPR/CCPA compliant processing ("data in use") of user data in the cloud as data is anonymized thanks to the enclave

TL;DR

```
curl -sSL https://raw.githubusercontent.com/enclaive/enclaive-docker-nginx-sgx/main/docker-c
docker-compose up -d
```

Warning: This quick setup is only intended for development environments. You are encouraged to change the insecure default credentials and check out the available configuration options in the build section for a more secure deployment.

How to deploy NGINX-SGX in a zero-trust cloud?

The following cloud infrastructures are SGX-ready out of the box

- Microsoft Azure Confidential Cloud
- OVH Cloud
- Alibaba Cloud

Confidential compute is a fast growing space. Cloud providers continiously add confidential compute capabilities to their portfolio. Please contact us if the infrastructure provider of your preferred choice is missing.

Getting started

Platform requirements

Check for *Intel Security Guard Extension (SGX)* presence by running the following

```
grep sgx /proc/cpuinfo
```

Alternatively have a thorough look at Intel's processor list. (We remark that macbooks with CPUs transitioned to Intel are unlikely supported. If you find a configuration, please contact us know.)

Note that in addition to SGX the hardware module must support FSGSBASE. FSGSBASE is an architecture extension that allows applications to directly write to the FS and GS segment registers. This allows fast switching to different threads in user applications, as well as providing an additional address register for application use. If your kernel version is 5.9 or higher, then the FSGSBASE feature is already supported and you can skip this step.

There are several options to proceed

- If: No SGX-ready hardware
  Azure Confidential Compute cloud offers VMs with SGX support. Prices are fair and have been recently reduced to support the developer community. First-time users get $200 USD free credit. Other cloud provider like OVH or Alibaba cloud have similar offerings.
- Elif: Virtualization
  Ubuntu 21.04 (Kernel 5.11) provides the driver off-the-shelf. Read the release. Go to download page.
- Elif: Kernel 5.9 or higher
  Install the DCAP drivers from the Intel SGX repo

```
sudo apt update
sudo apt -y install dkms
wget https://download.01.org/intel-sgx/sgx-linux/2.13.3/linux/distro/ubuntu20.04-serve
chmod +x sgx_linux_x64_driver.bin
sudo ./sgx_linux_x64_driver.bin

sudo apt -y install clang-10 libssl-dev gdb libsgx-enclave-common libsgx-quote-ex libp
```

- Else: Kernel older than version 5.9
  Upgrade to Kernel 5.11 or higher. Follow the instructions here.

Software requirements

Install the docker engine

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io
sudo usermod -aG docker $USER    # manage docker as non-root user (obsolete as of docker 19
```

Use `docker run hello-world` to check if you can run docker (without sudo).

Get this image

The recommended way to get the enclaive NGINX-SGX Open Source Docker Image is to pull the prebuilt image from the Docker Hub Registry.

```
docker pull enclaive/nginx-sgx:latest
```

To use a specific version, you can pull a versioned tag. You can view the list of available versions in the Docker Hub Registry.

```
docker pull enclaive/nginx-sgx:[TAG]
```

Build the image

If you wish, you can also build the image yourself.

```
docker build -t enclaive/nginx-sgx:latest 'https://github.com/enclaive/enclaive-docker-nginx
```

Hosting a static website

This NGINX-SGX Open Source repo exposes the folder at `/html`. Content mounted from this folder is served by the default catch-all server block.

Configure network ports

Edit `conf/nginx.conf` to eanble the ports the server should listen to. Default ports are 80 and 443 for non-secured and TLS-secured communication, respectively.

```
listen 80;
listen 443 ssl;
```

Accessing your server from the host

To access your web server from your host machine you can ask Docker to map a random port on your host to ports `80` and `443` exposed in the container.

```
docker run --name nginx-sgx -p 80:80 -p 443:443 \
    --device=/dev/sgx_enclave \
    -v /var/run/aesmd/aesm.socket:/var/run/aesmd/aesm.socket \
    enclaive/nginx-sgx:latest
```

Access your web server in the browser by navigating to `https://localhost` and `http://localhost` for a SSL/TLS secured and non-secure community, respectively.

Run `docker port` to determine the random ports Docker assigned.

```
docker port nginx-sgx
80/tcp -> 0.0.0.0:32769
```

You can also manually specify the ports you want forwarded from your host to the container.

```
docker run -p 9000:80 -p9443:443 \
    --device=/dev/sgx_enclave    \
    -v /var/run/aesmd/aesm.socket:/var/run/aesmd/aesm.socket \
     enclaive/nginx-sgx:latest
```

Access your web server in the browser by navigating to `https://localhost:9443` (SSL/TLS) and `http://localhost:9443` (non-secured).

Contributing

Contributions are what make the open source community such an amazing place to learn, inspire, and create. Any contributions you make are **greatly appreciated**. If you have a suggestion that would make this better, please fork the repo and create a pull request. You can also simply open an issue with the tag "enhancement".

1. Fork the Project
2. Create your Feature Branch (`git checkout -b feature/AmazingFeature`)
3. Commit your Changes (`git commit -m 'Add some AmazingFeature'`)
4. Push to the Branch (`git push origin feature/AmazingFeature`)
5. Open a Pull Request

Support

Don't forget to give the project a star! Spread the word on social media! Thanks again!

License

Distributed under the Apache License 2.0 License. See `LICENSE` for more information.

Contact

enclaive.io - @enclaive_io - contact@enclaive.io - https://enclaive.io

Acknowledgments

This project greatly celebrates all contributions from the gramine team. Special shout out to Dmitrii Kuvaiskii from Intel for his support.

- Gramine Project
- Intel SGX
- NGINX

Trademarks

This software listing is packaged by enclaive.io. The respective trademarks mentioned in the offering are owned by the respective companies, and use of them does not imply any affiliation or endorsement.

Docker Pull Command

```
docker pull enclaive/nginx-sgx
```

Why Docker
Overview
What is a Container

Products
Product Overview

Product Offerings
Docker Desktop
Docker Hub

Features
Container Runtime
Developer Tools
Docker App
Kubernetes

Developers
Getting Started
Play with Docker
Community
Open Source
Docs
Hub Release Notes

Company
About Us
Resources
Blog
Customers
Partners
Newsroom
Events and Webir
Careers
Contact Us