How to Deploy or Integrate a Service with Tor Onion on Elestio

To make your services accessible over Tor, you can configure a Tor service within your service Docker Compose setup. This will allow your service to function as an onion site, providing enhanced privacy and limiting access to Tor-compatible browsers. Here’s a guide to setting up your service with Tor on Elestio.

Step 1: Set Up Your Service

First, deploy a new service on Elestio or select an existing one you’ve already deployed.

Step 2: Open the Editor

Navigate to the **Tools** tab within your service and open the provided VS Code editor.

Step 3: Stop the Current Container

To stop the current container, run the following command:

```
docker-compose down -v;
```

Step 4: Configure Docker Compose with Tor

You’ll need to add a Tor service to your Docker Compose file. Below is an example Docker Compose configuration to run a nextcloud server accessible through a Tor onion address.

```
version: "3.9"
services:
  app:
    image: elestio/nextcloud:${SOFTWARE_VERSION_TAG}
    restart: always
    # ports:
    #   - 172.17.0.1:22000:80
    volumes:
```

```
      - ./nextcloud:/var/www/html
      - ./apps:/var/www/html/custom_apps
      - ./config:/var/www/html/config
      - ./data:/var/www/html/data
  tor:
    image: jakejarvis/tor:latest
    restart: unless-stopped
    volumes:
      - ./tor-data:/var/lib/tor/
      - ./torrc:/etc/tor/torrc:ro
    depends_on:
      - app
volumes:
  tor-data:
```

> In the Docker Compose example, we used the `jakejarvis/tor` image to demonstrate the setup, but you can substitute it with any other official or custom Tor image that suits your needs. This allows for flexibility in using a Tor configuration that aligns with specific requirements or preferences.

Step 5: Create the `torrc` File

In the root directory of your project, create a file named `torrc`. This file configures Tor to run as a hidden service and specifies the settings for connecting to the web service.

Add the following content to `torrc`:

```
# This folder contains the public and private keys of the hidden
# service, probably provided by the host but can also be generated
# by Tor if it's missing.
HiddenServiceDir /var/lib/tor/hidden_service

# Point the hidden service to a web server (in this case, the web
# server container listening on port 80).
HiddenServicePort 80 app:80

# SOCKS proxy is only used for the container's internal healthcheck.
SocksPort 127.0.0.1:9050
```

Step 6: Start the service.

To start your services, use the following commands:

```
docker-compose up -d;
```

This will bring up both the app and Tor services, allowing Tor to generate the necessary onion address.

Step 7: Obtain Your Onion URL

Once your services are running, Tor will create an onion address for your service. You can find this address by accessing the `hostname` file in the `tor-data/hidden_service` directory. Use the following command to view your onion URL:

```
cat tor-data/hidden_service/hostname
```

This will output an onion address (like `abcdefghijklmno.onion`) that you can use to access your web service in a Tor-compatible browser like Tor Browser or Brave.

Step 8: Update Service URL with Onion URL

If your application has domain or URL settings in its environment variables or configurations, replace the current URL with your Tor onion URL. This ensures that your application will direct users to the onion address.

Optional: Disable Access to the Public Internet

To restrict access exclusively to the Tor network and block regular web traffic, you can disable external access by blocking port 443 in your security firewall settings. This can be configured through the firewall settings within the Security tab of your service, or via your cloud provider's firewall if using a BYOVM (Bring Your Own Virtual Machine).

Summary

With these steps, you've configured your Elestio-deployed service to be accessible through a Tor onion address. This setup allows for private, anonymous access via Tor, enhancing your service's privacy and security.

Revision #5
Created 8 November 2024 09:26:07 by Amit
Updated 8 November 2024 10:25:16 by Amit