Cortex Certifai Installation Instructions

This document provides the system requirements and installation instructions for Cortex Certifai. For details about using Certifai and how it works please visit the Cortex Certifai Training website.

Certifai is configured to scan one or more ML models using an uploaded representative dataset. The scan evaluates the model predictions for robustness, fairness, and explainability by generating counterfactuals using the features and values provided in the dataset.

The scan components are configured and scan results visualizations are displayed in the web application on the client machine. During the scan, the Certifai Host requires access to the ML models' predict functions (service endpoints) hosted on an ML Model Server.

Prerequisites and System Requirements

Client Machine	
Web Browser	Chrome (preferred), Safari, Edge Latest Stable Version Required
Certifai Host Server	
Runtime: Kubernetes	Azure (AKS), AWS (EKS), GCP (GKE), RedHat (OpenShift)
OS	Linux (on server), Linux or MacOS (for personal experimentation)
Transport Protocols	HTTP / HTTPS
Port	5000
CPU	4 Cores
RAM	16GB
Disk Space	500 GB
ML Model Server	
Transport Protocols	HTTP / HTTPS
Port	5000
CPU	4 Cores
RAM	16GB
Disk Space	500 GB

Certifai Installation Instructions

Prerequisites

- **Docker Installation**: Certifai can be installed on any virtual machine instance from a major cloud provider as long as Docker has been installed. (Docker installation instructions)

- **Docker Hub access (for some installations)**: The pre-built docker images you need to install Certifai are served from a private Docker Hub repository. You have been granted “pull” access to this repo, and the credentials have been sent to your registration email.

- **Docker Compose file consisting of two services:** provided along with this document in the .zip file:
    - `certifai` - the Certifai web application and scan components
    - `certifai-model-server` - provides the predict endpoints for the reference models documented in 'Certifai Reference Models.pdf' in this .zip file

Install Certifai from Docker Hub

To install Certifai using images from the private Docker Hub repository, you must first login. Check with your CognitiveScale contact if you have not received a registration email with your credentials. .

1. Log into Docker Hub using the credentials supplied by CognitiveScale. Run the following command and enter the credentials as you are prompted.

   ```
   docker login
   ```

2. Create a directory for certifai and unzip the .zip file into it:

   ```
   mkdir certifai && unzip certifai.zip -d certifai
   ```

3. Change into the certifai directory and list its contents:

   ```
   cd certifai && ls
   ```

   You should see a number of files including the docker compose file (docker-compose.yml).

4. Run

   ```
   docker-compose up
   ```

   The logs from the containers are displayed in the terminal. You should see a line including text like the following that indicates the Certifai web application is running:

```
Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
```

5. Verify that the installation completed by opening the Cortex Certifai application in your browser at: `http://localhost:5000`

Install Certifai from Docker images provided in the .zip file

If you are unable to access Docker Hub and have requested an alternative, the .zip file may contain the images that you require in tar.gz format. To install Certifai, first load the two images into your local Docker instance, and then install using the docker-compose file.

1. Create a directory for certifai and unzip the .zip file into it:

   ```
   mkdir certifai && unzip certifai.zip -d certifai
   ```

2. Change into the certifai directory and list its contents:

   ```
   cd certifai && ls
   ```

   You should see a number of files including the docker compose file (docker-compose.yml).

3. Load the provided images. The file names in the following should match the tar file names from your .zip file:

   ```
   docker load < certifai.tar
   docker load < model_server.tar
   ```

   When each command completes, you should see a message to confirm it has loaded successfully:

   Loaded image: c12esolutions/cortex-certifai-xxx:yyy

4. `Run`

   ```
   docker-compose up
   ```

5. `Verify that the installation completed by opening the Cortex Certifai app in your browser at:  http://localhost:5000`

Configuring Certifai Persistence

By default, the docker-compose file is configured to persist data to the host machine. This means that any changes that you make will persist across restarts of the docker containers. If you do not wish to have data persisted, you can disable the persistent volumes in the docker-compose file.

1. Find the lines starting with “volumes” in the “docker-compose.yml” file in the Certifai package. Comment out those lines.

```
certifai:
  image: c12esolutions/cortex-certifai-xxx:yyy
  ...
  # volumes:
    # - .certifai:/root/.certifai
```

2. Run `docker compose up` command as described previously to start the containers without persistence.

The persisted data is saved in a `.certifai` folder that is located in the same folder as the docker-compose file. Delete this folder if you want to removed the saved data. You can reset its content from the `.certifai` folder in the .zip file, if desired.

Troubleshooting

Certifai runs on port 5000 on your machine by default. If the “docker-compose up” command fails with the error message: `Port allocation failed`, an IT administrator can open the port to resolve this issue. It may be running some other program, or the Certifai user may not have permission to use port 5000.

Additional Resources

Your .zip file also includes the following:

- **Datasets** (.csv files): These dataset files are provided for your convenience. They correspond to the Project use cases in the Certifai application and described in 'Certifai Reference Models.pdf'.

Project Use Case in the Certifai Application	**datasets (.csv files)**
Healthcare: disease prediction	diabetes.csv
Banking: predicting customer churn	customer_churn-prepped.csv
Banking: propensity to buy	bank_marketing-prepped.csv

Finance: income prediction	adult_income-prepped.csv
Banking: loan approval	german_credit-decoded.csv
Insurance: auto insurance claims	auto_insurance_claims_dataset.csv

- **Certifai Installation Instructions (pdf)**: This document provides instructions for installing Certifai for your Proof of Value and a description of the contents of the .zip file.
- **Certifai Reference Models (pdf)**: A document that provides details about each of the prepared projects you experience in the Certifai application.
- **certifai_config folder**: This folder contains a prebuilt Certifai database of the Reference Model use cases, as well as your license key and Certifai configuration files.

NOTE: The Certifai Reference Model GitHub repo is now available. You can obtain additional or updated reference use cases there.