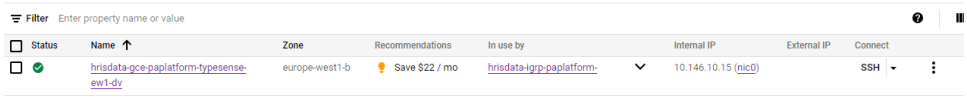
Installation of Typesense server and Security Agents on Typesense VM

Typesense server installation

For people analytics typesense server is required for search engine

following are the steps to install typesense.

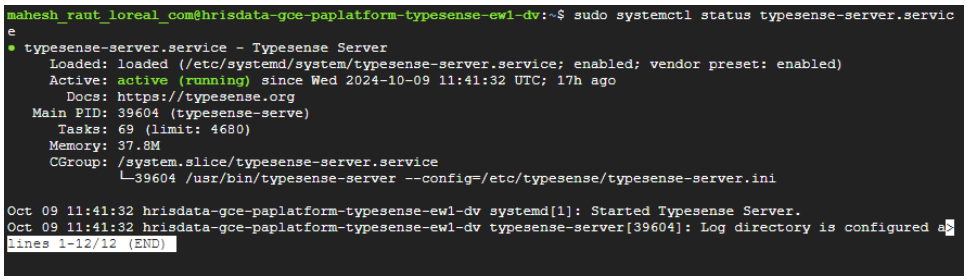
- download the typesense .deb file (typesense-server-0.21.0-amd64.deb) currently we are using 0.21 version (we can not use latest version (26.0) because our PAP code is not support for latest version)
- upload above file to bucket (paplatform-gcs-documents-ew1-<env_name>)
- merge code from STRY0441794_v1 this branch to environment branch
- Trigger the terraform cloud build trigger
- After successful of trigger connect to VM



click on SSH

- Check typesense is installed or not using below command

sudo systemctl status typesense-server.service



Press "q" to exit from status

- Open typesense-server.ini file and copy api-key and close the file
  sudo vi /etc/typesense/typesense-server.ini
- Then change the api-key in below code and run code to create search key

*curl -X POST 'http://localhost:80/keys' *
*-H "X-TYPESENSE-API-KEY: S1l7IDBNZaMSsa6YWUzittaLi9xOiPuqWCDdNK8DnKxc8DPS" *
*-H "Content-Type: application/json" *
-d '{
"description": "Search-only key",
"actions": search",
"collections": ""*
}'

- Copy search key generated from above command (e.g. 1VO8h9BKxl8pMBs6I9dNg1FVkZQjUDfm)
- Close the VM SSH window

Steps to update the Backend env secret

- Activate cloud shell in GCP
- Copy the latest version of backend-env secret to dev-backend-env.txt file using following command

gcloud beta secrets versions access latest --secret=backend-env --project=itg-paplatform-gbl-ww-dv |base64 -d > backend-env.txt

- Open the backend-env.txt and update the data for TYPESENSE_HOST, TYPESENSE_ADMIN_API_KEY, TYPESENSE_SEARCH_API_KEY and save the file
- Create the new version of backend-env secret using the below command

cat backend-env.txt | base64 -w 0 | gcloud beta secrets versions add backend-env --project=itg-paplatform-gbl-ww-dv --data-file=-

- Execute the backend deployment cloud build trigger to update the new env changes from secret
- At the end run scheduler to recreate the typesense index (paplatform-skd-recreate-index-ew1-dv)

Security agents installation steps

- **Uploading installation packages to GCS bucket**

  Below is the list of files to be uploaded on bucket (paplatform-gcs-documents-ew1-<env_name>):

  - (1) security_agent_setup_main_202403291.tar.gz (linux/security_agent_setup_main_202403291.tar.gz)
  - (2) taniumclient_7.4.10.1067-ubuntu22_amd64.deb(catelis_setup (2).tar.gz)
  - (3) libnl-3-200_3.4.0-1ubuntu0.1_amd64.deb(wget http://europe-west1.gce.archive.ubuntu.com/ubuntu/pool/main/libn/libnl3/libnl-3-200_3.4.0-1ubuntu0.1_amd64.deb)
  - (4) libnl-genl-3-200_3.4.0-1ubuntu0.1_amd64.deb(wget http://europe-west1.gce.archive.ubuntu.com/ubuntu/pool/main/libn/libnl3/libnl-genl-3-200_3.4.0-1ubuntu0.1_amd64.deb)
  - (5) catelis_setup.tar.gz(catelis_setup (2).tar.gz)
- After the upload,
- merge code from STRY0463163 this branch to environment branch
- Trigger the terraform cloud build trigger

After installation Below are the commands to check all security agents are running or not:

- Typesense:- sudo systemctl status typesense-server.service
- Tanium:- sudo systemctl status taniumclient.service
- Crowdstrike:- sudo systemctl status falcon-sensor.service
- Rapid7:- sudo systemctl status ir_agent.service