

# Project's screenshots

## – Cloud run –

Services

Déployer un conteneur

Connecter un dépôt

Écrire une fonction

Actualiser

Un service expose un point de terminaison unique et adapte automatiquement l'infrastructure sous-jacente pour gérer les requêtes entrantes. Déployez une image de conteneur, du code source ou une fonction pour créer un service.

Filtrer

Filtrer les services

<input type="checkbox"/>	<input checked="" type="radio"/>	Nom ↑	Type de déploiement	Requêtes/s	Région	Authentification	Ingress	Dernier déploiement	Déployé par
<input type="checkbox"/>	<input checked="" type="radio"/>	<a href="#">dfir-dashboard</a>	Source	0	us-central1	Accès public	Toutes	il y a 10 jours	Selimharzallah04@gmail.co
<input type="checkbox"/>	<input checked="" type="radio"/>	<a href="#">dfir-ingest</a>	Fonction	0	us-central1	Accès public	Toutes	il y a 10 jours	Fonctions Cloud Run
<input type="checkbox"/>	<input checked="" type="radio"/>	<a href="#">volatility-engine</a>	Source	0	us-central1	Accès public	Toutes	il y a 10 jours	Selimharzallah04@gmail.co

## – IAM and administration –

IAM

Apprendre

Autoriser

Refuser

Historique des recommandations

Afficher par compte principal

Afficher par rôle

Accorder l'accès

Supprimer l'accès

Filtrer

Saisissez le nom ou la valeur de la propriété

<input type="checkbox"/>	Type	Compte principal ↑	Nom	Rôle	Insights sur la sécurité
<input type="checkbox"/>		1003013388283-compute@developer.gserviceaccount.com	Default compute service account	Éditeur	
<input type="checkbox"/>		cf-dfir@digital-forensic-toolkit.iam.gserviceaccount.com	DFIR Cloud Functions SA	Accesreur de secrets Secret Manager Destinataire des événements Eventarc Lecteur d'objets Storage Utilisateur Cloud Datastore	
<input type="checkbox"/>		digital-forensic-toolkit@appspot.gserviceaccount.com	App Engine default service account	Éditeur	
<input type="checkbox"/>		erik.fredericks@gmail.com		Propriétaire	
<input type="checkbox"/>		Selimharzallah04@gmail.com	Selim	Propriétaire	12317 autorisations en excès/12353

## – Cloud storage - Buckets –

Buckets

Créer

Actualiser

Accéder au chemin

Apprendre

Filtrer

Filtrer les buckets

<input type="checkbox"/>	Nom ↑	Création	Type d'emplacement	Zone	Classe de stockage par défaut	Dernière modification	Accès public
<input type="checkbox"/>	<a href="#">dfir-evidence-digital-forensic-toolkit</a>	11 nov. 2025, 16:45:05	Region	us-central1	Standard	27 nov. 2025, 23:18:58	Soumise à des l
<input type="checkbox"/>	<a href="#">digital-forensic-toolkit_cloudbuild</a>	15 nov. 2025, 12:27:13	Multi-region	us	Standard	15 nov. 2025, 12:27:13	Soumise à des l
<input type="checkbox"/>	<a href="#">gcf-v2-sources-1003013388283-us-c...</a>	11 nov. 2025, 16:52:35	Region	us-central1	Standard	11 nov. 2025, 16:52:35	Non public
<input type="checkbox"/>	<a href="#">gcf-v2-uploads-1003013388283.us-c...</a>	11 nov. 2025, 16:52:33	Region	us-central1	Standard	11 nov. 2025, 16:52:33	Non public
<input type="checkbox"/>	<a href="#">run-sources-digital-forensic-toolkit-us...</a>	13 nov. 2025, 22:50:15	Region	us-central1	Standard	13 nov. 2025, 22:50:15	Non public

– Firestore –

Toutes les bases de données > Base de données (default)

Vue Panneau Générateur de requêtes

/ > evidence > SBSZGxnx7TEQd5TmEBH1

(default)	evidence	SBSZGxnx7TEQd5TmEBH1
+ Commencer une collection	+ Ajouter un document	+ Commencer une collection
evidence >	13ZmyJEKNAJ8zm3HAsE4 16iu9jB4CT9YMGvVLFJ 2cBJuL6pCVi09ltgX4Ki 2tJlmSyOPmDYGEFTIQHc 3zMsy9pSb4ucRMNh8FNG 4ERwTEC6iFo3MhOwpG5r 4ela7emWgfO1vdcEWLNb 5BSZGxnx7TEQd5TmEBH1 >	+ Ajouter un champ  bucket: "dfir-evidence-digital-forensic-toolkit" created_at: 24 novembre 2025 à 10:59:55,018 UTC-5 exif: null md5: null mime_type: "application/octet-stream" object_name: "uploads/0zapftis.vmem" processed_at: 24 novembre 2025 à 11:00:24,635 UTC-5 sha256: null size_bytes: 268435456 volatility netscan_exit: 1 netscan_stderr: "Progress: 0.00 Scanning FileLayer usi... netscan_stdout: "Volatility 3 Framework 2.26.2 Unsatis...

– After uploading an evidence –

DE	HEURE	RÉSUMÉ
>	2025-12-09 17:41:27.085	[2025-12-09 22:41:27 +0000] [1] [INFO] Starting unicorn 23.0.0
>	2025-12-09 17:41:27.086	[2025-12-09 22:41:27 +0000] [1] [INFO] Listening at: http://0.0.0.0:8080 (1)
>	2025-12-09 17:41:27.086	[2025-12-09 22:41:27 +0000] [1] [INFO] Using worker: gthread
>	2025-12-09 17:41:27.090	Default STARTUP TCP probe succeeded after 1 attempt for container "volatility-engine-1" on port 8080.
>	2025-12-09 17:41:27.107	[2025-12-09 22:41:27 +0000] [2] [INFO] Booting worker with pid: 2
>	2025-12-09 17:41:28.408	Default STARTUP TCP probe succeeded after 1 attempt for container "worker" on port 8080.
>	2025-12-09 17:41:28.415	Default STARTUP TCP probe succeeded after 1 attempt for container "worker" on port 8080.
>	2025-12-09 17:41:28.444	uploads/dump_memory_v6.raw
>	2025-12-09 17:41:28.470	uploads/dump_memory_v6.raw
>	2025-12-09 17:41:41.610	POST 405 306 B 47 ms APIs-Google;... https://volatility-engine-33m4z5lzxq-uc.a.run.app/?__GCP_CloudEventsMode=G...
>	2025-12-09 17:41:54.604	POST 405 306 B 4 ms APIs-Google;... https://volatility-engine-33m4z5lzxq-uc.a.run.app/?__GCP_CloudEventsMode=GC...
>	2025-12-09 17:42:12.662	POST 405 306 B 764 ms APIs-Google;... https://volatility-engine-33m4z5lzxq-uc.a.run.app/?__GCP_CloudEventsMode=...
>	2025-12-09 17:42:12.666	Starting new instance. Reason: AUTOSCALING - Instance started due to configured scaling factors (e.g. CPU utilization, request ...
>	2025-12-09 17:42:13.183	[2025-12-09 22:42:13 +0000] [1] [INFO] Starting unicorn 23.0.0
>	2025-12-09 17:42:13.184	[2025-12-09 22:42:13 +0000] [1] [INFO] Listening at: http://0.0.0.0:8080 (1)
>	2025-12-09 17:42:13.184	[2025-12-09 22:42:13 +0000] [1] [INFO] Using worker: gthread
>	2025-12-09 17:42:13.185	Default STARTUP TCP probe succeeded after 1 attempt for container "volatility-engine-1" on port 8080.
>	2025-12-09 17:42:13.203	[2025-12-09 22:42:13 +0000] [2] [INFO] Booting worker with pid: 2
>	2025-12-09 17:42:38.593	POST 405 306 B 4 ms APIs-Google;... https://volatility-engine-33m4z5lzxq-uc.a.run.app/?__GCP_CloudEventsMode=GC...
>	2025-12-09 17:43:04.613	POST 405 306 B 8 ms APIs-Google;... https://volatility-engine-33m4z5lzxq-uc.a.run.app/?__GCP_CloudEventsMode=GC...
>	2025-12-09 17:43:41.675	POST 405 306 B 19 ms APIs-Google;... https://volatility-engine-33m4z5lzxq-uc.a.run.app/?__GCP_CloudEventsMode=G...

Affichage des journaux pour les 5 minutes passé(e)s, du Undefined parameter - DATE au 09/12/2025 17:43. Durée de prolongement: 1 minute Modifier l'heure