Security by design

Comment construire un produit SECURE BY DESIGN?

Security by design

- Thème centraux de la sécurité de l'information

Confidentialité: Ne permettre que l'accès aux données pour lesquelles l'utilisateur est autorisé

Intégrité: S'assurer que les données ne sont pas falsifiées ou altérées par des utilisateurs non autorisés

Disponibilité: S'assurer que les systèmes et les données sont disponibles pour les utilisateurs autorisés quand ils en ont besoin

Security by design

Comment mettre en oeuvre ?

- ❑Minimiser la surface d'attaque
- ❑Établir des valeurs par défaut sécurisées
- ❑Principe du moindre privilège
- ❑Principe de défense en profondeur
- ❑Échouer en toute sécurité
- ❑Ne faites pas confiance aux services
- ❑Séparation des tâches
- ❑Évitez la sécurité par l'obscurité
- ❑Gardez la sécurité simple
- ❑Résoudre les problèmes de sécurité correctement

Security by design

Et concrètement, lorsque l'application est en production:

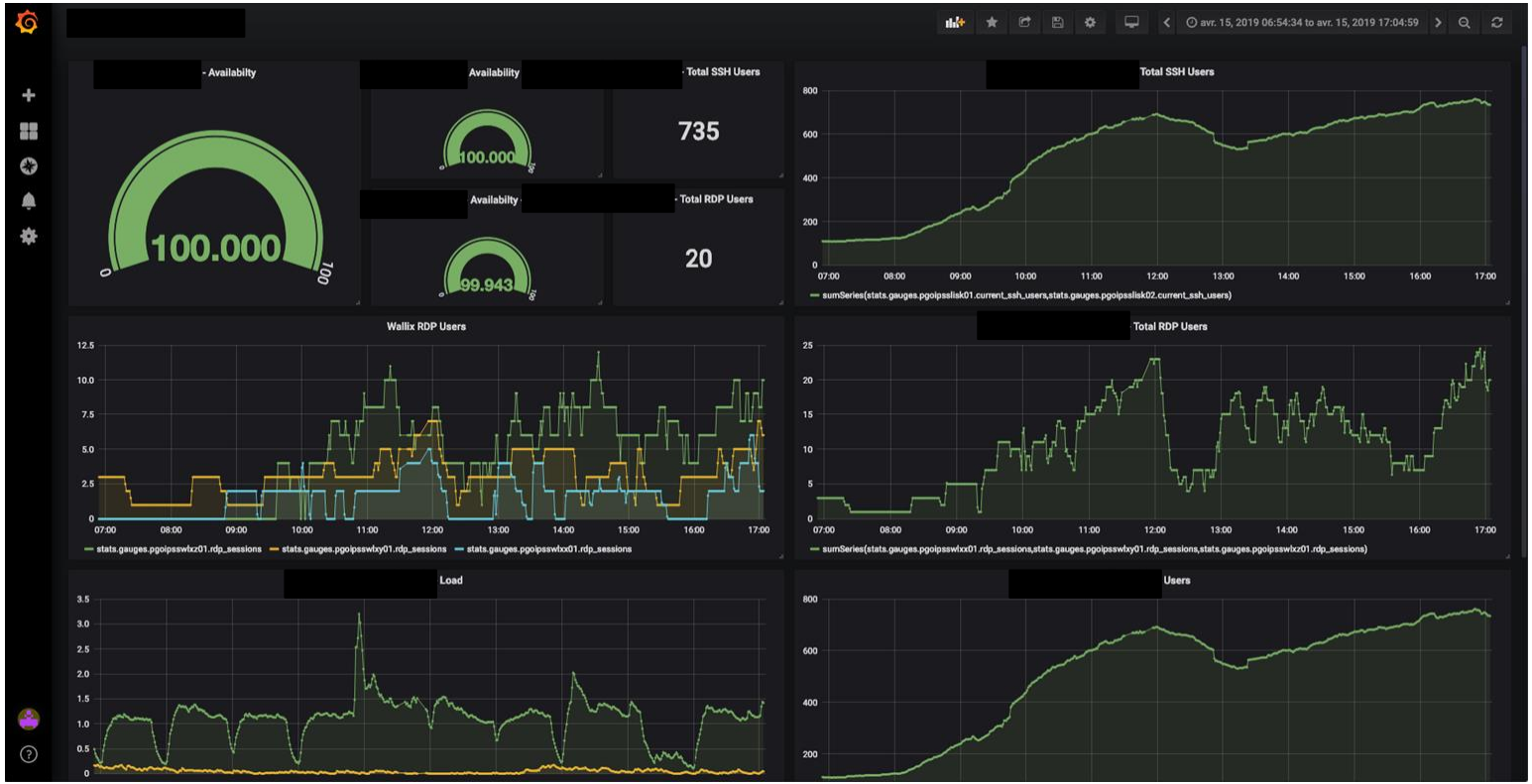
- ❑Utilisez un gestionnaire de mot de passe comme Vault. Il sera utile d'avoir des mots de passe de bonne qualité.
- ❑Mettez à jour votre système d'exploitation et tous les logiciels utilisés.
- ❑Implémentez des sauvegardes et testez-les.
- ❑Testez votre DRP périodiquement.
- ❑Séparez les différents comptes pour chaque utilisation.
- ❑Utilisez un bastion pour accéder au compte administrateur.
- ❑Faites attention aux différents composants que vous trouvez sur internet.

Une démonstration avec une solution de monitoring ?

Security by design - Cas d’usage

- **Notre client avait besoin d'une solution rapide et sécurisée pour surveiller les produits de sécurité.**
- **Capable de superviser des solutions propriétaires implémentées chez le client**
- **Flexible sur les méthodes d’authentification (Contrôles authentifiés RDP et SSH…)**
- **Infrastructure as code pour faciliter la maintenance**
- **Qui fonctionne avec l'infrastructure existante du client**

Un aperçu de l'application

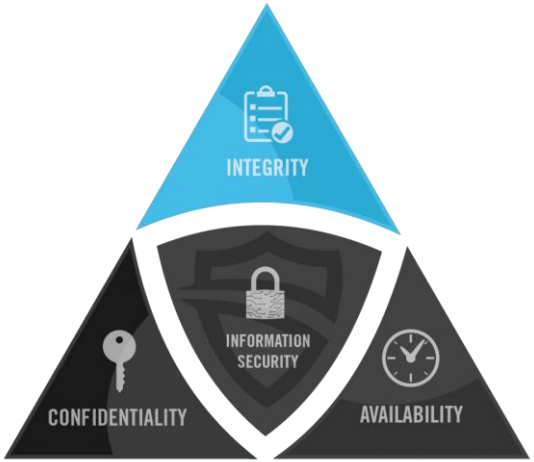


Un aperçu de l’application

L’architecture

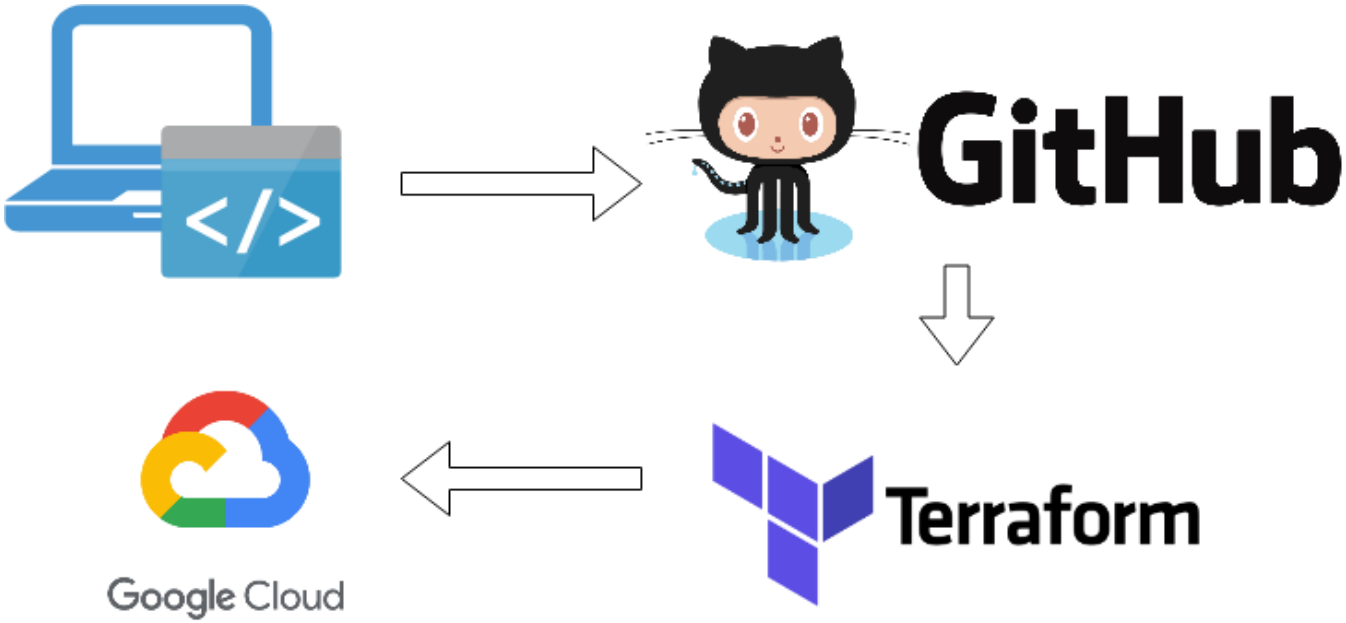
Comment cela fonctionne ?

Security by design - Intégrité

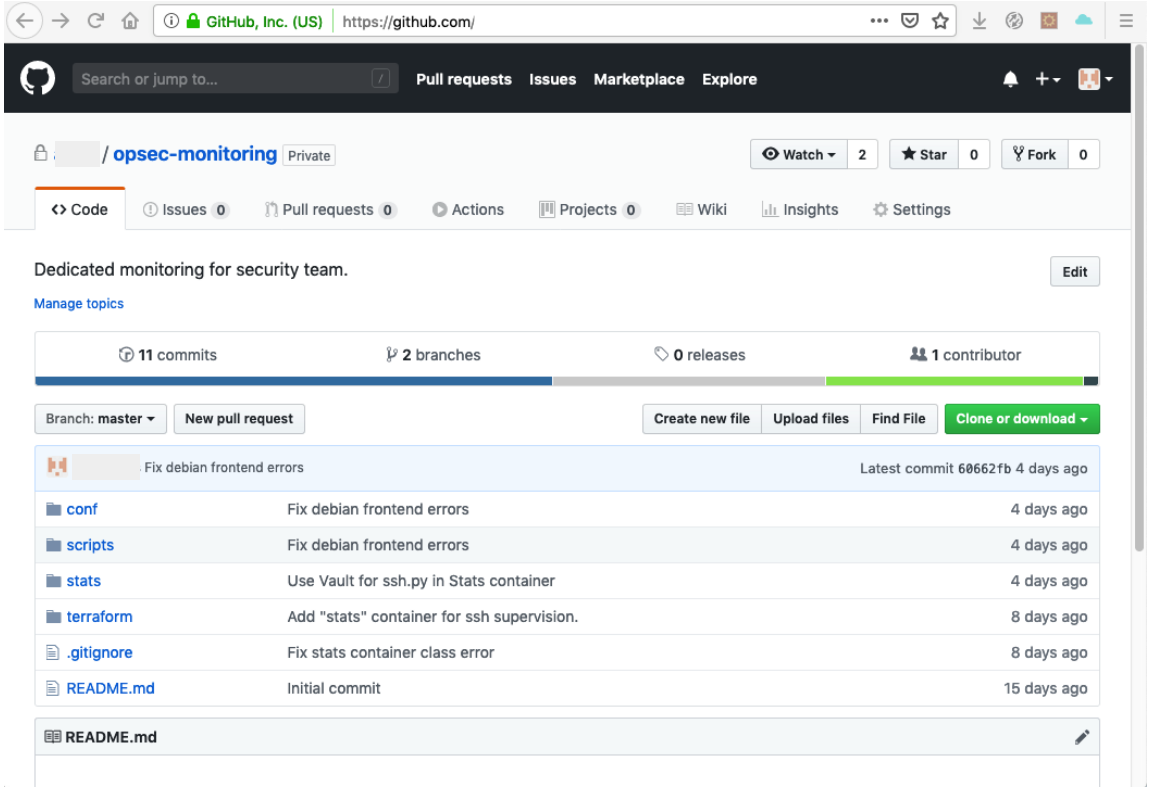


Un peu d’infrastructure as code

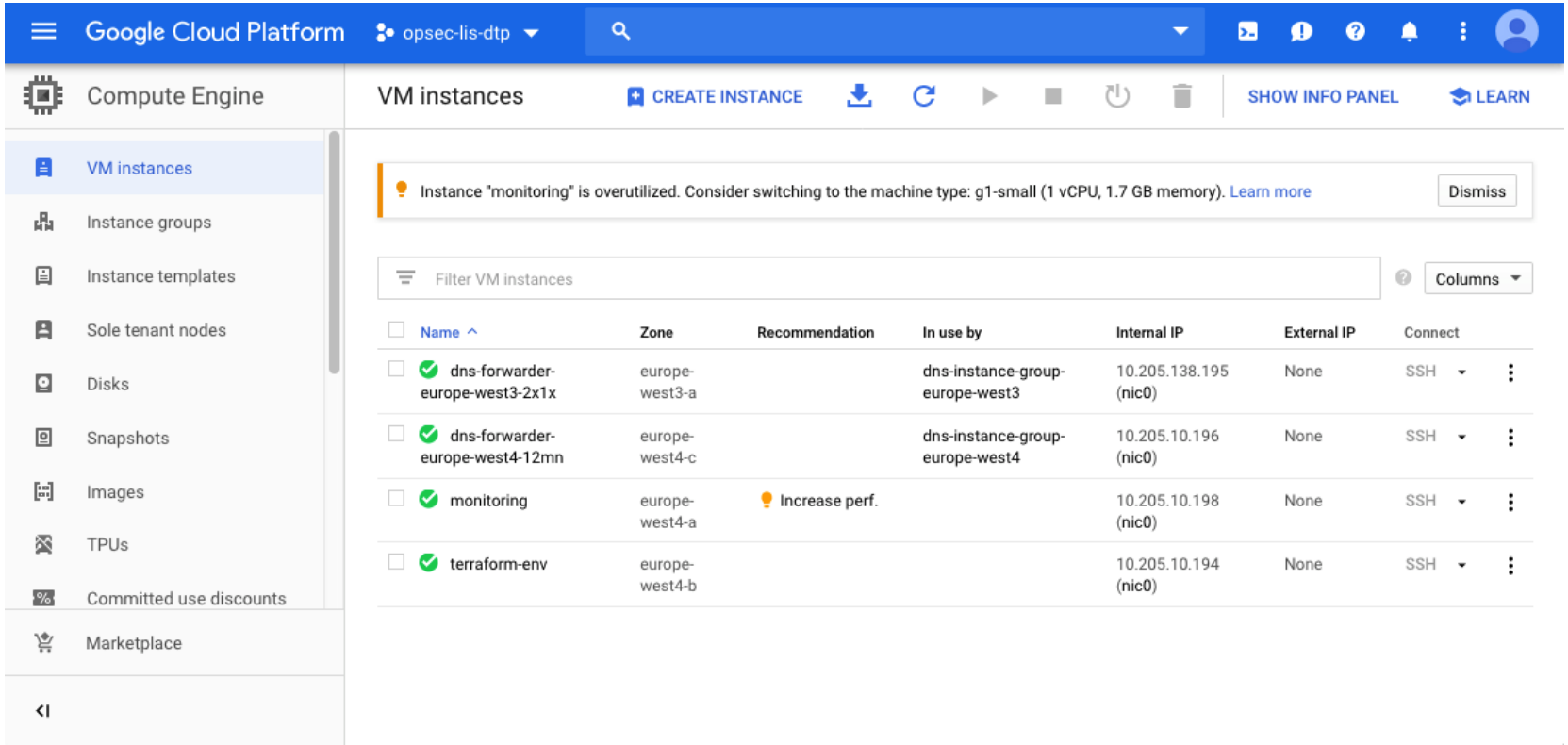
Security by design - Intégrité



Security by design - Intégrité



Security by design - Intégrité



Security by design - Disponibilité

Un peu de Docker

Security by design - Disponibilité

- **Base de données Time-series**
- **Conteneur de contrôle actif SSH**
- **Https proxy pour Graphite DB**

Security by design - Disponibilité

Nous utilisons WatchTower

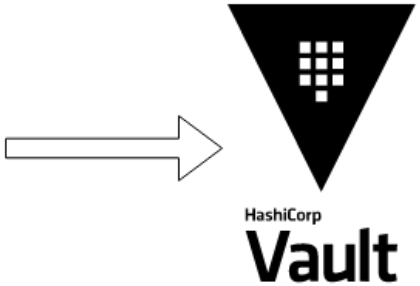
```
watchtower:
    image: containrrr/watchtower
    volumes:
    - /var/run/docker.sock:/var/run/docker.sock
    command: --interval 30 --cleanup
```

WatchTower vérifie régulièrement s'il existe une nouvelle image de chaque conteneur.
Si une nouvelle image est trouvée, le conteneur est mis à jour.
Ainsi, une vulnérabilité de sécurité est corrigée 30 secondes après la publication du correctif.

Security by design - Confidentialité

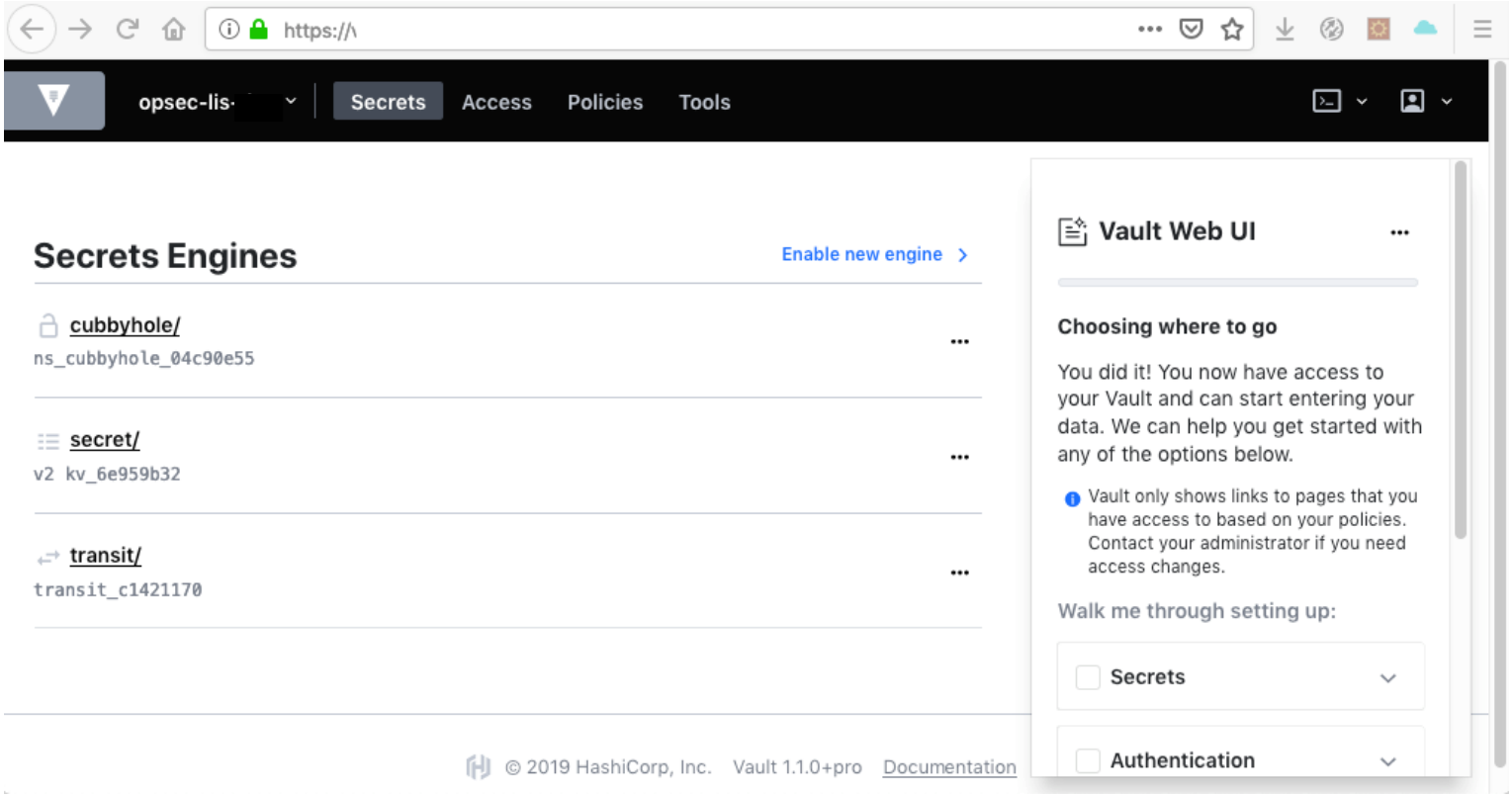
Un peu de Vault

Security by design - Confidentialité

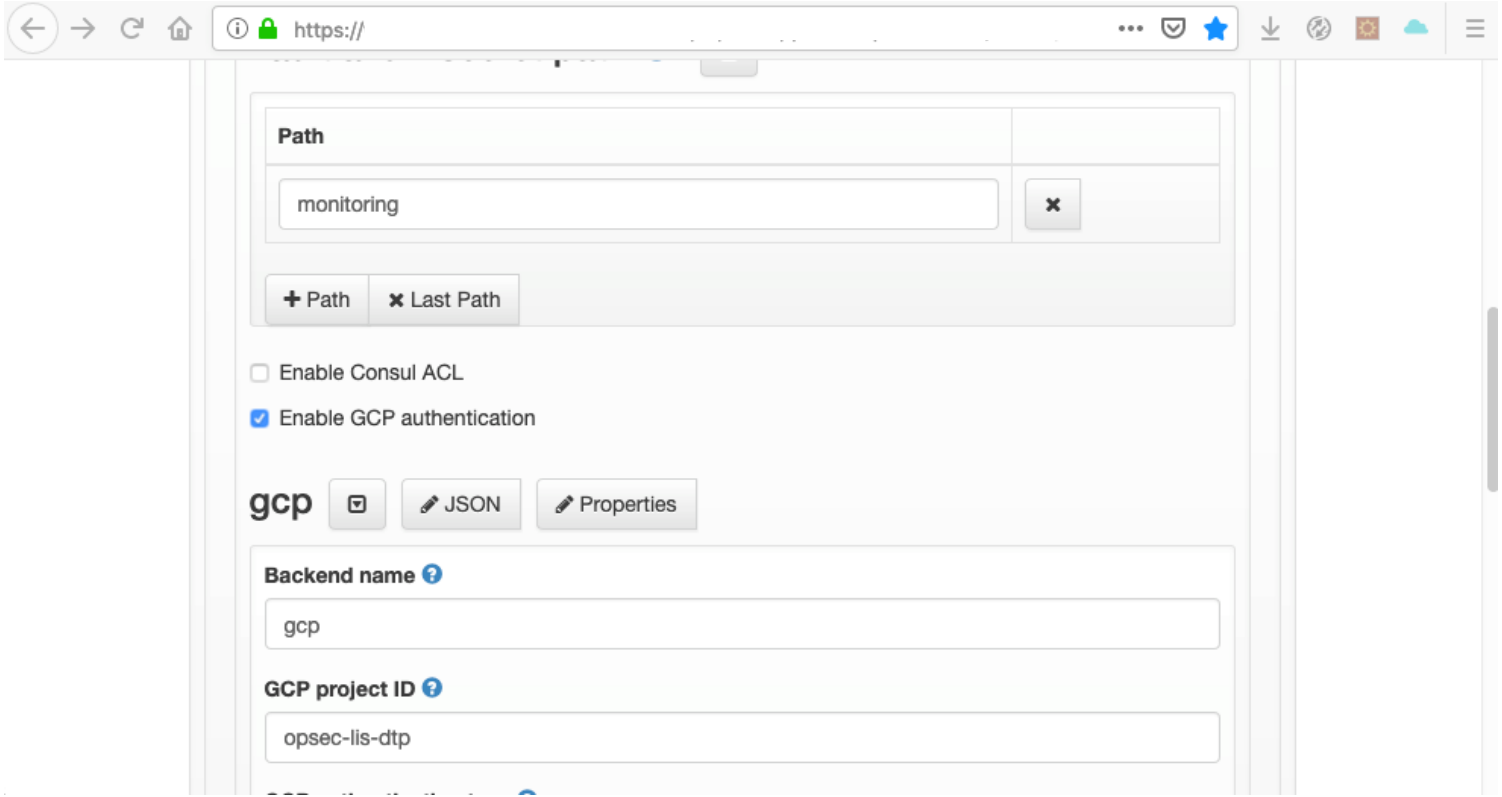


- **Récupérer le certificat SSL, les clés SSH et l'URL de l'API dans le coffre fort**
- **Authentification à l'aide du jeton JWT à partir des métadonnées internes de Google**

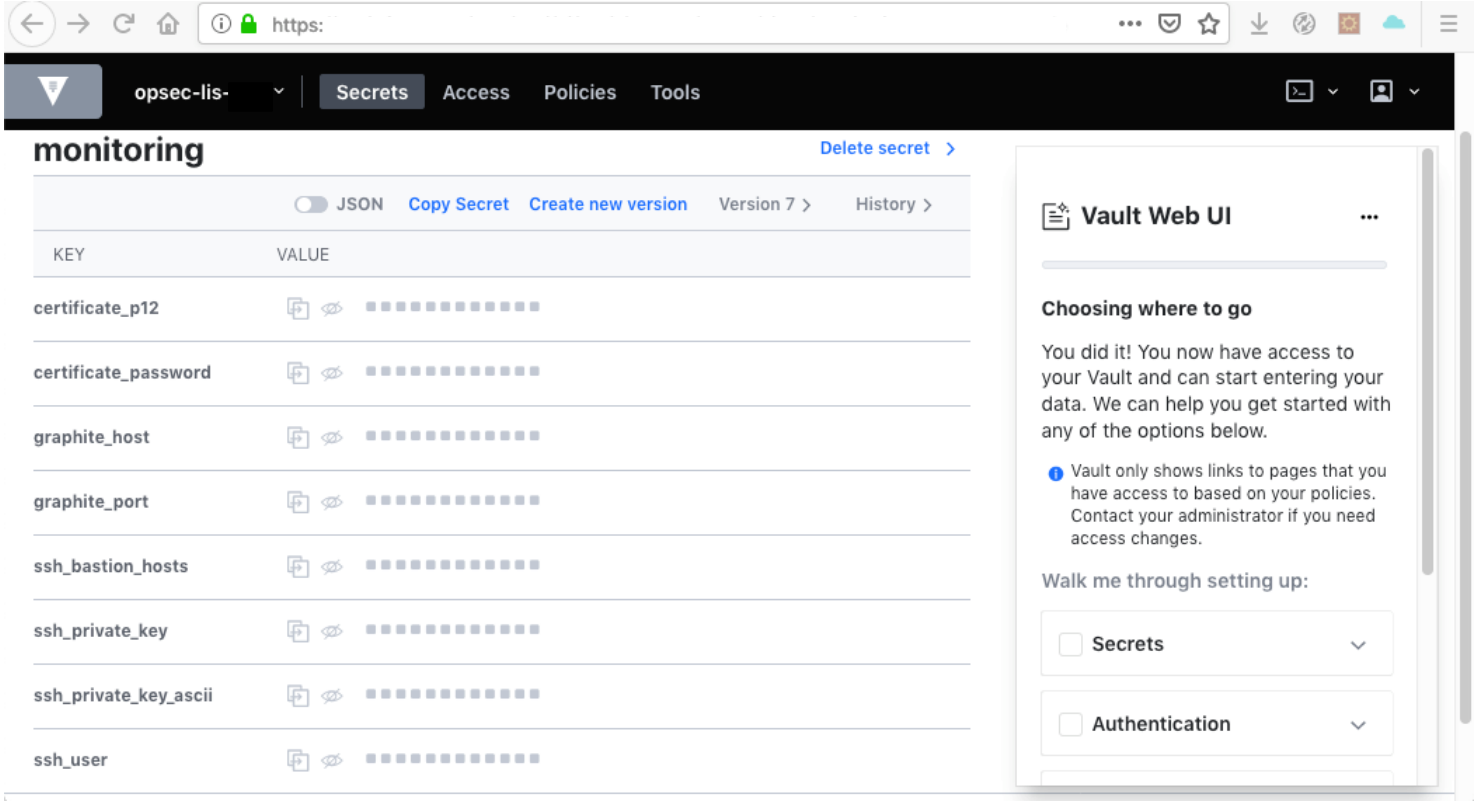
Security by design - Confidentialité



Security by design - Confidentialité



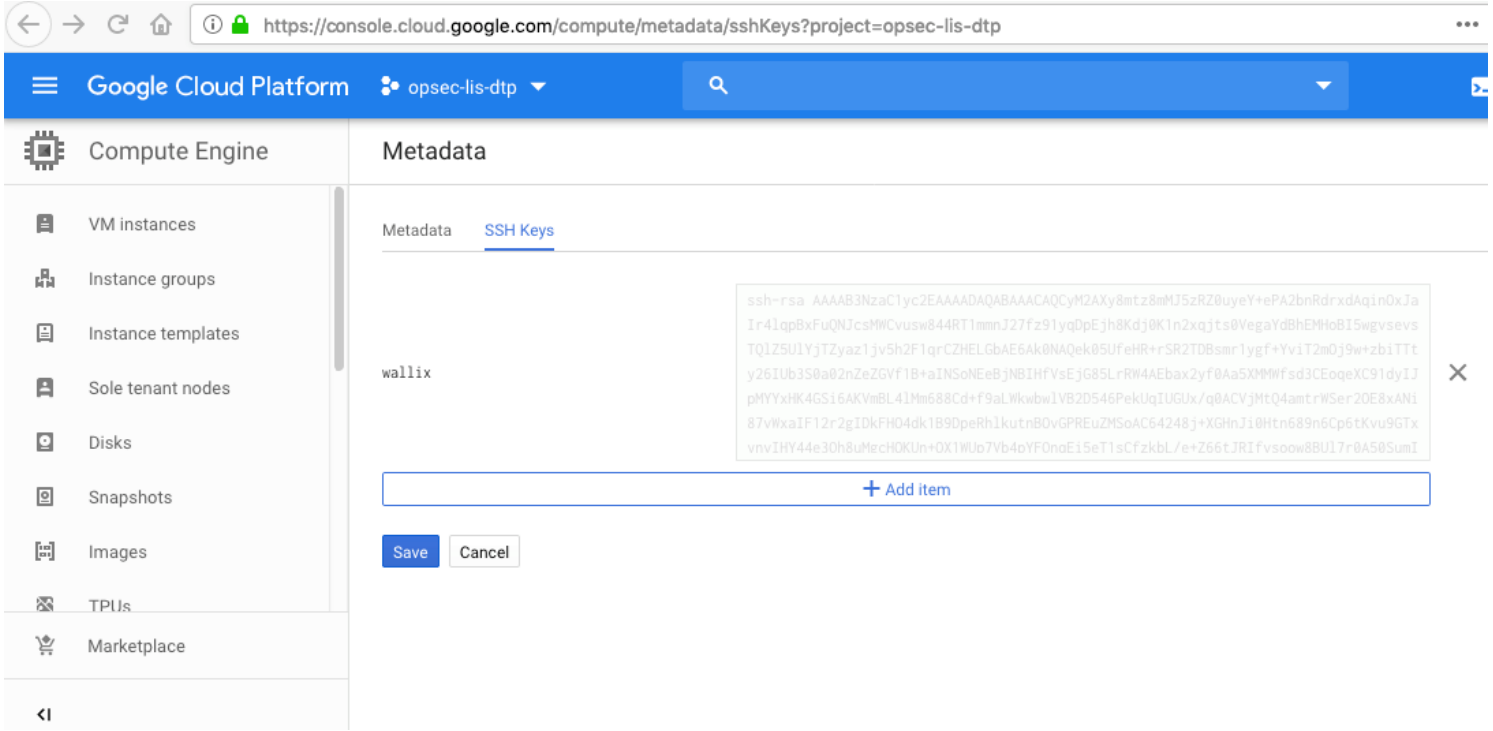
Security by design - Confidentialité



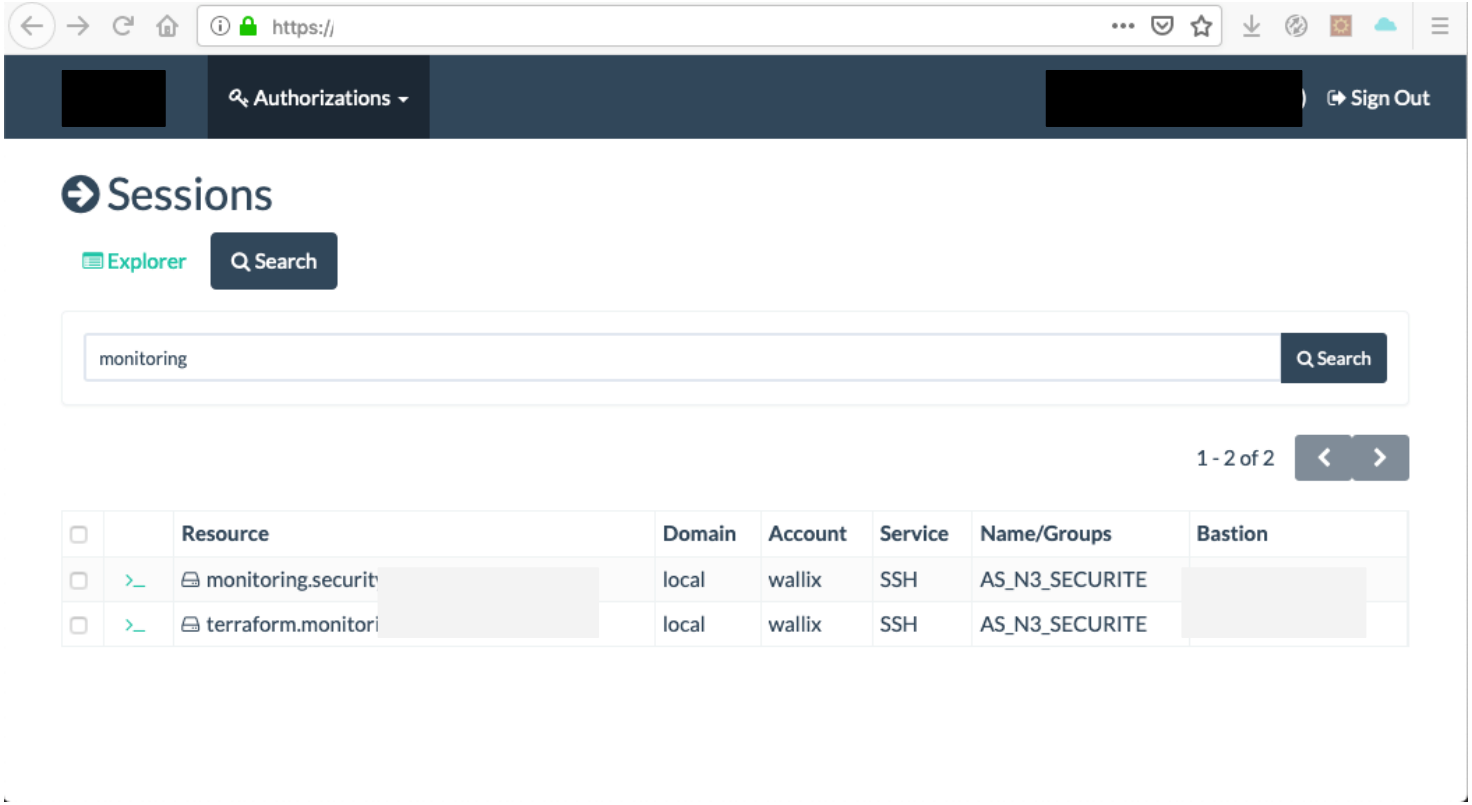
Security by design

Un peu de bastion

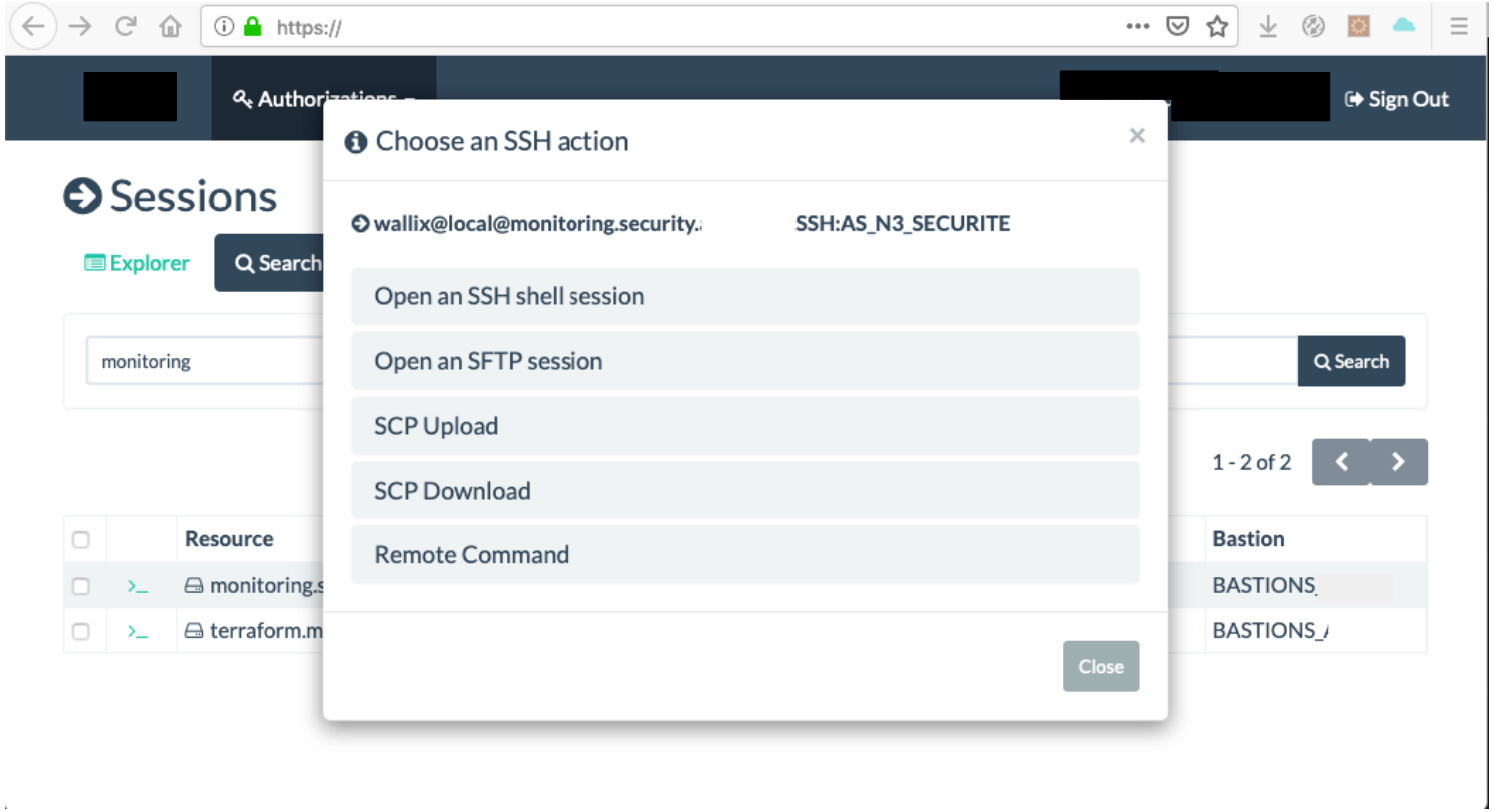
Security by design



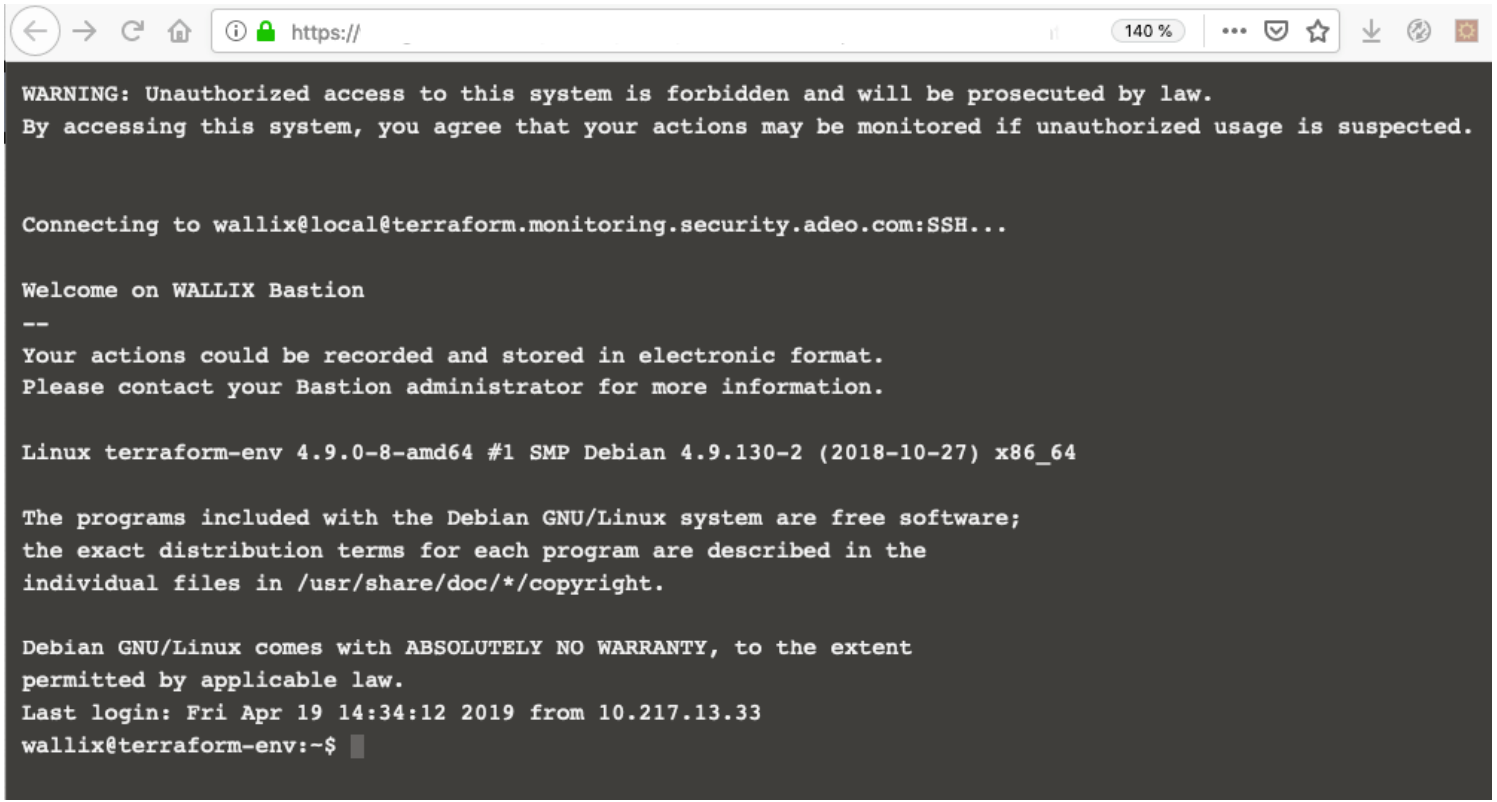
Security by design



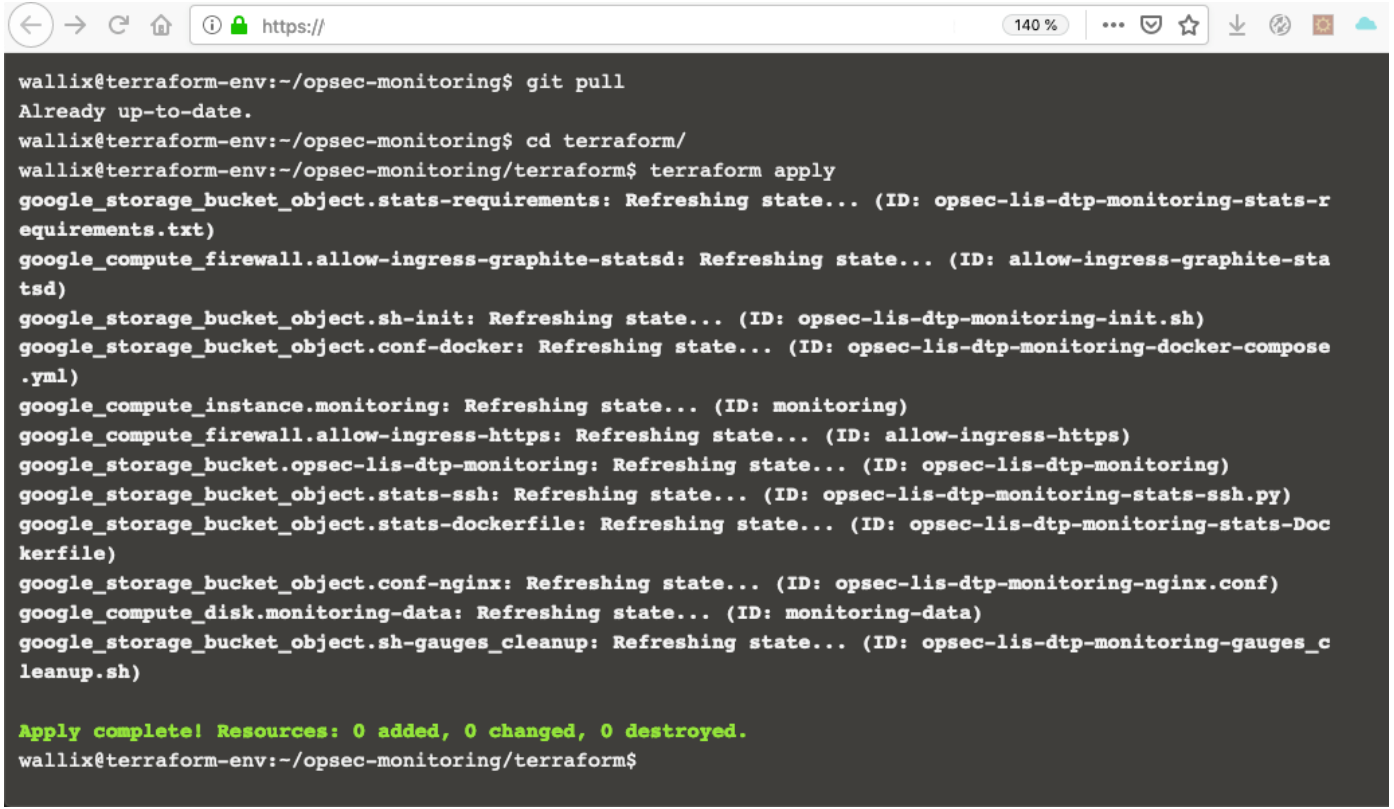
Security by design



Security by design



Security by design



Security by design

- **Nous utilisons un bastion et le fichier sudoers**

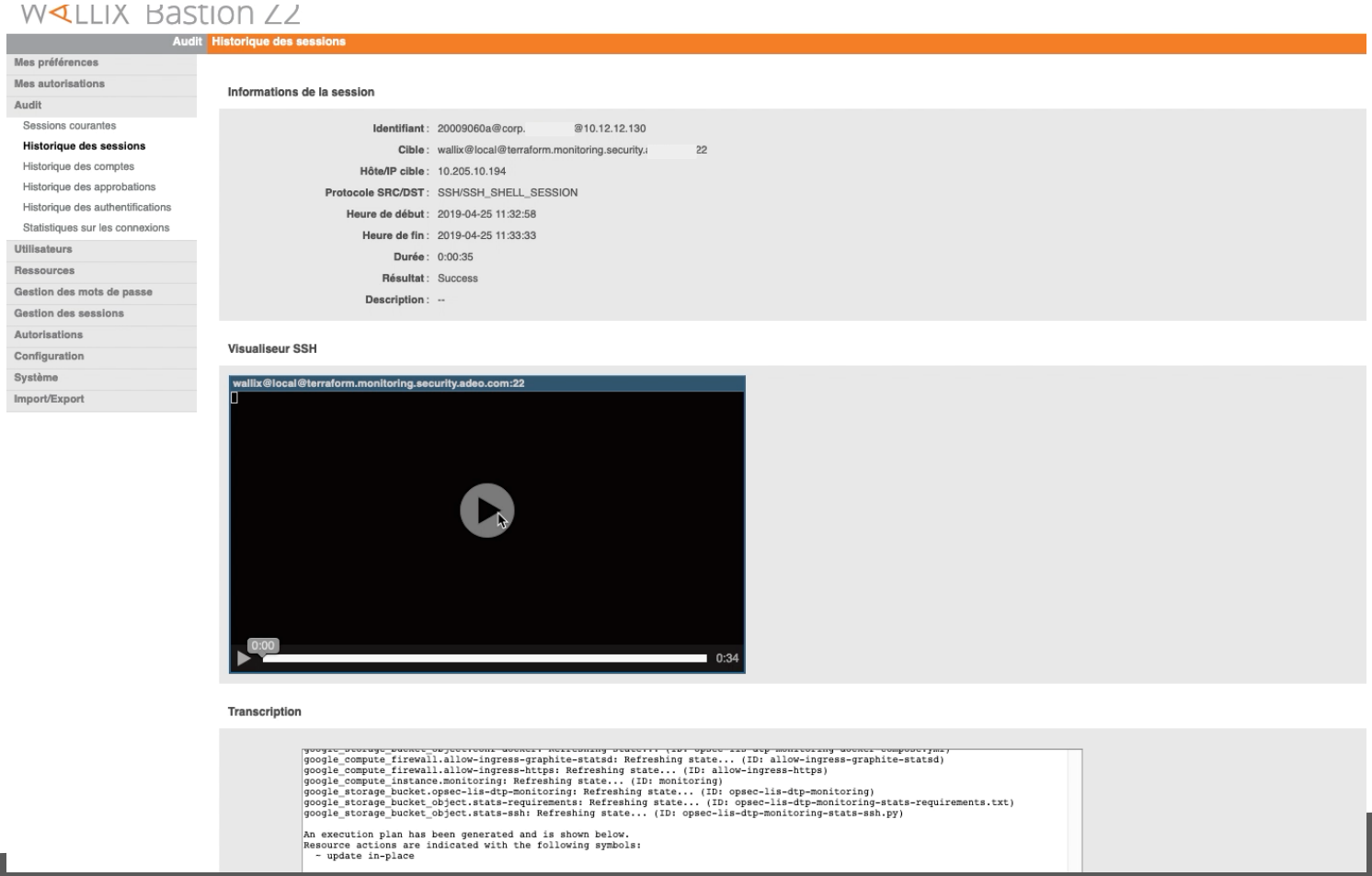
```
wallix@monitoring:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
wallix@monitoring:~$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
```

- **Toutes les actions sont tracées dans le fichier /var/log/auth.log**

```
Apr 23 15:31:56 monitoring sudo:    wallix : TTY=pts/0 ; PWD=/home/wallix ; USER=root ; COMMAND=/bin/cat /etc/sudoers
Apr 23 15:31:56 monitoring sudo: pam_unix(sudo:session): session opened for user root by wallix(uid=0)
```

Security by design

Visualization of logs on Wallix



Un peu de patch management

Security by design

Le redéploiement de l'instance pour mettre à jour tous les composants en une ligne de commande!

```
terraform destroy -target google_compute_instance.monitoring -auto-approve \
&&  terraform apply -auto-approve
```

Security by design - Intégrité

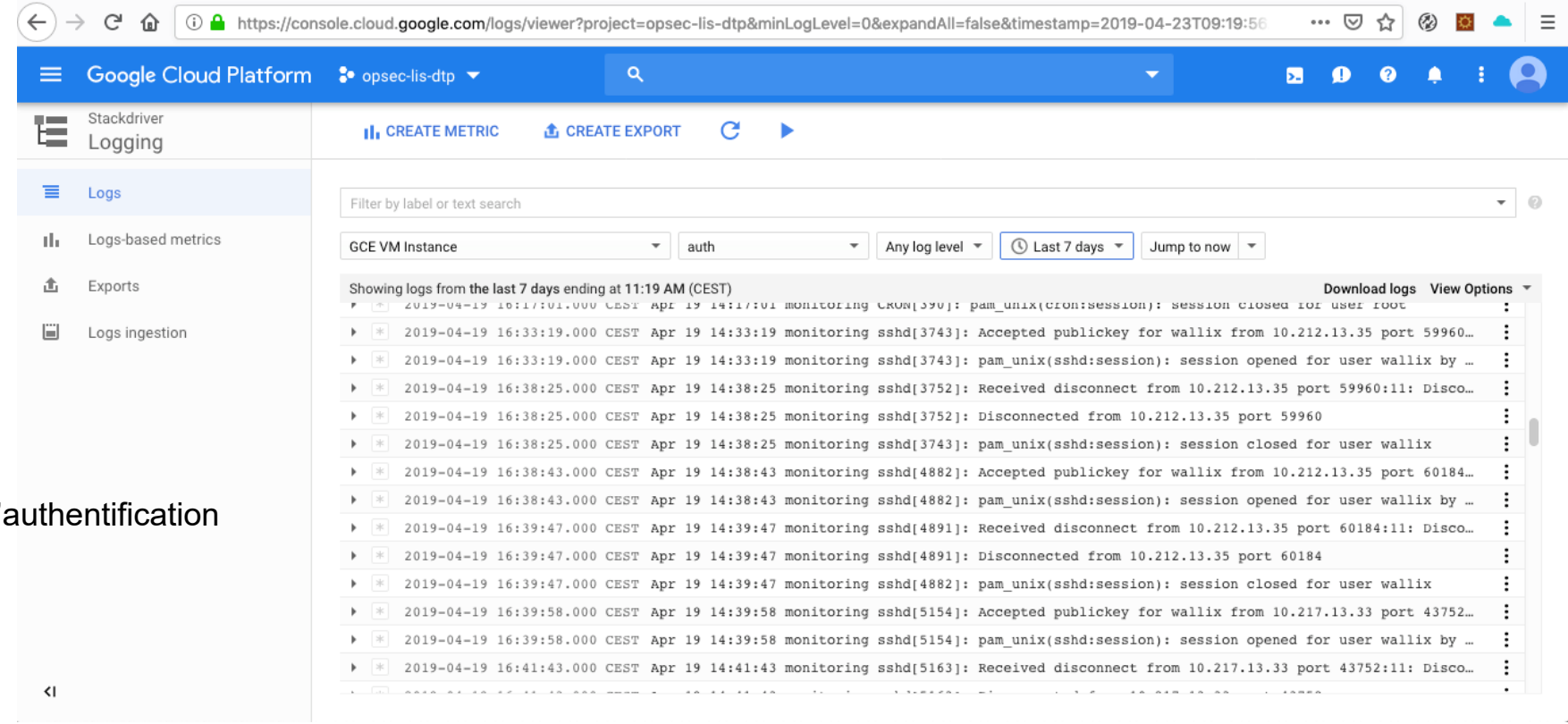
Et les logs?

Security by design - Intégrité

Nous utilisons  Stackdriver

```
curl -sSO https://dl.google.com/cloudagents/install-logging-agent.sh
sudo bash install-logging-agent.sh
```

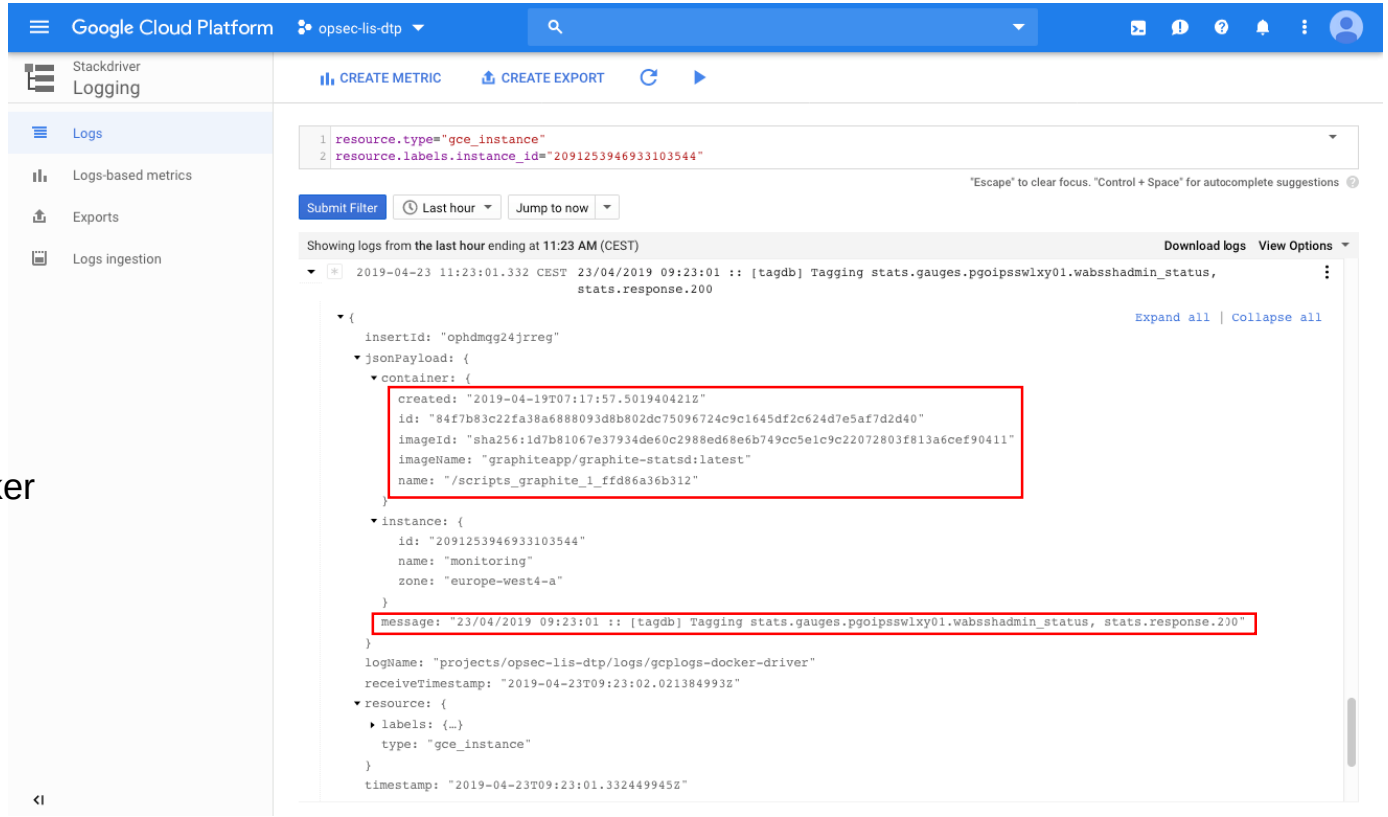
Security by design - Intégrité



Logs d’authentification

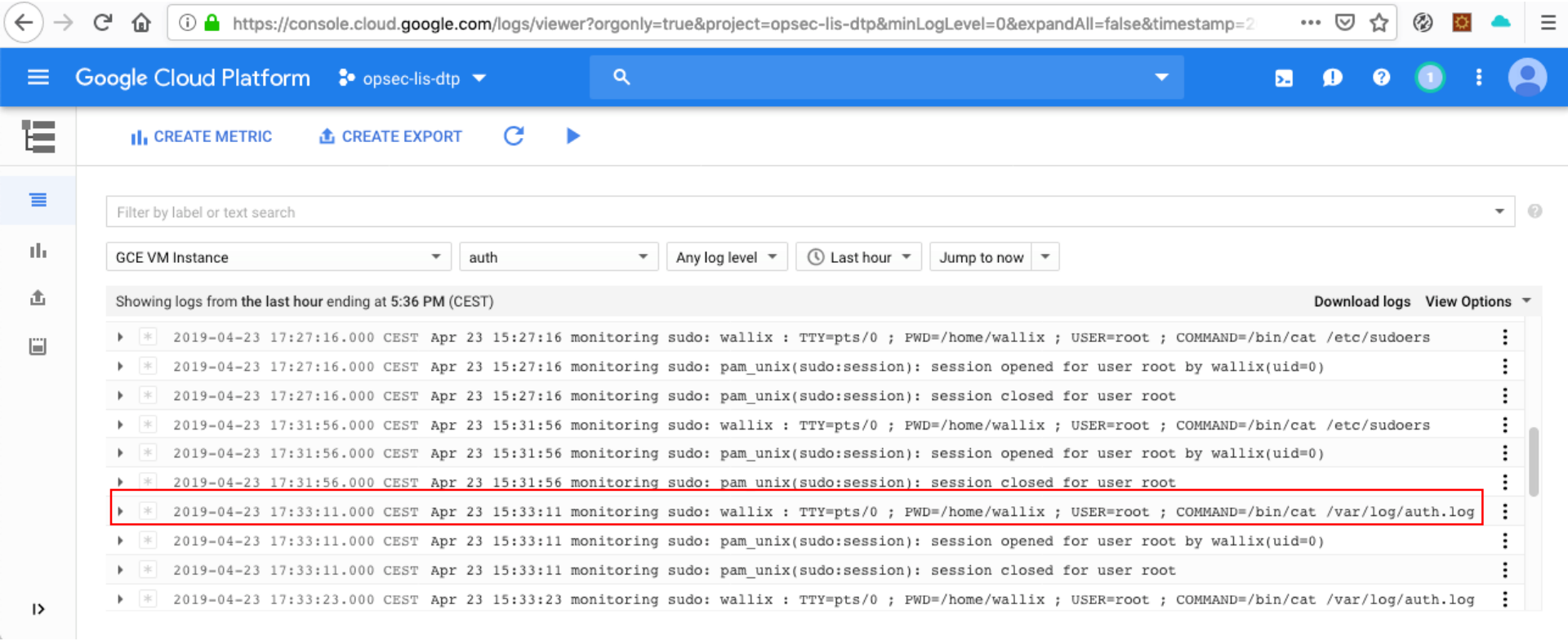
Security by design - Intégrité

Logs Docker



Security by design - Intégrité

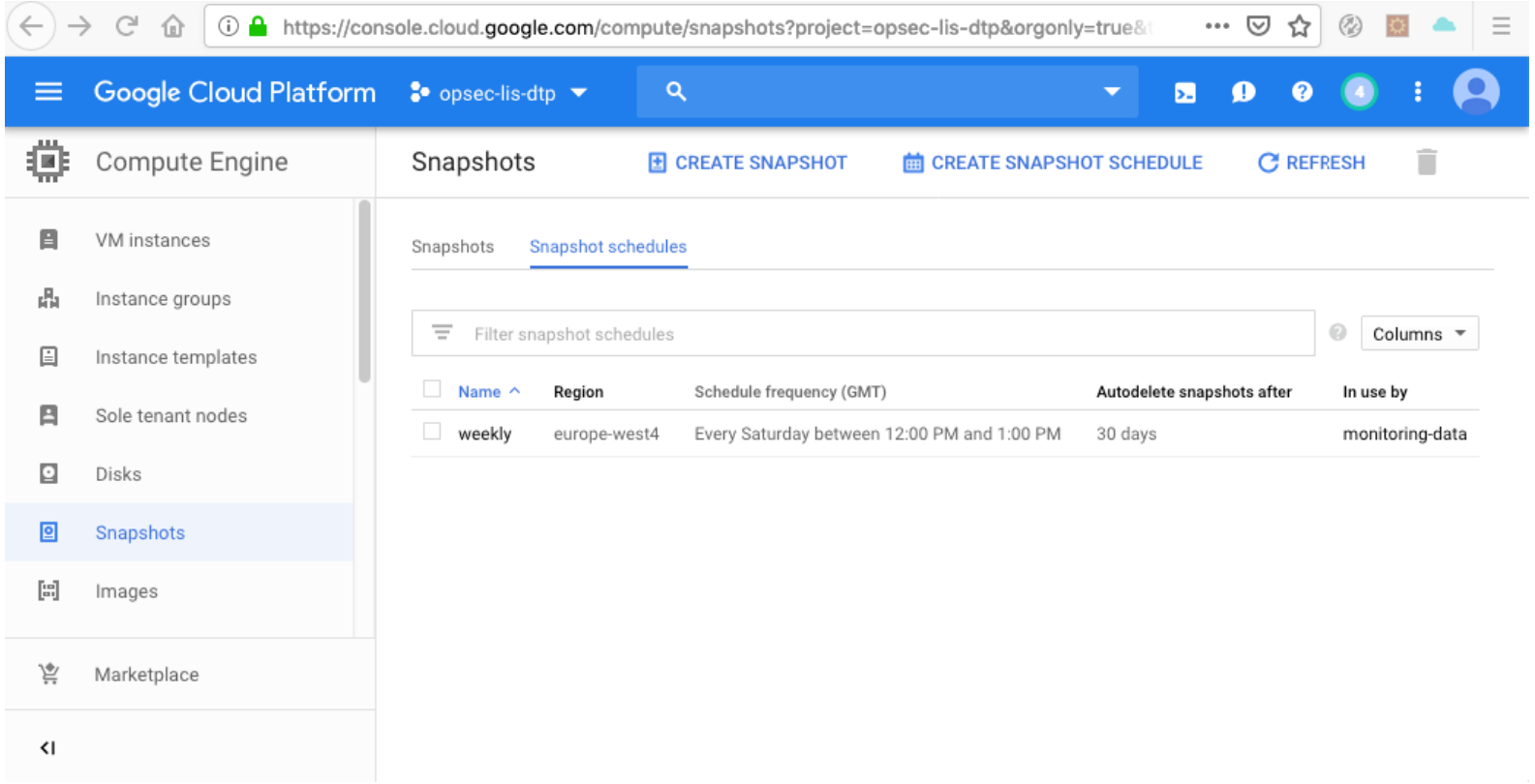
et les actions privilégiées



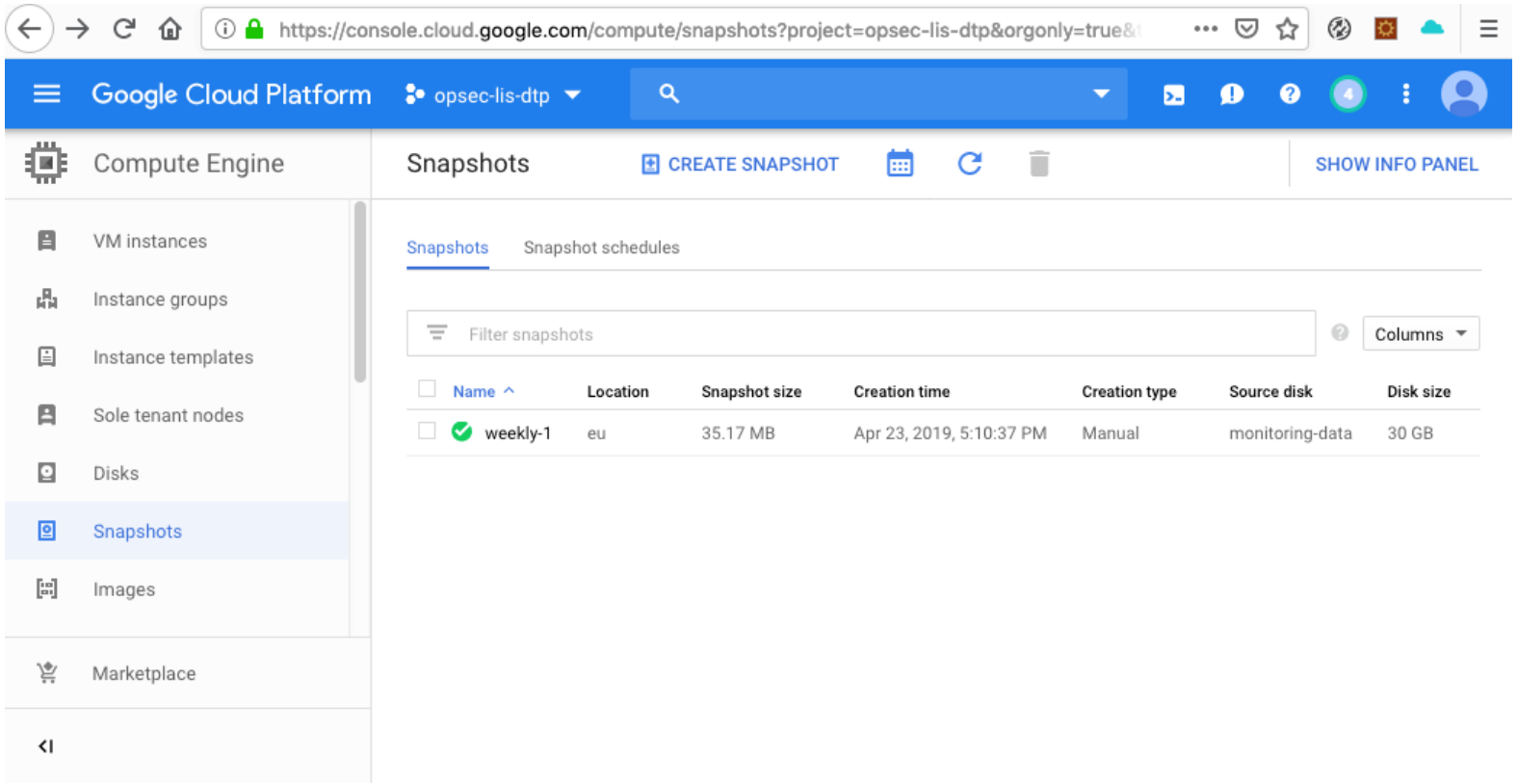
Security by design - Intégrité

Un peu de sauvegarde

Security by design - Intégrité



Security by design - Intégrité



Security by design - Intégrité

Nous utilisons simplement docker-compose pour définir la configuration de nos conteneurs

```
wallix@monitoring:~$ sudo cat /mnt/scripts/docker-compose.yml
version: '3.3'
services:
    graphite:
        image: 'graphiteapp/graphite-statsd:latest'
        volumes:
            - '/mnt/data/opt/graphite/conf:/opt/graphite/conf'
            - '/mnt/data/opt/graphite/storage:/opt/graphite/storage'
            - '/mnt/data/opt/statsd/config:/opt/statsd/config'
        restart: always
        ports:
            - '2003-2004:2003-2004'
            - '2023-2024:2023-2024'
            - '8125:8125/udp'
            - '8126:8126'
    nginx:
        image: 'nginx:latest'
        volumes:
            -
            -
            - '/mnt/data/etc/nginx/nginx.conf:/etc/nginx/nginx.conf'
        restart: always
        ports:
            - '443:443'
    stats:
        image: 'python:latest'
        restart: always
        build:
            context: /tmp
            dockerfile: stats-Dockerfile
        environment:
            VAULT_URL : https:
            VAULT_AUDIENCE_URL
            VAULT_AUTH_URL : h
            VAULT_NAMESPACE :
            VAULT_ROLE : monitoring
```

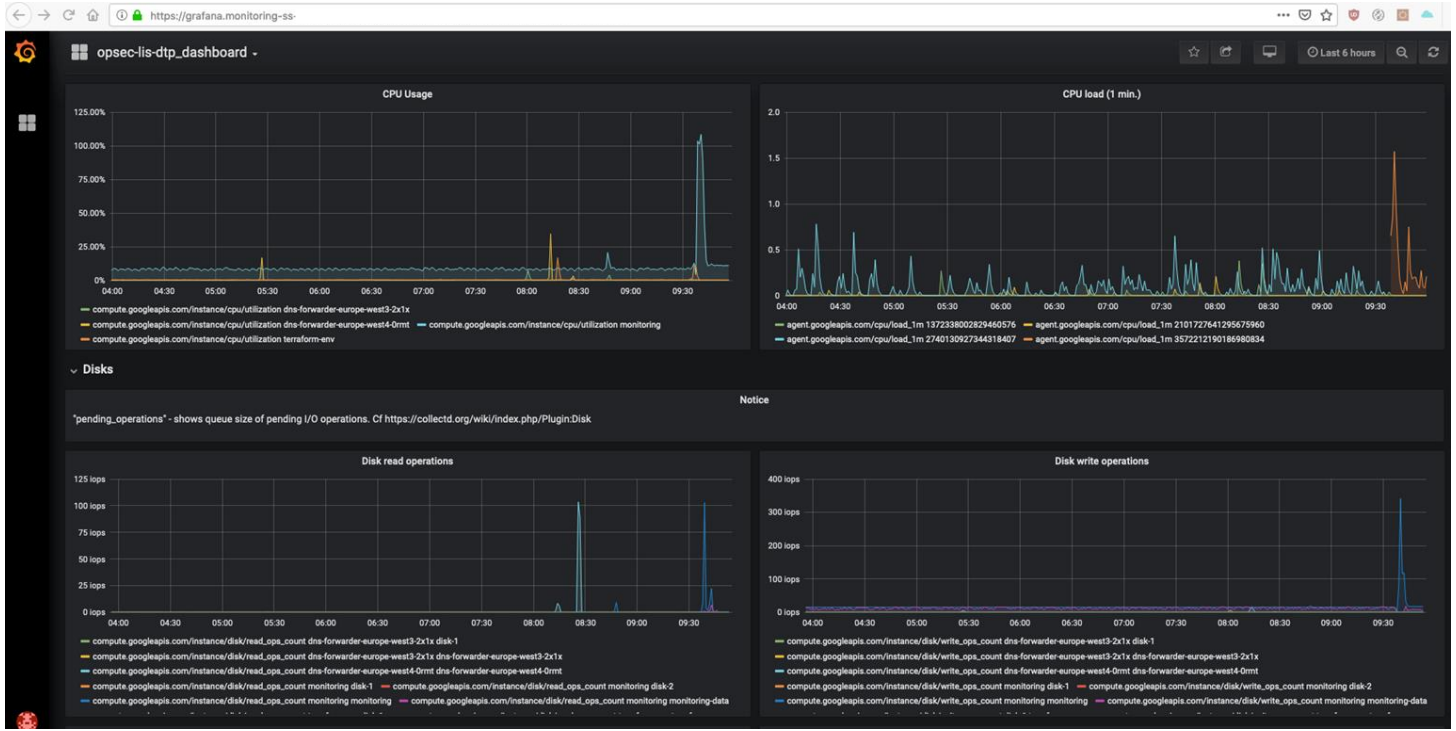
Security by design

Et nous bénéficions de tous les avantages de la landing zone

Security by design

Le Iaas nous fournit des statistiques

comme la CPU, Disk …



Security by design

réseau, Firewall
…