

Démarrer avec Ansible sur Google Cloud

Karim Roukoz

kroukoz@google.com

2021-03-18

Démarrer avec
Ansible sur Google
Cloud

15:00 - 17:15



Agenda

Google Cloud 001

Créer un inventaire dynamique

Gérer des instances Compute

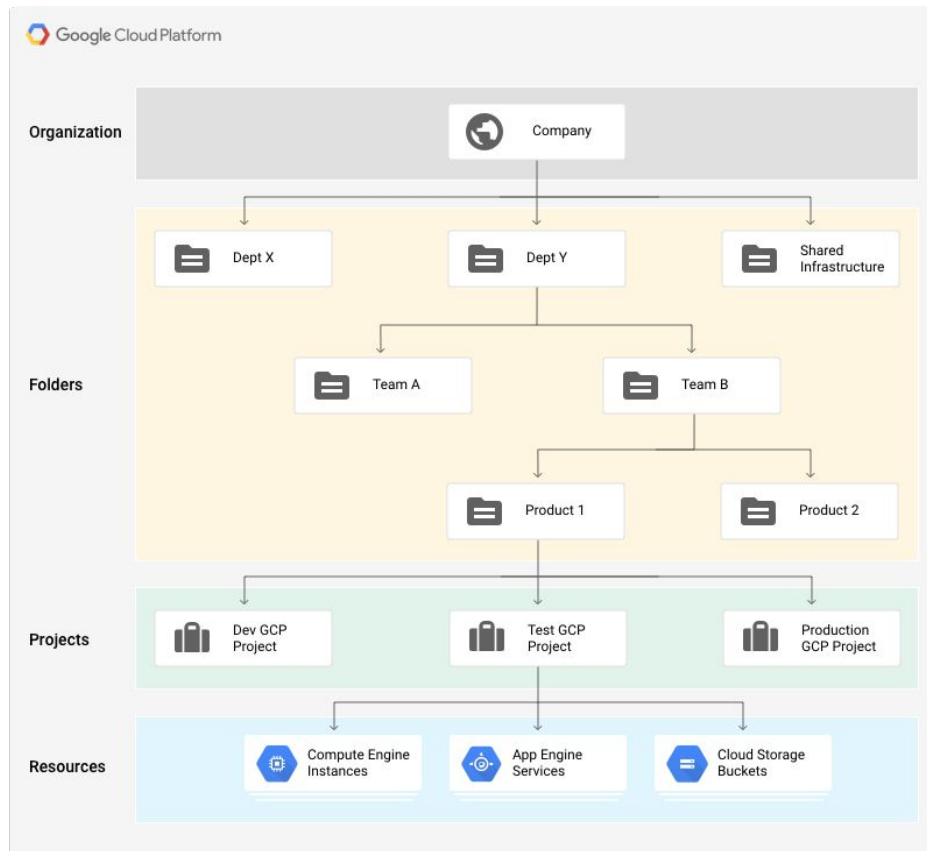
Gérer la plateforme Google Cloud

Going?

Yes No Maybe | ^

Google Cloud Sécurité et IAM 001

- Les ressources sont organisées dans des **projets (projects)**, qui peuvent être organisées dans des **dossiers (folder)**
- Les **comptes de services (service account)** appartiennent à **un projet**.
- Les **comptes de services (service account)**, les **utilisateurs (users)** et les **groupes (groups)** ont des permissions sur un/plusieurs **projet(s)**, et/ou sur un/plusieurs **dossier(s)**.



Gestion de Google Cloud avec Ansible



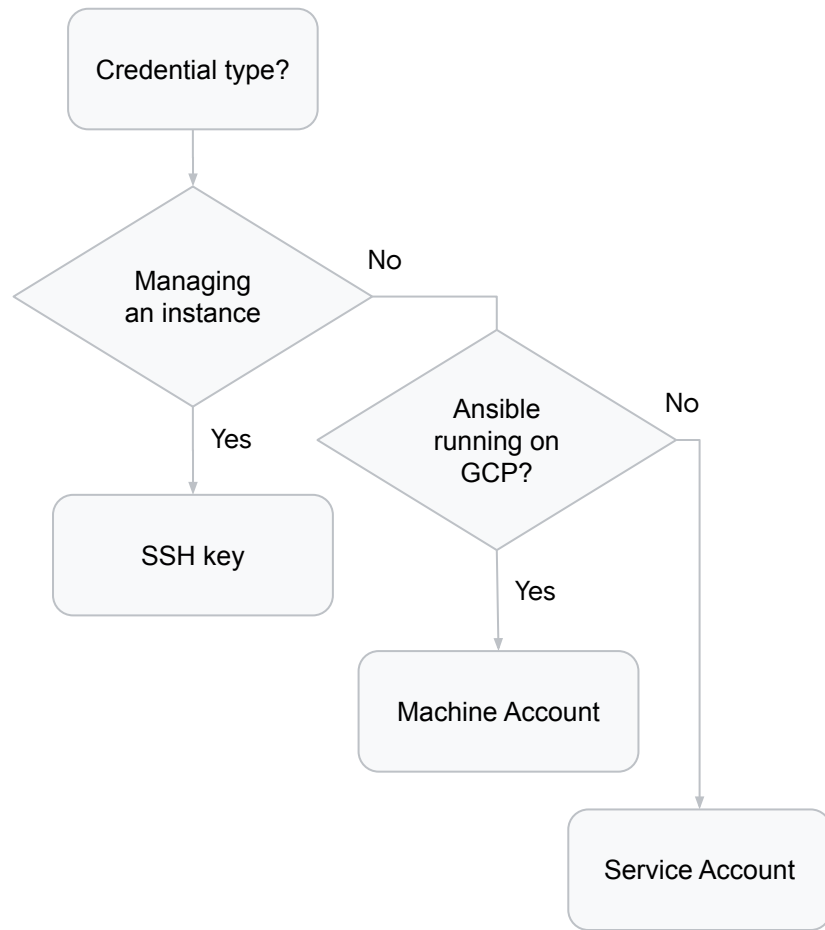
Gérer les services Cloud

- Exécuter des appels aux API de Google Cloud, ex:
 - Compute Engine API
 - Cloud DNS API
 - Authentification à travers un compte de service Google Cloud



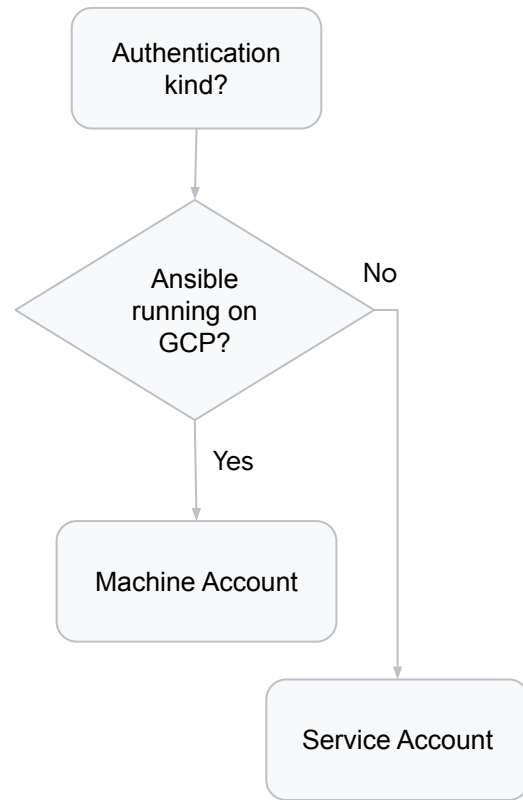
Gérer des instances (VM) sur le Cloud

- SSH à une VM
 - Clés gérées par l'utilisateur (enregistrées dans les métadonnées GCP du projet ou de l'instance)
 - Cloud "OS Login" pour gérer les clés, propagée via les permissions IAM (compute.osLogin & compute.osAdminLogin)
- Inventaires dynamiques



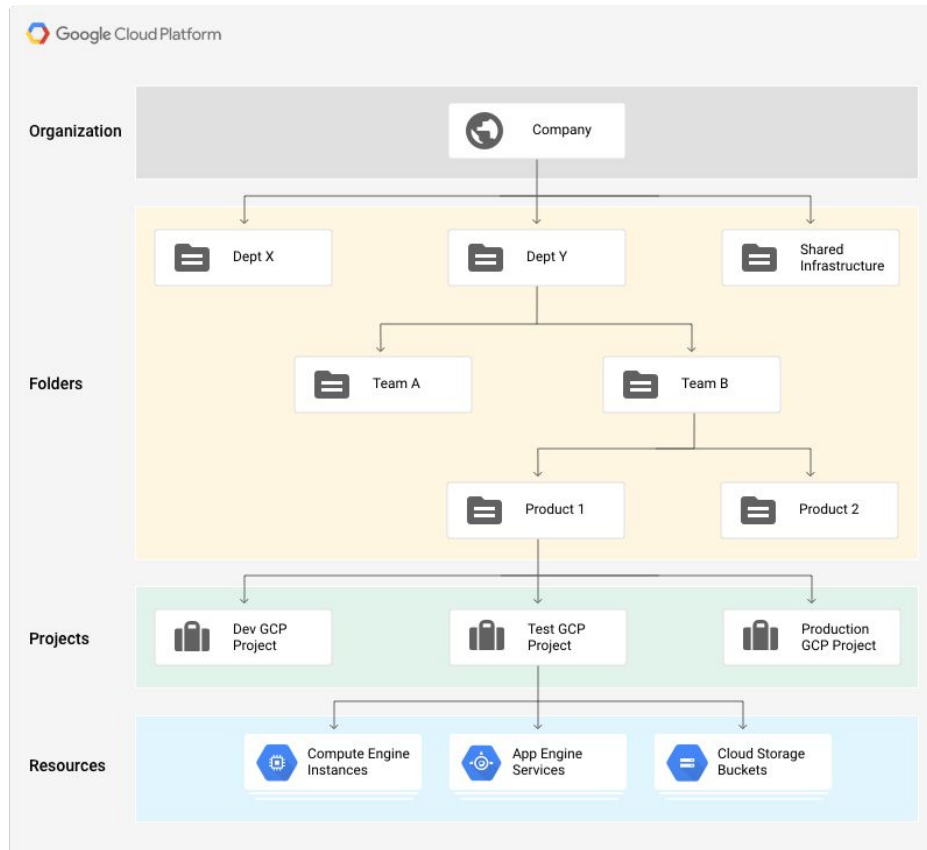
Inventaire dynamique pour Google Cloud

```
plugin: gcp_compute  
auth_kind: machineaccount  
service_account_email: "default"
```



Inventaire dynamique pour Google Cloud

```
plugin: gcp_compute
auth_kind: machineaccount
service_account_email: "default"
projects:
  - ecommerce-prod-534e
folders:
  - 123456789012
```



Inventaire dynamique pour Google Cloud

```
plugin: gcp_compute
auth_kind: machineaccount
service_account_email: "default"
projects:
  - ecommerce-prod-534e
folders:
  - 123456789012
hostnames:
  - name
# compose:
# ansible_host: networkInterfaces[0].accessConfigs[0].natIP
```

```
$ gcloud compute instances describe $instance_name
[...]
networkInterfaces:
- accessConfigs:
  - kind: compute#accessConfig
    name: external-nat
    natIP: 35.203.36.179
[...]
```

Inventaire dynamique pour Google Cloud

```
plugin: gcp_compute
auth_kind: machineaccount
service_account_email: "default"
projects:
  - ecommerce-prod-534e
folders:
  - 123456789012
hostnames:
  - name
keyed_groups:
  - key: zone
    prefix: gcp
  - key: labels
    prefix: gcp
groups:
  gcp: "' in name" # create a group with all GCE
nodes
```


\$ demo dynamic inventory

Gerer les services Google Cloud (ex: Creer une instance Compute Engine)

```
- name: Create an instance
  hosts: localhost
  gather_facts: no
  vars:
    auth_kind: machineaccount
    service_account_email: default
    project: ecommerce-prod-534e
    scopes:
      - https://www.googleapis.com/auth/compute
```

Gerer les services Google Cloud (ex: Creer une instance Compute Engine)

```
[...]
  tasks:
  - name: create a address
    google.cloud.gcp_compute_address:
      name: address-instance
      region: northamerica-northeast1
      project: "{{ project }}"
      auth_kind: "{{ auth_kind }}"
      service_account_email: "{{ service_account_email }}"
      state: present
    register: network
[...]
```

Gerer les services Google Cloud (ex: Creer une instance Compute Engine)

[...]

```
- name: create a instance
  google.cloud.gcp_compute_instance:
    name: "instance-{{ version }}"
    machine_type: n1-standard-1
    disks:
      - auto_delete: 'true'
        boot: 'true'
        initialize_params:
          source_image: projects/rhel-cloud/global/images/family/rhel-8
          disk_size_gb: 20
    metadata:
      cost-center: '12345'
    labels:
      environment: production
    network_interfaces:
      - network:
          access_configs:
            - name: External NAT
              nat_ip: "{{ network }}"
              type: ONE_TO_ONE_NAT
    zone: northamerica-northeast1-a
    project: "{{ project }}"
    auth_kind: "{{ auth_kind }}"
    service_account_email: "{{ service_account_email }}"
    state: "{{ state }}"
```

```
$ demo instance creation
```

En apprendre d'avantage

- Google Cloud Infrastructure as Code
 - <https://cloud.google.com/solutions/infrastructure-as-code>
- Google Cloud Platform Guide — Ansible Documentation
 - https://docs.ansible.com/ansible/latest/scenario_guides/guide_gce.html
- Ansible Galaxy for Google Cloud
 - <https://galaxy.ansible.com/google/cloud>
- Github: GoogleCloudPlatform/magic-modules
 - <https://github.com/GoogleCloudPlatform/magic-modules>
- Github: ansible-collections/google.cloud
 - <https://github.com/ansible-collections/google.cloud>

Questions?

Karim Roukoz

kroukoz@google.com