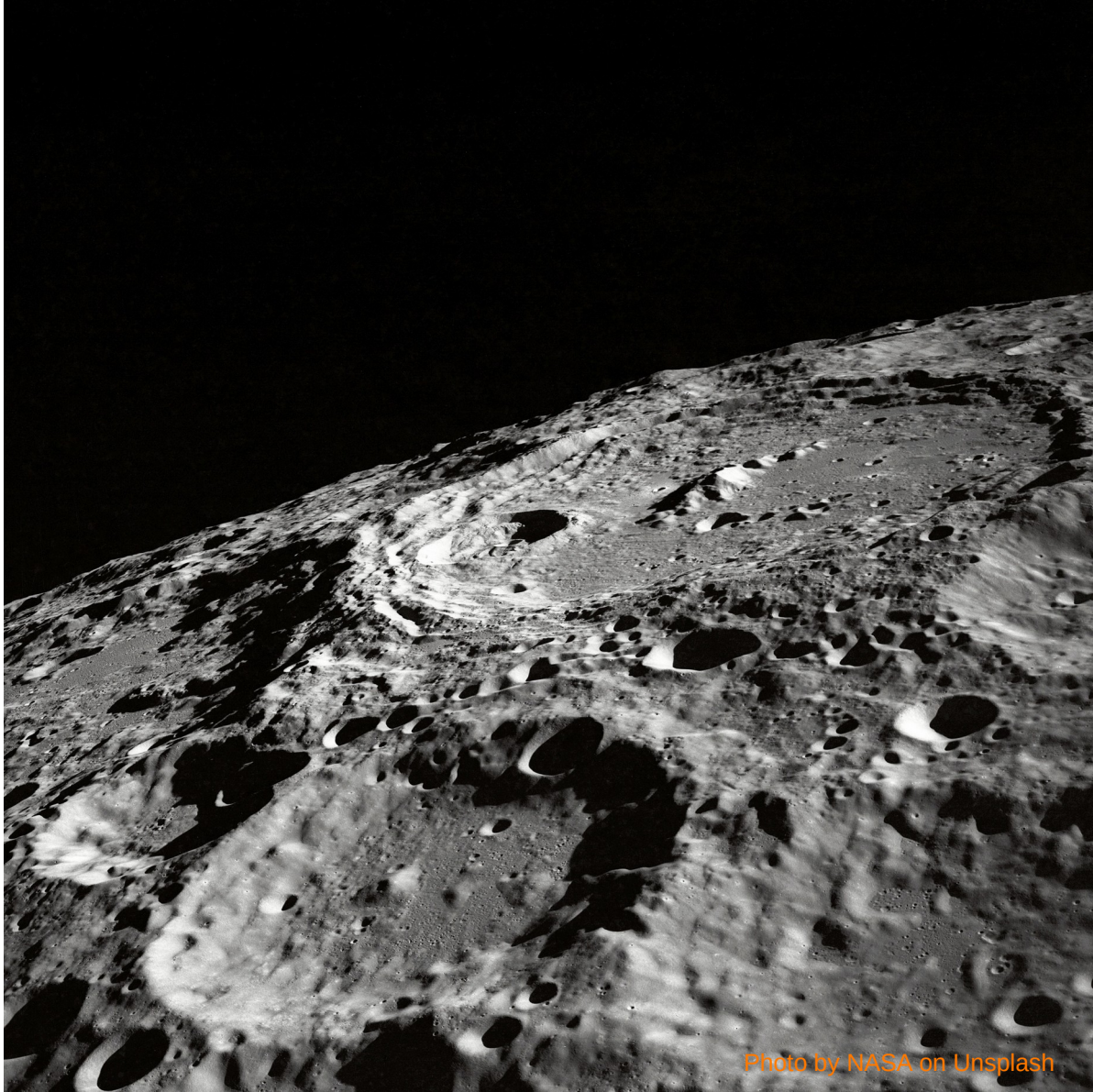
Moon Project

Thomas Duval
Dimitri Darthenay
Philippe Calvet

orange™

June 2020

SSTIC



Introduction

- Les mécanismes d’autorisation jouent un rôle vital sur nos plateformes mais :
  - Le modèle utilisé est statique
  - La granularité des règles n’est pas celle souhaitée
  - La configuration est parfois décentralisée

orange™

Exemple d’OpenStack

- Librairie : Oslo Policy
- Gestion par chaque composant : interne
- Gestion de la configuration : par fichier
- Gestion par l’administrateur
- Seule politique utilisable : RBAC

orange™

Exemple policy.json

```
  137 cinder/policy.json
   63 glance/policy.json
  193 keystone/policy.json
  235 neutron/policy.json
  172 nova/policy.json
```

$ head /etc/nova/policy.json

"os_compute_api:os-evacuate": "rule:admin_api"

"os_compute_api:servers:create": "rule:admin_or_owner"

"os_compute_api:os-extended-volumes": "rule:admin_or_owner"

"os_compute_api:servers:create:forced_host": "rule:admin_api"

"os_compute_api:os-aggregates:remove_host": "rule:admin_api"

"os_compute_api:os-console-output": "rule:admin_or_owner"

"os_compute_api:os-floating-ips": "rule:admin_or_owner"

"os_compute_api:os-aggregates:update": "rule:admin_api"

"os_compute_api:server-metadata:show": "rule:admin_or_owner"

"os_compute_api:os-flavor-manage:create": "rule:os_compute_api:os-flavor-manage"

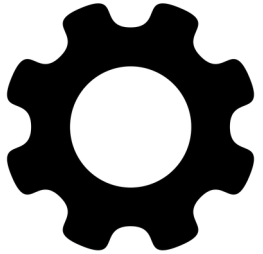
orange™

Moon : description

- Plateforme de gestion centralisée
  - de politique de sécurité
  - d’autorisation
- Protège chaque projet OpenStack par une couche de sécurité supplémentaire
- Chaque couche est gérée par l’utilisateur

orange™

Méta modèle



- Le méta modèle :
  - perimeter ⇄ data
  - données extérieures ⇄ internes
- Par exemple :
  - utilisateurs ⇄ rôles
  - actions ⇄ types d’actions

orange™

Moon

- Exemple d’utilisation de l’IHM de Moon
  - Avec un cas typique OpenStack

orange™

Moon : Premiers pas...

- Installation
- Configuration de Moon
- Configuration d’OpenStack
- Importation d’un modèle de politique

```
python3 -m pip install moon_manager

git clone https://git.opnfv.org/moon
```

orange™

Cas d'Orange France

- Plateforme OpenStack / SDN
- Plateforme hautement sécurisée
- Le besoin client :
  - mode « build » / « run »
  - « grant » / « deny » rapide sur une règle
- Exemple sur l'IHM

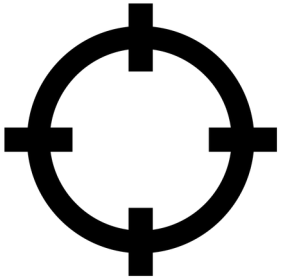
orange™

Restrictions

- Sur les informations récupérées :
  - Certains composants ne fournissent pas tous les informations nécessaires

orange™

Utilisation et tests



- Prêt pour une utilisation en production
- Capacité de 150/200 req/s
  - 300 req/s dans certaines configurations
  - 1 vCPU & 1Go de RAM sur un PC standard

orange™

Conclusion

- Moon permet une gestion des autorisations :
  - plus fine :
    - au niveau des politiques de sécurité utilisées
    - au niveau des données externes gérées
  - centralisée
  - centrée sur l’utilisateur
  - dynamique

orange™

Futurs développements

- Les futurs développements permettront :
  - Intégration de Kubernetes
  - Améliorations de l’interface Web / CLI

orange™

Merci

thomas.duval@orange.com
dimitri.darthenay@orange.com
philippe.calvet@orange.com

https://git.opnfv.org/moon