

Les 10 Commandements d'Ansible

Pour que l'automatisation reste une discipline, et non une superstition.

01

Idempotent tu seras

Toute tâche doit pouvoir tourner cent fois sans dégât. **shell** et **command** exigent **changed_when** ou **creates**.

02

Le module natif tu préféreras

Au shell tu n'auras recours qu'en dernier ressort. Chaque appel à **shell** est un aveu de paresse.

03

En rôles tu structureras

Le playbook monolithique est l'œuvre du malin. **tasks/**, **handlers/**, **defaults/**, **templates/** — la séparation des préoccupations comme dogme.

04

Tes secrets tu chiffreras

Ansible Vault, ou rien. Jamais de clé en clair, même en pre-prod, même « juste pour tester ».

05

Tes variables tu hiérarchiseras

defaults/ < **vars/** < **group_vars/** < **host_vars/** < **extra-vars**. Connais l'ordre, vis par lui.

06

Tes collections tu épingleras

requirements.yml versionné, **ansible-galaxy install** dans la CI. Le flou des versions est le terreau du chaos.

07

Tes tâches tu nommeras

Un **name**: clair vaut mille commentaires. Le futur toi te remerciera à 3h du matin.

08

Avec Molecule tu testeras

Un rôle non testé n'existe pas. Driver Docker en local, scénarios **default** et **verify**.

09

En check-mode et diff tu valideras

--check --diff avant tout **apply** en prod. Le dry-run est ta repentance préventive.

10

Ton inventaire dynamique sera

NetBox, Proxmox, AWS — jamais de **hosts.ini** figé pour de l'infra vivante. La source de vérité est unique.