The 10 Commandments of Ansible

So that automation remains a discipline, not a superstition.

01

Thou shalt be idempotent

Every task must run a hundred times without harm. **shell** and **command** require **changed_when** or **creates**.

02

Thou shalt prefer the native module

Reach for **shell:** only as a last resort. Every shell call is a confession of laziness.

03

Thou shalt structure in roles

The monolithic playbook is the work of the devil. **tasks/**, **handlers/**, **defaults/**, **templates/** — separation of concerns as dogma.

04

Thou shalt encrypt thy secrets

Ansible Vault, or nothing. Never a key in cleartext, not even in staging, not even « just to test ».

05

Thou shalt hierarchize thy variables

defaults/ < **vars/** < **group_vars/** < **host_vars/** < **extra-vars**. Know the order, live by it.

06

Thou shalt pin thy collections

requirements.yml versioned, **ansible-galaxy install** in the CI. Version drift is the breeding ground of chaos.

07

Thou shalt name thy tasks

A clear **name:** is worth a thousand comments. Future-you will thank present-you at 3 AM.

08

With Molecule thou shalt test

An untested role does not exist. Docker driver locally, scenarios **default** and **verify**.

09

In check-mode and diff thou shalt validate

--check --diff before any **apply** in production. The dry-run is thy preventive repentance.

10

Thy inventory shall be dynamic

NetBox, Proxmox, AWS — never a static **hosts.ini** for living infrastructure. The source of truth is singular.