Работа с данными в Ansible

План

- Приоритеты переменных
- Разделение данных по разным слоям
- Работа с окружениями
- Секретные данные

Приоритеты переменных

- Повторение — мать учения
- Не стоит использовать все многообразие переменных

- **role defaults**
- inventory vars
- **inventory group_vars**
- inventory host_vars
- playbook group_vars
- playbook host_vars
- host facts
- **play vars**
- play vars_prompt - лучше прятать в vault
- **play vars_files**
- registered vars
- set_facts
- **role and include vars**
- **block vars (only for tasks in block)**
- task vars (only for the task)
- extra vars (always win precedence)

Role defaults

- Здесь описываются значения по-умолчанию для переменных ролей

- В остальных местах переменные уточняются для работы роли в определенном окружении

Переменные inventory

- Надо пользоваться или файлом inventory или group_vars, но не стоит их смешивать

- Мы не рекомендуем пользоваться host_vars без особой необходимости

- Роли лучше параметризовать явно, если нет отличий в окружениях

Окружения

```
├── dev
│   ├── group_vars
│   │   ├── all
│   │   ├── webserver
│   │   └── zabbix_server
│   └── inventory
├── production
│   ├── group_vars
│   │   ├── all
│   │   ├── webserver
│   │   └── zabbix_server
│   └── inventory
└── stage
    ├── group_vars
    │   ├── all
    │   ├── webserver
    │   └── zabbix_server
    └── inventory
```

- В environments должно лежать только то, что отличается для разных окружений

- Хосты не имеют никакого значения, важна лишь их группа (в идеале)

- Мы рекомендуем для каждого хоста одну группу и один плейбук для каждой группы

- Есть смысл иметь одну базовую роль для всех хостов (настройки ОС, мониторинга и т.д.)

- Ansible должен быть единственным “источником правды” для всех систем (мониторинг, логирование и т.д.)

- Все файлы, кроме секретного ключа ansible-vault, должны лежать в системе контроля версий

- Все секретные данные (сертификаты, логины, пароли и т.д.) лучше хранить в ansible-vault

- Административно решите, кто, когда и что будет менять, чтобы не мешать друг другу

Service Discovery

- После того, как у вас появляется 30-50 компонент, лучше использовать Service Discovery

- Consul / Etcd / ZooKeeper и т.д.

ansible-vault

- Консольная утилита для работы с секретными данными (сертификаты, приватные ключи и т.д.)

- Симметричное шифрование

- Переменные можно подключать через vars_files

- Ключи могут быть разными для разных окружений

- Для более сложных случаев пользуйтесь hashicorp vault и аналогами

```yaml
vars_files:
  - "{{inventory_dir}}/secrets.yml"

tasks:
  - name: Show secret var
    debug:
      var: secret_key
```

```
➜  practice cat environments/dev/secrets.yml
$ANSIBLE_VAULT;1.1;AES256
33623531666233626133653732366562333265633663334626363326165623562643135653463643033636639353434666431616165613366316165393337320a653531616263626433346662656363323164613339613439333262373563383534306630373563376138383233343361633233333165356363316638646361650a6365656664383635636631326332666561616331366663316430636131373164646535306532613663323933626139303135623338393630656362303138613900
➜  practice ansible-vault view environments/dev/secrets.yml
secret_key: asdf
➜  practice ansible-playbook vars.yml

PLAY [Ideal playbook] **********************************************************

TASK [Show secret var] *********************************************************
ok: [common] => {
    "secret_key": "asdf"
}

PLAY RECAP *********************************************************************
common                     : ok=1    changed=0    unreachable=0    failed=0
```