

Ansible Master

????????????????????

??????????

```
sudo apt install -y ansible sshpass dpkg-dev apt-utils git
```

??????????

```
sudo mkdir -p /opt/ansible
sudo chown $USER: /opt/ansible
cd /opt/ansible
mkdir -p inventory/production/group_vars playbooks roles/offline_packages/{tasks,defaults}
logs
git init
echo -e "logs/\n*.retry\n.vault_pass" > .gitignore
```

Файл **ansible.cfg**

ansible.cfg

```
cat > /opt/ansible/ansible.cfg <<'EOF'
[defaults]
inventory          = inventory/production/hosts.yml
roles_path         = roles
remote_user        = ansible
private_key_file    = ~/.ssh/ansible_ed25519
host_key_checking   = False
forks              = 20
retry_files_enabled = False
interpreter_python   = auto_silent
log_path           = logs/ansible.log

[privilege_escalation]
```

```
become          = True
become_method = sudo

[ssh_connection]
pipelining = True
EOF
```

Генерация SSH-ключа

```
ssh-keygen -t ed25519 -f ~/.ssh/ansible_ed25519 -N "" -C "ansible-master"
```

Генерация inventory файла

scan-inventory.sh

```
cat > /opt/ansible/scan-inventory.sh <<'EOF'
#!/bin/bash
# Использование: ./scan-inventory.sh [подсеть] [исключения]
set -euo pipefail
NET=${1:-192.168.10.0/24}
EXCLUDE=${2:-192.168.10.1}          # сам сервер и другие адреса через запятую
OUT=/opt/ansible/inventory/production/hosts.yml
TMP=$(mktemp)

[ -f "$OUT" ] && cp "$OUT" "$OUT.bak.$(date +%F_%H%M)"

nmap -n -p 22 --open --exclude "$EXCLUDE" -oG - "$NET" \
  | awk '/22\open/{print $2}' | sort -V > "$TMP"

{
  echo "all:"
  echo "  children:"
  echo "    astra_clients:"
  echo "    hosts:"
  while read -r ip; do
    echo "      pc-${ip//./-}: { ansible_host: $ip }"
  done < "$TMP"
} > "$OUT"
```

```
echo "Найдено хостов с SSH: $(wc -l < "$TMP") -> $OUT"
rm -f "$TMP"
EOF
chmod +x /opt/ansible/scan-inventory.sh
```

Запуск скрипта сканирования сети

```
/opt/ansible/scan-inventory.sh 192.168.10.0/24 192.168.10.1
```

???? bootstrap

Создаёт на клиентах пользователя `ansible` с ключом и `sudo`. Он выполняется один раз под `admin`.

bootstrap.yml

```
cat > playbooks/bootstrap.yml <<'EOF'
---
- name: Создать служебного пользователя ansible
  hosts: astra_clients
  become: true
  tasks:
    - name: Пользователь ansible
      ansible.builtin.user:
        name: ansible
        shell: /bin/bash
        create_home: true

    - name: Публичный ключ
      ansible.posix.authorized_key:
        user: ansible
        key: "{{ lookup('file', '~/ssh/ansible_ed25519.pub') }}"

    - name: sudo без пароля
      ansible.builtin.copy:
        dest: /etc/sudoers.d/ansible
        content: "ansible ALL=(ALL) NOPASSWD:ALL\n"
        mode: "0440"
```

```
validate: "visudo -cf %S"
```

```
EOF
```

?????? playbook

site.yml

```
cat > playbooks/site.yml <<'EOF'
---
# 1. Кто уже пускает под ansible
- name: Проверка доступа под учёткой ansible
  hosts: astra_clients
  gather_facts: false
  become: false
  tasks:
    - name: Проверить вход
      ansible.builtin.ping:
      ignore_unreachable: true
      register: access_check

    - name: Разложить хосты по группам access_ok / access_missing
      ansible.builtin.group_by:
        key: "access_{{ 'missing' if (access_check.unreachable | default(false)) else 'ok'
}}}"

# 2. Пароль admin спрашиваем только если есть новые ПК
- name: Запрос пароля admin
  hosts: localhost
  connection: local
  gather_facts: false
  become: false
  tasks:
    - name: Ввод пароля
      when: groups['access_missing'] | default([]) | length > 0
      block:
        - name: Пароль admin
          ansible.builtin.pause:
            prompt: "Пароль admin на новых клиентах ({{ groups['access_missing'] | length
```

```
}} шт.)"

    echo: false
    register: admin_pw

- name: Запомнить пароль на время прогона
  ansible.builtin.set_fact:
    bootstrap_password: "{{ admin_pw.user_input }}"
  no_log: true

# 3. Создание учётки ansible на новых ПК
- name: Bootstrap новых клиентов
  hosts: access_missing
  gather_facts: false
  become: true
  vars:
    ansible_user: admin
    ansible_password: "{{ hostvars['localhost'].bootstrap_password }}"
    ansible_become_password: "{{ hostvars['localhost'].bootstrap_password }}"
  roles:
    - bootstrap

# 4. Пакеты на всех
- name: Офлайн-установка пакетов
  hosts: astra_clients
  become: true
  serial: 10
  roles:
    - offline_packages

EOF
```

Revision #9

Created 2026-10-23 12:56:12 UTC by xeon

Updated 2026-10-23 17:47:53 UTC by xeon