ANSIBLE

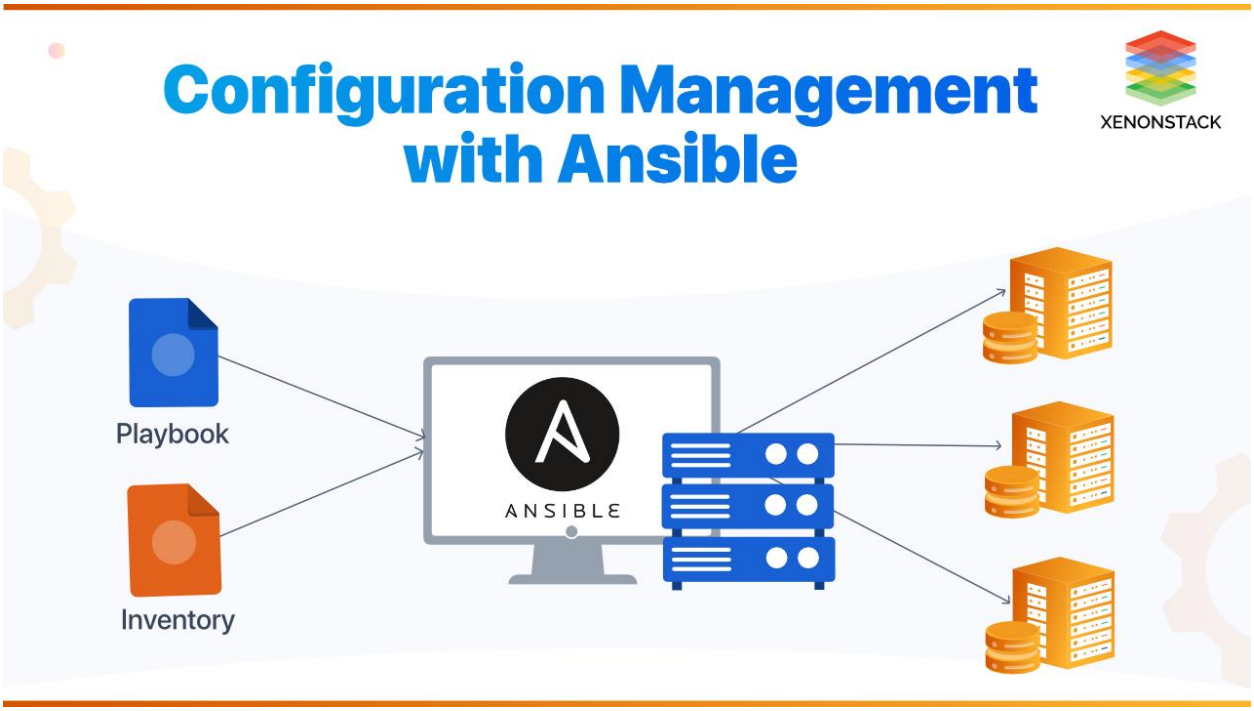
By:Mostafa Mahmoud Bahgat

LinkedIn:https://www.linkedin.com/in/mostafamahmoudbahgat

Ansible

ال ansible هي من ال Configuration Management tool وهي اني بعمل config بطريقه Automation

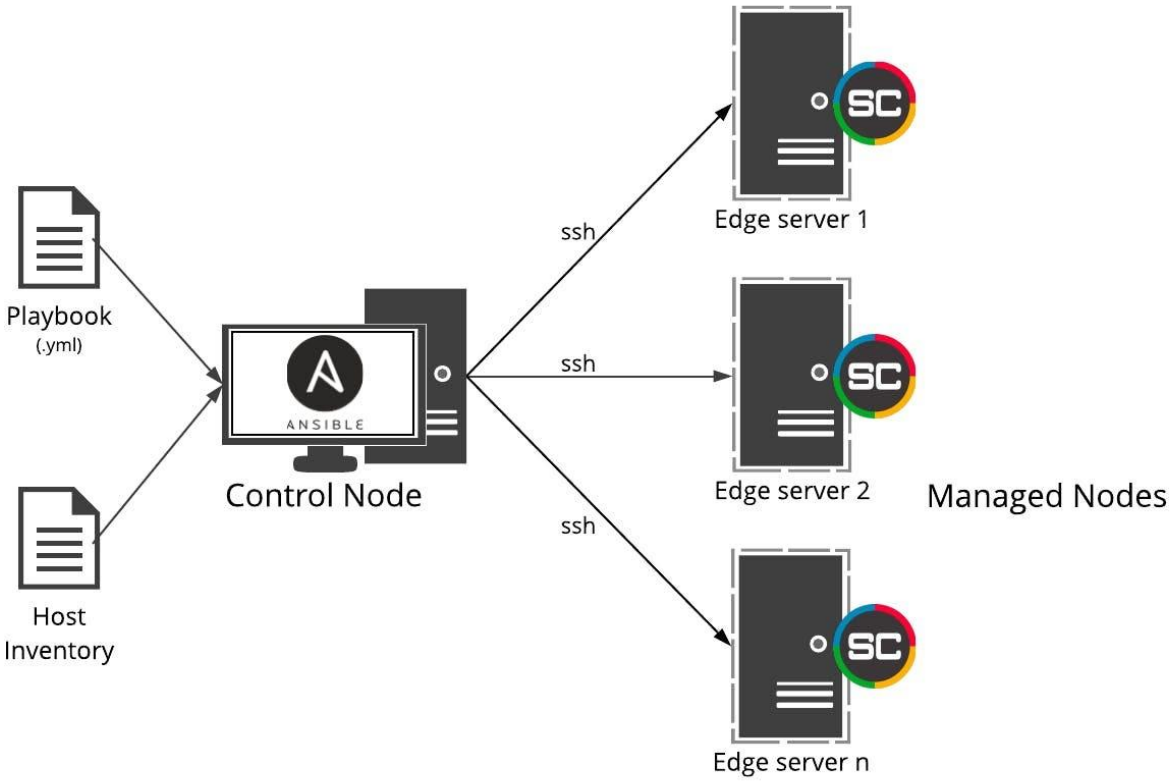
بنستخدم مع ال ansible برتوكول ال SSH



من مميزاتها:

- No Agent (Agentless) : مش بتحتاج منك انك تعمل install لاي agent عند ال client.
- Idempotent: هي ان لو عندي مثلا script ونفذته وعملت عليه أي تعديل وجيت انفذه تاني ال هيتم تنفيذه هو التغييرات ال حصلت ع الscript فقط
- Declarative: يعني بيقارن state ب state ودا عكس طريقه ال procedural ال هي line by line

infrastructure



Host Inventory	Playbook	Control Node	Edge server
دا ال file ال بيكون فيه ال hosts او ال servers ال عاوز اوصلها ال هي ال edge server	دا ال scrip بتاعي ال هكتبه وانفذ بيه ال tasks ال عاوزها	دا ال server ال عليه ال ansible ال هعمل عليه ال tasks ولازم يكون فيه ssh connectivity بينه وبين ال edge servre	دا ال server ال عاوز انفذ عليه ال Tasks

عشان ابدا اشتغل محتاج 4خطوات

1-اعمل install لل ansible

```
[root@ansible ~]# sudo dnf install -y ansible-core
Updating Subscription Management repositories.
Last metadata expiration check: 0:02:27 ago on Mon 15 Apr 2024 03:35:59 AM EDT.
Dependencies resolved.
================================================================================
 Package                 Architecture   Version              Repository                      Size
================================================================================
Installing:
 ansible-core            x86_64         1:2.14.9-1.el9       rhel-9-for-x86_64-appstream-rpms  2.6 M
Installing dependencies:
 git-core                x86_64         2.39.3-1.el9_2       rhel-9-for-x86_64-appstream-rpms  4.3 M
 python3-cffi            x86_64         1.14.5-5.el9         rhel-9-for-x86_64-baseos-rpms     257 k
 python3-cryptography    x86_64         36.0.1-4.el9         rhel-9-for-x86_64-baseos-rpms     1.2 M
 python3-packaging       noarch         20.9-5.el9           rhel-9-for-x86_64-appstream-rpms   81 k
 python3-ply             noarch         3.11-14.el9          rhel-9-for-x86_64-baseos-rpms     111 k
 python3-pycparser       noarch         2.20-6.el9           rhel-9-for-x86_64-baseos-rpms     139 k
 python3-pyparsing       noarch         2.4.7-9.el9          rhel-9-for-x86_64-baseos-rpms     154 k
 python3-resolvelib      noarch         0.5.4-5.el9          rhel-9-for-x86_64-appstream-rpms   38 k
 sshpass                 x86_64         1.09-4.el9           rhel-9-for-x86_64-appstream-rpms   30 k
```

```
[root@ansible ~]# ansible --version
ansible [core 2.14.9]
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3.9/site-packages/ansible
  ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/bin/ansible
  python version = 3.9.16 (main, Dec  8 2022, 00:00:00) [GCC 11.3.1 20221121 (Red Hat 11.3.1-4)] (/usr/bin/python3)
  jinja version = 3.1.2
  libyaml = True
```

2- هعمل create لل inventory hosts ودا ال file ال بيكون فيه ال hosts بتاعتي ال عاوز اوصلها عشان انفذ عليها ال tasks

وال directory default بتاعها بيكون ف ال /etc/ansible/hosts

- والأفضل نقسم ال file لل group وطريقه كتابته كالتالي

```
[root@ansible project1]# vim hosts
[root@ansible project1]# cat hosts
[webserver]
192.168.93.151
[DBserver]
192.168.93.150
[root@ansible project1]#
```

وبعد كدا ف ال playbook احدد group معينه واعمل عليها tasks معينه

3-اعمل create لل ansible.cfg ودا ال config بتاع ال ansible وبحدد فيها اكتر من حاجه

```
[root@ansible project1]# vim ansible.cfg
[root@ansible project1]# cat ansible.cfg
[defaults]

# some basic default values...

inventory      = ./hosts
remote_user    = mostafa
ask_pass       = false
roles_path     = ./roles
host_key_checking = false

# privilege user

[privilege_escalation]
become=True
become_method=sudo
become_user=root
become_ask_pass=False
[root@ansible project1]#
```

ال default ال حاجات ال بقول ال ansible استخدمها زي مكان ال inventory – ال user .

ال privilege عشان لما استخدم sudo مع مستخدم عادي ميطلبش مني ال password .

ملحوظة: اول cfg بيبص عليه هو ال directory ال انت واقف فيه – ثم لو ملقاش بيدور في ال home dir – لو ملقاش بيبص علي ال default ال هو /etc/ansible/ansible.cfg .

4- ssh connection Without password:

علي ال master هكتب ال comm دا ssh-keygen

```
[root@ansible ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:YUWZWqNwZ56uqAFdzmEo3hpmnQFCZN1PfOp0ySxQOgU root@ansible
The key's randomart image is:
+---[RSA 3072]----+
|++o .E+o .oo     |
|.. o ++o.oB      |
|  . ooBoBB.o     |
| . = B.Bo*o      |
|  * = = S.       |
| o +   .  .      |
|  . .  . .       |
|     .. .        |
|    ..           |
+----[SHA256]-----+
[root@ansible ~]#
```

ال هيحصل انه هينشا 2key ال public وال privet تحت المسار دا ~/.ssh

```
[root@ansible ~]# cd .ssh/
[root@ansible .ssh]# ls
id_rsa  id_rsa.pub
[root@ansible .ssh]#
```

فهاخد ال public

```
[root@ansible .ssh]# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDp
6nFMxPXyd9wIMmsSh2afSvQd0Klg6ZODIqxEIVHF
QgKjCQ2igDL4hdwBGIzdyr9r/g7O/nlNewT7ZVKe
MItG9cEEaknPPDkoIqNQcg2DR/ZY2zghyGsKBbSx
k53UEZOfsQavw6jeJUl6PUOhCCJOITZVyeMrTop+
9hidSvE7Cm+hU7cxCMiRCwOZ34T9kUzLXBwUgGuh
GDSHk+GwrIvqVtW6J1FarCjgV4sei8Ye62uZU+sJ
[root@ansible .ssh]#
```

واضعه عند ال client تحت ال .ssh/authorized_keys

```
[root@client ~]# vim .ssh/authorized_keys
[root@client ~]#
[root@client ~]#
[root@client ~]# cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDpo
xEIVHFGvflUWoEll9PHXfFHSnVG9gwZp7N8/OKiOh
a6h2DrB19A7JhccMItG9cEEaknPPDkoIqNQcg2DR/
6PUOhCCJOITZVyeMrTop+NtkuYOsBW9OsEvxa5/pf
wdFM/CShzgDVlLvIN0yXlAvYlMg7lqGDSHk+GwrIv
[root@client ~]#
```

ومهم اتاكد ان ال file معه permission (rw) وال dir معه permission (rwx)

```
[root@client .ssh]# ls -l
total 4
-rw-r--r--. 1 root root 566 Apr 15 04:54 authorized_keys
[root@client .ssh]# ls -ld
drwx------. 2 root root 29 Apr 15 04:54 .
[root@client .ssh]#
```

نعمل test عن طريق ال comm دا ودا بينفذلي امر واحد فقط

```
[root@ansible project1]# ansible webserver  -m shell -a 'id'
192.168.93.151 | CHANGED | rc=0 >>
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@ansible project1]#
```

علي ال host هتخلي ال user ال هتنفذ ال task دي بيه تخليها بصلاحيه ال root

```
## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
mostafa        ALL=(ALL)       NOPASSWD: ALL
```

ال playbook ودا ال script ال هنفذه علي ال client وبيكون عباره عن yml file

```
- name: Install the latest version of Apache
  ansible.builtin.yum:
    name: httpd
    state: lates
```

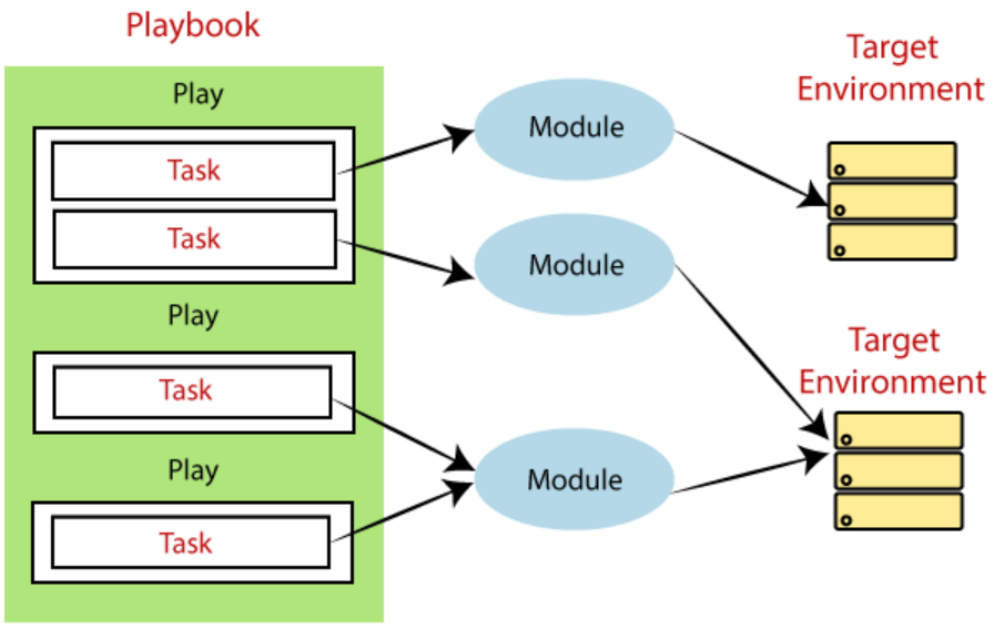
```
[root@ansible project1]# vim pb1.yml
[root@ansible project1]#
[root@ansible project1]#
[root@ansible project1]# cat pb1.yml
- name: Install the latest version of Apache
  ansible.builtin.yum:
    name: httpd
    state: lates


[root@ansible project1]#
```

كدا جهزت ال playbook هبدا اعمل run عن طريق الامر دا

```
[root@ansible project1]# ansible-playbook pb1.yml

PLAY [webserver] ***************************************************************************

TASK [Gathering Facts] *********************************************************************
ok: [192.168.93.151]

TASK [Install the latest version of Apache] ************************************************
changed: [192.168.93.151]

PLAY RECAP *********************************************************************************
192.168.93.151             : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0
gnored=0

[root@ansible project1]#
```

```
[root@ansible project1]# ansible webserver  -m shell -a 'systemctl start httpd'
192.168.93.151 | CHANGED | rc=0 >>

[root@ansible project1]# ansible webserver  -m shell -a 'systemctl status httpd'
192.168.93.151 | CHANGED | rc=0 >>
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2024-04-15 06:39:11 EDT; 7s ago
       Docs: man:httpd.service(8)
   Main PID: 35076 (httpd)
     Status: "Started, listening on: port 80"
      Tasks: 213 (limit: 21556)
     Memory: 37.3M
        CPU: 147ms
     CGroup: /system.slice/httpd.service
             ├─35076 /usr/sbin/httpd -DFOREGROUND
             ├─35078 /usr/sbin/httpd -DFOREGROUND
             ├─35079 /usr/sbin/httpd -DFOREGROUND
             ├─35080 /usr/sbin/httpd -DFOREGROUND
             └─35081 /usr/sbin/httpd -DFOREGROUND

Apr 15 06:39:09 client systemd[1]: Starting The Apache HTTP Server...
Apr 15 06:39:10 client httpd[35076]: AH00558: httpd: Could not reliably determine the server's fully quali
fied domain name, using fe80::20c:29ff:fed7:8e78%ens160. Set the 'ServerName' directive globally to suppre
ss this message
Apr 15 06:39:11 client httpd[35076]: Server configured, listening on: port 80
Apr 15 06:39:11 client systemd[1]: Started The Apache HTTP Server.
[root@ansible project1]#
```

- اقدر اعمل اكتر من play داخل ال playbook



ملحوظه : لو عاوز vim يظبتلك المسافات وانت بتكب ال yml file هتعمل الخطوات دي

1- هتفتح ال file دا

```
[root@client ~]# vim ~/.vimrc
```

2- هتكتب السطر دا

```
autocmd FileType yaml setlocal ai ts=2 sw=2 et
```

هنا بقوله لما يبقي نوع file يكون yml خلي المسافة الواحدة تساوي مسافتين ف بتسهل عليا ف الكتابة شويا

ال Ansible Ad Hoc : من خلاله اقدر استخدم module واحد فقط ع عكس ال playbook ال من خلاله بقدر استخدم اكتر من module

وبتتكتب بالطريق دي

```
$ ansible [pattern] -m [module] -a "[module options]"
```

	Host Group	Module	Arguments to the module
ansible	webserver	-m yum	-a "name=httpd state=latest"
ansible	allservers	-m shell	-a " find /opt/oracle -type f -mtime +10 -name '*.log' "
ansible	appserver	-m user	-a "name=saravak group=admins append=yes shell=/bin/bash"

```
[root@ansible project1]# ansible webserver  -m shell -a 'id'
192.168.93.151 | CHANGED | rc=0 >>
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@ansible project1]#
```

هنا بستخدم ال module ال اسمها Shell عشان انفذ task معين علي ال host group ال اسمها webserver في ال inventory file

---

: Variables

بيتم كتابه ال variables كدا "{{var}}"

فيه طريقتين عشان استخدم ال Variables اول طريقه هي اني هكتبها في ال playbook بتاعي بالشكل دا

```
- hosts: webserver
  vars:
    - user: user1
      home: /home/user1
```

ودي مش الطريقه ال recommend

الطريقه التانية وال هي الطريقه ال recommend

هي انك تعمل file منفصل لل var ويكون yml file برضو بالطريقه دي

1- هتعمل create yml fail

```
vim vars_users.yml
```

2- هتكتب بداخله ال Variables ال انت عاوزها بالشكل دا

```
user: user1
home: /home/user1
```

3-هتكتب اسم ال file ال فيه ال Variables في ال playbook بشكل دا

```
- hosts: webserver
  vars_files:
    - vars_users.yml
```

لازم تكتب اسم ال file صح وهتلاقي الدنيا اشتغلت بكل سهوله

```
[root@ansible project1]# ansible-playbook adduser.yml

PLAY [webserver] ***************************************************************************************

TASK [Gathering Facts] *********************************************************************************
ok: [1[redacted]1]

PLAY RECAP *********************************************************************************************
[redacted]                 : ok=1    changed=0    unreachable=0    failed=0    skipped=0    rescued=0
  ignored=0

[root@ansible project1]#
```

وال Variables فيه نوعين

List Variables	Dictionary Variables

بتكون عبارة عن list بالشكل دا
`region:`
`- northeast`
`- southeast`
`- midwest`
او عباره عن Key بالشكل دا
`region: "{{ region[0] }}"`
	بيكون عباره عن Value بالشكل دا
	`foo:`
	`field1: one`
	`field2: two`

ال Facts

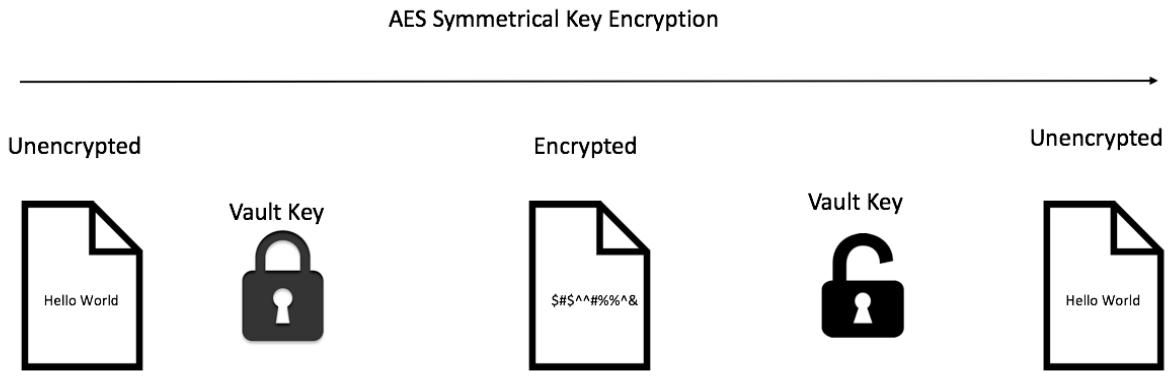
```
TASK [Gathering Facts]
ok: [192.168.93.151]
```

هي تعتبر Variables بيجمع معلومات عن ال host قبل تنفيذ ال task فلو انت مش محتاجها اقفلها لانها بتستهلك CPU وRAM

واعرف المعلومات ال جمعها عن طريق الامر دا

```
[root@ansible project1]# ansible webserver  -m setup
192.168.93.151 | SUCCESS => {
    "ansible_facts": {
        "ansible_all_ipv4_addresses": [
            "192.168.93.151"
        ],
        "ansible_all_ipv6_addresses": [
            "fe80::20c:29ff:fed7:8e78"
        ],
        "ansible_apparmor": {
            "status": "disabled"
        },
        "ansible_architecture": "x86_64",
        "ansible_bios_date": "11/12/2020",
        "ansible_bios_vendor": "Phoenix Technologies LTD",
        "ansible_bios_version": "6.00",
        "ansible_board_asset_tag": "NA",
        "ansible_board_name": "440BX Desktop Reference Platform",
        "ansible_board_serial": "None",
        "ansible_board_vendor": "Intel Corporation",
        "ansible_board_version": "None",
        "ansible_chassis_asset_tag": "No Asset Tag",
        "ansible_chassis_serial": "None",
```

: Ansible Vault



هي tool من خلالها بعمل encrypt ل file ولكن عندي file فيه password فمن خلال ال vault اقدر اعمل encrypt لل file دا بالطريقه دي

1- هعمل create file بال vault

```
[root@ansible ~]# ansible-vault create pass.yml
New Vault password:
Confirm New Vault password:
```

بيطلب مني password لل file بكتبه وبعدين بيفتحلي ال file عشان اكتب ال انا محتاج اكتبه

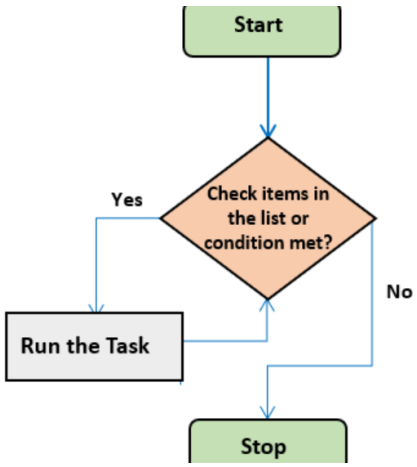
2- لو عملت cat لل file داه يظهر انه encrypt بالطريقه دي

```
[root@ansible ~]# cat pass.yml
$ANSIBLE_VAULT;1.1;AES256
38353266643662383735346636633532383062663164363062656436636534616630363962663335
35363164316463306332636566636536343037336439323 70a6330373139366532656465666316535
31366430373965303265653037643334663963363734663936623163393936306234373134633030
61313637393430333 50a39316630346232643033656264636636356133653661326364383039386 2
3964
[root@ansible ~]#
```

3- لو محتاج انك تعرض الداتا دي هتكون بالطريقه دي فالاول هيطلب منك ال password بتاع ال file اول م تكتبه هيعرض الداتا

```
[root@ansible ~]# ansible-vault view pass.yml
Vault password:
hello
[root@ansible ~]#
```

: Ansible Loops



بستخدم ال loop في حاله اني محتاج اعمل تكرار لل task وليكن مثلا محتاج اعمل 2user فالطريقه العادية من غير ال loop هتكون بالشكل دا

```yaml
- name: Add user testuser1
  ansible.builtin.user:
    name: "testuser1"
    state: present
    groups: "wheel"

- name: Add user testuser2
  ansible.builtin.user:
    name: "testuser2"
    state: present
    groups: "wheel"
```

اني هعمل 2task لكل user هعمل task لوحدها

لكن هنا ممكن استخدم ال loop بحيث بدل م اعمل 2task لا اعمل task واحده واعمل loop تكرر ال task مره ب اسم اول user ومره ب اسم تاني user بالشكل دا

```yaml
- name: Add several users
  ansible.builtin.user:
    name: "{{ item }}"
    state: present
    groups: "wheel"
  loop:
     - testuser1
     - testuser2
```

هنا عملت task واحده هيجي ينفذ هيشيل ال var ال اسمه item ويضع مكانه testuser1 ويكرر ال task ويشيل ال var ويضع مكانه testuser2

Ansible Conditionals : بقدر من خلالها احدد شرط معين بناءا عليه يعمل run لل task ولو الشرط متحققش يعمل skip لل task دا

```yaml
tasks:
  - name: Configure SELinux to start mysql on any port
    ansible.posix.seboolean:
      name: mysql_connect_any
      state: true
      persistent: true
    when: ansible_selinux.status == "enabled"
```

هنا عملت شرط عشان ال task تتنفذ وهو ان لاوم ال selinux status تكون enabled

```yaml
tasks:
  - name: Shut down Debian flavored systems
    ansible.builtin.command: /sbin/shutdown -t now
    when: ansible_facts['os_family'] == "Debian"
```

هنا برضو بقوله عشان تنفذ ال task دي لازم يكون ال os بتاعي يكون Debian طب لو مش Debian مش هينفذ ال task وقدر اضع اكتر من شرط واستخدم ال And-or-not

```yaml
- hosts: all
  become: true
  tasks:
  - name: update repository index Ubuntu
    apt:
      update_cache: yes
    when: ansible_distribution == "Ubuntu"

  - name: update repository index Centos
    yum:
      update_cache: yes
    when: ansible_distribution == "CentOS"
```

هنا مثلا برضو بقوله استخدم ال pakg ال اسمها apt لو ال os كان ubuntu او yum لو ال os كان centos

---

Ansible Handlers : من خلالها بحدد ان task معينه يتعملها run بناءا علي task تانيه

مثال: عندي مثلا ال Apache لما بيحصل عليه علي تعديل بيطلب restart لل service ف بدل م اعمل task لل restart ويحصل restart عطول لما اعمل run لل task لا هعمل handlers وهعمله notify بعد task ميعنه لما يحصل فيها أي change لل ntify دا يبدا يشغل ال handlers .

```yaml
---
- name: Verify apache installation
  hosts: webservers
  vars:
    http_port: 80
    max_clients: 200
  remote_user: root
  tasks:
    - name: Ensure apache is at the latest version
      ansible.builtin.yum:
        name: httpd
        state: latest

    - name: Write the apache config file
      ansible.builtin.template:
        src: /srv/httpd.j2
        dest: /etc/httpd.conf
      notify:
        - Restart apache

    - name: Ensure apache is running
      ansible.builtin.service:
        name: httpd
        state: started

  handlers:
    - name: Restart apache
      ansible.builtin.service:
        name: httpd
        state: restarted
```

فلما يحصل أي تغيير ف ال task ال اسمها write the apache config file ال notifyi هتستدعي ال handlers ال اسمها restart apache ال هي بتعمل restart لل service ال اسمها httpd

-ال error handling : ببساطه دي handler بنستخدمها مع ال task عشان لو ال task دي فيها error او هيحصلها failed ال playbook تكمل باقي ال task عادي وبيحصلش failed لل playbook كله

اسمها ignore_errors وبستخدمها بالشكل دا

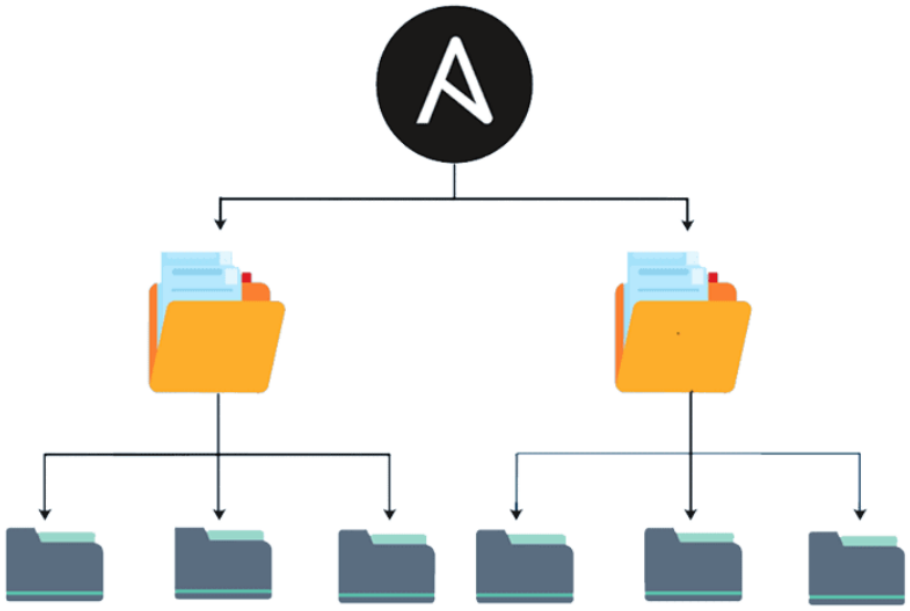
```
- name: Do not count this as a failure
  ansible.builtin.command: /bin/false
  ignore_errors: true
```

ملحوظة : ال command دا /bin/false انا بقول ال shell انه يطلعلي error

-يوجد أيضا handler اخري تسمي ignore_unreachable ممكن استخدمها ف حاله ان لو عارف ان host من ال عندي واقع او فيه مشكله مخليه ال ansible مش هيقدر يوصله وبتكون بالشكل دا

```
- name: This executes, fails, and the failure is ignored
  ansible.builtin.command: /bin/true
  ignore_unreachable: true
```

: Ansible Roles



الهدف منها اني بقلل ال playbook بتاعي بمعني اني بمعل directory لكل حاجه عندي واعمل main.yml تحت كل dir ال

- ال Ansible Galaxy : هو community زي ال GitHub كدا الناس بتنزل عليه ال roles ال بتعملها

ودي ال command ال اكتر استخدمها مع ال galaxy

```
[root@ansible ~]# ansible-galaxy --h
usage: ansible-galaxy role [-h] ROLE_ACTION ...

positional arguments:
  ROLE_ACTION
    init        Initialize new role with the base structure of a role.
    remove      Delete roles from roles_path.
    delete      Removes the role from Galaxy. It does not remove or alter the actual GitHub repository.
    list        Show the name and version of each role installed in the roles_path.
    search      Search the Galaxy database by tags, platforms, author and multiple keywords.
    import      Import a role into a galaxy server
    setup       Manage the integration between Galaxy and the given source.
    info        View more details about a specific role.
    install     Install role(s) from file(s), URL(s) or Ansible Galaxy

optional arguments:
  -h, --help    show this help message and exit
[root@ansible ~]#
```

مثال : هنعمل role وهنشوف ازاي هتكون عمليه منظمة جدا

1- هعمل role ب اسم mywebserver بالطريقه دي

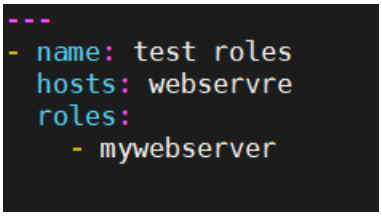
```
[root@ansible ~]# ansible-galaxy init mywebserver
- Role mywebserver was created successfully
```

2- لما اعمل tree هيكون هو قسم كل حاجه ممكن احتاجها بالطريقه دي

```
[root@ansible ~]# cd mywebserver/
[root@ansible mywebserver]#
[root@ansible mywebserver]#
[root@ansible mywebserver]#
[root@ansible mywebserver]# ls
defaults  files  handlers  meta  README.md  tasks  templates  tests  vars
[root@ansible mywebserver]# tree
.
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── main.yml
├── README.md
├── tasks
│   └── main.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml

8 directories, 8 files
```

وتحت كل main.yml اشوف هي تخص أي واكتب ال انا محتاجه فيها

3- هبدا اعمل ال playbook بتاعي باطريقه دي



ال roles ال هي mywebserver ال انا انشائتها فوق وتحتها كل حاجه كنا بنكتبها في ال playbook

---

By: Mostafa Mahmoud Bahgat

LinkedIn:https://www.linkedin.com/in/mostafamahmoudbahgat