

## Task – 27

### ANSIBLE ROLES AND VAULTS

#### **Ansible roles:**

Ansible roles are the primary mechanism for organizing and packaging related automation content (tasks, variables, files, templates, and handlers) into a reusable and modular structure. They help in breaking down large, complex playbooks into smaller, manageable, and shareable components, following the principle of separation of concerns.

#### **Standard Directory Structure**

When you create a new role (often using the `ansible-galaxy role init [role_name]` command), Ansible sets up a specific directory structure. Ansible automatically looks for a `main.yml` file within each of these standard directories.

- **tasks/** - Contains the main list of tasks executed by the role (`main.yml`).
- **handlers/** - Stores handlers that run only when notified (for example, restarting a service after configuration changes).
- **defaults/** - Holds low-priority default variables that can be easily overridden.
- **vars/** - Contains high-priority variables, mainly for internal role usage and harder to override.
- **files/** - Stores static files that are copied directly to target hosts without modification.
- **templates/** - Contains Jinja2 template files used to generate dynamic configuration files.
- **meta/** - Defines role metadata such as author, license, supported platforms, and role dependencies.
- **library/** - Includes custom Ansible modules specific to the role (optional and advanced).

## Creating 3 instance both control and managed nodes

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances (selected), Images, and Elastic Block Store. The main area displays a table of instances. The first instance, 'control\_node' (i-0025044b66fdc3c92), is selected and highlighted with a blue border. It has an 'Instance ID' of i-0025044b66fdc3c92, is 'Running', and is a 't3.micro' type. The second and third instances are 'managed\_node' instances, also running and of type 't3.micro'. Below the table, a detailed view for the selected 'control\_node' instance is shown, including its Public IPv4 address (44.202.220.213) and Private IPv4 address (172.31.4.5).

## Installing pip and ansible in control node

```
ec2-user@ip-172-31-4-5:~$ 
[ec2-user@ip-172-31-4-5:~$ login as: ec2-user
[ec2-user@ip-172-31-4-5:~$ Authenticating with public key "my_ans" from agent
[ec2-user@ip-172-31-4-5:~$ 
[ec2-user@ip-172-31-4-5:~$ Amazon Linux 2023
[ec2-user@ip-172-31-4-5:~$ 
[ec2-user@ip-172-31-4-5:~$ https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-4-5:~$ 
[ec2-user@ip-172-31-4-5:~$ wget https://raw.githubusercontent.com/ansible/ansible/stable-2.11/examples/ansible.cfg
[ec2-user@ip-172-31-4-5:~$ wget https://raw.githubusercontent.com/ansible/ansible/stable-2.11/examples/ansible.cfg
[ec2-user@ip-172-31-4-5:~$ Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
[ec2-user@ip-172-31-4-5:~$ Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
[ec2-user@ip-172-31-4-5:~$ HTTP request sent, awaiting response... 200 OK
[ec2-user@ip-172-31-4-5:~$ Length: 20353 (20K) [text/plain]
[ec2-user@ip-172-31-4-5:~$ Saving to: 'ansible.cfg'
[ec2-user@ip-172-31-4-5:~$ 
[ec2-user@ip-172-31-4-5:~$ ansible.cfg
[ec2-user@ip-172-31-4-5:~$ 100%[=====] 19.88K --.-KB/s   in 0s
[ec2-user@ip-172-31-4-5:~$ 2025-12-29 13:54:27 (144 MB/s) - 'ansible.cfg' saved [20353/20353]
[ec2-user@ip-172-31-4-5:~$ 
[ec2-user@ip-172-31-4-5:~$ vi inventory.txt
[ec2-user@ip-172-31-4-5:~$ ls
[ec2-user@ip-172-31-4-5:~$ ansible.cfg inventory.txt
[ec2-user@ip-172-31-4-5:~$ sudo yum install pip
[ec2-user@ip-172-31-4-5:~$ Last metadata expiration check: 0:04:35 ago on Mon Dec 29 13:50:44 2025.
[ec2-user@ip-172-31-4-5:~$ Package python3-pip-21.3.1-2.amzn2023.0.14.noarch is already installed.
[ec2-user@ip-172-31-4-5:~$ Dependencies resolved.
[ec2-user@ip-172-31-4-5:~$ Nothing to do.
[ec2-user@ip-172-31-4-5:~$ Complete!
[ec2-user@ip-172-31-4-5:~$ pip install ansible
[ec2-user@ip-172-31-4-5:~$ Defaulting to user installation because normal site-packages is not writeable
[ec2-user@ip-172-31-4-5:~$ Collecting ansible
[ec2-user@ip-172-31-4-5:~$   Downloading ansible-8.7.0-py3-none-any.whl (48.4 MB)
[ec2-user@ip-172-31-4-5:~$     48.4 MB 209 kB/s
[ec2-user@ip-172-31-4-5:~$ Collecting ansible-core==2.15.7
[ec2-user@ip-172-31-4-5:~$   Downloading ansible_core-2.15.13-py3-none-any.whl (2.3 MB)
[ec2-user@ip-172-31-4-5:~$     2.3 MB 70.1 kB/s
[ec2-user@ip-172-31-4-5:~$ Collecting resolvelib<1.1.0,>=0.5.3
[ec2-user@ip-172-31-4-5:~$   Downloading resolvelib-1.0.1-py2.py3-none-any.whl (17 kB)
[ec2-user@ip-172-31-4-5:~$ Collecting jinjate2<3.1.0,>=2.11.3
[ec2-user@ip-172-31-4-5:~$   Downloading jinjate2-3.1.6-py3-none-any.whl (134 kB)
[ec2-user@ip-172-31-4-5:~$     134 kB 84.2 kB/s
[ec2-user@ip-172-31-4-5:~$ Collecting packaging
[ec2-user@ip-172-31-4-5:~$   Downloading packaging-25.0-py3-none-any.whl (66 kB)
[ec2-user@ip-172-31-4-5:~$     66 kB 8.9 kB/s
```

## Creating a role using ansible galaxy command:

```
[root@ip-172-31-4-5- ~]# ansible-galaxy init newrole
Requirement already satisfied: cryptography in /usr/lib64/python3.9/site-packages (from ansible-core==2.15.7->ansible) (36.0.1)
Collecting importlib-resources==5.1.5
  Downloading importlib_resources-5.1.5-py3-none-any.whl (24 kB)
Requirement already satisfied: PyYAML>=5.1 in /usr/lib64/python3.9/site-packages (from ansible-core==2.15.7->ansible) (5.4.1)
Collecting MarkupSafe==2.0
  Downloading MarkupSafe-2.0-py3.9-cp39-manylinux2014_x86_64.manylinux_2_27_x86_64.manylinux_2_29_x86_64.whl (30 kB)
Requirement already satisfied: cffi>=1.12 in /usr/lib64/python3.9/site-packages (from cryptography->ansible-core==2.15.7->ansible) (1.14.5)
Requirement already satisfied: pycparser in /usr/lib/python3.9/site-packages (from cffi>=1.12->cryptography->ansible-core==2.15.7->ansible) (2.20)
Requirement already satisfied: ply==3.11 in /usr/lib/python3.9/site-packages (from pycparser->cffi>=1.12->cryptography->ansible-core==2.15.7->ansible) (3.11)
Installing collected packages: MarkupSafe, resolvelib, packaging, jinja2, importlib-resources, ansible-core, ansible
  Successfully installed MarkupSafe-3.0.3 ansible-6.7.0 ansible-core-2.15.13 importlib-resources-5.0.7 jinja2-3.1.6 packaging-25.0 resolvelib-1.0.1
[ec2-user@ip-172-31-4-5- ~]# ls
ansible.cfg  inventory.txt
[ec2-user@ip-172-31-4-5- ~]# ansible.cfg
Role newrole was created successfully
[ec2-user@ip-172-31-4-5- ~]# cat inventory.txt
[ec2-user@ip-172-31-4-5- ~]# cd newrole
[ec2-user@ip-172-31-4-5- newrole]$ ls
README.md  default  files  handlers  meta  tasks  templates  tests  vars
[ec2-user@ip-172-31-4-5- newrole]$ sudo yum install tree
Last metadata expiration check: 0:09:38 ago on Mon Dec 29 29 13:50:44 2025.
Dependencies resolved.
-----  


| Package                                                 | Architecture | Version              | Repository  | Size |
|---------------------------------------------------------|--------------|----------------------|-------------|------|
| <b>Installing:</b>                                      |              |                      |             |      |
| tree                                                    | x86_64       | 1.8.0-6.amzn2023.0.2 | amazonlinux | 56 k |
| <b>Transaction Summary</b>                              |              |                      |             |      |
| Install 1 Package                                       |              |                      |             |      |
| Total download size: 56 k                               |              |                      |             |      |
| Installed size: 56 k                                    |              |                      |             |      |
| Is this ok? [y/N]:                                      |              |                      |             |      |
| Downloading Packages:                                   |              |                      |             |      |
| tree-1.8.0-6.amzn2023.0.2.x86_64.rpm                    |              |                      |             |      |
| -----                                                   |              |                      |             |      |
| total 1.2 MB/s   56 kB 00:00                            |              |                      |             |      |
| 678 kB/s   56 kB 00:00                                  |              |                      |             |      |
| -----                                                   |              |                      |             |      |
| tx0\$                                                   |              |                      |             |      |
| running transaction check                               |              |                      |             |      |
| Transaction check succeeded.                            |              |                      |             |      |
| Running transaction test                                |              |                      |             |      |
| Transaction test succeeded.                             |              |                      |             |      |
| Running transaction                                     |              |                      |             |      |
| Preparing transaction: 1/1                              |              |                      |             |      |
| Installing : tree-1.8.0-6.amzn2023.0.2.x86_64 1/1       |              |                      |             |      |
| Running scriptlet: tree-1.8.0-6.amzn2023.0.2.x86_64 1/1 |              |                      |             |      |


```

## Code should store into rolee.yaml:

```
name: Install Java 17 on Amazon
Linux hosts: all
become: yes
roles:
  - newrole
```

## Code should store into main.yaml file and download java:

```
# tasks file for newrole
- name: Update yum
  packages yum:
    name: "*"
    state:
      latest
- name: Install Java 17 (Amazon Corretto) yum:
  name: java-17-amazon-corretto
  state: present
- name: Verify Java
  installation command: java
  -version register:
    java_output ignore_errors:
      yes
- name: Show Java
  version debug:
    var: java_output.stderr
```

```
ec2-user@ip-172-31-4-5:~$ ls
└── main.yml

ec2-user@ip-172-31-4-5:~$ cd ..
[ec2-user@ip-172-31-4-5 ~]$ pwd
/home/ec2-user
[ec2-user@ip-172-31-4-5 ~]$ ls
ansible.cfg  inventory.txt  newrole  rolee.yaml
[ec2-user@ip-172-31-4-5 ~]$ cat newrole
[ec2-user@ip-172-31-4-5 ~]$ cat rolee.yaml
README.md  defaults  files  handlers  meta  tasks  templates  tests  vars
[ec2-user@ip-172-31-4-5 ~]$ cd tasks
[ec2-user@ip-172-31-4-5 tasks]$ ls
main.yml
[ec2-user@ip-172-31-4-5 tasks]$ nano main.yml
[ec2-user@ip-172-31-4-5 tasks]$ cd ..
[ec2-user@ip-172-31-4-5 ~]$ cd ..
[ec2-user@ip-172-31-4-5 ~]$ ls
ansible.cfg  inventory.txt  newrole  rolee.yaml
[ec2-user@ip-172-31-4-5 ~]$ ansible-playbook -i inventory.txt rolee.yaml

PLAY [Install Java 17 on Amazon Linux] ****
*****
*
* TASK [Gathering Facts] ****
*
The authenticity of host '172.31.11.29 (172.31.11.29)' can't be established.
ED25519 key fingerprint is SHA256:KhVyaAbhKURKBTgZl2bEUFg+qSBzAm87jPQut20wf+o.
This key is not known by any other names
The authenticity of host '172.31.5.168 (172.31.5.168)' can't be established.
ED25519 key fingerprint is SHA256:FfjxL7/yStIly95gNv0JdzttVUDlrcyehGDShnImU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
[WARNING]: Platform linux on host 172.31.11.29 is using the discovered Python
interpreter at /usr/bin/python3.9, but future installation of another Python
interpreter could change the meaning of that path. See
https://docs.ansible.com/ansible
core/2.15/reference_appendices/interpreter_discovery.html for more information.
ok: [172.31.11.29]
```

**Then run the yaml file(playbook):**

**Command:** ansible-playbook -l inventory.txt rolee.yaml

```
[ec2-user@ip-172-31-4-5 ~]$ ansible-playbook -i inventory.txt role.yml

PLAY [Install Java 17 on Amazon Linux] *****

TASK [Gathering Facts] *****
[WARNING]: Platform linux on host 172.31.5.168 is using the discovered Python interpreter at /usr/bin/python3.9, but future installation of another Python interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.15/reference_appendices/interpreter_discovery.html for more information.
ok: [172.31.5.168]

[WARNING]: Platform linux on host 172.31.11.29 is using the discovered Python interpreter at /usr/bin/python3.9, but future installation of another Python interpreter could change the meaning of that path. See https://docs.ansible.com/ansible-core/2.15/reference_appendices/interpreter_discovery.html for more information.
ok: [172.31.11.29]

TASK [newrole : Update yum packages] *****
ok: [172.31.5.168]
ok: [172.31.11.29]

TASK [newrole : Install Java 17 (Amazon Corretto)] *****
ok: [172.31.11.29]
changed: [172.31.5.168]

TASK [newrole : Verify Java installation] *****
changed: [172.31.11.29]
changed: [172.31.5.168]

TASK [newrole : Show Java version] *****
ok: [172.31.5.168] => {
    "java_output.stderr": "openjdk version \"17.0.17\" 2025-10-21 LTS\\nOpenJDK Runtime Environment Corretto-17.0.17.10.1 (build 17.0.17+10-LTS)\\nOpenJDK 64-Bit Server VM Corretto-17.0.17.10.1 (build 17.0.17+10-LTS, mixed mode, sharing)"
}
ok: [172.31.11.29] => {
    "java_output.stderr": "openjdk version \"17.0.17\" 2025-10-21 LTS\\nOpenJDK Runtime Environment Corretto-17.0.17.10.1 (build 17.0.17+10-LTS)\\nOpenJDK 64-Bit Server VM Corretto-17.0.17.10.1 (build 17.0.17+10-LTS, mixed mode, sharing)"
}

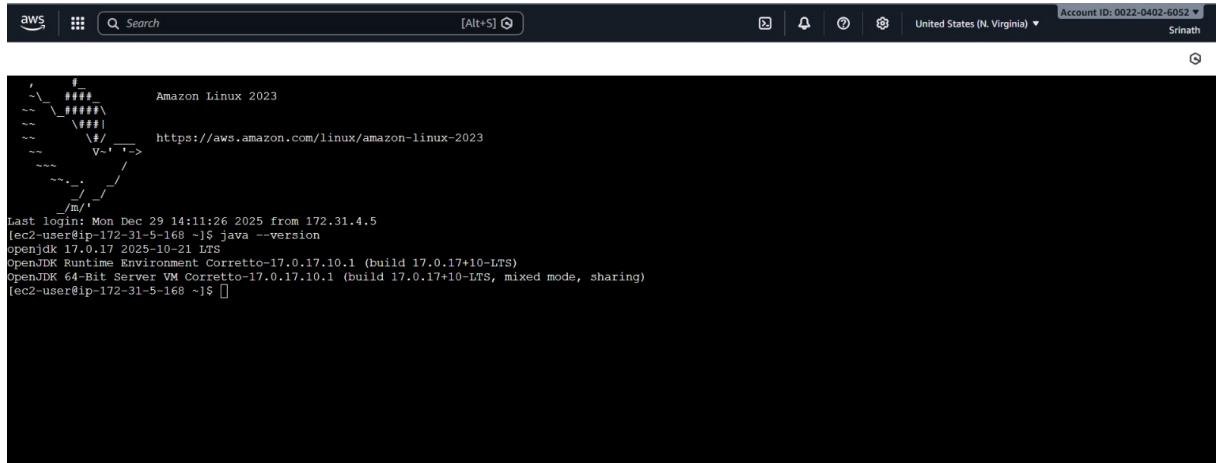
PLAY RECAP *****
172.31.11.29 : ok=5    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
172.31.5.168 : ok=5    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

[ec2-user@ip-172-31-4-5 ~]$
```

**Checking whether java is installed in managed nodes...**

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

Last login: Mon Dec 29 14:11:26 2025 from 172.31.4.5
[ec2-user@ip-172-31-11-29 ~]$ java --version
openjdk 11.0.17 2025-10-21 LTS
OpenJDK Runtime Environment Corretto-17.0.17.10.1 (build 17.0.17+10-LTS)
OpenJDK 64-Bit Server VM Corretto-17.0.17.10.1 (build 17.0.17+10-LTS, mixed mode, sharing)
[ec2-user@ip-172-31-11-29 ~]$ [ ]
```



AWS CloudShell terminal window showing a Java version check on Amazon Linux 2023. The terminal output includes a welcome banner, system information, and a Java --version command.

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

Last login: Mon Dec 29 14:11:26 2025 from 172.31.4.5
[ec2-user@ip-172-31-5-168 ~]$ java --version
openjdk 17.0.17 2025-10-21 LTS
OpenJDK Runtime Environment Corretto-17.0.17.10.1 (build 17.0.17+10-LTS)
OpenJDK 64-Bit Server VM Corretto-17.0.17.10.1 (build 17.0.17+10-LTS, mixed mode, sharing)
[ec2-user@ip-172-31-5-168 ~]$ 
```

i-09a293f822501fdcb (managed\_node) X

Public IPs: 98.80.136.147 Private IPs: 172.31.5.168

[CloudShell](#) [Feedback](#) [Console Mobile App](#) © 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

## Ansible vaults:

Ansible Vault is a built-in Ansible feature that encrypts sensitive data, like passwords, API keys, and tokens, within Ansible files (playbooks, variables) to prevent them from being stored in plain text, allowing secure management of secrets alongside automation code, with operations like encryption, decryption, viewing, and editing handled by a password. It uses AES256 encryption and ensures that even if someone gets the file, the secrets remain unreadable without the correct password, making it safe for version control systems like Git.



```
[ec2-user@ip-172-31-4-5 ~]$ ansible-vault encrypt rolee.yaml
New Vault password:
Confirm New Vault Password:
Encryption successful
[ec2-user@ip-172-31-4-5 ~]$ 
```