

Task – 27

ANSIBLE ROLES AND VAULTS

Ansible roles:

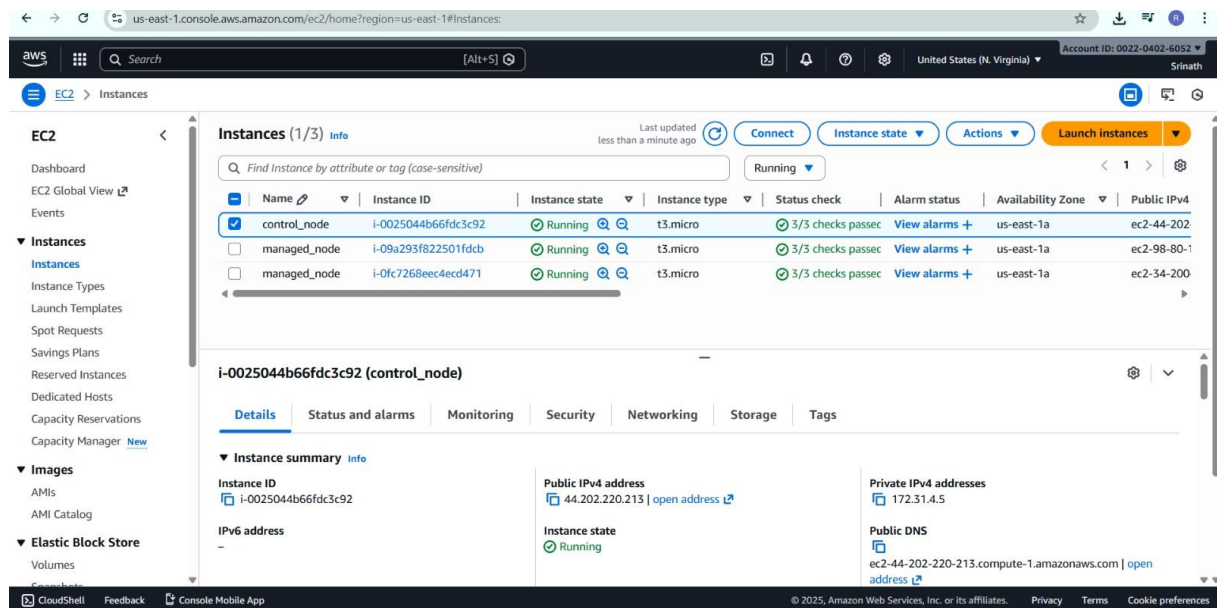
Ansible roles are the primary mechanism for organizing and packaging related automation content (tasks, variables, files, templates, and handlers) into a reusable and modular structure. They help in breaking down large, complex playbooks into smaller, manageable, and shareable components, following the 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 Management Console for the 'us-east-1' region. The 'Instances' page displays three EC2 instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
control_node	i-0025044b666fdc3c92	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-44-202
managed_node	i-09a293f822501fdb	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-98-80-1
managed_node	i-0fc7268eec4ecd471	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-34-200

The 'control_node' instance details are expanded, showing the following information:

- Instance ID:** i-0025044b666fdc3c92
- Public IPv4 address:** 44.202.220.213
- Private IPv4 addresses:** 172.31.4.5
- Instance state:** Running
- Public DNS:** ec2-44-202-220-213.compute-1.amazonaws.com

Installing pip and ansible in control node

```
ec2-user@ip-172-31-4-5:~$ login as: ec2-user
ec2-user@ip-172-31-4-5:~$ Authenticating with public key "my_aws" from agent
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

[ec2-user@ip-172-31-4-5 ~]$ wget https://raw.githubusercontent.com/ansible/ansible/stable-2.11/examples/ansible.cfg
--2025-12-29 13:54:26-- https://raw.githubusercontent.com/ansible/ansible/stable-2.11/examples/ansible.cfg
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20353 (20K) [text/plain]
Saving to: 'ansible.cfg'

ansible.cfg                               100%[=====] 19.88K --.-KB/s  in 0s

2025-12-29 13:54:27 (144 MB/s) - 'ansible.cfg' saved [20353/20353]

[ec2-user@ip-172-31-4-5 ~]$ vi inventory.txt
[ec2-user@ip-172-31-4-5 ~]$ ls
ansible.cfg  inventory.txt
[ec2-user@ip-172-31-4-5 ~]$ sudo yum install pip
Last metadata expiration check: 0:04:35 ago on Mon Dec 29 13:50:44 2025.
Package python3-pip-21.3.1-2.amzn2023.0.14.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-4-5 ~]$ pip install ansible
Defaulting to user installation because normal site-packages is not writeable
Collecting ansible
  Downloading ansible-8.7.0-py3-none-any.whl (48.4 MB)
    48.4 MB 209 kB/s
Collecting ansible-core==2.15.7
  Downloading ansible_core-2.15.13-py3-none-any.whl (2.3 MB)
    2.3 MB 70.1 MB/s
Collecting resolvelib<1.1.0,>=0.5.3
  Downloading resolvelib-1.0.1-py2.py3-none-any.whl (17 kB)
Collecting jinja2>=3.0.0
  Downloading jinja2-3.1.6-py3-none-any.whl (134 kB)
    134 kB 84.2 MB/s
Collecting packaging
  Downloading packaging-25.0-py3-none-any.whl (66 kB)
    66 kB 8.9 MB/s
```

Creating a role using ansible galaxy command:

```
ec2-user@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,>=5.0
  Downloading importlib_resources-5.0.7-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-2.0.3-cp39-cp39-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64.whl (20 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-8.7.0 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-galaxy init newrole
- Role newrole was created successfully
[ec2-user@ip-172-31-4-5 ~]$ ls
ansible.cfg  inventory.txt  newrole
[ec2-user@ip-172-31-4-5 ~]$ cd newrole
[ec2-user@ip-172-31-4-5 newrole]$ ls
README.md  defaults  files  handlers  meta  tasks  templates  tests  vars
[ec2-user@ip-172-31-4-5 newrole]$ sudo yum install tree
Last metadata expiration check: 0:06:38 ago on Mon Dec 29 13:50:44 2025.
Dependencies resolved.
=====
Package                               Architecture      Version           Repository        Size
Installing:
tree                                  x86_64            1.8.0-6.amzn2023.0.2  amazonlinux      56 k
Transaction Summary
-----
Install 1 Package
Total download size: 56 k
Installed size: 113 k
Is this ok [y/N]: y
Downloading Packages:
tree-1.8.0-6.amzn2023.0.2.x86_64.rpm                                1.2 MB/s | 56 kB    00:00
-----
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing                :
  Installing               : tree-1.8.0-6.amzn2023.0.2.x86_64
  Running scriptlet        : tree-1.8.0-6.amzn2023.0.2.x86_64
  1/1
  1/1
  1/1
```

Code should store into roleee.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
├── meta
│   ├── main.yml
│   ├── tasks
│   │   ├── main.yml
│   │   └── templates
│   ├── tests
│   │   ├── inventory
│   │   └── test.yml
│   └── vars
│       └── main.yml
└── 0 directories, 8 files
[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 ~]$ nano rolee.yaml
[ec2-user@ip-172-31-4-5 ~]$ ls
ansible.cfg  inventory.txt  newrole  rolee.yaml
[ec2-user@ip-172-31-4-5 ~]$ cd newrole
[ec2-user@ip-172-31-4-5 newrole]$ ls
README.md  defaults  files  handlers  meta  tasks  templates  tests  vars
[ec2-user@ip-172-31-4-5 newrole]$ 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:RbWYA0bKR8Tgzi2bFUIG+qSBZAmS7jPQout20wI+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:FfjxrlA7/yST1Y9SgNWnoJdttVUDirkeoyhGDSnlmW.
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]

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.stdout": "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.stdout": "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 ~]$
```

Then run the yaml file(playbook):

Command: ansible-playbook -i inventory.txt 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] *****
[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.stdout": "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.stdout": "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...

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh/home?region=us-east-1&connType=standard&instanceId=i-0fc7268eec4ec471&osUser=ec2-user&sshPort=22&addressFami...

Search

[Alt+S]

United States (N. Virginia) Account ID: 0022-0402-6052 Srinath

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 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-172-31-11-29 ~]\$

i-0fc7268eec4ec471 (managed_node)

PublicIPs: 34.200.214.145 PrivateIPs: 172.31.11.29

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS CloudShell interface. At the top, there's a search bar and navigation icons. The main terminal area displays the following output:

```
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 ~]$
```

Below the terminal output, the instance ID `i-09a293f822501fdcb (managed_node)` is shown, along with public and private IP addresses. The bottom of the interface includes a footer with 'CloudShell', 'Feedback', 'Console Mobile App', and copyright information for Amazon Web Services.

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 roleee.yaml
New Vault password:
Confirm New Vault password:
Encryption successful
[ec2-user@ip-172-31-4-5 ~]$
```