Ansible IV

Dónal Cunningham, HEAnet
Orchestration, Automation and Virtualisation (OAV)
Training Development Team
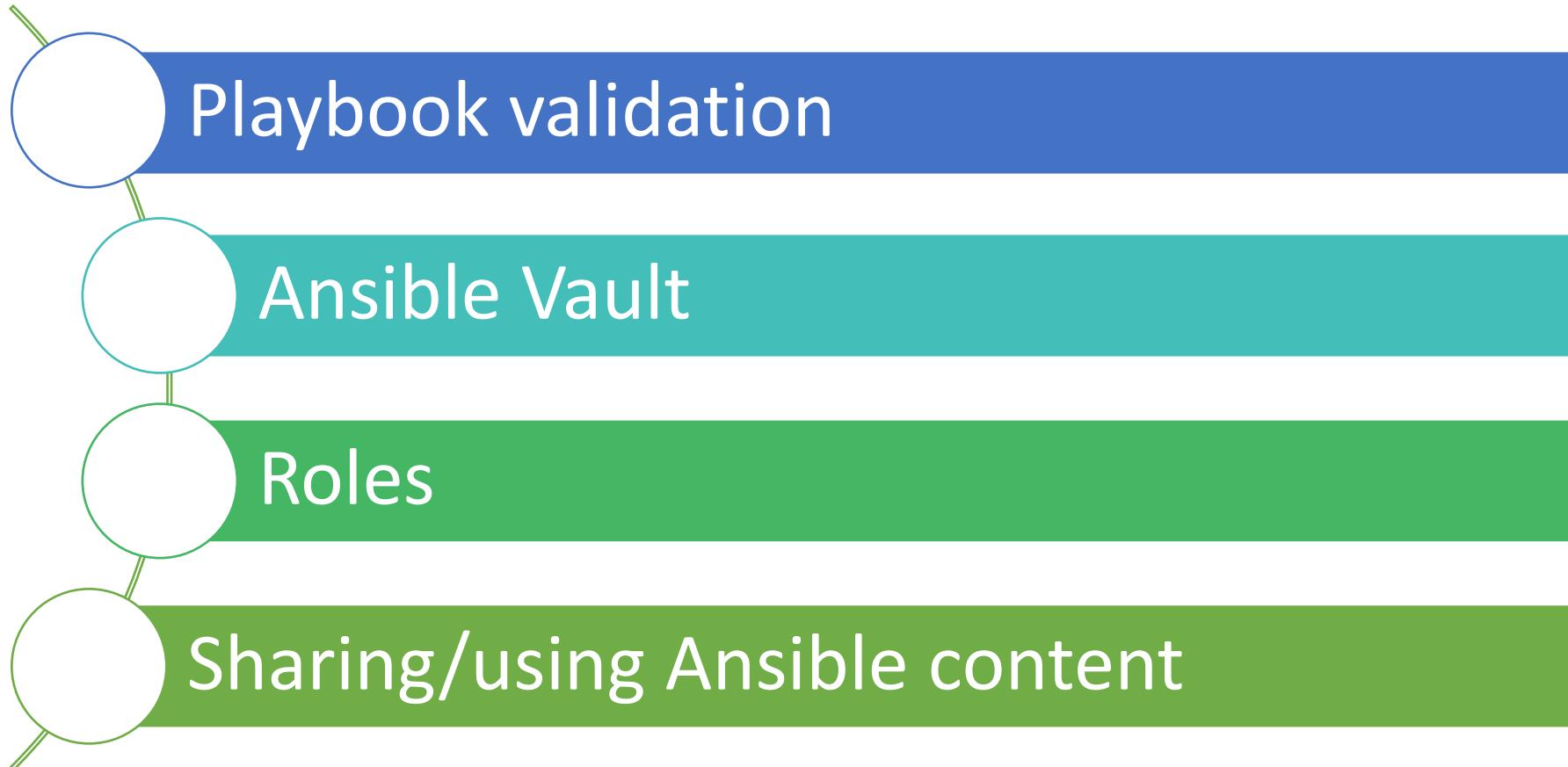
OAV training by the GÉANT project:

https://wiki.geant.org/display/NETDEV/OAV+Training+Portal

oav@lists.geant.org

www.geant.org

In this section...

Playbook validation

Ansible Vault

Roles

Sharing/using Ansible content

GÉANT

Restricting hosts on the command line

```
$ ansible-playbook -l canary_host push_new_vlan.yaml
```

The argument to `-l` is similar to a `hosts:` parameter, and can be…

- A single host or a list of hostnames
- A single group or a list of group names
- A regular expression

```
$ ansible-playbook -i hosts --step show-version.yaml

PLAY [Show the software version] ***********************************
Perform task: TASK: Gather version (N)o/(y)es/(c)ontinue: y


TASK [Gather version] **********************************************


changed: [veos]
Perform task: TASK: Print output (N)o/(y)es/(c)ontinue: y


TASK [Print output] ************************************************
ok: [veos] => {
    "out.stdout_lines[0]": "Software image version: 4.25.2F"
}


PLAY ***************************************************************
veos: ok=1      changed=1      unreachable=0      failed=0
```

GÉANT

Playbook validation

- --syntax-check
  - Check the syntax but do **not** execute

```
$ ansible-playbook -i hosts --syntax-check show-
version.yaml


playbook: show-version.yaml
```

```
$ ansible-playbook -i hosts --syntax-check show-version.yaml
ERROR! We were unable to read either as JSON nor YAML, these are
the errors we got from each:
JSON: Expecting value: line 1 column 1 (char 0)


Syntax Error while loading YAML.
  mapping values are not allowed in this context


The error appears to be in ; 'show-version.yaml':
line 8, column 10, but may be elsewhere in the file depending on
the exact syntax problem.


The offending line appears to be:


  - name: Gather version
    raw: 'show version | include Software'
        ^ here
```

Playbook Annotation : Tags

```yaml
tasks:
- name: Install the web servers
  debug: msg="Installing web servers"
  tags:
    - webservers

- name: Install the database servers
  debug: msg="Installing database servers"
  tags:
    - dbservers
```

```
$ ansible-playbook --tags webservers ./playbook_with_tags.yaml
…
TASK [Installing web servers] ********************************
…


$ ansible-playbook --tags dbservers ./playbook_with_tags.yaml
…
TASK [Installing database servers] ********************************
…


$ ansible-playbook --tags loadbalancers ./playbook_with_tags.yaml
…
PLAY [Play to install service daemons] ********************************


PLAY RECAP ********************************
```

```
$ ansible-playbook --tags "webservers,dbservers"  ./playbook_with_tags.yaml


PLAY [Play to install service daemons]*************************************


TASK [Install web servers] ************************************************
ok: [localhost] => {
    "msg": "Installing web servers"
}


TASK [Install the database servers] ***************************************
ok: [localhost] => {
    "msg": "Installing database servers"
}


PLAY RECAP ****************************************************************
localhost                      : ok=2    changed=0    unreachable=0    failed=0
```

Playbook Annotation : Skipping Tags

```
$ ansible-playbook --skip-tags "webservers"  ./playbook_with_tags.yaml


PLAY [Play to install service daemons]*************************************

TASK [Install the database servers] ***************************************
ok: [localhost] => {
    "msg": "Installing database servers"
}


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

Playbook validation

- --check
  - No changes on remote systems

  - **check_mode: no**   will *always* make changes

  - **check_mode: yes** will *never* make changes

  - `when: not ansible_check_mode`

```
$ ansible-playbook -i hosts --check show-version.yaml

PLAY [Show version] *****************************************************

TASK [Gather version] ***************************************************
skipping: [veos]

TASK [Print output] *****************************************************
ok: [veos] => {
    "showversion_output.stdout_lines[0]": "VARIABLE IS NOT DEFINED!"
}

PLAY RECAP **************************************************************
veos : ok=1     changed=0     unreachable=0     failed=0     skipped=1 …
```

GÉANT

```
$ ansible-playbook -i hosts --check --diff change_hostname.yaml


PLAY [Change the hostname] **************************

TASK [Run the hostname command] *******************************
--- system:/running-config
+++ session:/ansible_1626193414-session-config
@@ -8,7 +8,7 @@
 !
 service routing protocols model ribd
 !
-hostname ar1-cwt
+hostname ar1-testlab
 !
 spanning-tree mode mstp
 !
[changed: [veos]
```

Ansible Vault

- Encrypts/decrypts sensitive information
  - Variables
    - group_vars
    - host_vars
  - Files

- Encrypted files may be loaded by playbooks…
  - …and automatically decrypted

```
$ cat secrets.yaml
---
ansible_user: zork
ansible_password: swordfish

$ ansible-vault encrypt secrets.yaml
New Vault password:
Confirm New Vault password:
Encryption successful

$ cat secrets.yaml
$ANSIBLE_VAULT;1.1;AES256
62653565343966646362306436656130653138376133376562383536313061343033653037316337
…
```

www.geant.org

```yaml
---
- name: Play to show the software version on an Arista switch
  hosts: veos
  gather_facts: no
  connection: network_cli

  tasks:
  - name: Import encrypted credentials
    include_vars: secrets.yaml


  - name: Gather version from switches
    arista.eos.eos_command:
      commands:
        - 'show version | include Software'
    register: showvers


  - name: Print first line of the stdout array
    ansible.builtin.debug: var=showvers.stdout[0]
```

```
$ cat hosts
veos ansible_host=localhost ansible_port=9022 ansible_network_os=eos


$ cat secrets.yaml
$ANSIBLE_VAULT;1.1;AES256
```
```
3735303239306537373130373737303536623038643561373234633338396462383063613532323
3132626139303264643037379373362313165531666333620a3833303665313431303433262363637
3532653237323562363238535373431653736373376435333261313462643639656130313035636662
326437633433338646640a36656130323130366646386663333766343930343664326393936633934
323336303566623630313232340333333361303430366330303336366616262343933303666343736
353161393366387303363323364613863386363356336323133389303732373666356433656131
3533343461336636633073743838636333334
```

```
$ ansible-vault view secrets_encrypted.yaml
Vault password:
---
ansible_user: zork
ansible_password: swordfish
```

www.geant.org

GÉANT

```
$ ansible-playbook -i hosts --ask-vault-password show-version-with-vault.yaml
Vault password:


PLAY [Play to show the software version on an Arista switch] *******************


TASK [Import encrypted credentials] ********************************************
ok: [veos]


TASK [Gather version from switches] ********************************************
ok: [veos]


TASK [Print first line of the stdout array] ************************************
ok: [veos] => {
    "showvers.stdout[0]": "Software image version: 4.25.2F"
}


PLAY RECAP *********************************************************************
veos                       : ok=3    changed=0    unreachable=0    failed=0
```

Roles

- Split work up into smaller units
  - Separate tasks and templates

- You can share Ansible roles with others
  - Collections
  - Ansible Galaxy

- System-wide role directory - `/etc/ansible/roles`

- There are also `import_role` and `include_role`

```yaml
---

- name: Apply CW Spine configuration
  hosts: Citywest-spines
  gather_facts: no
  roles:
  - make-directories
  - base
  - Citywest-vlans
  - nni-interfaces
  - uni-interfaces
  - ebgp
  - controlplane-acl
  - assemble-configs
```

www.geant.org

```
./roles
├── assemble-configs
|   └── tasks
|       └── main.yaml
├── base
│   ├── files
│   ├── handlers
│   |   └── handlers.yaml
│   ├── tasks
│   |   └── main.yaml
│   └── templates
│   |   └── base.j2
│   └── vars
…
```

```
- name: BUILD CONFIGURATION
   template:
      src=vlans.j2
    dest=configs/{{ inventory_hostname }}/{{ inventory_hostname }}-vlans.conf
   tags: build


- name: Apply vlan configuration
   ios_config:
      src: configs/{{ inventory_hostname }}/{{ inventory_hostname }}-vlans.conf
      authorize: yes
      save: yes
   tags: push
```

GÉANT

Sharing and using Ansible content

- Collections
  - Playbooks, Roles, Modules, Plugins

- Ansible Galaxy is the default repo for collections…
  - `https://galaxy.ansible.com`
  - …but you can use git repositories too

- Can install specific versions

```
$ ansible-galaxy collection list


# /usr/local/Cellar/ansible/4.0.0/libexec/lib/python3.9/site-packages/ansible_collections


Collection                     Version
------------------------------ -------
amazon.aws                     1.5.0
ansible.netcommon              2.0.2
ansible.posix                  1.2.0
ansible.utils                  2.1.0
ansible.windows                1.5.0
arista.eos                     2.1.1
awx.awx                        19.0.0
azure.azcollection             1.5.0
check_point.mgmt               2.0.0
chocolatey.chocolatey          1.1.0
cisco.aci                      2.0.0
cisco.asa                      2.0.1
…
```

```
$ ansible-galaxy collection install paloaltonetworks.panos

Starting galaxy collection install process

Process install dependency map

Starting collection install process

Downloading https://galaxy.ansible.com/download/paloaltonetworks-panos-
2.6.0.tar.gz to /Users/dcunningham/.ansible/tmp/ansible-local-
11455hgddd3za/tmp0g4a6xww/paloaltonetworks-panos-2.6.0-l7h2hfgg

Installing 'paloaltonetworks.panos:2.6.0' to
'/Users/dcunningham/.ansible/collections/ansible_collections/paloaltonetworks/pa
nos'

paloaltonetworks.panos:2.6.0 was installed successfully


$ tree ~/.ansible/collections/

/Users/dcunningham/.ansible/collections/
└── ansible_collections
    └── paloaltonetworks
        └── panos
            ├── FILES.json
            ├── LICENSE
…
```

```yaml
---
- name: Show info on all Palo Alto devices
  hosts: PAN-7k
  collections:
    - paloaltonetworks.panos

  tasks:
  - name: Get the system info
    panos_op:
      cmd: 'show system info'
    register: res

  - debug:
      msg: '{{ res.stdout }}'
```

Thank you

If you have any questions, or would like to discuss any of these topics further, please email:

oav@lists.geant.org

This material is distributed under a
CC BY-NC-SA licence

www.geant.org