



Ansible pour professionnels

Linux / Unix



Le support du cours «Ansible pour professionnel Linux/Unix » est non contractuel ; il ne doit pas être redistribué et/ou reproduit en partie ou en totalité sans permission explicite et écrite de la société Adlere.

Red Hat, le logo Red Hat, OpenShift et Ansible sont des marques déposées ou commerciales de Red Hat, Inc ou ses filiales aux États-Unis et dans d'autre pays. Linux® est une marque déposée de Linus Torvalds aux États-Unis et dans d'autre pays.

UNIX ® est une marque déposée par « The Open Group » aux Etats-Unis et dans d'autres pays.
Wiindows® est une marque déposée de Microsoft Corporation aux États-Unis et dans d'autre pays.

Les autres marques citées sont déposées par leurs propriétaires respectifs.

- Présentation(s)
Instructeur, participants
- Objectifs et organisation de la session



- Introduction à l'écosystème Ansible
- Installation, fichier de configuration, inventaires
- Commandes ad-hoc
- Variables
- Structures des playbooks
- Modules usuels
- Ansible Vault
- Rôles
- Bonus ?



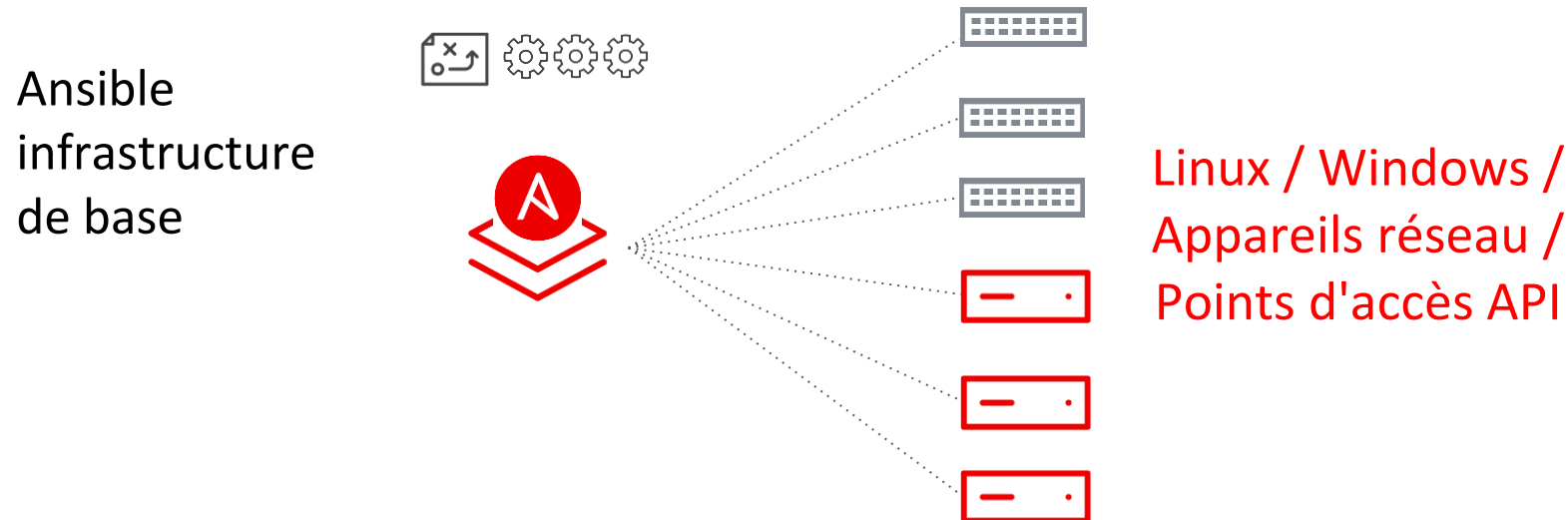


Introduction à l'écosystème Ansible

+a Fonctionnement Ansible

Qu'est-ce que Ansible ?

- 2012 (Michael de Haan → Cobbler), disponible via Ansible Inc., rachetée par Red Hat en 2015
- Ansible est un *langage simple d'automatisation* pour déployer une infrastructure d'application informatique décrite dans des fichiers texte (playbooks)
- Ansible est aussi un *moteur d'automatisation* qui exécute des playbooks Ansible
- Ansible peut *s'adapter à de nombreux workflows et environnements*, grâce à la richesse de ses modules et ses capacités d'extensions



Idempotence

Agentless

** limitations may apply*

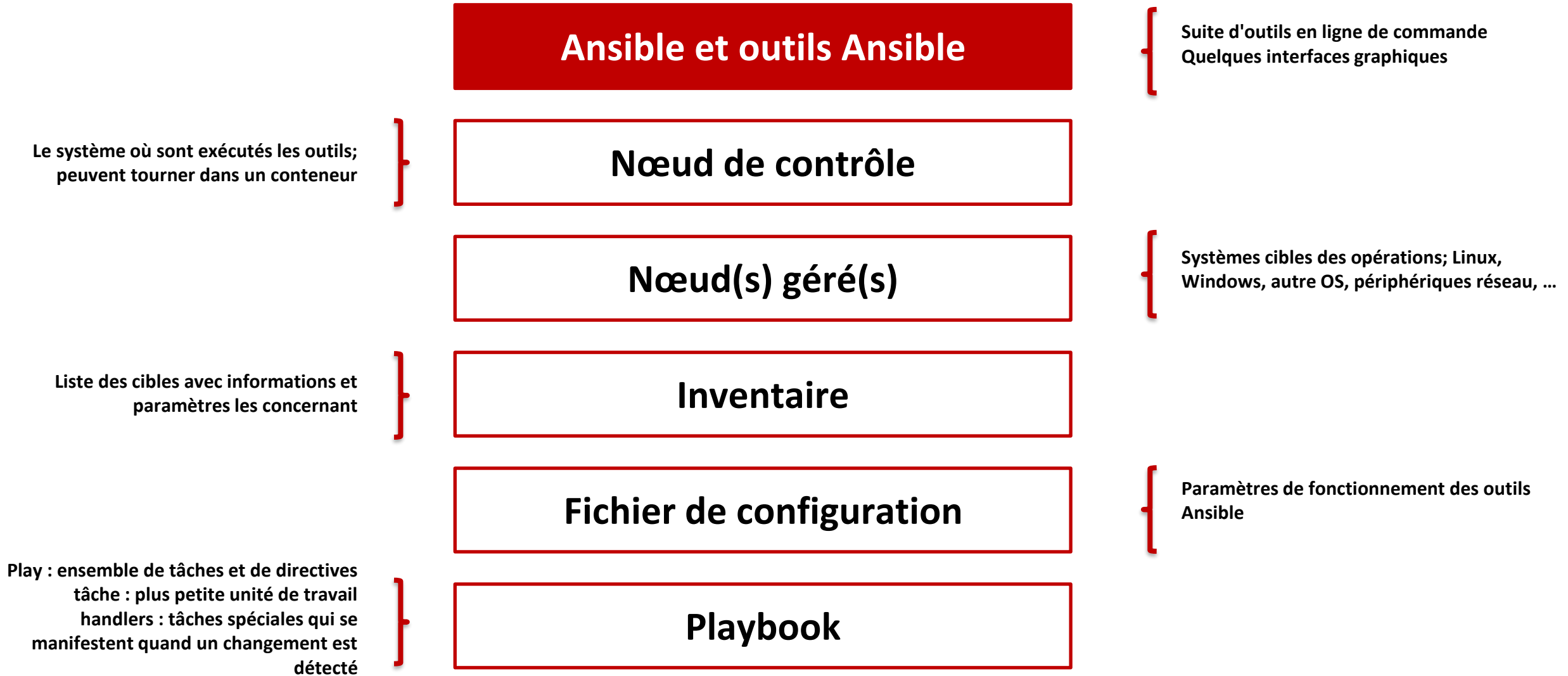


Ansible, pourquoi ?

Cas d'usage

- Provisionnement de système
configuration initiale en sortie d'usine : comptes, systèmes de fichiers, paramètres noyau, ...
- Configuration
application de règles de configuration (changement de DNS, NTP, ...)
exploitation système récurrente
- Déploiement d'applications
installation / mise en œuvre des prérequis (utilisateurs, variables, répertoires, ...)
déploiement des paquetages logiciels
paramétrage applicatif (fichiers de configuration applicatifs)
- Gestion applicative
traitements batch, sauvegardes, run applicatif
- Remédiation
quand des écarts sont détectés (paramètres noyau, sécurité, ...)
- Sécurisation
déploiement de règles de sécurité







Programmes en Python étendant les fonctionnalités d'Ansible. Peuvent porter sur la façon dont Ansible se connecte à des cibles (plugins de connexion), manipule les données (plugins de filtre) ou modifient ce qui s'affiche sur la console (plugins de callback / retour)

Format pour distribuer du contenu Ansible (playbooks, rôles, modules, plugins, ...). On les installe généralement depuis le site galaxy.ansible.com

Modules

Le code ou les binaires qu'Ansible recopie et exécute sur chaque cible pour accomplir les actions d'une tâche

Plugins

Rôles

Playbooks packagés pour être ré-utilisables les et partageables

Collections

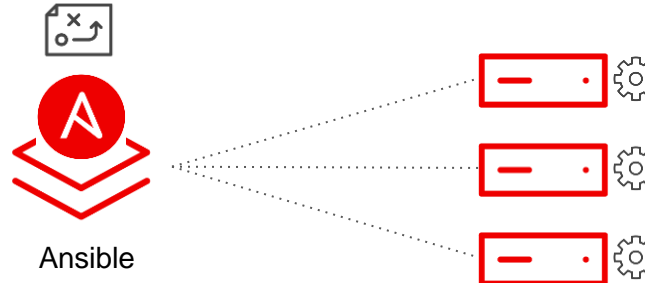
Environnements d'exécution

Image de conteneurs dans laquelle s'exécute un playbook et toutes ses dépendances (modules Python, collections, commandes systèmes, ...)



Deux grands modes de fonctionnement

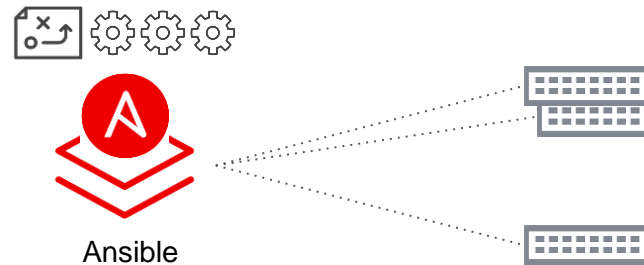
Le code du module est copié sur le nœud géré, exécuté, puis supprimé.



cibles Linux /
Windows

Exécution à distance

Le code du module est exécuté localement sur le nœud de contrôle.

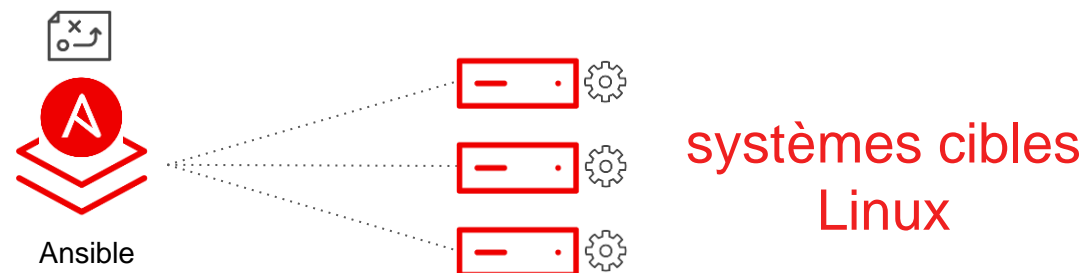


Appareils réseau / Points
d'accès API

Exécution Locale



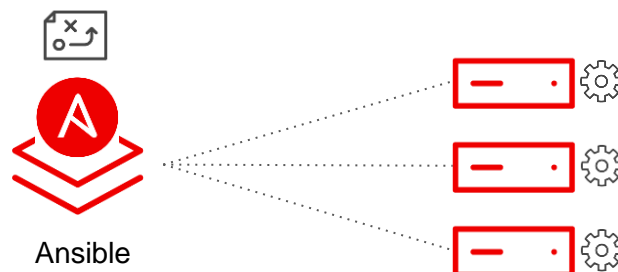
- Protocole par défaut = ssh (OpenSSH supporté depuis Ansible 0.5, par défaut depuis 1.3)



- Utilise les mécanismes ssh standards (`~/.ssh/config`, port 22, ...)
- Par défaut, utilisateur de connexion sur la cible = nom de l'utilisateur qui invoque la commande ansible
- La connexion se fait en utilisant les clefs ssh disponibles dans `~/.ssh` ou en demandant un mot de passe
- de nombreuses options existent pour personnaliser la méthodologie de connexion
 - peuvent se définir dans le fichier d'inventaire, dans le fichier de configuration ansible, dans des variables d'environnement
- Autres options : paramiko, local, winrm
- Plugins disponibles : `ansible-doc -l -t connection`
- Ne jamais lancer une automatisation sans s'assurer que la connexion est fonctionnelle (`ansible -m ping all`)



- Protocole par défaut = WinRM



systèmes cibles
Windows

- ports 5985 (http) et 5986 (https)
- Configuration à faire côté serveur Windows
 - listener, protocole de connexion, chiffage, certificats, ...
 - https://docs.ansible.com/ansible/latest/os_guide/index.html
 - https://docs.ansible.com/ansible/latest/os_guide/windows_winrm.html
- Modules en PowerShell et non Python
- préfixés par win_
- s'assurer que le connexion est fonctionnelle : `ansible -m win_ping all`

- Setting up a Windows Host
 - Host Requirements
 - WinRM Setup
 - Windows SSH Setup
- Using Ansible and Windows
 - Use Cases
 - Path Formatting for Windows
 - Limitations
 - Developing Windows Modules
- Windows Remote Management
 - What is WinRM?
 - WinRM authentication options
 - Non-Administrator Accounts
 - WinRM Encryption
 - Inventory Options
 - IPv6 Addresses
 - HTTPS Certificate Validation
 - TLS 1.2 Support
 - WinRM limitations

[app1srv]

```
appserver01 ansible_host=10.42.0.2  
appserver02 ansible_host=10.42.0.3  
appserver03
```

[web]

```
node-[1:30]
```

[web:vars]

```
apache_listen_port=8080  
apache_root_path=/var/www/mywebdocs/
```

[infra:children]

```
app1srv  
web
```

[all:vars]

```
ansible_user=automation  
ansible_ssh_private_key_file=/home/automation/.ssh/automation_rsa
```

- Dans sa forme la plus simple, un fichier texte avec une liste de cible et des informations de connexion
- On peut ajouter des variables spécifiques à chaque groupe ou chaque hôte.



```
[defaults]
inventory = ./inventory
remote_user = user
ask_pass = false
host_key_checking = false
```

```
[privilege_escalation]
become = true
become_method = sudo
become_user = root
become_ask_pass = true
```

- Fichier texte au format .ini
- Organisé en blocs
- Définit le fonctionnement et des paramètres par défaut d'Ansible
- Certains paramètres peuvent être redéfinis dans l'inventaire



Un playbook (playbook.yml)

```
---  
- name: Installe et démarre Apache  
  hosts: web  
  become: yes  
  
  tasks:  
    - name: Installation Apache  
      ansible.builtin.dnf:  
        name: httpd  
        state: latest  
  
- name: Installe et démarre une base de données  
  hosts: dbservers  
  become: yes  
  
  tasks:  
    - name: Installation MariaDB  
      ansible.builtin.dnf:  
        name: mariadb  
        state: latest
```

2 plays

yamllint ou
ansible-lint
pour vérifier la
syntaxe d'un
playbook

Playbook = fichier texte ascii au format **YAML**



Présentation d'un playbook (2/2)

17

play

```
---  
- name: Installe et démarre Apache  
  hosts: web  
  become: yes
```

en-tête

tasks:

```
- name: Installation Apache  
  ansible.builtin.dnf:  
    name: httpd  
    state: latest
```

```
- name: Génère index.html  
  ansible.builtin.template:  
    src: index.html.j2  
    dest: /var/www/html/
```

```
- name: Démarre httpd  
  ansible.builtin.service:  
    name: httpd  
    state: started
```

modules

paramètres de module

tâches

yamllint ou
ansible-lint
pour vérifier la
syntaxe d'un
playbook

https://docs.ansible.com/ansible/latest/reference_appendices/playbooks_keywords.html#play

De nombreuses options de configuration

```
$ ansible-playbook ./install_software.yml  
$ ansible-navigator run install_software.yaml
```

Commande	Fonction
<code>ansible</code>	exécuter un module simple
<code>ansible-playbook</code>	exécuter un playbook
<code>ansible-doc</code>	afficher la documentation d'un module, plugin, ...
<code>ansible-config</code>	visualiser un paramètre de configuration
<code>ansible-inventory</code>	visualiser un inventaire
<code>ansible-navigator</code>	Combine plusieurs commandes précédentes, tout en permettant d'exécuter des playbooks dans un environnement d'exécution donné. S'installe à part.



```
$ ansible-playbook main.yml

PLAY [localhost] *****

TASK [Arrête service] *****
changed: [localhost]

TASK [Vérifie service toujours UP]
*****fatal: [localhost]:
FAILED! => {"changed": true, "cmd": ["/opt/appli/check.sh"], "delta": "0:00:00.017622", "end": "2024-04-06 08:19:30.026910", "msg": "non-zero return
code", "rc": 1, "start": "2024-04-06 08:19:30.009288", "stderr": "", "stderr_lines": [], "stdout": "", "stdout_lines": []}
...ignoring

TASK [Récupère données] *****
ok: [localhost]

PLAY RECAP *****localhost
: ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=1
```

Tâche exécutée, mais n'a généré aucun changement

Tâche non exécutée (probablement à cause d'une condition)

Tâche exécutée, a effectué un changement

Une erreur a été générée

Si nécessaire : mot-clef 'ignore_errors: true'



Quelles interfaces graphiques ?

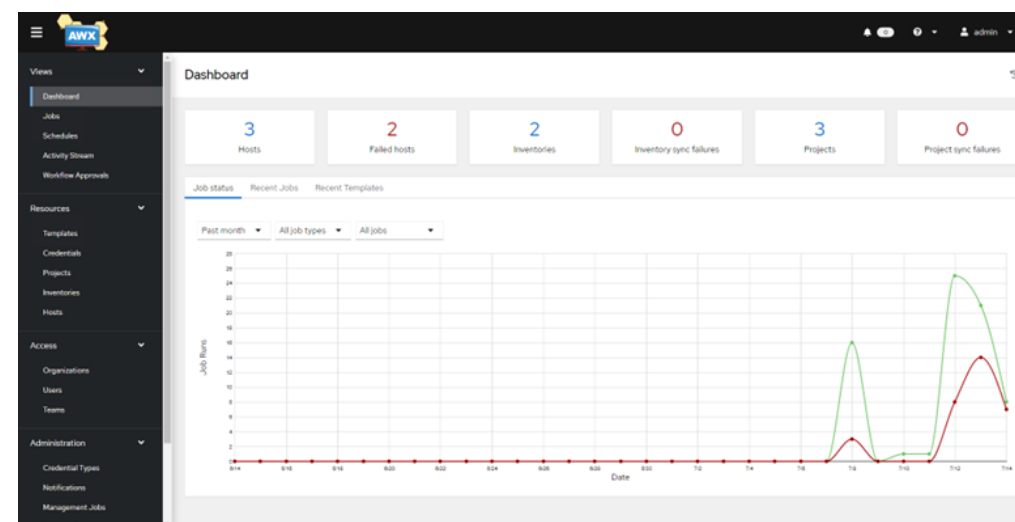
Quelques exemples

- Rundeck (<https://docs.rundeck.com/docs/>)
- Ansible forms (<https://ansibleforms.com/>)
- Semaphore (<https://www.semui.co/>)
- GitLab CI / gitlab-runner
- Ansible AWX (<https://github.com/ansible/awx>)
 - CIQ Ascender Automation
<https://ciq.com/products/ascender/>
 - Oracle Linux Automation Manager
<https://docs.oracle.com/en/learn/olam-quick-start/index.html>
 - CapGemini Intelligent Automation Platform
- Ansible Automation Platform
<https://www.redhat.com/en/technologies/management/ansible>

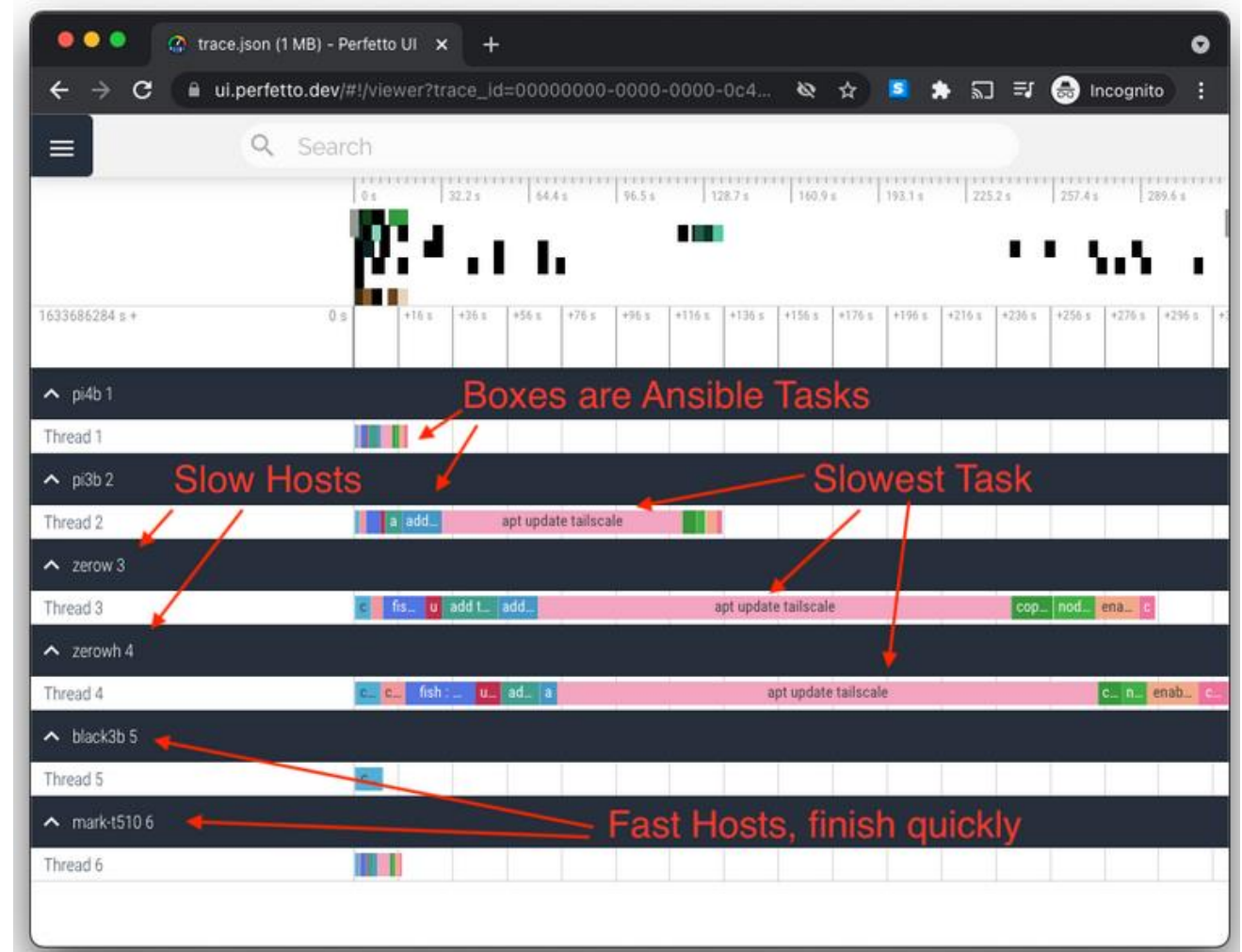
NAME	VERSION	STATUS	LAST TASK	PLAYBOOK	INVENTORY	ENVIRONMENT	REPOSITORY	ACTIONS
helloworld	--	Success	#2147483624 by Logan an hour ago	hello_world_playbook.yml	localhost	empty	gitTest	RUN

TASK ID	VERSION	STATUS	USER	START	DURATION	ACTIONS
#2147483624	--	Success	Logan	an hour ago	a few seconds	RERUN
#2147483625	--	Success	Logan	an hour ago	a few seconds	RERUN
#2147483626	--	Failed	Logan	an hour ago	a few seconds	RERUN
#2147483631	--	Failed	Logan	--	--	RERUN
#2147483632	--	Failed	Logan	--	--	RERUN

NAME	VERSION	STATUS	LAST TASK	PLAYBOOK	INVENTORY	ENVIRONMENT	REPOSITORY	ACTIONS
ssh hello	--	Failed	#2147483629 by Logan 2 hours ago	hello_world_playbook.yml	localhost	empty	sshRepo	RUN
git hello	--	Failed	#2147483627 by Logan an hour ago	hello_world_playbook.yml	localhost	empty	gitTest	RUN



- Représentation graphique du temps passé dans des tâches de playbooks
- <https://github.com/mhansen/ansible-trace>





ansible 2.10 :

La plupart des modules inclus avec Ansible ont été supprimés

→ Ansible 2.9 : les modules installées représentaient env. 12 000 fichiers

Ansible maintenant référencé sous le nom d'ansible-base, puis ansible-core à partir de 2.11.



Conséquences principales :

Recommandation d'utiliser le nom complet de classe qualifié (FQCN) pour référencer les modules

→ par ex. `ansible.builtin.debug` au lieu de `debug`

→ il faut probablement avoir à ré-écrire les anciens playbooks

(ils peuvent avoir des dépendances sur des modules qui ne sont plus inclus par défaut)



Packaging Ansible actuel

2 versions disponibles

23

outils CLI

ansible-community
ansible
ansible-config
ansible-console
ansible-doc
ansible-galaxy
ansible-inventory
ansible-playbook
ansible-pull
ansible-test
ansible-vault

ansible-core
~ 62M

amazon arista awx
azure check_point chocolatey
cisco cloud cloudscale_ch
community cyberark dellemc
f5networks fortinet google
grafana hetzner ibm
ieisystem infinidat infoblox
inspur junipernetworks kaytus
kubevirt lowlydba microsoft
netapp netapp_eseries netbox
ngine_io openstack ovirt
purestorage redhat sensu
splunk telekom_mms theforeman
vmware vultr vyos wti

ansible "batteries included"
~ 500M

**collections liées à
un constructeur /
éditeur**



- Noeud de contrôle vs noeud géré (control node / managed node)
- https://docs.ansible.com/ansible/latest/reference_appendices/release_and_maintenance.html#ansible-core-support-matrix

Version	Support	End Of Life	Control Node Python	Target Python / PowerShell
2.18	GA: 04 Nov 2024 Critical: 19 May 2025 Security: 03 Nov 2025	May 2026	Python 3.11 - 3.13	Python 3.8 - 3.13 PowerShell 5.1
2.17	GA: 20 May 2024 Critical: 04 Nov 2024 Security: 19 May 2025	Nov 2025	Python 3.10 - 3.12	Python 3.7 - 3.12 PowerShell 5.1
2.16	GA: 06 Nov 2023 Critical: 20 May 2024 Security: Nov 2024	May 2025	Python 3.10 - 3.12	Python 2.7 Python 3.6 - 3.12 Powershell 5.1
2.15	GA: 22 May 2023 Critical: 06 Nov 2023 Security: 20 May 2024	EOL Nov 2024	Python 3.9 - 3.11	Python 2.7 Python 3.5 - 3.11 PowerShell 3 - 5.1
2.14	GA: 07 Nov 2022 Critical: 22 May 2023 Security: 06 Nov 2023	EOL 20 May 2024	Python 3.9 - 3.11	Python 2.7 Python 3.5 - 3.11 PowerShell 3 - 5.1



Installer Ansible

Où trouver cela ?

- En tant que composant de la distribution Linux
 - RHEL < 8.6 : repo ansible-2-for-rhel-8-x86_64-rpms (<https://access.redhat.com/articles/3174981>)
 - RHEL 8.6 et + (<https://access.redhat.com/articles/6393361>) :
 - dépôt RH8 AppStream ou les référentiels Automation Platform de RedHat
 - Debian-like : apt-get install ansible-core ou apt-get install ansible
- En tant que module Python :
 - téléchargement / installation via pip3, eg python3 -m pip install ansible-core
 - préférablement dans un venv
- Code source à partir du dépôt Git du projet
 - <https://github.com/ansible>
- Depuis une image de conteneur
 - prépackagé : execution environment
 - nécessite ansible-navigator
 - s'installe depuis un package python ou un dépôt Red Hat Ansible Automation Platform
 - à faire soi-même
 - <https://hackmd.io/@the-ansible-book/B1y5tXers>





TOUS DROITS RÉSERVÉS ©ADLERE

[Topics](#)[Groups](#)[Community Events](#)[Open Polls](#)[More](#)[Categories](#)[News & Announcements](#)[Get Help](#)[Project Discussions](#)[Events](#)[Social Space](#)[International Communities](#)[Forum Guide & Feedback](#)[All categories](#)[Tags](#)[awx](#)[all categories](#)[all tags](#)[Categories](#)[Latest](#)[Top](#)

Category


Topics



News & Announcements

4 / month

All the latest activity in the Ansible Community.

 Newsletter  Ecosystem Releases  Blog



Get Help

119 /

month

Need help? This is the place! Get started with Ansible, debug your playbooks, set up your tooling ... whatever your question, ask it here!

 Guides, FAQs & Howtos



Project Discussions

12 / month

Discuss any aspect of the Ansible Project here! This space is organized by tag, and tag generally correspond to a [Working Group](#) or [Ecosystem Project](#). There are also some high-level tags such as [mindshare](#), [community](#) and so on.



Events

4 / month

Latest



Welcome to the Ansible Community! 🎉

5

Jul '23


 News & Announcements



Connexion a l'aide de Winrm

3

39m

 Get Help


[collections](#) [windows](#)



Unable to parse /runner /inventory/hosts as an inventory source

20

5h

 Get Help


[awx](#) [collections](#) [galaxy-ng](#) [playbook](#)
[vmware](#) [fedora](#)



VSCode spawn C:\WINDOWS\system32\cmd.exe ENOENT

0

6h

 Get Help

[collections](#) [windows](#) [vscode-ansible](#)

r/ansible

Search in r/ansible

9

3

Share

u/cybette

Ansible Community Team

• 18 days ago

The Bullhorn #126 (Ansible Newsletter)

3

1

Share

u/tigerblue77

• 13 hr. ago

How to limit the scope of variables passed to a role from the playbook?

playbooks, roles and collections

Hello, I have a working playbook that deploys Docker stacks. I want to be able to deploy these stacks without starting them. The playbook looking like this :

```
vars:
  Docker_service_number_of_replicas: 2
roles:
- role: deploy_X_Docker_container
- role: deploy_Y_Docker_container
vars:
  ...
  Docker_stack_stopped: "true"
  ...
- role: deploy_Z_Docker_container
vars:
  ...
```

[View full post](#)

3

13

Share

u/ImpactFit211

• 1 day ago

What's today's best way to setup a local dev environment in wsl2?

Ansible - Simple IT Automation

Automation for the People! A Subreddit dedicated to fostering communication in the Ansible Community, includes Ansible, AWX, Ansible Tower, Ansible Galaxy, ansible-lint, Molecule, etc.

60K

27

Top 2%

Members

Online

Rank by size ↗

RULES

1

Follow Ansible's Code of Conduct ↗

Follow https://docs.ansible.com/ansible/latest/community/code_of_conduct.html

RELATED REDDITS

r/awx

2,150 members

USEFUL DOCS

Ansible Community

Ansible Collections

MODERATORS

u/mikeoquinn

u/gundalow

u/cybette

Actualité du monde Ansible et des principaux composants, date de release, évolutions technologiques

Hebdomadaire

Inscription = aller dans la catégorie Newsletter, cliquer sur la cloche.

Jusque juin 2024 mailing liste.



This category holds the post archive from our newsletter, The Bullhorn. Subscribe to the category if you'd like a weekly roundup of news from the Ansible Ecosystem!

 News & Announcements ▾

 Newsletter ▾







tags ▾

Latest

Top

Bookmarks



Topic		Replies	Views	Activity
🚩 About the Newsletter category				
This category holds the post archive from our newsletter, The Bullhorn. Subscribe to the category if you'd like a weekly roundup of news from the Ansible Ecosystem! To propose a news item for the newsletter, simply hop ... read more		0	1.0k	19d
The Bullhorn #143				
awx galaxy-ng windows kubernetes ee fedora		0	317	3d
The Bullhorn #142				
awx collections galaxy-ng ansible-lint ansible-navigator devtools	  	2	598	17d
The Bullhorn #141				
awx collections windows ee aws meetup ansible fedora		0	340	21d

- D'une façon générale, les IA savent produire des playbooks ou morceaux de playbooks exploitables
- La qualité des réponses est variable, on a déjà vu des références à des modules ou filtres inexistant
- **Attention à la confidentialité des données**

ChatGPT	OpenAI	https://chatgpt.com
Claude AI	Anthropic	https://claude.ai
Gemini	Google	https://gemini.google.com/
Le Chat	Mistral	https://chat.mistral.ai
LLaMa	Meta/Facebook	https://www.meta.ai/ - pas encore accessible en France
Bing Copilot	Microsoft	https://copilot.microsoft.com/
Grok2	Twitter / X	Depuis l'application mobile, pour les abonnés X Premium/premium +
llama3-70b	nvidia	https://build.nvidia.com/meta/llama3-70b



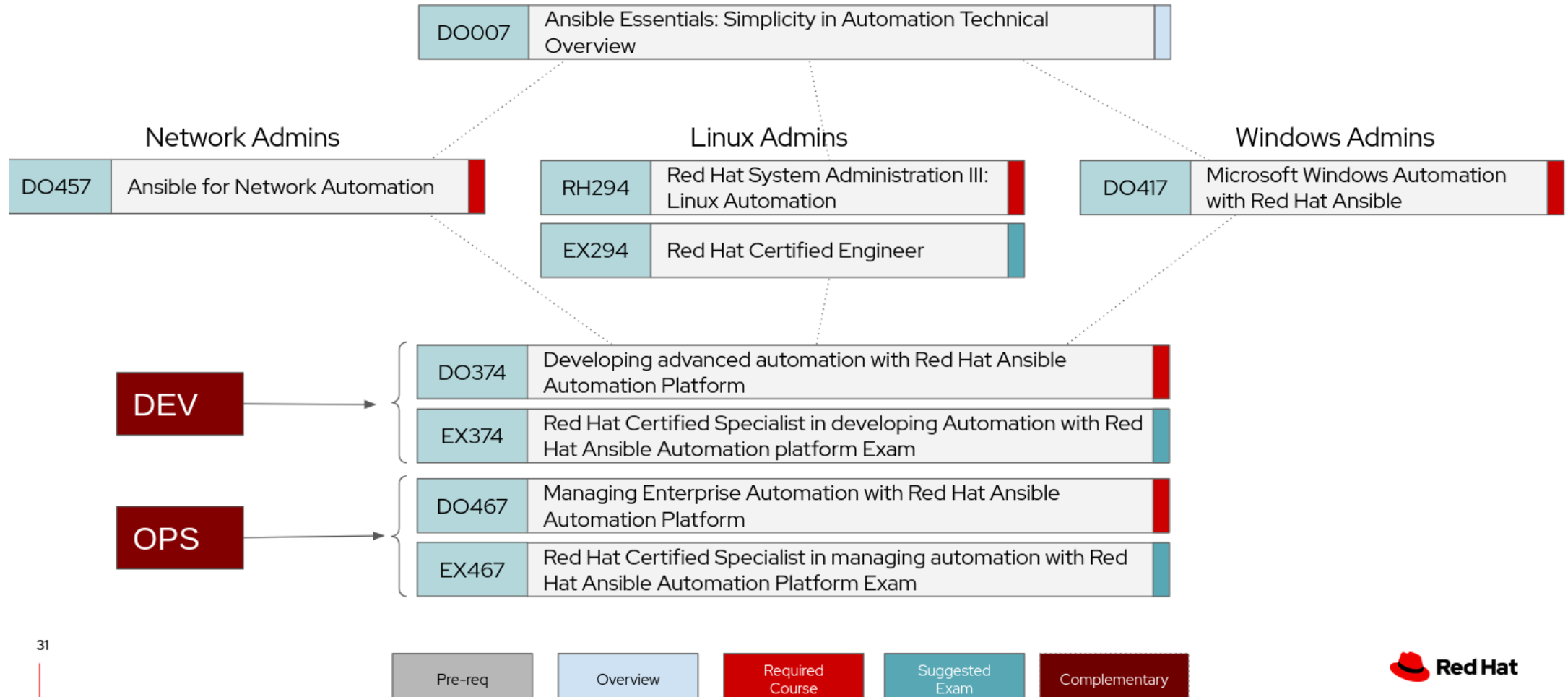
Clipart d'illustration conçu avec Microsoft Designer®

« Globalement, elle [l'IA] me donne un début de solution mais je repasse toujours derrière »
Mon collègue



cheminement de formation Ansible

Ansible curriculum





- Ansible travaille avec une myriade de fichiers textes / YAML
 - il faut versionner les playbooks et autres composants texte Ansible
 - il ne faut pas stocker de secrets dans un repository Git
 - il ne faut pas stocker de binaires dans un repository Git
 - mettre au point un système de branches et de tags
 - il faut faire des commits sur des unités de travail

Commandes usuelles

```
git config -l (system =/etc/gitconfig; global=~/.gitconfig; local = .git/config)
git config --global user.name="JKL"
git config --global user.email="mail@example.org"
git clone http://FQDN/repo.git
vi .gitignore
git add .
git commit -m "Message signifiant"
git push
```



© [XKCD](https://xkcd.com/152/)



Best practices GIT

Recommandations génériques

33

- il faut utiliser des messages de commit parlants
 - "update fichier XXX" → NON

OUI

	changement clef ssh publique Johan Klotz authored 7 hours ago
	correction typo dans définitions fs Johan Klotz authored 7 hours ago
	ajout tâches configuration systèmes de fichiers Johan Klotz authored 7 hours ago
	ajout paramétrages kernel Johan Klotz authored 7 hours ago
	ajout tâches configuration réseau système cible Johan Klotz authored 7 hours ago
	Initial commit Johan Klotz authored 7 hours ago

NON

	Johan Klotz @jklotz ⇄ Pushed to branch main c9b002e3 · update tmux.conf
	Johan Klotz @jklotz ⇄ Pushed to branch main 914b6966 · update tmux.conf
	Johan Klotz @jklotz ⇄ Pushed to branch main 8eacc460 · update tmux.conf



Merci





Seeding Ansible Automation Platform Content At Installation Time

By [Phil Griffiths](#) on October 4, 2023

**Rien entre septembre 2023 et mai 2024,
probablement abandonné.**

Articles techniques autour du
produit Ansible Automation
Platform

<https://www.ansible.com/blog>



Importing Ansible Validated Content into Private Automation Hub

By [Hicham Mourad](#) on October 3, 2023



Now serving: Event-Driven Ansible with a dash of durability

By [Colin McNaughton](#) on October 2, 2023



- Noeud de contrôle vs noeud géré (control node / managed node)
- https://docs.ansible.com/ansible/latest/reference_appendices/release_and_maintenance.html#ansible-core-support-matrix

Version	Support	End Of Life	Control Node Python	Target Python / PowerShell
2.17	GA: 20 May 2024 Critical: 04 Nov 2024 Security: 19 May 2025	Nov 2025	Python 3.10 - 3.12	Python 3.7 - 3.12 PowerShell 5.1
2.16	GA: 06 Nov 2023 Critical: 20 May 2024 Security: Nov 2024	May 2025	Python 3.10 - 3.12	Python 2.7 Python 3.6 - 3.12 Powershell 5.1
2.15	GA: 22 May 2023 Critical: 06 Nov 2023 Security: 20 May 2024	Nov 2024	Python 3.9 - 3.11	Python 2.7 Python 3.5 - 3.11 PowerShell 3 - 5.1
2.14	GA: 07 Nov 2022 Critical: 22 May 2023 Security: 06 Nov 2023	EOL 20 May 2024	Python 3.9 - 3.11	Python 2.7 Python 3.5 - 3.11 PowerShell 3 - 5.1
2.13	GA: 23 May 2022 Critical: 07 Nov 2022 Security: 22 May 2023	EOL 06 Nov 2023	Python 3.8 - 3.10	Python 2.7 Python 3.5 - 3.10 PowerShell 3 - 5.1