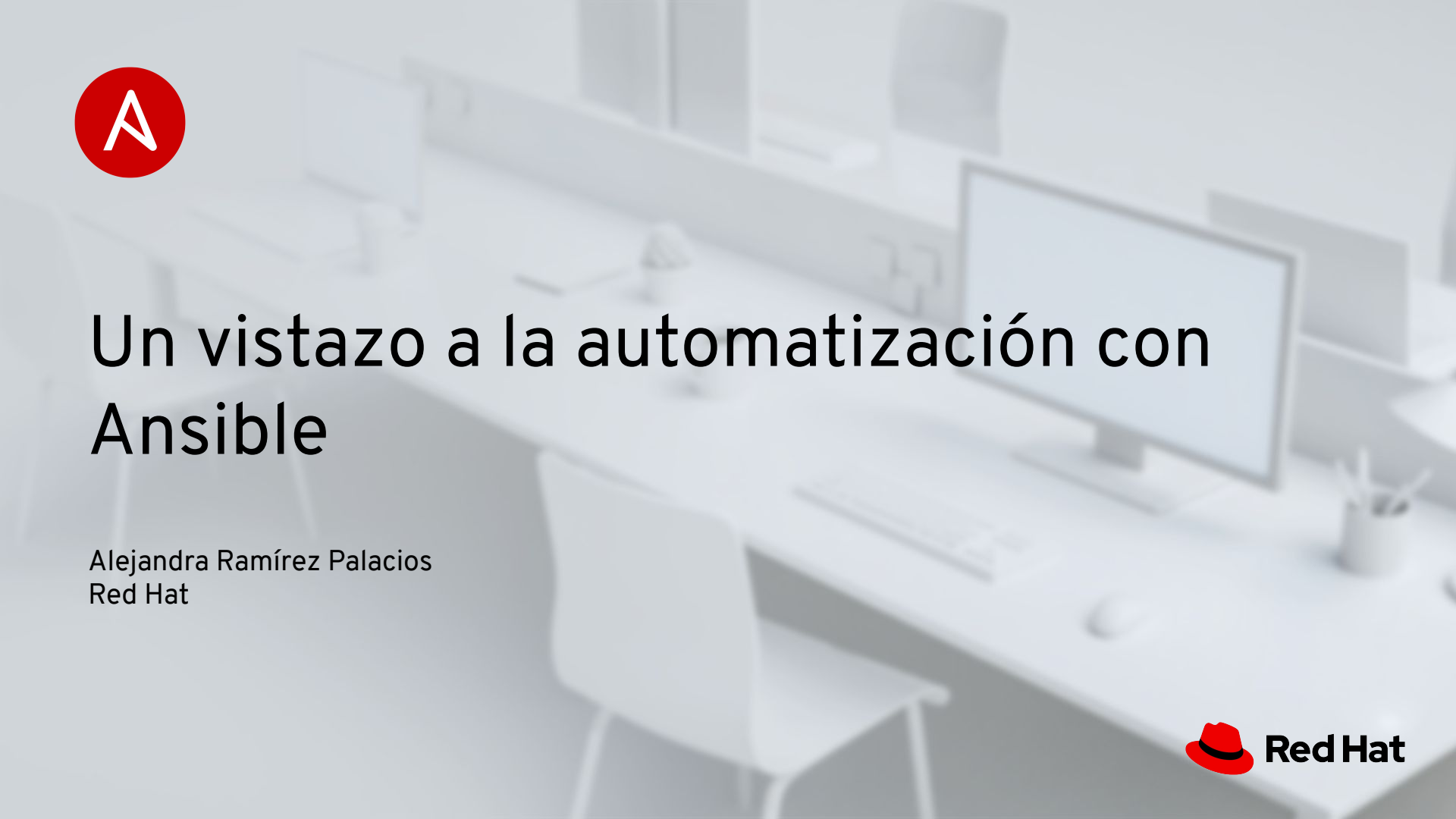


Un vistazo a la automatización con Ansible

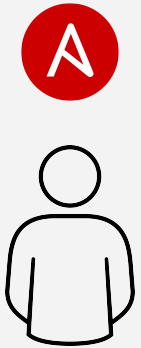
Alejandra Ramírez Palacios
Red Hat

Red Hat

¿De qué se trata?

La automatización tiene lugar cuando una persona se encuentra con una tarea que no quiere llevar a cabo de nuevo.

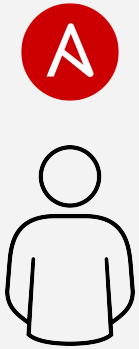
¿De qué se trata?



La automatización tiene lugar cuando una persona se encuentra con una tarea que no quiere llevar a cabo de nuevo.

¿De qué se trata?

Poderoso



La automatización tiene lugar cuando una persona se encuentra con una tarea que no quiere llevar a cabo de nuevo.

¿De qué se trata?

Poderoso

Simple

La automatización tiene lugar cuando una persona se encuentra con una tarea que no quiere llevar a cabo de nuevo.

Red Hat

¿De qué se trata?

Poderoso

Simple

La automatización tiene lugar cuando una persona se encuentra con una tarea que no quiere llevar a cabo de nuevo.

Sin agentes

Red Hat


Red Hat
Ansible
Engine
Instalación
Red Hat

No puede ser más simple

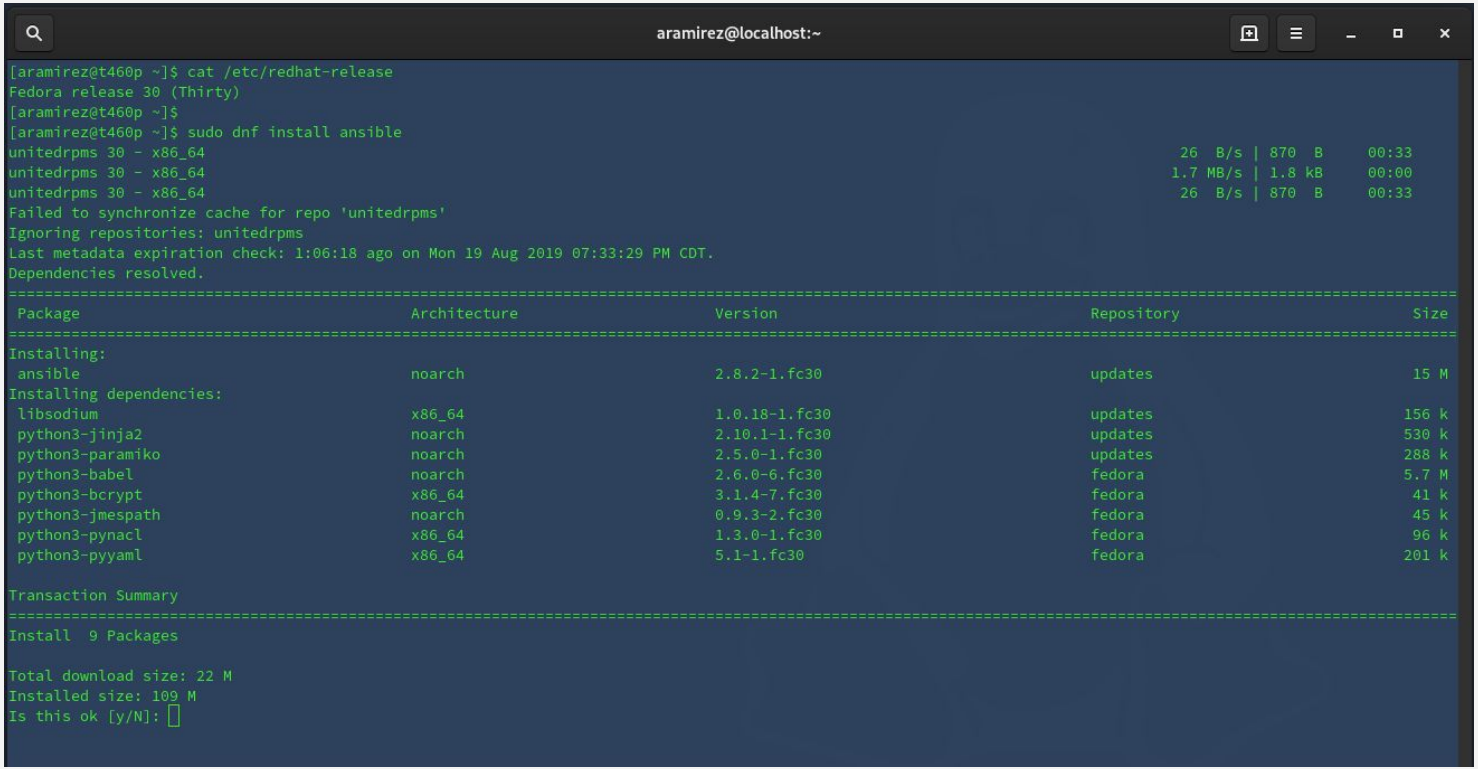
- En Red Hat Enterprise Linux

```
~]$ yum install ansible
```

- En Fedora

```
~]$ dnf install ansible
```

Red Hat


aramirez@localhost:~
[aramirez@t460p ~]$ cat /etc/redhat-release
Fedora release 30 (Thirty)
[aramirez@t460p ~]$
[aramirez@t460p ~]$ sudo dnf install ansible
unitedrpms 30 - x86_64 26 B/s | 870 B 00:33
unitedrpms 30 - x86_64 1.7 MB/s | 1.8 kB 00:00
unitedrpms 30 - x86_64 26 B/s | 870 B 00:33
Failed to synchronize cache for repo 'unitedrpms'
Ignoring repositories: unitedrpms
Last metadata expiration check: 1:06:18 ago on Mon 19 Aug 2019 07:33:29 PM CDT.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
ansible noarch 2.8.2-1.fc30 updates 15 M
Installing dependencies:
libsodium x86_64 1.0.18-1.fc30 updates 156 k
python3-jinja2 noarch 2.10.1-1.fc30 updates 530 k
python3-paramiko noarch 2.5.0-1.fc30 updates 288 k
python3-babel noarch 2.6.0-6.fc30 fedora 5.7 M
python3-bcrypt x86_64 3.1.4-7.fc30 fedora 41 k
python3-jmespath noarch 0.9.3-2.fc30 fedora 45 k
python3-pynacl x86_64 1.3.0-1.fc30 fedora 96 k
python3-pyyaml x86_64 5.1-1.fc30 fedora 201 k
Transaction Summary
Install 9 Packages
Total download size: 22 M
Installed size: 109 M
Is this ok [y/N]:

Red Hat

Archivos de configuración

Configuración base

`/etc/ansible/ansible.cfg`

`/etc/ansible/hosts`

Ejemplo:

ansible.cfg

```
[defaults]
inventory       = ./inventory
remote_user = root
```

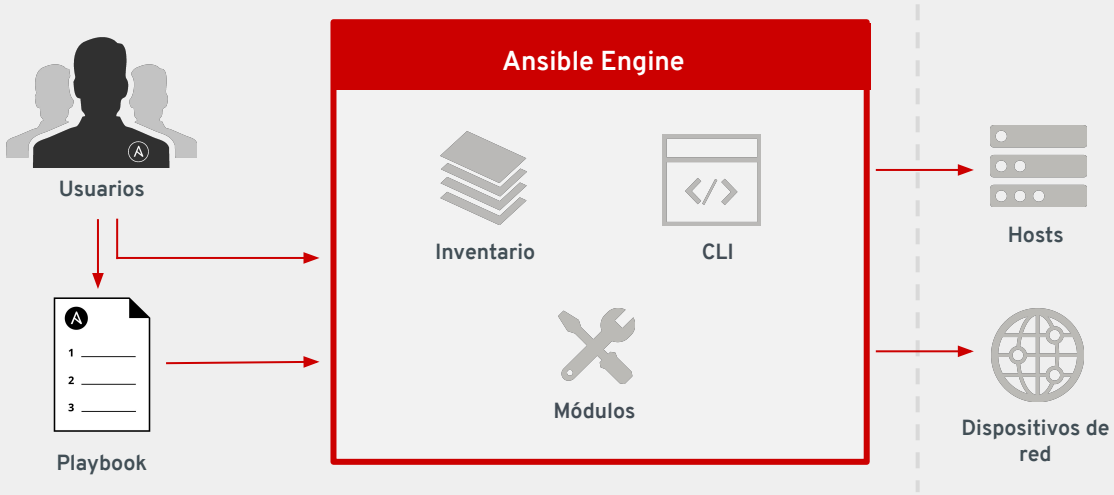
La práctica recomendada es crear el archivo `ansible.cfg` en un directorio desde el que se ejecute instrucciones de Ansible.

Este directorio también contendría el `inventario` y los `playbooks`.

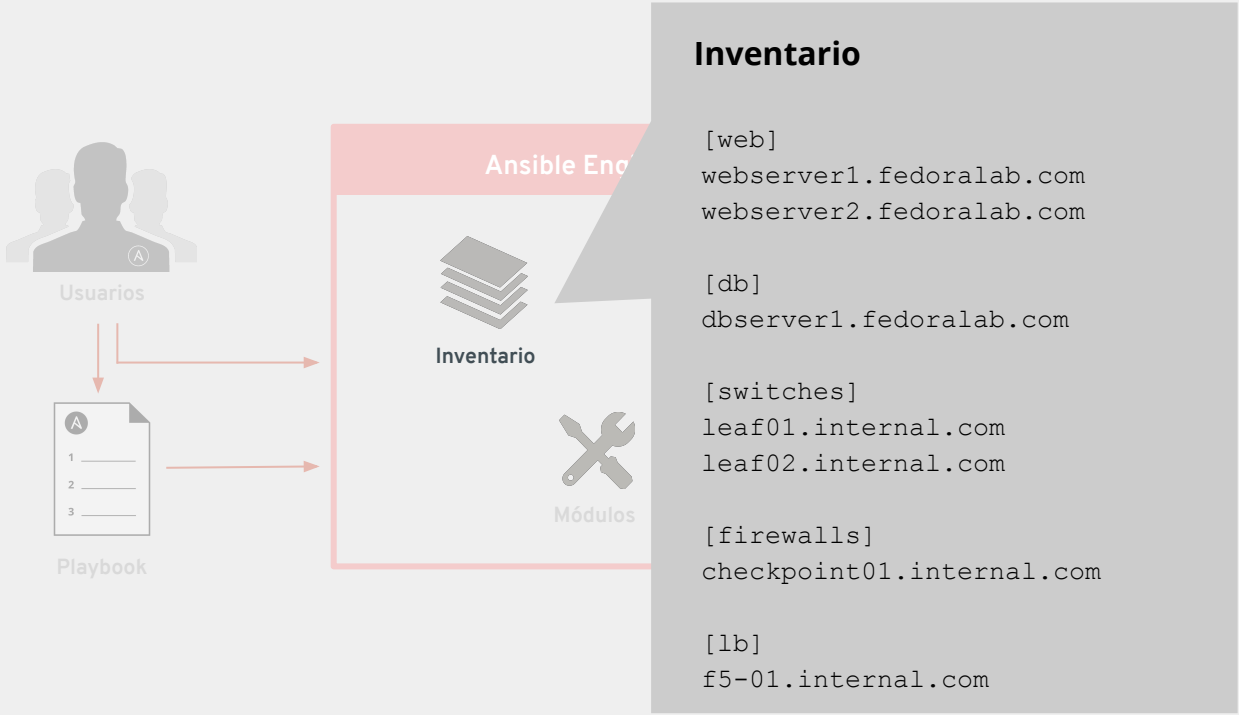
Red Hat


Red Hat
Ansible
Engine
El lenguaje de la automatización
Red Hat

Componentes básicos

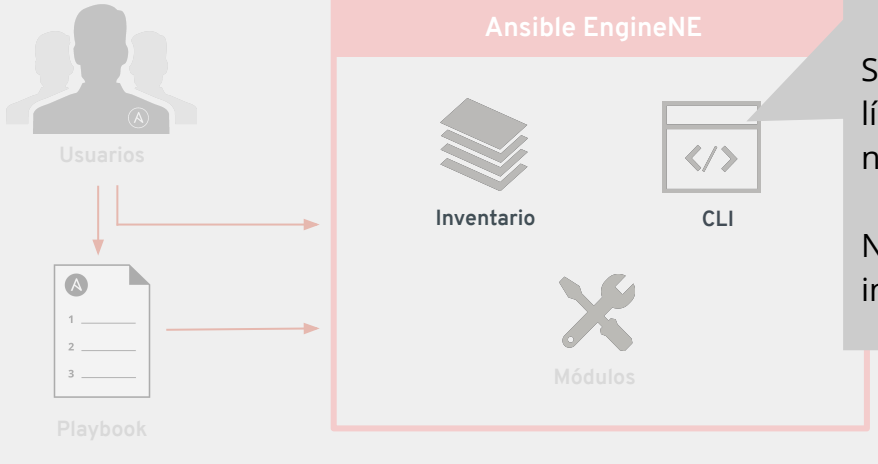


Componentes básicos



Red Hat

Componentes básicos



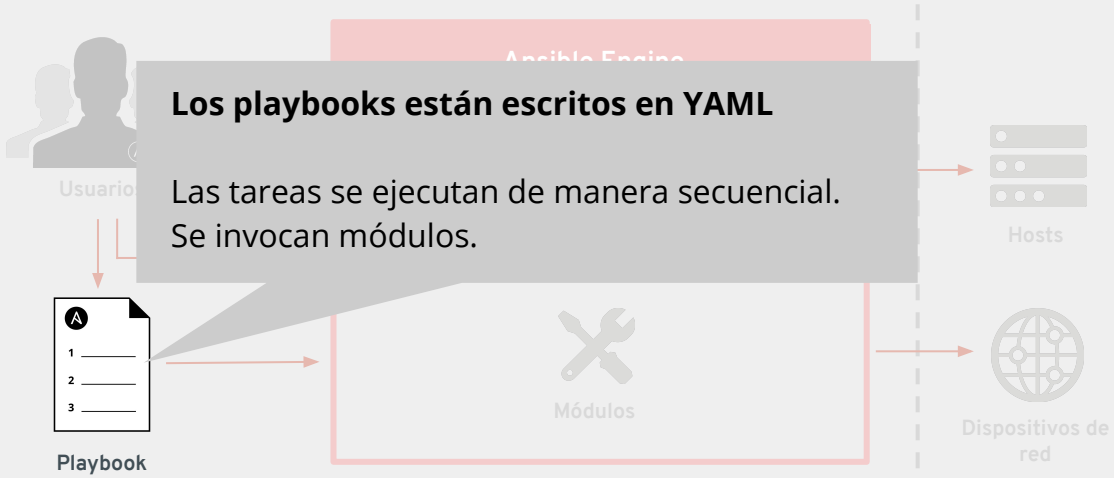
Ansible Ad-Hoc

Se refiere a un comando de una línea para realizar alguna tarea en nuestro inventario de hosts.

No nos interesa guardar la instrucción para después.

Red Hat

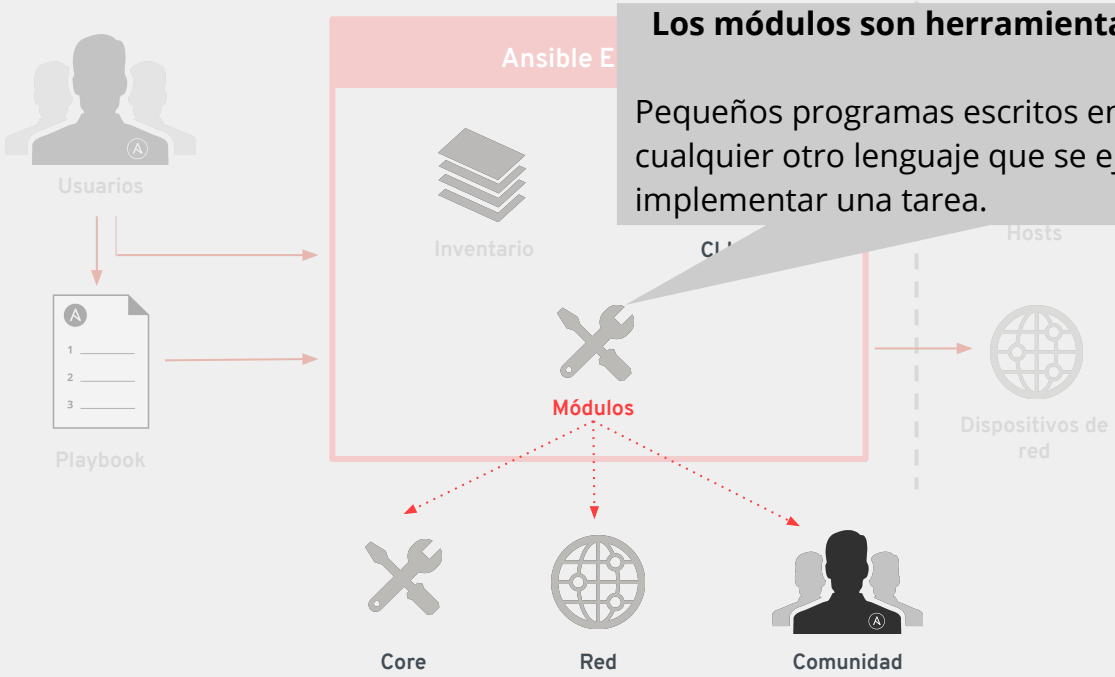
Componentes básicos



Los playbooks están escritos en YAML

Las tareas se ejecutan de manera secuencial.
Se invocan módulos.

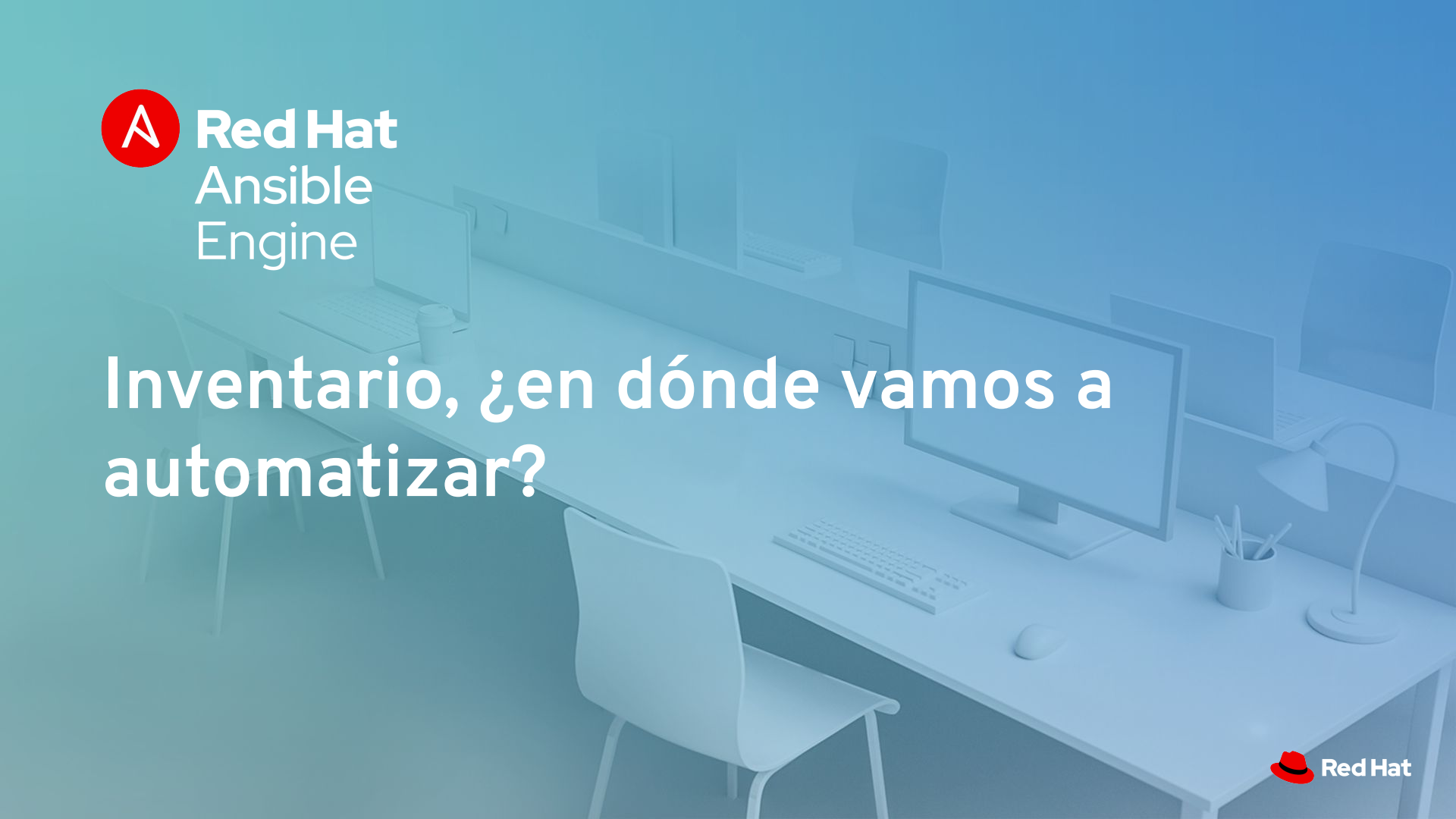
Componentes básicos



Los módulos son herramientas en el toolkit

Pequeños programas escritos en Python, PowerShell o cualquier otro lenguaje que se ejecutan para implementar una tarea.

Red Hat


Red Hat
Ansible
Engine
Inventario, ¿en dónde vamos a automatizar?
Red Hat

Inventario

Es una colección de hosts y agrupaciones que Ansible puede utilizar.

- Estático
- Dinámico

Ejemplo de inventario estático

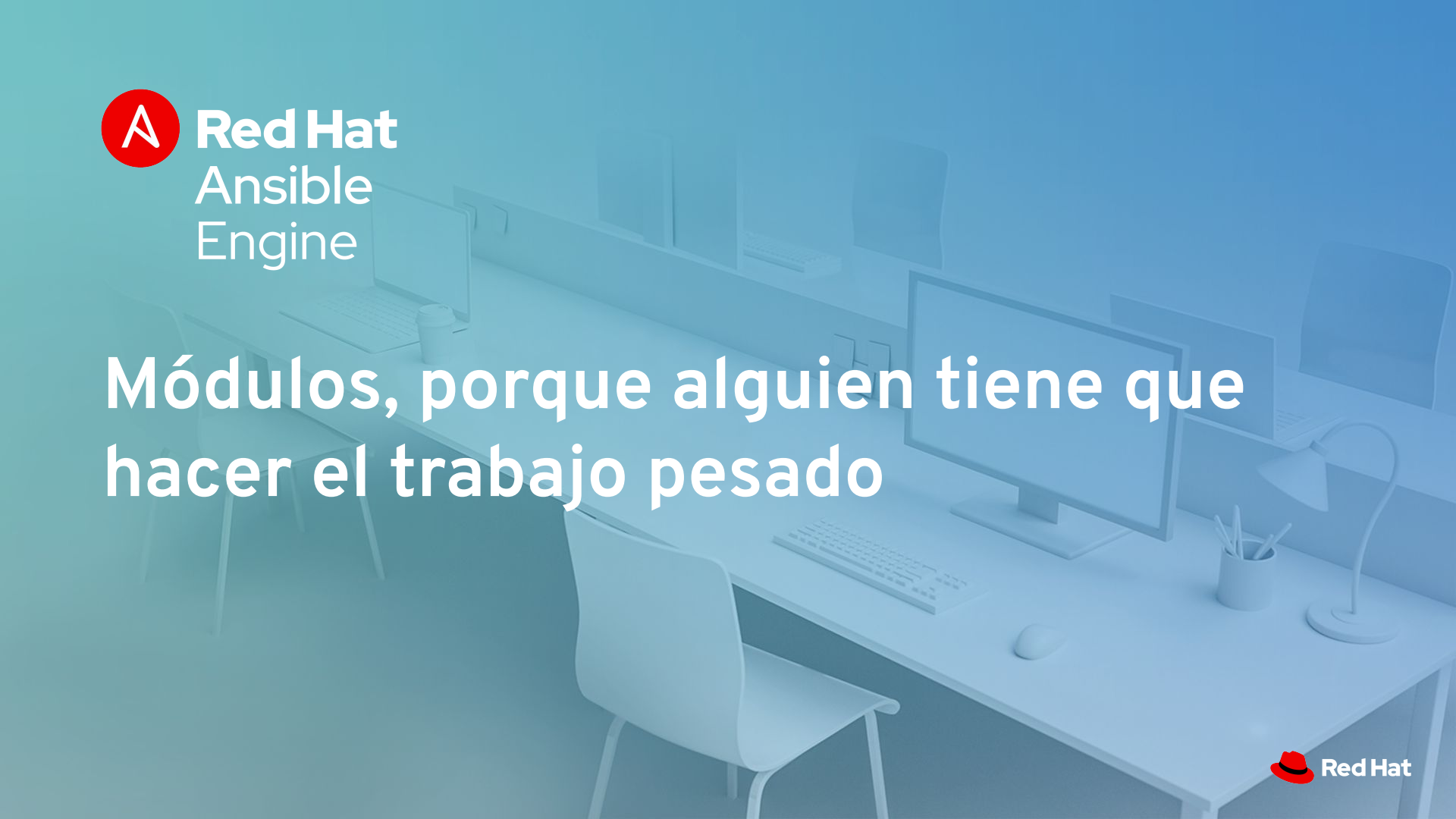
```
[web]
web1.fedora.net
web2.fedora.net
web3.fedora.net

[db]
db1.fedora.net
db2.fedora.net
```

Inventario

```
[web]

web1.fedora.net

[db]

db1.fedora.net

[dns]

dns1.fedora.net

[frontend:children]

web

[backend:children]

dns

db
```

Se pueden tener grupos de grupos:

[groupname:children]


Red Hat
Ansible
Engine
Módulos, porque alguien tiene que hacer el trabajo pesado
Red Hat

Módulos

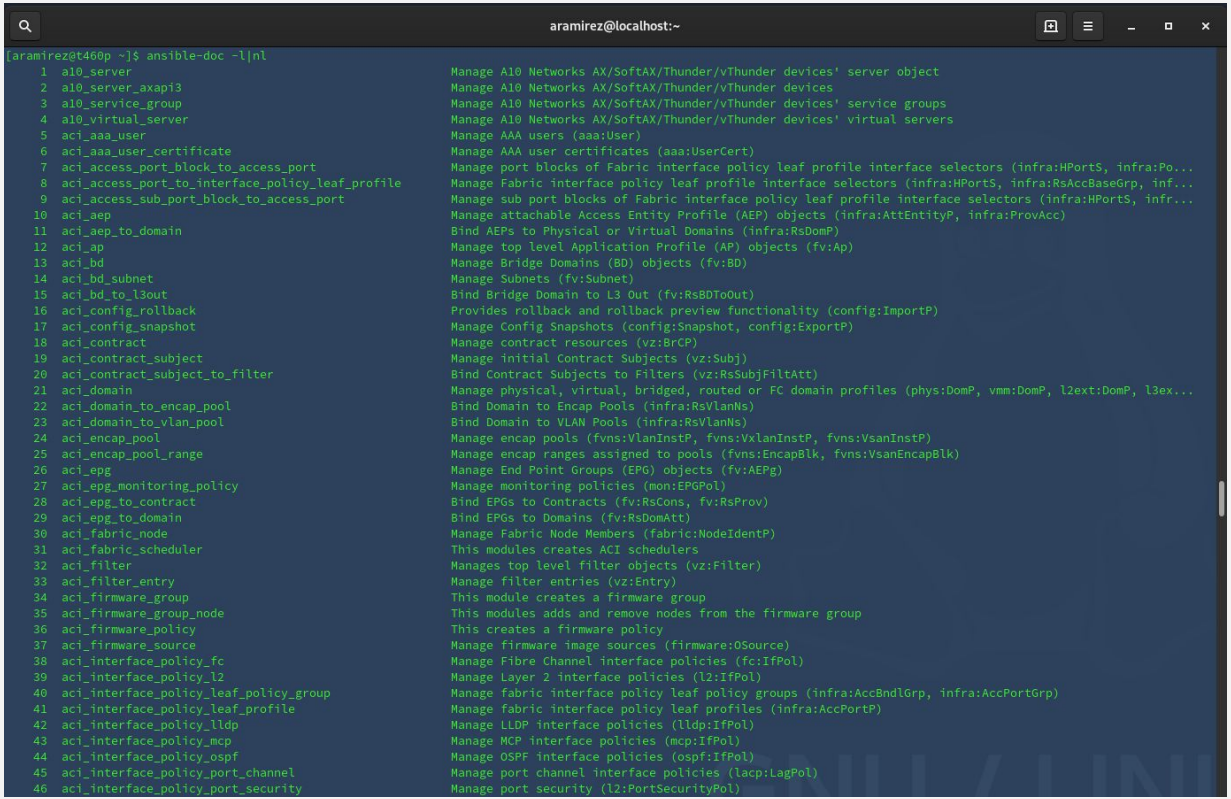
Podemos revisar la lista de módulos disponibles para uso por medio de:

```
~] ansible-doc -l
```

Ejemplo de módulos

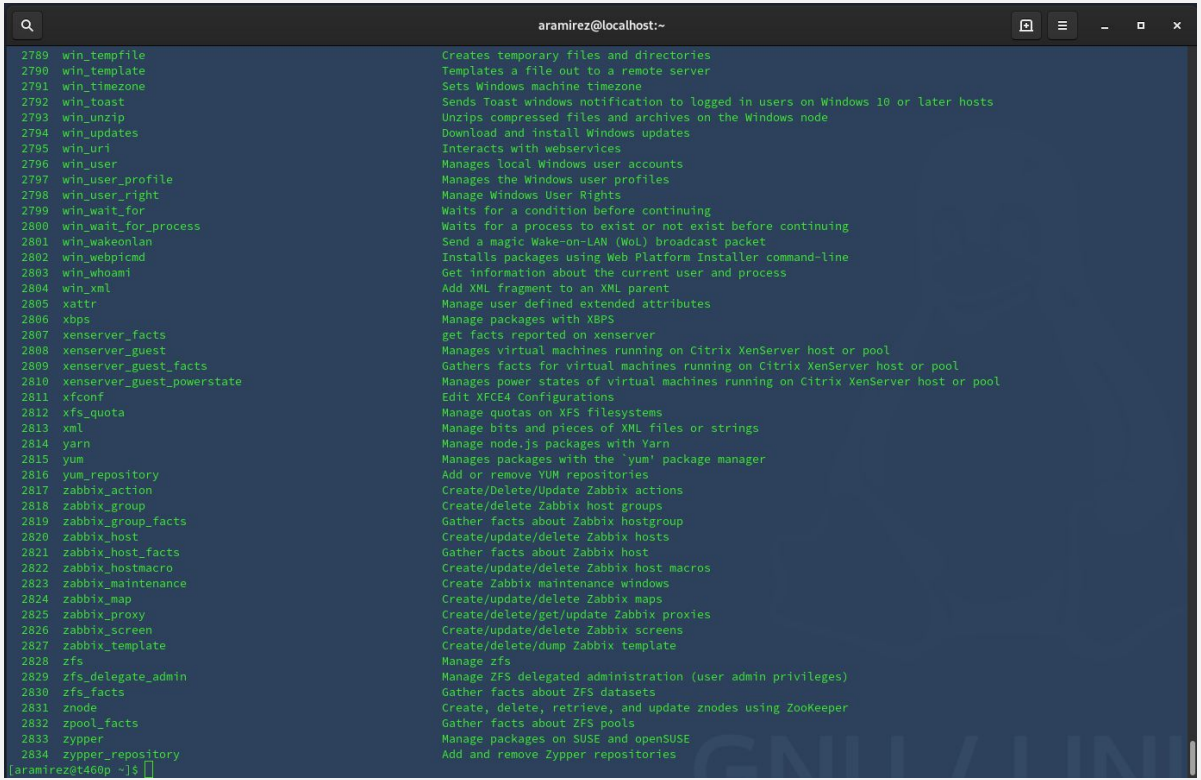
- **yum**
- **copy**
- **file**
- **ping**
- **debug**
- **service**
- **user**
- **firewalld**

Módulos



Red Hat

Módulos

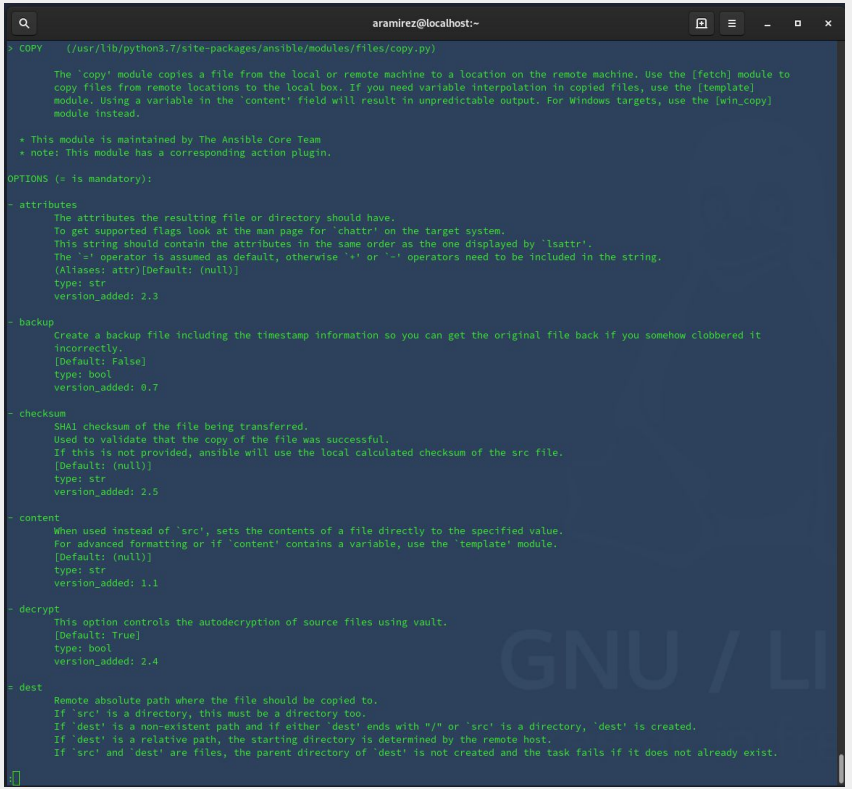


Red Hat

Documentación de los módulos

Para obtener la documentación detallada de un módulo, digamos del módulo “copy”:

```
~] ansible-doc copy
```



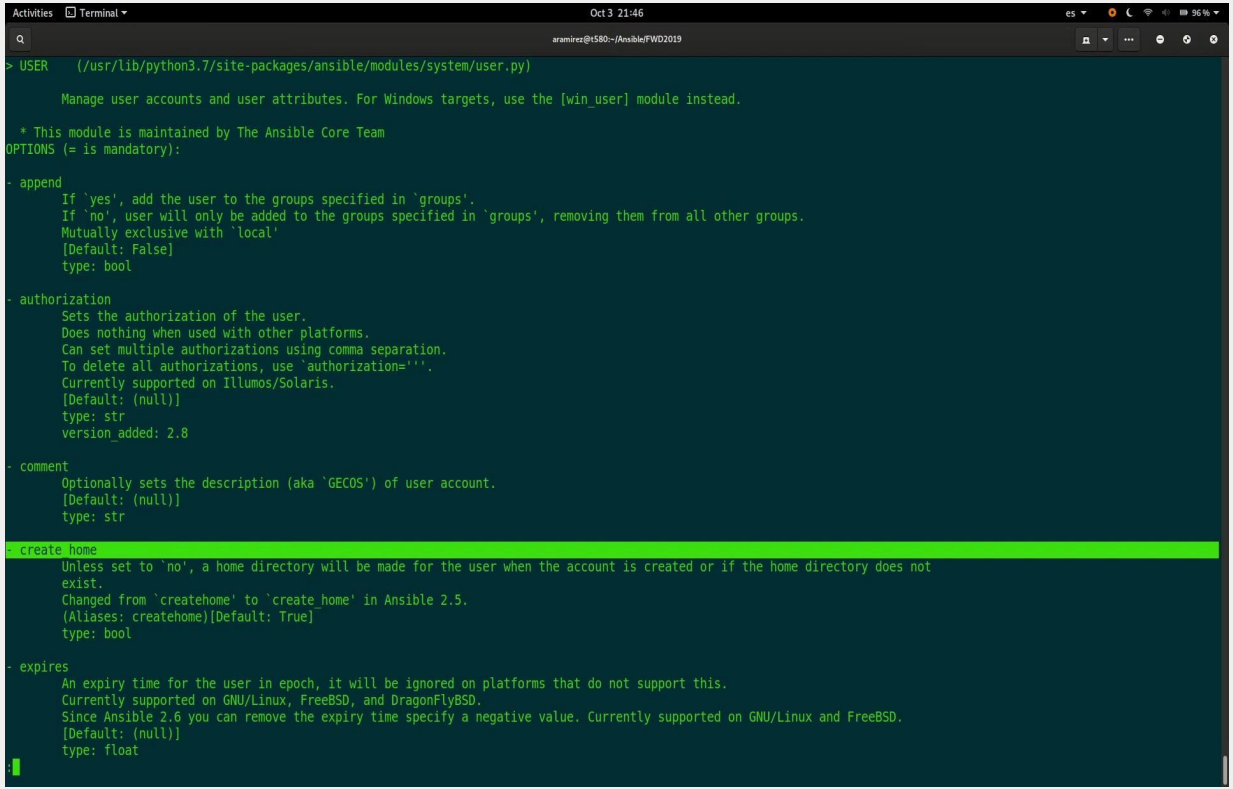
Red Hat

Ejemplos

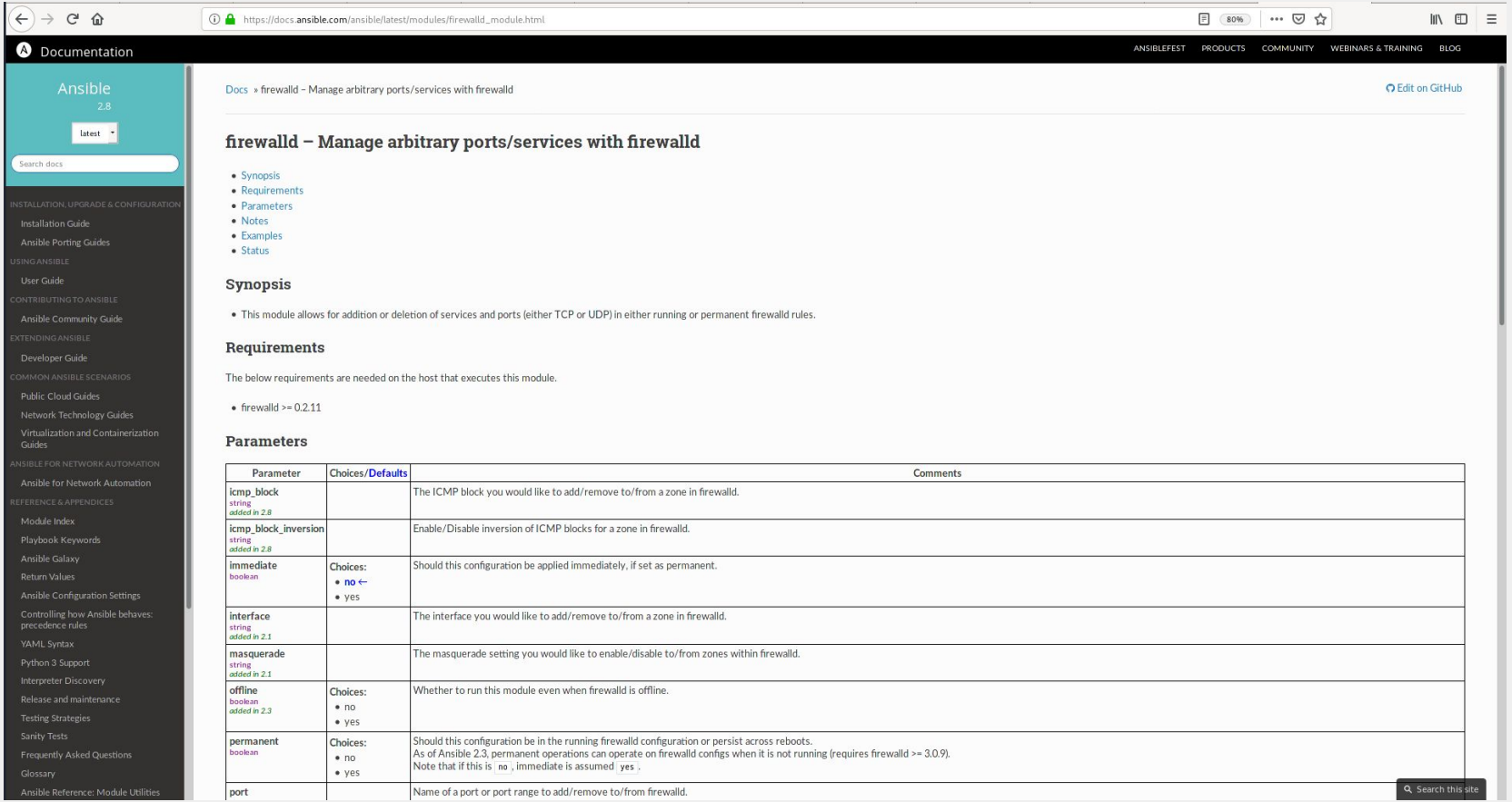
Veamos un ejemplo usando el módulo ‘copy’:

```
- name: Copiando un archivo
  copy:
    src: /home/aramirez/fedora_30.txt
    dest: /remote/fedora_30.txt
    owner: aramirez
    group: aramirez
    mode: '0644'
```

Ejemplos



Red Hat


https://docs.ansible.com/ansible/latest/modules/firewalld_module.html
80%
Documentation
ANSIBLEFEST
PRODUCTS
COMMUNITY
WEBINARS & TRAINING
BLOG
Ansible
2.8
latest
Search docs
INSTALLATION, UPGRADE & CONFIGURATION
Installation Guide
Ansible Porting Guides
USING ANSIBLE
User Guide
CONTRIBUTING TO ANSIBLE
Ansible Community Guide
EXTENDING ANSIBLE
Developer Guide
COMMON ANSIBLE SCENARIOS
Public Cloud Guides
Network Technology Guides
Virtualization and Containerization Guides
ANSIBLE FOR NETWORK AUTOMATION
Ansible for Network Automation
REFERENCE & APPENDICES
Module Index
Playbook Keywords
Ansible Galaxy
Return Values
Ansible Configuration Settings
Controlling how Ansible behaves: precedence rules
YAML Syntax
Python 3 Support
Interpreter Discovery
Release and maintenance
Testing Strategies
Sanity Tests
Frequently Asked Questions
Glossary
Ansible Reference: Module Utilities
Docs » firewalld – Manage arbitrary ports/services with firewalld
Edit on GitHub
firewalld – Manage arbitrary ports/services with firewalld
Synopsis
Requirements
Parameters
Notes
Examples
Status
Synopsis
This module allows for addition or deletion of services and ports (either TCP or UDP) in either running or permanent firewalld rules.
Requirements
The below requirements are needed on the host that executes this module.
firewalld >= 0.2.11
Parameters
Parameter
Choices/Defaults
Comments
icmp_block
string
added in 2.8
The ICMP block you would like to add/remove to/from a zone in firewalld.
icmp_block_inversion
string
added in 2.8
Enable/Disable inversion of ICMP blocks for a zone in firewalld.
immediate
boolean
Choices:
no ←
yes
Should this configuration be applied immediately, if set as permanent.
interface
string
added in 2.1
The interface you would like to add/remove to/from a zone in firewalld.
masquerade
string
added in 2.1
The masquerade setting you would like to enable/disable to/from zones within firewalld.
offline
boolean
added in 2.3
Choices:
no
yes
Whether to run this module even when firewalld is offline.
permanent
boolean
Choices:
no
yes
Should this configuration be in the running firewalld configuration or persist across reboots.
As of Ansible 2.3, permanent operations can operate on firewalld configs when it is not running (requires firewalld >= 3.0.9).
Note that if this is no, immediate is assumed yes.
port
Name of a port or port range to add/remove to/from firewalld.
Search this site

Red Hat


Red Hat
Ansible
Engine
Instrucciones Ad-Hoc,
rápido y fácil
Red Hat

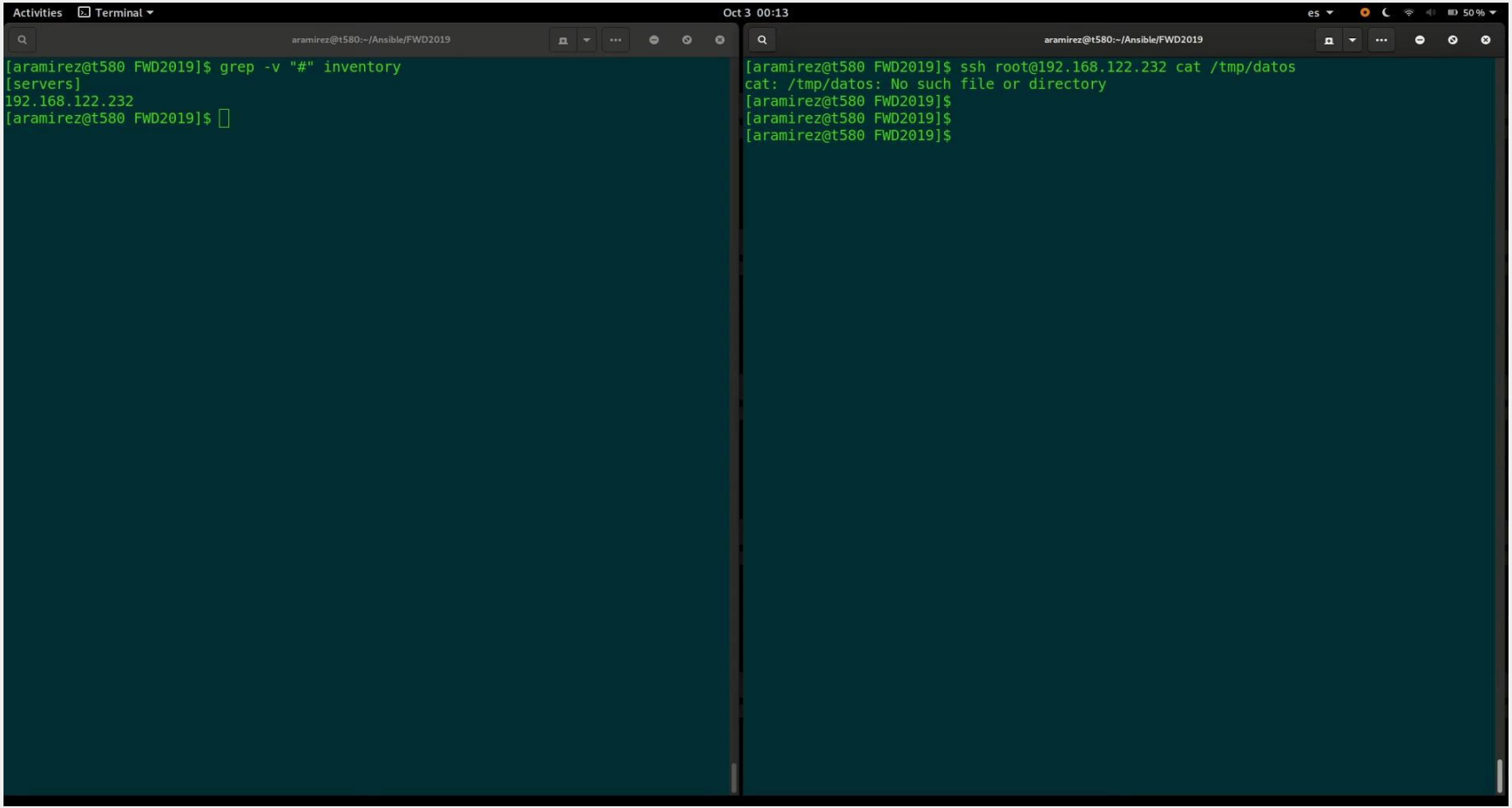
Instrucciones Ad-hoc

Se trata de tareas únicas Ansible que se realizan rápidamente, pero no se desea guardar para más adelante.

```
~]$ ansible all -m ping
```

```
~]$ ansible web -m command -a “uptime”
```

Red Hat


Activities
Terminal
Oct 3 00:13
es
50 %
aramirez@t580:~/Ansible/FWD2019
[aramirez@t580 FWD2019]$ grep -v "#" inventory
[servers]
192.168.122.232
[aramirez@t580 FWD2019]$
aramirez@t580:~/Ansible/FWD2019
[aramirez@t580 FWD2019]$ ssh root@192.168.122.232 cat /tmp/datos
cat: /tmp/datos: No such file or directory
[aramirez@t580 FWD2019]$
[aramirez@t580 FWD2019]$
[aramirez@t580 FWD2019]$

Red Hat


Red Hat
Ansible
Engine
Playbooks,
ahora sí, automaticemos
Red Hat

Ejemplos

```
---
- name: Actualiza los servidores
  hosts: web, db

  tasks:
    - name: Actualiza los servidores
      yum:
        name: '*'
        state: latest
```

- Formato YAML.
- Inicio con 3 guiones (-).
- Sangrías iguales para datos en el mismo nivel de jerarquía.
- Se define como una lista de reproducciones, en donde un elemento comienza con guión.
- Se usan espacios, no tabulación.

Ejemplos

```
---
- name: Instala y levanta Apache
  hosts: web

  tasks:
    - name: Instala Apache
      yum:
        name: httpd
        state: present

    - name: Servicio activo
      service:
        name: httpd
        state: started
```


Red Hat
Ansible
Engine
Handlers,
tareas especiales
Red Hat

Handlers

Se trata de tareas que únicamente se ejecutan cuando existe una directiva de notificación dentro del playbook que indica que hubo un cambio que la require.

```
tasks:
  - name: Configuración local del Mail Transfer Agent
    lineinfile:
      dest: /etc/postfix/main.cf
      regexp: "^inet_interfaces"
      line: "inet_interfaces = loopback-only"
```

Handlers

```
tasks:
  - name: Configuración local del Mail Transfer Agent
    lineinfile:
      dest: /etc/postfix/main.cf
      regexp: "^inet_interfaces"
      line: "inet_interfaces = loopback-only"

  - name: Reinicio de Postfix
    service:
      name: postfix
      state: restarted
```

Handlers

```
tasks:
  - name: Configuración local del Mail Transfer Agent
    lineinfile:
      dest: /etc/postfix/main.cf
      regexp: "^inet_interfaces"
      line: "inet_interfaces = loopback-only"

  - name: Reinicio de Postfix
    service:
      name: postfix
      state: restarted
```

Handlers

Se trata de tareas que únicamente se ejecutan cuando existe una directiva de notificación dentro del playbook que indica que hubo un cambio que la require.

```
tasks:
  - name: Configuración local del Mail Transfer Agent
    lineinfile:
      dest: /etc/postfix/main.cf
      regexp: "^inet_interfaces"
      line: "inet_interfaces = loopback-only"
    notify: Reinicia postfix
```

En el playbook:

```
tasks:
  - name: Configuración local del Mail Transfer Agent
    lineinfile:
      dest: /etc/postfix/main.cf
      regexp: "^inet_interfaces"
      line: "inet_interfaces = loopback-only"
    notify: Reinicia postfix
```

Notificamos al handler:

```
handlers:
  - name: Reinicia postfix
    service:
      name: postfix
      state: restarted
```

Red Hat


Red Hat
Ansible
Engine
Roles
Una colección de todo lo anterior
Red Hat


```
aramirez@t580:~/FWD2019
[aramirez@t580 FWD2019]$ tree .
.
├── ansible.cfg
├── cis_security_rhel.yml
├── inventory
├── LICENSE
├── README.md
└── roles
    └── cis_security_rhel
        ├── files
        │   ├── check_archivos_dot.sh
        │   ├── check_archivos_forward.sh
        │   ├── check_archivos_netrc.sh
        │   ├── check_archivos_rhosts.sh
        │   ├── check_gids_duplicados.sh
        │   ├── check_groups_duplicados.sh
        │   ├── check_groups.sh
        │   ├── check_home_directorios.sh
        │   ├── check_home_permisos.sh
        │   ├── check_home_propiedad.sh
        │   ├── check_path_integrity.sh
        │   ├── check_uids_duplicados.sh
        │   ├── check_usernames_duplicados.sh
        │   ├── chrony.conf
        │   ├── password-auth
        │   ├── su
        │   └── system-auth
        ├── handlers
        │   └── main.yml
        ├── tasks
        │   ├── fwd2019_cis_1-1.yml
        │   ├── fwd2019_cis_1-2.yml
        │   ├── fwd2019_cis_1-3.yml
        │   ├── fwd2019_cis_1-4.yml
        │   ├── fwd2019_cis_1-5.yml
        │   ├── fwd2019_cis_1-8.yml
        │   ├── fwd2019_cis_2-1.yml
        │   ├── fwd2019_cis_2-2.yml
        │   ├── fwd2019_cis_2-3.yml
        │   ├── fwd2019_cis_3-1.yml
        │   ├── fwd2019_cis_3-2.yml
        │   ├── fwd2019_cis_3-3.yml
        │   ├── fwd2019_cis_3-4.yml
        │   ├── fwd2019_cis_3-6.yml
        │   ├── fwd2019_cis_4-2.yml
        │   ├── fwd2019_cis_5-1.yml
        │   ├── fwd2019_cis_5-2.yml
        │   ├── fwd2019_cis_5-3.yml
        │   ├── fwd2019_cis_5-4.yml
        │   ├── fwd2019_cis_5-6.yml
        │   ├── fwd2019_cis_6-1.yml
        │   ├── fwd2019_cis_6-2.yml
        │   └── main.yml
        └── vars
            └── main.yml

6 directories, 47 files
[aramirez@t580 FWD2019]$
```

Red Hat

Tareas y Handlers

aramirez@t580:~/Ansible/FWD2019

```
---
- set_fact:
    politica: CIS_5-2

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Validando instalación de ssh'
  yum:
    name: openssh-server
    state: present

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: SSH habilitado y corriendo'
  service:
    name: sshd
    enabled: yes
    state: started

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Definiendo permisos en /etc/ssh/sshd_config'
  file:
    path: /etc/ssh/sshd_config
    owner: root
    group: root
    mode: 0600

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Estableciendo Protocolo'
  lineinfile:
    path: '/etc/ssh/sshd_config'
    regexp: '^Protocol'
    line: 'Protocol 2'
    state: present
  notify: 'FWD2019 :::: Handler :--> Restarting sshd'

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Estableciendo LogLevel'
  lineinfile:
    path: '/etc/ssh/sshd_config'
    regexp: '^LogLevel'
    line: 'LogLevel INFO'
    state: present
  notify: 'FWD2019 :::: Handler :--> Restarting sshd'

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Deshabilitando reenvío X11'
  lineinfile:
    path: '/etc/ssh/sshd_config'
    regexp: '^X11Forwarding'
    line: 'X11Forwarding no'
    state: present
  notify: 'FWD2019 :::: Handler :--> Restarting sshd'

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Estableciendo MaxAuthTries'
  lineinfile:
    path: '/etc/ssh/sshd_config'
    regexp: '^MaxAuthTries'
    line: 'MaxAuthTries 4'
    state: present
  notify: 'FWD2019 :::: Handler :--> Restarting sshd'

- name: '{{ client }} :::: {{ project }} :::: {{ politica }} :::: Estableciendo IgnoreRhosts'
  lineinfile:
-- INSERT --                                                    1,4           Top
```

aramirez@t580:~/Ansible/FWD2019

```
---
# handlers file for cis_security_servers

- name: 'FWD2019 :::: Handler :--> Restarting chronyd'
  service:
    name: chronyd
    state: restarted

- name: 'FWD2019 :::: Handler :--> Restarting postfix'
  service:
    name: postfix
    state: restarted

- name: 'FWD2019 :::: Handler :--> Flushing Cache'
  command: sysctl -w net.ipv4.route.flush=1

- name: 'FWD2019 :::: Handler :--> Restarting sshd'
  service:
    name: sshd
    state: restarted
~
~
~
                                                             20,22         All
```

Red Hat

Variables

aramirez@t580:~/FWD2019

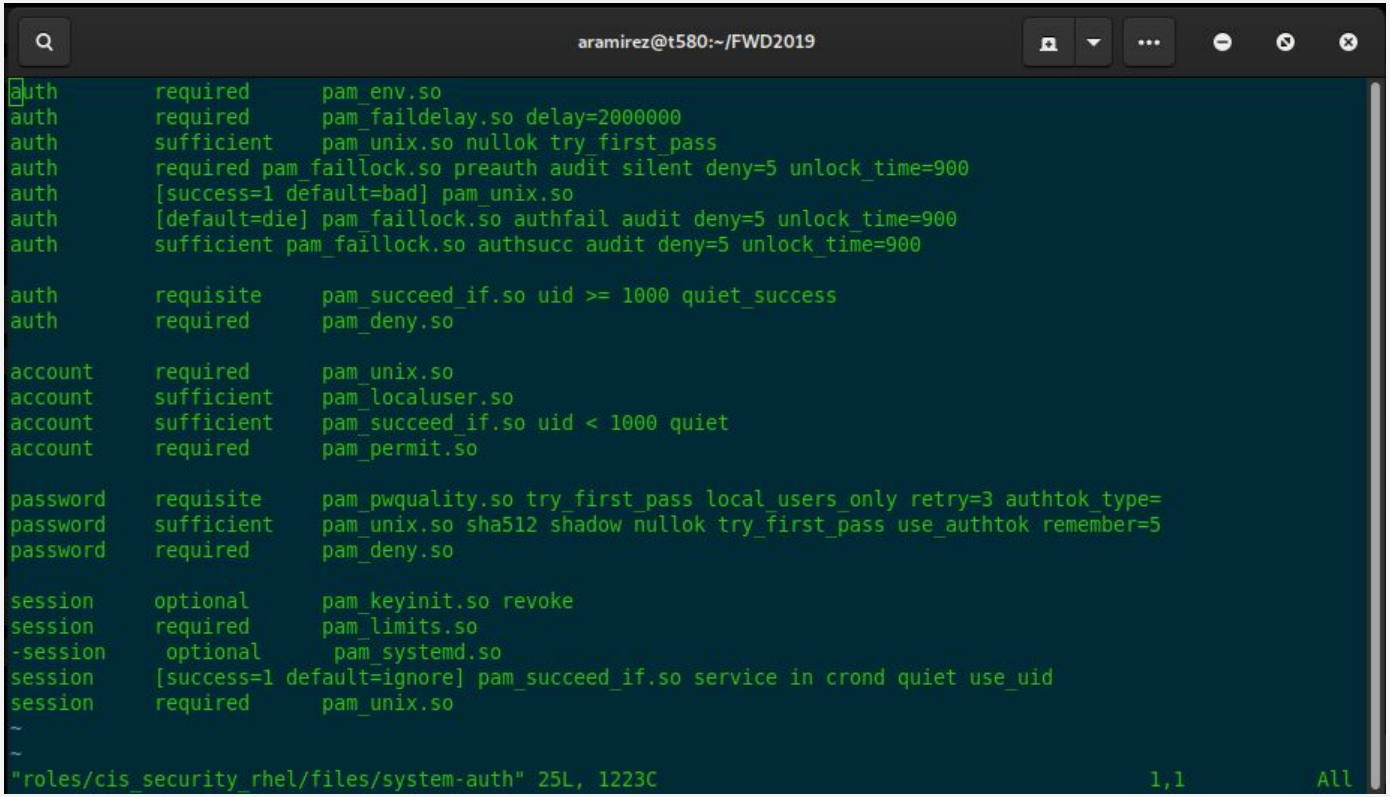
```
---
# vars file for baz_cis_security_ocpservers
#-------------------- Cliente --------------------#
project: 'Hardening for Servers'
client: 'FW2019'
#--------------------  FS  --------------------#
fs2install:
  - "install cramfs /bin/true"
  - "install freevxfs /bin/true"
  - "install jffs2 /bin/true"
  - "install hfs /bin/true"
  - "install hfsplus /bin/true"
  - "install squashfs /bin/true"
  - "install udf /bin/true"
#---------------------- banners ---------------#
banner_message: "  "
#-----------------  Servicios  ---------------#
servicios_no_necesarios:
  - "xorg-x11*"
  - "avahi"
  - "cups"
  - "dhcp-libs"
  - "openldap-servers"
  - "rpcbind"
  - "nfslock"
  - "bind"
  - "vsftpd"
  - "httpd"
  - "dovecot"
  - "samba"
  - "squid"
  - "ypserv"
  - "net-snmp"
  - "nfslock"
  - "rsh-server"
  - "talk-server"
  - "telnet-server"
  - "tftp-server"
  - "rsync"
clientes_no_necesarios:
  - "ypbind"
  - "telnet"
  - "talk"
  - "rsh"
  - "openldap-clients"
                                                1,3           Top
```

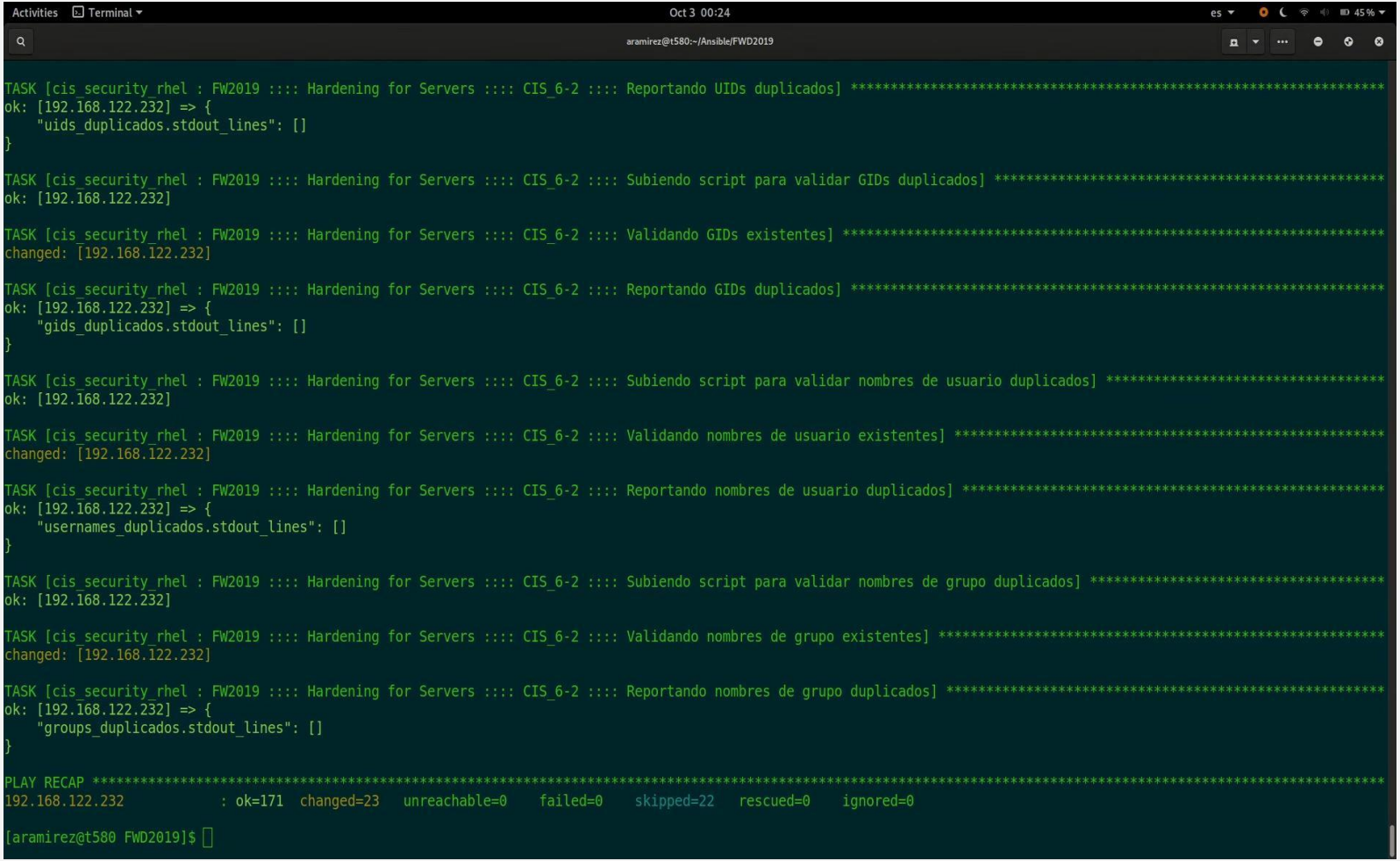
aramirez@t580:~/FWD2019

```
archivos_umask:
  - "/etc/bashrc"
  - "/etc/profile"
#---------------------- PASSWORDS --------------------#
pw_quality:
  - minlen = 14
  - dcredit = -1
  - ucredit = -1
  - ocredit = -1
  - lcredit = -1
passwords_644:
  - "/etc/passwd"
  - "/etc/group"
  - "/etc/passwd-"
  - "/etc/group-"
passwords_000:
  - "/etc/shadow"
  - "/etc/gshadow"
  - "/etc/shadow-"
  - "/etc/gshadow-"
#-------USER/GROUP de archivos sin user/group ---------#
                                                81,1          97%
```

Red Hat

Archivos que se subirán a los hosts




Activities
Terminal
Oct 3 00:24
es
45 %
aramirez@t580:~/Ansible/FWD2019
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Reportando UIDs duplicados] ********
ok: [192.168.122.232] => {
"uids_duplicados.stdout_lines": []
}
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Subiendo script para validar GIDs duplicados] ********
ok: [192.168.122.232]
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Validando GIDs existentes] ********
changed: [192.168.122.232]
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Reportando GIDs duplicados] ********
ok: [192.168.122.232] => {
"gids_duplicados.stdout_lines": []
}
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Subiendo script para validar nombres de usuario duplicados] ********
ok: [192.168.122.232]
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Validando nombres de usuario existentes] ********
changed: [192.168.122.232]
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Reportando nombres de usuario duplicados] ********
ok: [192.168.122.232] => {
"usernames_duplicados.stdout_lines": []
}
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Subiendo script para validar nombres de grupo duplicados] ********
ok: [192.168.122.232]
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Validando nombres de grupo existentes] ********
changed: [192.168.122.232]
TASK [cis_security_rhel : FW2019 :::: Hardening for Servers :::: CIS_6-2 :::: Reportando nombres de grupo duplicados] ********
ok: [192.168.122.232] => {
"groups_duplicados.stdout_lines": []
}
PLAY RECAP ********
192.168.122.232 : ok=171 changed=23 unreachable=0 failed=0 skipped=22 rescued=0 ignored=0
[aramirez@t580 FWD2019]$


Red Hat
Ansible
Engine
¿Preguntas?
Red Hat

¡Gracias!

Si quieres saber más sobre Ansible, no dejes de visitar:

https://www.ansible.com/resources/get-started

Red Hat