



# Un vistazo a la automatización con Ansible

Alejandra Ramírez Palacios  
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.

# ¿De qué se trata?



**Poderoso**

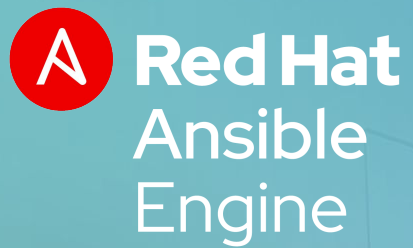


**Simple**

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



**Sin agentes**



# Instalación

# No puede ser más simple

- En Red Hat Enterprise Linux

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

- En Fedora

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



```
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]:

# Archivos de configuración

## Configuración base

`/etc/ansible/ansible.cfg`

`/etc/ansible/hosts`

Ejemplo:

`ansible.cfg`

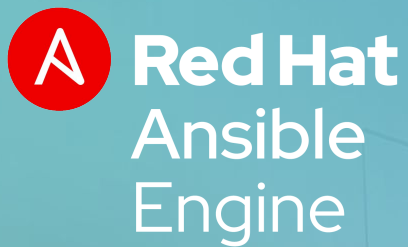
`[defaults]`

`inventory = ./inventory`

`remote_user = root`

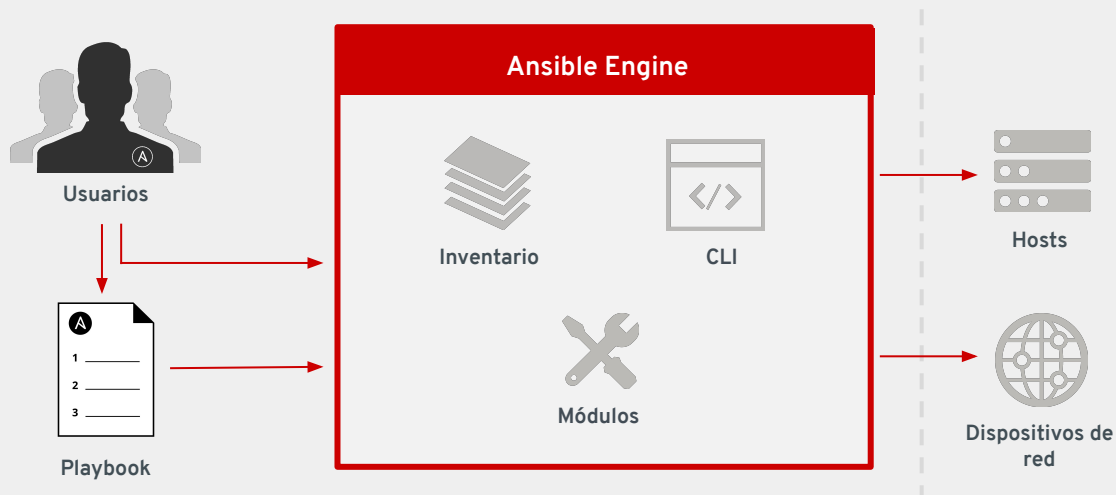
**La práctica recomendada es crear el archivo `ansible.cfg` en un directorio desde el que se ejecute instrucciones de Ansible.**

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

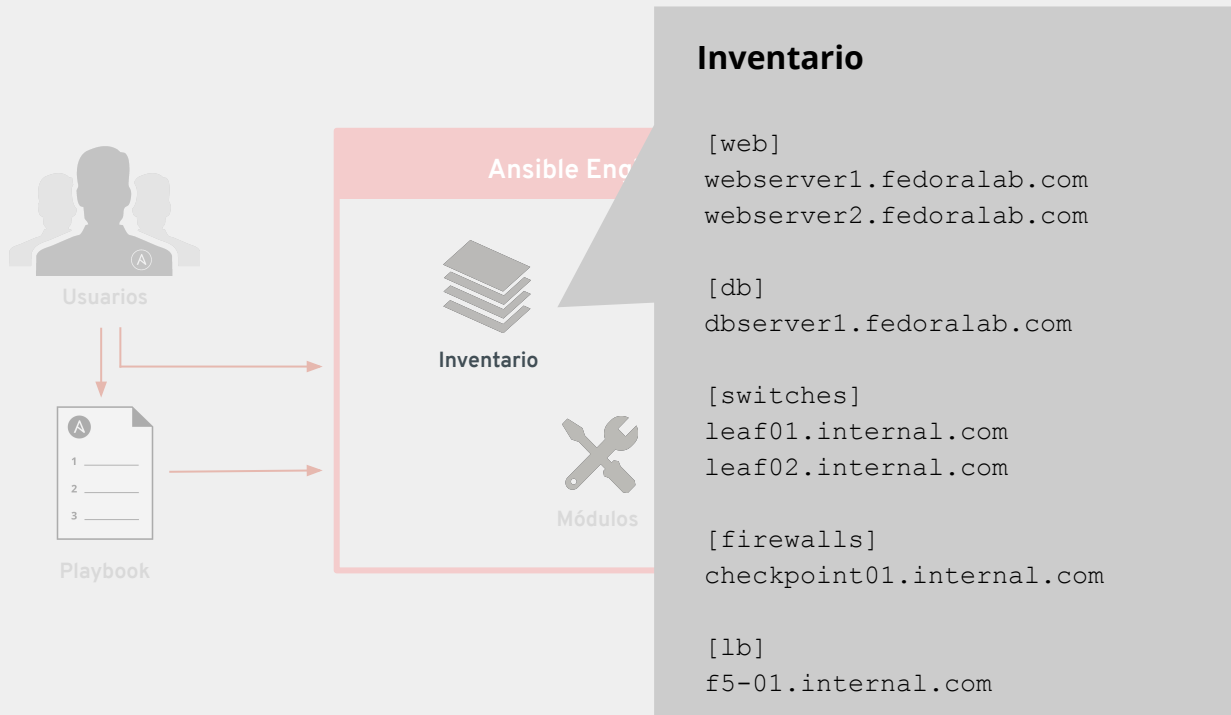


# El lenguaje de la automatización

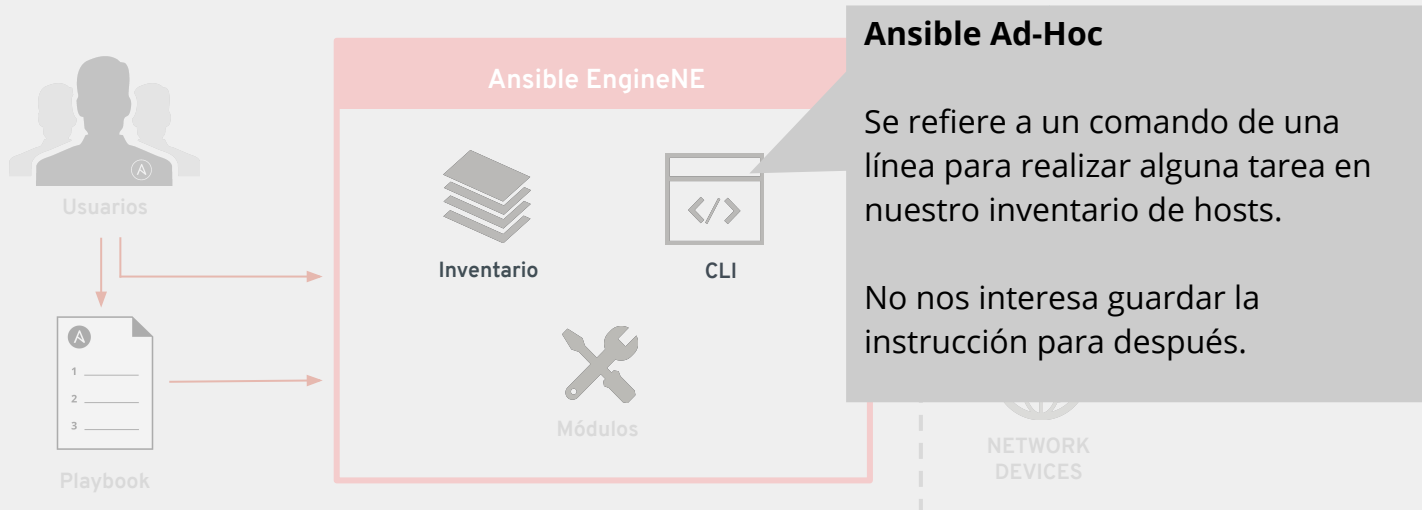
# Componentes básicos



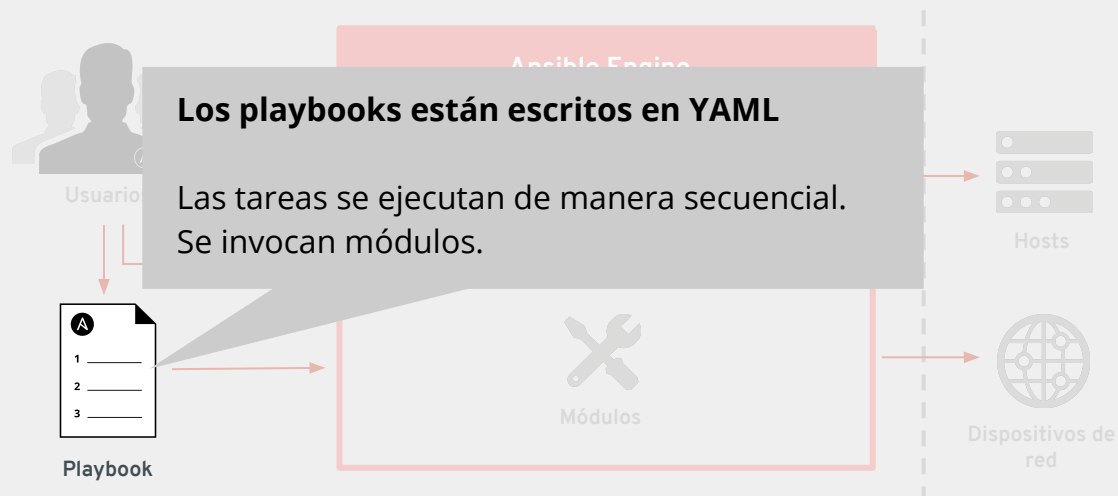
# Componentes básicos



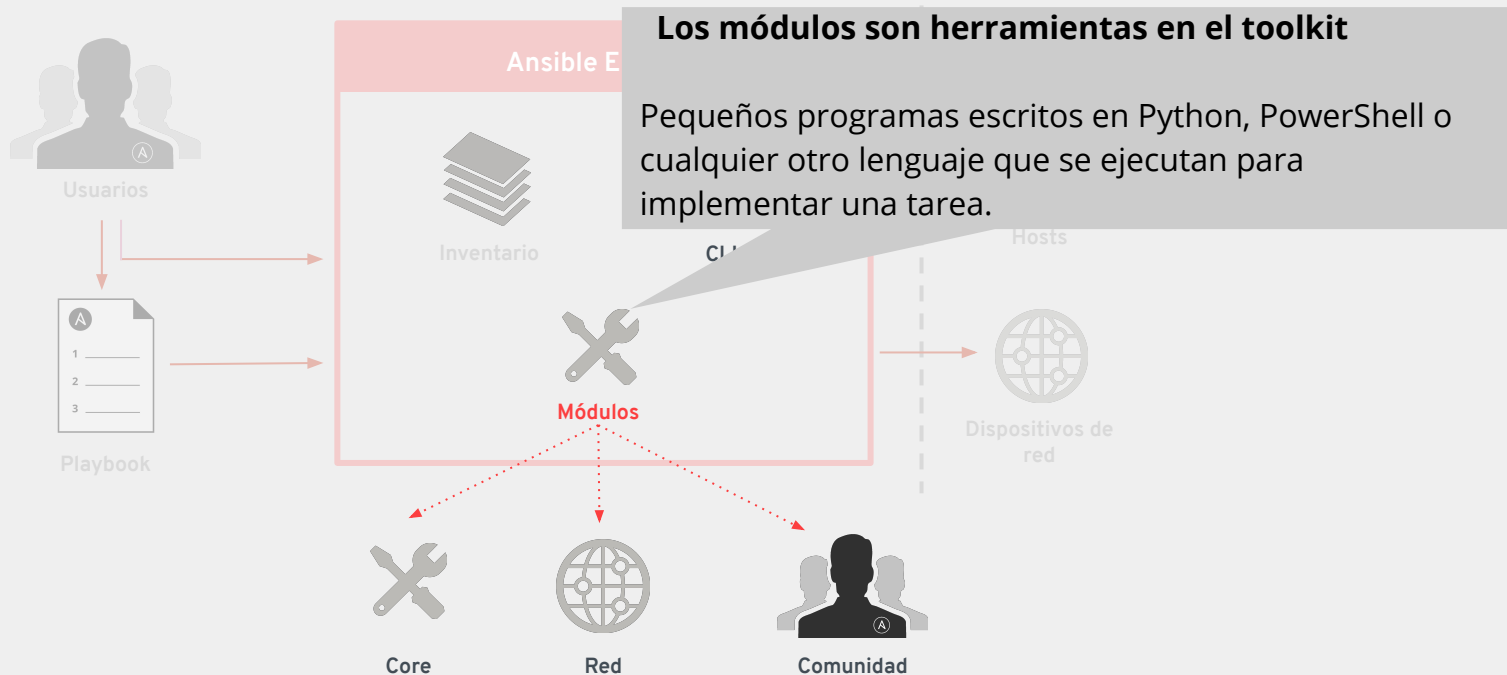
# Componentes básicos



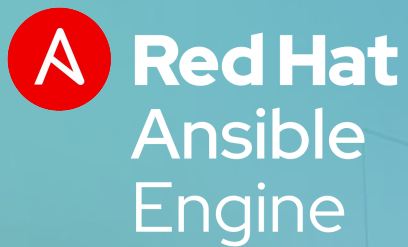
# Componentes básicos



# Componentes básicos







Inventario, ¿en dónde vamos a automatizar?

# 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

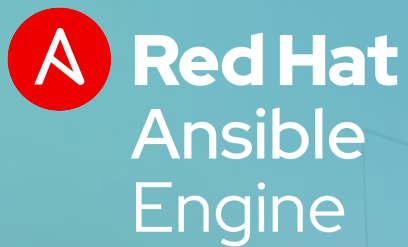
[backend:children]

dns

db

Se pueden tener grupos de grupos:

[groupname:children]



Módulos, porque alguien tiene que  
hacer el trabajo pesado

# 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

```
aramirez@localhost:~$ ansible-doc -l|nl
1  a10_server          Manage A10 Networks AX/SoftAX/Thunder/vThunder devices' server object
2  a10_server_axapi3    Manage A10 Networks AX/SoftAX/Thunder/vThunder devices
3  a10_service_group    Manage A10 Networks AX/SoftAX/Thunder/vThunder devices' service groups
4  a10_virtual_server   Manage A10 Networks AX/SoftAX/Thunder/vThunder devices' virtual servers
5  aci_aaa_user         Manage AAA users (aaa:User)
6  aci_aaa_user_certificate Manage AAA user certificates (aaa:UserCert)
7  aci_access_port_block_to_access_port Manage port blocks of Fabric interface policy leaf profile interface selectors (infra:HPorts, infra:Po...
8  aci_access_port_to_interface_policy_leaf_profile Manage Fabric interface policy leaf profile interface selectors (infra:HPorts, infra:RsAccBaseGrp, infr...
9  aci_access_sub_port_block_to_access_port Manage sub port blocks of Fabric interface policy leaf profile interface selectors (infra:HPorts, infr...
10 aci_aep              Manage attachable Access Entity Profile (AEP) objects (infra:AttEntityP, infra:ProvAcc)
11 aci_aep_to_domain    Bind AEPs to Physical or Virtual Domains (infra:RsDomP)
12 aci_ap               Manage top level Application Profile (AP) objects (fv:Ap)
13 aci_bd               Manage Bridge Domains (BD) objects (fv:BD)
14 aci_bd_subnet        Manage Subnets (fv:Subnet)
15 aci_bd_to_l3out       Bind Bridge Domain to L3 Out (fv:RsBDToOut)
16 aci_config_rollback  Provides rollback and rollback preview functionality (config:ImportP)
17 aci_config_snapshot  Manage Config Snapshots (config:Snapshot, config:ExportP)
18 aci_contract          Manage contract resources (vz:BrCP)
19 aci_contract_subject  Manage initial Contract Subjects (vz:Subj)
20 aci_contract_subject_to_filter Bind Contract Subjects to Filters (vz:RsSubjFiltAtt)
21 aci_domain            Manage physical, virtual, bridged, routed or FC domain profiles (phys:DomP, vmm:DomP, l2ext:DomP, l3ex...
22 aci_domain_to_encap_pool Bind Domain to Encap Pools (infra:RsVlanNs)
23 aci_domain_to_vlan_pool Bind Domain to VLAN Pools (infra:RsVlanNs)
24 aci_encap_pool        Manage encap pools (fvns:VlanInstP, fvns:VxlanInstP, fvns:VsanInstP)
25 aci_encap_pool_range  Manage encap ranges assigned to pools (fvns:EncapBlk, fvns:VsanEncapBlk)
26 aci_epg               Manage End Point Groups (EPG) objects (fv:AEPg)
27 aci_epg_monitoring_policy Manage monitoring policies (mon:EPGPOL)
28 aci_epg_to_contract   Bind EPGs to Contracts (fv:RsCons, fv:RsProv)
29 aci_epg_to_domain     Bind EPGs to Domains (fv:RsDomAtt)
30 aci_fabric_node       Manage Fabric Node Members (fabric:NodeIdentP)
31 aci_fabric_scheduler  This modules creates ACI schedulers
32 aci_filter            Manages top level filter objects (vz:Filter)
33 aci_filter_entry       Manage filter entries (vz:Entry)
34 aci_firmware_group     This module creates a firmware group
35 aci_firmware_group_node This modules adds and remove nodes from the firmware group
36 aci_firmware_policy    This creates a firmware policy
37 aci_firmware_source    Manage firmware image sources (firmware:OSource)
38 aci_interface_policy_fc Manage Fibre Channel interface policies (fc:IfPol)
39 aci_interface_policy_l2 Manage Layer 2 interface policies (l2:IfPol)
40 aci_interface_policy_leaf_policy_group Manage fabric interface policy leaf policy groups (infra:AccBndGrp, infra:AccPortGrp)
41 aci_interface_policy_leaf_profile Manage fabric interface policy leaf profiles (infra:AccPortP)
42 aci_interface_policy_lldp Manage LLDP interface policies (lldp:IfPol)
43 aci_interface_policy_mcp Manage MCP interface policies (mcp:IfPol)
44 aci_interface_policy_ospf Manage OSPF interface policies (ospf:IfPol)
45 aci_interface_policy_port_channel Manage port channel interface policies (l2:PortSecurityPol)
46 aci_interface_policy_port_security Manage port security (l2:PortSecurityPol)
```

# Módulos

```
aramirez@localhost:~$  
2789 win_tempfile      Creates temporary files and directories  
2790 win_template        Templates a file out to a remote server  
2791 win_timezone        Sets Windows machine timezone  
2792 win_toast            Sends Toast windows notification to logged in users on Windows 10 or later hosts  
2793 win_unzip            Unzips compressed files and archives on the Windows node  
2794 win_updates          Download and install Windows updates  
2795 win_uri              Interacts with webservices  
2796 win_user             Manages local Windows user accounts  
2797 win_user_profile     Manages the Windows user profiles  
2798 win_user_right       Manage Windows User Rights  
2799 win_wait_for         Waits for a condition before continuing  
2800 win_wait_for_process Waits for a process to exist or not exist before continuing  
2801 win_wakeonlan        Send a magic Wake-on-LAN (WoL) broadcast packet  
2802 win_webpicmd         Installs packages using Web Platform Installer command-line  
2803 win_whoami           Get information about the current user and process  
2804 win_xml              Add XML fragment to an XML parent  
2805 xattr                Manage user defined extended attributes  
2806 xbps                 Manage packages with Xbps  
2807 xenserver_facts      get facts reported on xenserver  
2808 xenserver_guest       Manages virtual machines running on Citrix XenServer host or pool  
2809 xenserver_guest_facts Gathers facts for virtual machines running on Citrix XenServer host or pool  
2810 xenserver_guest_powerstate Manages power states of virtual machines running on Citrix XenServer host or pool  
2811 xfconf               Edit XFCE4 Configurations  
2812 xfs_quota             Manage quotas on XFS filesystems  
2813 xml                  Manage bits and pieces of XML files or strings  
2814 yarn                 Manage node.js packages with Yarn  
2815 yum                  Manages packages with the 'yum' package manager  
2816 yum_repository       Add or remove YUM repositories  
2817 zabbix_action         Create/Delete/Update Zabbix actions  
2818 zabbix_group          Create/delete Zabbix host groups  
2819 zabbix_group_facts    Gather facts about Zabbix hostgroup  
2820 zabbix_host           Create/update/delete Zabbix hosts  
2821 zabbix_host_facts     Gather facts about Zabbix host  
2822 zabbix_hostmacro      Create/update/delete Zabbix host macros  
2823 zabbix_maintenance   Create Zabbix maintenance windows  
2824 zabbix_map           Create/update/delete Zabbix maps  
2825 zabbix_proxy         Create/delete/get/update Zabbix proxies  
2826 zabbix_screen        Create/update/delete Zabbix screens  
2827 zabbix_template      Create/delete/dump Zabbix template  
2828 zfs                   Manage zfs  
2829 zfs_delegate_admin    Manage ZFS delegated administration (user admin privileges)  
2830 zfs_facts             Gather facts about ZFS datasets  
2831 znode                 Create, delete, retrieve, and update znodes using ZooKeeper  
2832 zpool_facts           Gather facts about ZFS pools  
2833 zypper               Manage packages on SUSE and openSUSE  
2834 zypper_repository    Add and remove Zypper repositories  
[aramirez@t460p ~]$
```

# Documentación de los módulos

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

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

```
aramirez@localhost:~  
- COPY (/usr/lib/python3.7/site-packages/ansible/modules/files/copy.py)  
  
The 'copy' module copies a file from the local or remote machine to a location on the remote machine. Use the [fetch] module to copy files from remote locations to the local box. If you need variable interpolation in copied files, use the [template] module. Using a variable in the 'content' field will result in unpredictable output. For windows targets, use the [win_copy] module instead.  
  
+ This module is maintained by The Ansible Core Team  
+ note: This module has a corresponding action plugin.  
  
OPTIONS (= is mandatory):  
  
- attributes  
  The attributes the resulting file or directory should have.  
  To get supported flags look at the man page for 'chattr' on the target system.  
  This string should contain the attributes in the same order as the one displayed by 'lsattr'.  
  The 'a' operator is assumed as default, otherwise '+' or '-' operators need to be included in the string.  
  (Aliases: attr)[Default: (null)]  
  type: str  
  version_added: 2.3  
  
- backup  
  Create a backup file including the timestamp information so you can get the original file back if you somehow clobbered it incorrectly.  
  [Default: False]  
  type: bool  
  version_added: 0.7  
  
- checksum  
  SHA1 checksum of the file being transferred.  
  Used to validate that the copy of the file was successful.  
  If this is not provided, ansible will use the local calculated checksum of the src file.  
  [Default: (null)]  
  type: str  
  version_added: 2.5  
  
- content  
  When used instead of 'src', sets the contents of a file directly to the specified value.  
  For advanced formatting or if 'content' contains a variable, use the 'template' module.  
  [Default: (null)]  
  type: str  
  version_added: 1.1  
  
- decrypt  
  This option controls the autodecryption of source files using vault.  
  [Default: True]  
  type: bool  
  version_added: 2.4  
  
- dest  
  Remote absolute path where the file should be copied to.  
  If 'src' is a directory, this must be a directory too.  
  If 'dest' is a non-existent path and if either 'dest' ends with "/" or 'src' is a directory, 'dest' is created.  
  If 'dest' is a relative path, the starting directory is determined by the remote host.  
  If 'src' and 'dest' are files, the parent directory of 'dest' is not created and the task fails if it does not already exist.
```



# 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

```
Activities Terminal Oct 3 21:46
aramirez@t1580:~/AnsibleFWO2019

> USER (/usr/lib/python3.7/site-packages/ansible/modules/system/user.py)

Manage user accounts and user attributes. For Windows targets, use the [win_user] module instead.

* This module is maintained by The Ansible Core Team
OPTIONS (= is mandatory):

- append
    If 'yes', add the user to the groups specified in 'groups'.
    If 'no', user will only be added to the groups specified in 'groups', removing them from all other groups.
    Mutually exclusive with 'local'
    [Default: False]
    type: bool

- authorization
    Sets the authorization of the user.
    Does nothing when used with other platforms.
    Can set multiple authorizations using comma separation.
    To delete all authorizations, use 'authorization=''.
    Currently supported on Illumos/Solaris.
    [Default: (null)]
    type: str
    version_added: 2.8

- comment
    Optionally sets the description (aka 'GECOS') of user account.
    [Default: (null)]
    type: str

- create home
    Unless set to 'no', a home directory will be made for the user when the account is created or if the home directory does not
    exist.
    Changed from 'createhome' to 'create_home' in Ansible 2.5.
    (Aliases: createhome)[Default: True]
    type: bool

- expires
    An expiry time for the user in epoch, it will be ignored on platforms that do not support this.
    Currently supported on GNU/Linux, FreeBSD, and DragonFlyBSD.
    Since Ansible 2.6 you can remove the expiry time specify a negative value. Currently supported on GNU/Linux and FreeBSD.
    [Default: (null)]
    type: float
```

Documentation

Ansible2.8

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

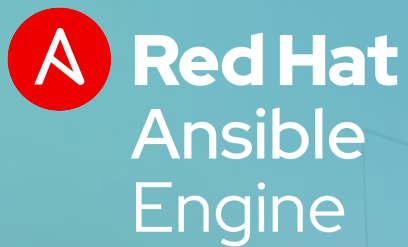
The below requirements are needed on the host that executes this module.

- firewalld >= 0.2.11

Parameters

| Parameter                                                      | Choices/Defaults                                                          | Comments                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| icmp_block<br><small>string<br/>added in 2.8</small>           |                                                                           | The ICMP block you would like to add/remove to/from a zone in firewalld.                                                                                                                                                                                                                                           |
| icmp_block_inversion<br><small>string<br/>added in 2.8</small> |                                                                           | Enable/Disable inversion of ICMP blocks for a zone in firewalld.                                                                                                                                                                                                                                                   |
| immediate<br><small>boolean</small>                            | Choices: <ul style="list-style-type: none"><li>no ←</li><li>yes</li></ul> | Should this configuration be applied immediately, if set as permanent.                                                                                                                                                                                                                                             |
| interface<br><small>string<br/>added in 2.1</small>            |                                                                           | The interface you would like to add/remove to/from a zone in firewalld.                                                                                                                                                                                                                                            |
| masquerade<br><small>string<br/>added in 2.1</small>           |                                                                           | The masquerade setting you would like to enable/disable to/from zones within firewalld.                                                                                                                                                                                                                            |
| offline<br><small>boolean<br/>added in 2.3</small>             | Choices: <ul style="list-style-type: none"><li>no</li><li>yes</li></ul>   | Whether to run this module even when firewalld is offline.                                                                                                                                                                                                                                                         |
| permanent<br><small>boolean</small>                            | Choices: <ul style="list-style-type: none"><li>no</li><li>yes</li></ul>   | Should this configuration be in the running firewalld configuration or persist across reboots.<br>As of Ansible 2.3, permanent operations can operate on firewalld configs when it is not running (requires firewalld >= 3.0.9).<br>Note that if this is <code>no</code> , immediate is assumed <code>yes</code> . |
| port                                                           |                                                                           | Name of a port or port range to add/remove to/from firewalld.                                                                                                                                                                                                                                                      |

Search this site



# Instrucciones Ad-Hoc, rápido y fácil

# 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"
```

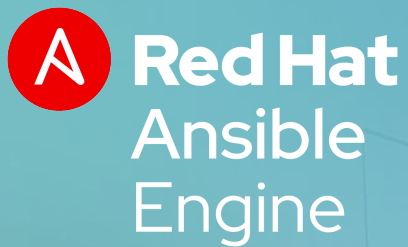
Activities Terminal

Oct 3 00:13

aramirez@t580:~/Ansible/FWD2019

aramirez@t580 FWD2019]\$ grep -v "#" inventory  
[servers]  
192.168.122.232  
[aramirez@t580 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]\$



Playbooks,  
ahora sí, automaticemos

# Ejemplos

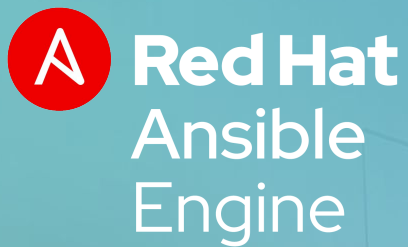
```
---  
- name: Actualiza los servidores  
  hosts: web, db  
  
  tasks:  
    - name: Actualiza los servidores  
      yum:  
        name: '*'  
        state: latest
```

- 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
```



# Handlers, tareas especiales

# 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 requiere.

```
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 requiere.

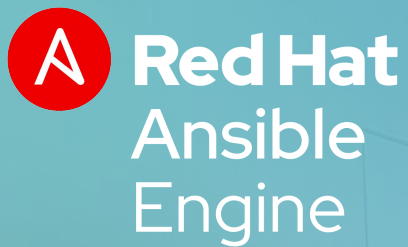
```
tasks:
  - name: Configuración local del Mail Transfer Agent
    lineinfile:
      dest: /etc/postfix/main.cf
      regexp: "^inet_interfaces"
      line: "inet_interfaces = loopback-only"
      notify: Reinicia postfix
```

## 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:

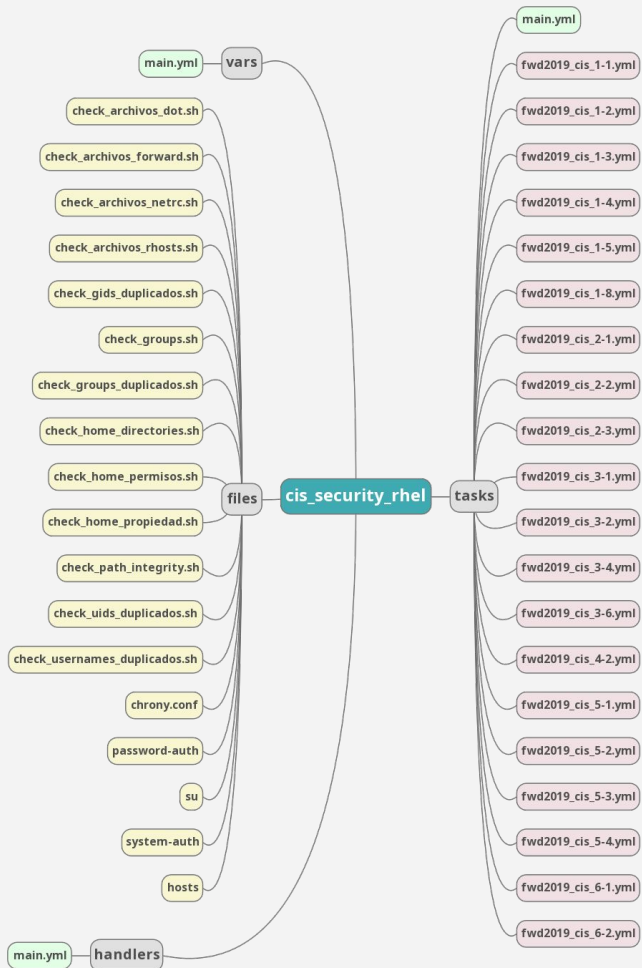
```
handlers:
  - name: Reinicia postfix
    service:
      name: postfix
      state: restarted
```



# Roles

Una colección de todo lo anterior





```

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_3-4.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_6-1.yml
│           └── fwd2019_cis_6-2.yml
└── vars
    └── main.yml

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

# 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 --
```

```
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

# 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-lib"
- "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%
```

# Archivos que se subirán a los hosts

```
aramirez@t580:~/FWD2019
[auth] required pam_env.so
auth required pam_faildelay.so delay=2000000
auth sufficient pam_unix.so nullok try_first_pass
auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
auth [success=1 default=bad] pam_unix.so
auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900

auth requisite pam_succeed_if.so uid >= 1000 quiet_success
auth required pam_deny.so

account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 1000 quiet
account required pam_permit.so

password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok type=
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password required pam_deny.so

session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
~
~
"roles/cis_security_rhel/files/system-auth" 25L, 1223C 1,1 All
```

```
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]

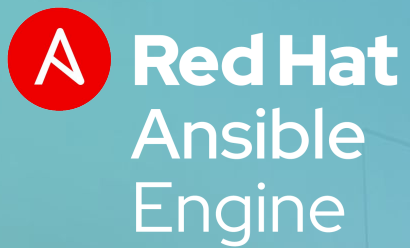
TASK [cis_security_rhel : FW2019 ::: Hardening for Servers ::: CIS_6-2 ::: Validando nombres de grupo existentes] *****
changed: [192.168.122.232]

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]$
```





¿Preguntas?



# ¡Gracias!

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

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

