Obligatorio: Taller de Linux 2025

- Documento informativo

Autores:

- Pablo Delucchi - N° 315123
- Agustín Guarteche - N° 240159

Requerimientos previos:

En el directorio "collections" del repositorio se encuentra el archivo "requirements.yml" con los nombres de las colecciones de ANSIBLE necesarias para ejecutar los playbook correctamente. Estas, bien pueden instalarse manualmente mediante ansible galaxy:

```bash
ansible-galaxy ansible.posix install
ansible-galaxy community.general install
ansible-galaxy community.crypto install
```

o bien en forma automática invocando el archivo de definisiones desde la raíz:

```bash
ansible-galaxy install -r collections/requirements.yml
```

Pruebas de ejecución

Módulo PING (todos los hosts):

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible -i inventories.ini all -m ping
Centos-SRV | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
Ubuntu-srv | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
Bastion | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
}
[sysadmin@bastion Obligatorio_taller2025]$
```

Obtención del tiempo de actividad (todos los hosts):

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible -i inventories.ini all -m shell -a "uptime" --become --ask-become-pass
BECOME password:
Ubuntu-srv | CHANGED | rc=0 >>
 16:14:08 up  1:02,  2 users,  load average: 0.00, 0.00, 0.00
Centos-SRV | CHANGED | rc=0 >>
 13:14:08 up  1:02,  2 users,  load average: 0.00, 0.04, 0.00
Bastion | CHANGED | rc=0 >>
 13:14:09 up  1:04,  3 users,  load average: 1.23, 0.50, 0.42
[sysadmin@bastion Obligatorio_taller2025]$
```

Instalación de apache (en webserver Centos):

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible -i inventories.ini webserver -m shell -a "dnf install httpd -y" --become --a
sk-become-pass
BECOME password:
Centos-SRV | CHANGED | rc=0 >>
Last metadata expiration check: 0:07:46 ago on Sat 22 Feb 2025 12:51:12 PM -03.
Dependencies resolved.
================================================================================
 Package                 Architecture Version           Repository       Size
================================================================================
Installing:
 httpd                   x86_64       2.4.62-4.el9      appstream        47 k
Installing dependencies:
 apr                     x86_64       1.7.0-12.el9      appstream       123 k
 apr-util                x86_64       1.6.1-23.el9      appstream        95 k
 apr-util-bdb            x86_64       1.6.1-23.el9      appstream        13 k
 centos-logos-httpd      noarch       90.8-2.el9        appstream       1.5 M
 httpd-core              x86_64       2.4.62-4.el9      appstream       1.5 M
 httpd-filesystem        noarch       2.4.62-4.el9      appstream        13 k
 httpd-tools             x86_64       2.4.62-4.el9      appstream        82 k
 mailcap                 noarch       2.1.49-5.el9      baseos           33 k
Installing weak dependencies:
 apr-util-openssl        x86_64       1.6.1-23.el9      appstream        15 k
 mod_http2               x86_64       2.0.26-2.el9      appstream       163 k
 mod_lua                 x86_64       2.4.62-4.el9      appstream        60 k

Transaction Summary
================================================================================
Install  12 Packages

Total size: 3.7 M
Installed size: 8.7 M
Downloading Packages:
[SKIPPED] mailcap-2.1.49-5.el9.noarch.rpm: Already downloaded
[SKIPPED] apr-1.7.0-12.el9.x86_64.rpm: Already downloaded
[SKIPPED] apr-util-1.6.1-23.el9.x86_64.rpm: Already downloaded
```

Uso de espacio en disco (en servidor Ubuntu):

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible -i inventories.ini ubuntu -m shell -a "df -h" --become --ask-become-pass
BECOME password:
[WARNING]: Could not match supplied host pattern, ignoring: ubuntu
[WARNING]: No hosts matched, nothing to do
[sysadmin@bastion Obligatorio_taller2025]$ ansible -i inventories.ini Ubuntu -m shell -a "df -h" --become --ask-become-pass
BECOME password:
Ubuntu-srv | CHANGED | rc=0 >>
Filesystem                  Size  Used Avail Use% Mounted on
tmpfs                       197M  1.1M  196M   1% /run
/dev/mapper/ubuntu--vg-root  8.0G  2.3G  5.7G  29% /
tmpfs                       985M     0  985M   0% /dev/shm
tmpfs                       5.0M     0  5.0M   0% /run/lock
/dev/mapper/ubuntu--vg-var   3.0G  489M  2.5G  17% /var
/dev/sda2                   960M  146M  815M  16% /boot
tmpfs                       197M   12K  197M   1% /run/user/1000
[sysadmin@bastion Obligatorio_taller2025]$
```

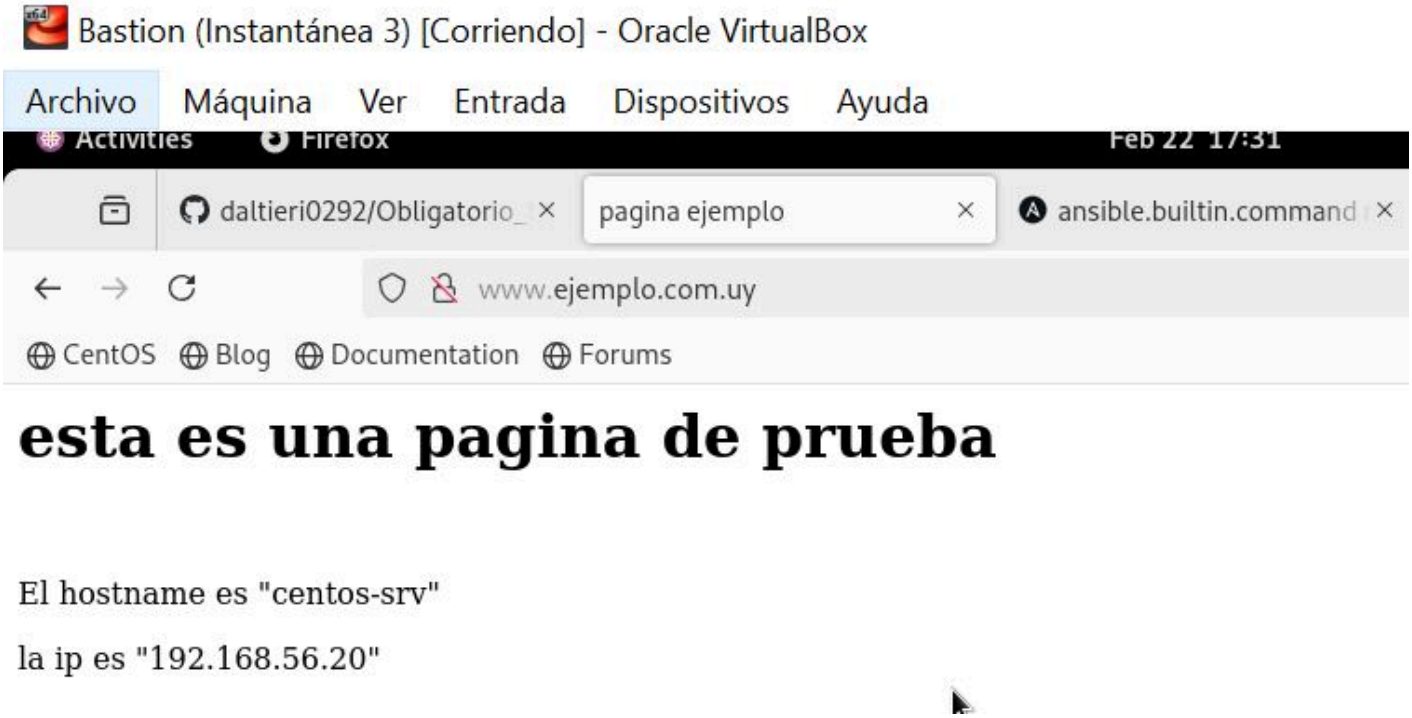
Verificación de sintaxis playbook "web_setup.yml", ejecución y resultado (en webserver Centos):

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible-playbook -i inventory.ini web_setup.yml --syntax-check
[WARNING]: Collection ansible.posix does not support Ansible version 2.14.18

playbook: web_setup.yml
[sysadmin@bastion Obligatorio_taller2025]$
```

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible-playbook -i inventory.ini --limit webserver web_setup.yml --become --ask-become-pass
BECOME password:
[WARNING]: Collection ansible.posix does not support Ansible version 2.14.18

PLAY [Despliegue Apache web server y configuración] ****************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************
ok: [Centos-SRV]

TASK [Instalar apache (HTTPD)] *************************************************************************************************************************
ok: [Centos-SRV]

TASK [Iniciar servicio apache y habilitarlo] ***********************************************************************************************************
ok: [Centos-SRV]

TASK [Reglas de firewall] ******************************************************************************************************************************
ok: [Centos-SRV] => (item=http)

TASK [Agrego registro al archivo host] *****************************************************************************************************************
ok: [Centos-SRV -> localhost]

TASK [Modificar la configuración de apache] ************************************************************************************************************
ok: [Centos-SRV]

TASK [Verifico existencia de directorio para configurar vhost] *****************************************************************************************
ok: [Centos-SRV]

TASK [Verificar si existe el directorio para alojar el sitio] ******************************************************************************************
ok: [Centos-SRV]

TASK [Configurar vhost] ********************************************************************************************************************************
ok: [Centos-SRV]

TASK [Página índice generada por template] *************************************************************************************************************
ok: [Centos-SRV]

PLAY RECAP *********************************************************************************************************************************************
Centos-SRV                 : ok=10   changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

```
[sysadmin@centos-srv vhost.d]$ ls
ejemplo.com.uy.conf
[sysadmin@centos-srv vhost.d]$ cat ejemplo.com.uy.conf
<VirtualHost *:80>
  ServerName "www.ejemplo.com.uy"
  ServerAdmin "webmaster@ejemplo.com.uy
  DocumentRoot /var/www/ejemplo.com.uy/html

  <Directory /var/www/ejemplo.com.uy/html>
    Options Indexes FollowSymLinks
    AllowOverride none
    Require all granted
  </Directory>
</VirtualHost>
[sysadmin@centos-srv vhost.d]$ _
```

```
[sysadmin@centos-srv www]$ ls
cgi-bin  ejemplo.com.uy  html
[sysadmin@centos-srv www]$ cd ejemplo.com.uy/
[sysadmin@centos-srv ejemplo.com.uy]$ ls
html
[sysadmin@centos-srv ejemplo.com.uy]$ cd html/
[sysadmin@centos-srv html]$ ls
index.html
[sysadmin@centos-srv html]$ cat index.html
<html>
  <head>
    <title>pagina ejemplo</title>
  </head>
  <body>
    <h1>esta es una pagina de prueba</h1>
  <br>
  <p> El hostname es "centos-srv"
  <p> la ip es "192.168.56.20" </p>
 </body>
</html>
[sysadmin@centos-srv html]$ _
```



Verificación de sintaxis playbook "hardening.yml", ejecución y resultados (en servidor Ubuntu):

```
[sysadmin@bastion Obligatorio_taller2025]$ ansible-playbook -i inventory.ini hardening.yml --syntax-check
[WARNING]: Collection community.general does not support Ansible version 2.14.18
[WARNING]: Collection ansible.posix does not support Ansible version 2.14.18

playbook: hardening.yml
[sysadmin@bastion Obligatorio_taller2025]$
```

Comando: ansible-playbook -i inventory.ini hardening.yml --become --ask-become-pass

```
PLAY [Hardenizado de servidor Ubuntu] ******************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************
ok: [Ubuntu-srv]

TASK [Habilito el firewall UFW] ************************************************************************************************
ok: [Ubuntu-srv]

TASK [Bloqueo todo trafico entrante y reinicio UFW] ****************************************************************************
ok: [Ubuntu-srv]

TASK [Permito el trafico saliente y reinicio UFW] ******************************************************************************
ok: [Ubuntu-srv]

TASK [Permito el trafico por el puerto 22 (puerto por defecto del servicio SSH)] ***********************************************
ok: [Ubuntu-srv]

TASK [Verifico existencia del archivo Authorized_keys] *************************************************************************
changed: [Ubuntu-srv]

TASK [Verifico que la clave SSH del usuario sysadmin esté agregada en el archivo authorized_keys] ******************************
changed: [Ubuntu-srv]

TASK [Genero un par de claves SSH para el usuario sysadmin solo en caso de que la salida estándar esté vacía] ******************
skipping: [Ubuntu-srv]

TASK [Copio la clave SSH pública del usuario sysadmin al archivo authorized_keys en el servidor] ******************************
skipping: [Ubuntu-srv]

TASK [Permito el login solamente con clave SSH] ********************************************************************************
changed: [Ubuntu-srv]

RUNNING HANDLER [Reiniciar SSH] ************************************************************************************************
changed: [Ubuntu-srv]

PLAY RECAP *********************************************************************************************************************
Ubuntu-srv                 : ok=9    changed=4    unreachable=0    failed=0    skipped=2    rescued=0    ignored=0

[sysadmin@bastion Obligatorio_taller2025]$
```

Archivo visualizado: "/etc/ssh/sshd/sshd_config"

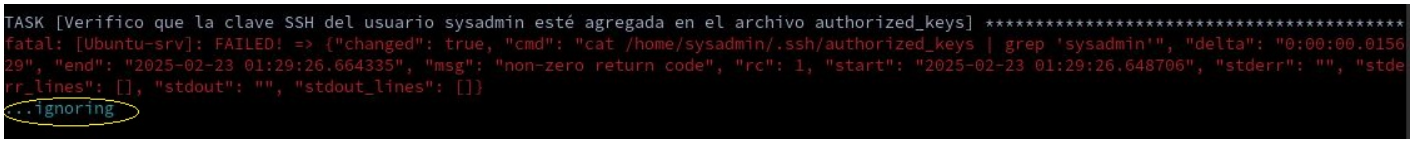
```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

```
root@ubuntu-srv:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22                         ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
```

Obs: Como ya se encontraba habilitado el tráfico por el puerto por defecto de SSH, procedimos a agregarlo nuevamente (sin especificar protocolo para que pudiera verse el cambio generado)

Desafíos/problemas encontrados

- Problema: IP dinámica de "Bastión".
    - Durante el taller establecimos como fijas las IP de los host "Ubuntu-srv" y "Centos-SRV", pero a bastión no le configuramos una IP, por lo que esta es obtenida por DHCP. Debido a ello esta puede cambiar según que equipo ejecute el playbook y hacer que falle.
    - **Solución encontrada**: Establecimos una variable "bastion_ip" en el archivo "inventory.ini" y la referenciamos en el grupo.
- Problema: Caso borde clave pública SSH inexistente al conectar.
    - Se solicitaba por letra que nos asegurráramos de que la clave pública de bastión se encontraba en el servidor de Ubuntu. Puede darse el caso de borde de que el archivo "know_host" no exista en el servidor o que no contenga la clave pública de bastión, en cuyo caso ANSIBLE no es capaz de establecer conexión con el host.
    - **Solución encontrada**: Se establece la variable "ansible_ssh_pass" en el archivo de inventario para una permitir una primera conexión al servidor por SSH con contraseña, de esta manera, si el archivo no existe o la clave no está presente, de igual manera el playbook se ejecuta y, llegado el caso, crea el archivo o añade la clave. Posteriormente se deshabilita el acceso mediante contraseña, pero al haberse verificado la existencia de la clave, esto ya no es un problema.
- Problema: Error de ejecución en playbook en caso de no existir archivo de host conocidos. Creación de clave propietaria
    - **Solución encontrada**: Durante la ejecución del playbook se verifica si hay alguna clave SSH para el usuario "sysadmin" en el archivo de host conocidos. (el cual previamente se crea si no existe) El problema que estábamos teniendo era que si la clave no existe en el archivo (es decir si la salida era vacía) nos generaba un error que detenía el playbook. como solución encontramos que podíamos agregar una instrucción "ignore_errors: true" para que en dicho caso continuara la ejecución.



Otro error contrado fue que debíamos generar las claves para el usuario "sysadmin" y no para el usuario root (estaba especificado become:true pero no se especificó un usuario particular), esto se solucionó adicionando "become_user = sysadmin" cuando fuera necesario para generarle sus claves SSH.

Referencias

- Material del curso
- Documentación propia de ANSIBLE para cada Collection: https://docs.ansible.com/
- ChatGPT

Prompt: "En un playbook de ansible, hay alguna forma de conectarse a un equipo remoto si aun no tengo definida una clave pública SSH para conectarme? le puedo indicar una contraseña? como?"

Prompt 2: "Si en un playbook de ansible necesito crear una clave SSH pública, pero tengo la instrucción "become=true", necesariamente dicha llave se creará para el usuario root?"