Septiembre de 2022

Laboratorio 1

Monitoreo y supervisión de redes

Datos Personales:

Nombre:	
Número estudiante:	
Fecha:	

INTRODUCCIÓN

Topología

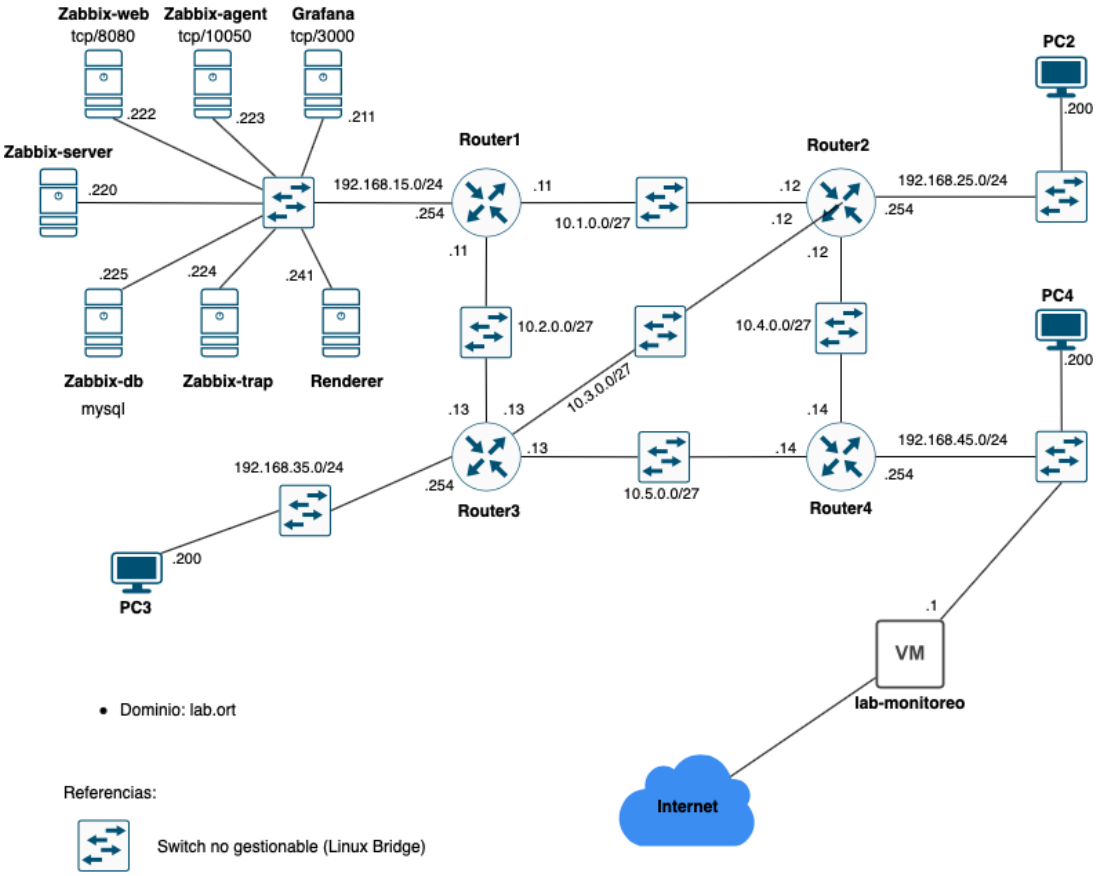

Imagen 1: Topología de red

La red consta de:

- 7 servidores
- 4 routers
- 3 hosts "PC"

La conexión se realiza mediante SSH a la máquina virtual lab-monitoreo. Por defecto se presenta en el puerto tcp/2222 de la interface de red de la computadora personal del estudiante

Usuario	estudiante
Password	estudiante
Puerto	2222

Requerimientos para el despliegue de la VM:

	Mínimo	Recomendado
Disco	20GB	40GB
RAM	4GB	8GB
CPU	2	4

PRÁCTICOS

Práctico 1

Reconocimiento del ambiente

El próposito de este práctico es verificar la conectividad entre los dispositivos del laboratorio

1. Conectarse por SSH a la VM lab-monitoreo

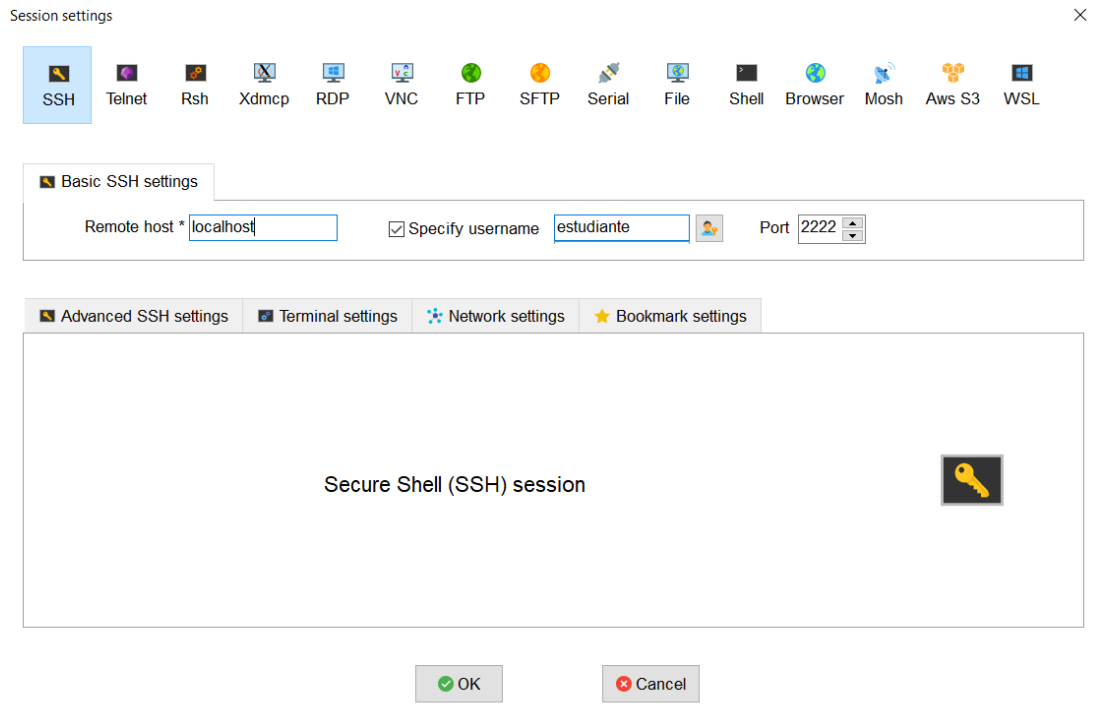

Imagen 2: Ejemplo en MobaXterm[1]

2. Prueba de conectividad con ping
    - *ping router1.lab.ort*
    - *ping router2.lab.ort*
    - *ping router3.lab.ort*
    - *ping router4.lab.ort*
    - *ping pc2.lab.ort*
    - *ping pc3.lab.ort*
    - *ping pc4.lab.ort*
3. Acceso SSH
    - *ssh router1.lab.ort*

Práctico 1 continúa en la siguiente página...

- *ssh router2.lab.ort*
- *ssh router3.lab.ort*
- *ssh router4.lab.ort*
- *ssh pc2.lab.ort*
- *ssh pc3.lab.ort*
- *ssh pc4.lab.ort*

¿Por qué no solicita password?

4. Traceroute

- *traceroute router1.lab.ort*
- *traceroute router2.lab.ort*
- *traceroute router3.lab.ort*
- *traceroute router4.lab.ort*
- *traceroute pc2.lab.ort*
- *traceroute pc3.lab.ort*
- *traceroute pc4.lab.ort*

¿Los resultados concuerdan con lo representado en el diagrama de topología (ver Imagen 1)?

Práctico 2

SNMP

En este práctico veremos como configurar y realizar operaciones con SNMP

1. En lab-monitoreo ejecutar:

   - *lab1*

Código 1: ejecutar - lab1

```
1 (ansible-2.9.0) estudiante@lab-monitoreo:~$ lab1
```

   Este script preparará el ambiente para el práctico

2. Consulta SNMP

   - Para consultar una variable especifica de un host utilizaremos el comando snmpget
     Ejemplo: *snmpget -v2c -c micomunidad router1.lab.ort sysContact.0 1.3.6.1.2.1.1.6.0*
     (a) snmpget: es el comando que utilizaremos para obtener variables de un host
     (b) -v: define la versión de SNMP en la que queremos trabajar
     (c) 2c: versión 2c (puede ser 1, 2c, 3)
     (d) -c: indica la comunidad a utilizar
     (e) micomunidad: nombre de la comunidad (debe coincidir con lo configurado en el agente SNMP)
     (f) router1.lab.ort: nombre del host al que realizaremos la consulta
     (g) sysContact.0: nombre de una variable
     (h) 1.3.6.1.2.1.1.6.0: OID de otra variable (sysLocation.0)

3. Consulta SNMP por OID - Router1

   - *snmpget -v2c -c public router1.lab.ort 1.3.6.1.2.1.1.5.0*

4. Consulta SNMP por OID - Router2

   - *snmpget -v2c -c public router2.lab.ort 1.3.6.1.2.1.1.5.0*

   ¿Router1 que devuelve?

   ¿Router2 muestra error de timeout?

Código 2: snmpget - router2

```
1 (ansible-2.9.0) estudiante@lab-monitoreo:~$ snmpget -v2c -c
    public router2.lab.ort 1.3.6.1.2.1.1.5.0
2 Timeout: No Response from router2.lab.ort.
```

Los servidores linux utilizan el servicio snmpd como agente SNMP. El archivo de configuración del agente se encuentra en /etc/snmp/snmpd.conf

5. Acceso a router2.lab.ort
   - *ssh router2.lab.ort*
6. Verificación del servicio snmpd
   - *service snmpd status*

   ¿El servicio snmpd se encuentra activo?

7. Consulta SNMP desde router2
   - *snmpget -v2c -c public localhost 1.3.6.1.2.1.1.5.0*

   ¿Probando localmente sí responde?

8. Hagamos un respaldo del archivo /etc/snmp/snmpd.conf antes de comenzar
   - *cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bk*
9. Editemos el archivo de configuración /etc/snmp/snmpd.conf
   (a) *nano /etc/snmp/snmpd.conf*

Código 3: /etc/snmp/snmpd.conf - Listen localhost

```
1
2 #  AGENT BEHAVIOUR
3 #
4
5 #  Listen for connections from the local system only
6 agentAddress  udp:127.0.0.1:161
7 #  Listen for connections on all interfaces (both IPv4 *and*
    IPv6)
8 #agentAddress udp:161
```

   (b) Veremos que se encuentra aceptando conexiones unicamente a la ip de Localhost (linea 6)
   (c) Comentemos la linea 6 y descomentemos la linea 8, de forma que permita las conexiones desde cualquier dispositivo

Código 4: /etc/snmp/snmpd.conf - Listen on all interfaces

```
1
2  #  AGENT BEHAVIOUR
3  #
4
5  #  Listen for connections from the local system only
6  #agentAddress  udp:127.0.0.1:161
7  #  Listen for connections on all interfaces (both IPv4 *and*
       IPv6)
8  agentAddress udp:161
```

(d) Para aplicar los cambios debemos reiniciar el servicio snmpd

- service snmpd restart

(e) Repetir consulta snmp desde lab-monitoreo

- *snmpget -v2c -c public router2.lab.ort 1.3.6.1.2.1.1.5.0*

10. Modificación de comunidad

(a) Para modificar la comunidad debemos editar el archivo /etc/snmp/snmpd.conf, en la sección "ACCESS CONTROL"

- *nano /etc/snmp/snmpd.conf*

Código 5: /etc/snmp/snmpd.conf - Access control

```
1  ###########################################################
2  #
3  #  ACCESS CONTROL
4  #
5
6  view    systemonly  included   .1.3.6.1.2.1.1
7  view    systemonly  included   .1.3.6.1.2.1.25.1
8
9  #rocommunity public  localhost
10  rocommunity public  default    -V systemonly
11 # rocommunity6 public  default   -V systemonly
12
13
14 #rocommunity secret  10.0.0.0/16
15
16  rouser    authOnlyUser
```

(b) Analicemos la siguiente linea de configuración:

view systemonly included .1.3.6.1.2.1.1

i. view: refiere a que se configurará una vista especifica de variables
ii. systemonly: nombre de la vista
iii. included .1.3.6.1.2.1.1: incluye todas las variables que se encuentren por debajo de esa rama del árbol

Código 6: Rama .1.3.6.1.2.1.1

```
+--system(1)
   |
   +-- -R-- String     sysDescr(1)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- ObjID      sysObjectID(2)
   +-- -R-- TimeTicks  sysUpTime(3)
   |  |
   |  +--sysUpTimeInstance(0)
   |
   +-- -RW- String     sysContact(4)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String     sysName(5)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String     sysLocation(6)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- INTEGER    sysServices(7)
   |        Range: 0..127
   +-- -R-- TimeTicks  sysORLastChange(8)
   |        Textual Convention: TimeStamp
   |
   +--sysORTable(9)
      |
      +--sysOREntry(1)
         |  Index: sysORIndex
         |
         +-- ---- INTEGER    sysORIndex(1)
         |        Range: 1..2147483647
         +-- -R-- ObjID      sysORID(2)
         +-- -R-- String     sysORDescr(3)
         |        Textual Convention: DisplayString
         |        Size: 0..255
         +-- -R-- TimeTicks  sysORUpTime(4)
                  Textual Convention: TimeStamp
```

(c) Ahora veamos la linea de configuración:

rocommunity public default -V systemonly

i. rocommunity: indica que estamos definiendo una comunidad de solo lectura
ii. public: nombre de la comunidad
iii. default: define desde que redes se puede consultar, puede ser un prefijo de red o "default" que indica que se aplica lo que esté configurado globalmente en agentAdress (ver Código 4)
iv. -V: se permitirá consultar solo variables que se encuentren en la vista

v. systemonly: nombre de la vista que se aplica

(d) Si quisieramos definir una comunidad de lectura/escritura deberíamos respetar el mismo criterio

rwcommunity private default -V systemonly

de esta forma permitiríamos tanto leer como escribir variables que se encuentren dentro de la rama System (ver Código 6)

(e) En la sección SYSTEM INFORMATION del archivo /etc/snmp/snmpd.conf podremos definir valores propios del host

Código 7: /etc/snmp/snmpd.conf - System Information

```
1 ##########################################################
2 #
3 #  SYSTEM INFORMATION
4 #
5
6 #  Note that setting these values here, results in the
     corresponding MIB objects being 'read-only'
7 #  See snmpd.conf(5) for more details
8 sysLocation     Sitting on the Dock of the Bay
9 sysContact      Me <me@example.org>
```

observemos que se definen las variables sysLocation y sysContact (lineas 8 y 9). Tener en cuenta: si estas variables se definen en este archivo de configuración NO serán editables con la función SET de SNMP.

(f) Cerremos el archivo sin hacer cambios

11. Volvamos al host lab-monitoreo.lab.ort y verifiquemos:

(a) sysContact:

- *snmpget -v2c -c public router2.lab.ort .1.3.6.1.2.1.1.4.0*

(b) sysLocation:

- *snmpget -v2c -c public router2.lab.ort .1.3.6.1.2.1.1.6.0*

(c) Para hacer una consulta masiva utilizaremos el comando snmpwalk

Ejemplo: *snmpwalk -v2c -c micomunidad router1.lab.ort .1.3.6.1.2.1.1*

i. snmpwalk: es el comando que utilizaremos para ejecutar un a consulta masiva
ii. -v: define la versión de SNMP en la que queremos trabajar
iii. 2c: versión 2c (puede ser 1, 2c, 3)
iv. -c: indica la comunidad a utilizar
v. micomunidad: nombre de la comunidad (debe coincidir con lo configurado en el agente SNMP)
vi. router1.lab.ort: nombre del host al que realizaremos la consulta
vii. sysContact.0: nombre de una variable

viii. .1.3.6.1.2.1.1: OID del punto del árbol desde el que se quiere realizar la consulta. Si no se especifica nada se asume que se quiere obtener todas las variables del host

(d) Consultemos todos los valores de router2.lab.ort:

- *snmpwalk -v2c -c public router2.lab.ort*

(e) Consultemos ahora todos los valores de router1.lab.ort:

- *snmpwalk -v2c -c public router1.lab.ort*

¿Por qué cree que hay tanta diferencia en los resultados?

¿Que cambio realizaría en router2 para que responda de la misma forma?

(f) Hasta el momento hemos realizado consultas por OID en formato númerico
Probemos realizar una operación SNMP GET con un nombre de variable, por ejemplo:

- *snmpget -v2c -c public router1.lab.ort hrSystemDate.0*

Debería fallar y mostrar la siguiente salida:

Código 8: snmpget hrSystemDate

```
1 (ansible-2.9.0) estudiante@lab-monitoreo:~$ snmpget -v2c -
    c public router1.lab.ort hrSystemDate.0
2 hrSystemDate.0: Unknown Object Identifier (Sub-id not
    found: (top) -> hrSystemDate)
```

Esto se debe a que por defecto el cliente SNMP instalado en el sistema operativo viene sin configuración respecto al directorio donde consultar las MIBs

- Configuremos el archivo /etc/snmp/snmp.conf

Código 9: /etc/snmp/snmp.conf

```
1 # As the snmp packages come without MIB files due to
    license reasons, loading
2 # of MIBs is disabled by default. If you added the MIBs
    you can reenable
3 # loading them by commenting out the following line.
4 mibs :
```

- Comentemos la linea 4

Código 10: /etc/snmp/snmp.conf

```
1 # As the snmp packages come without MIB files due to
    license reasons, loading
2 # of MIBs is disabled by default. If you added the MIBs
    you can reenable
3 # loading them by commenting out the following line.
4 #mibs :
```

- Probemos nuevamente a realizar una consulta de la variable hrSystemDate

  snmpget -v2c -c public router1.lab.ort hrSystemDate.0

  Cuidado: los nombres de variables son sensibles a minúsculas y mayúsculas