AS2 : Practica 3

Objetivo : Puesta en marcha de 1 dominio FreeIPA y NFS mediante CentOS.

Entrega: La entrega de la Práctica 3 se realizará a través de la tarea habilitada para tal efecto en Moodle, siendo la **fecha límite el 30 de marzo** de 2023 y la **evaluación el 31 de marzo**.

Se deberá **entregar, una memoria** en la que, al menos, se incluya:

1.- Resumen

2.- Introducción, objetivos y Arquitectura de elementos relevantes

3.- Explicación de elementos significativos de la práctica (máquinas, subredes, componentes e información de servicios distribuidos, recursos sistema, configuraciones)

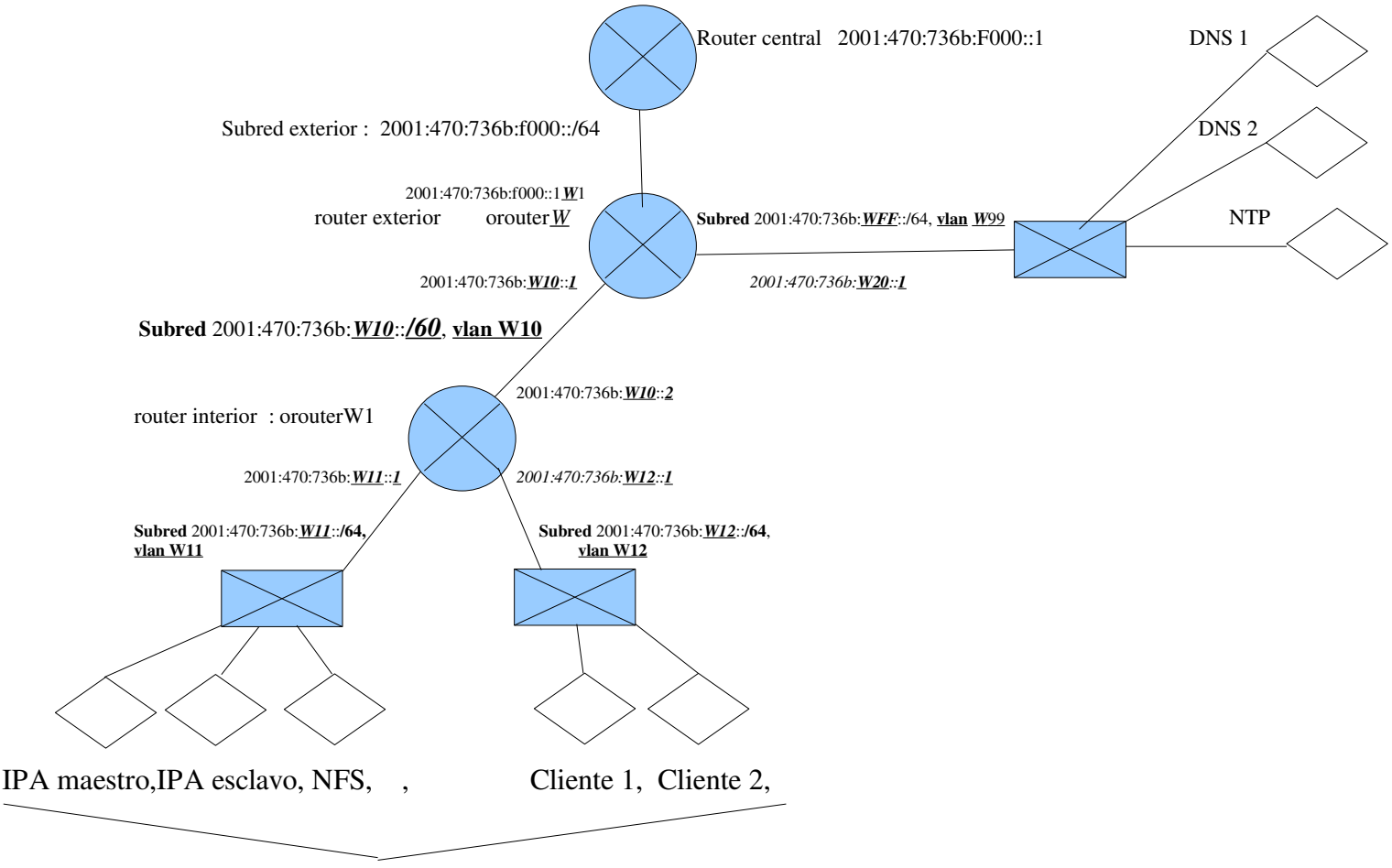
4.- Explicación del desarrollo de la puesta en marcha y configuración de los diferentes aspectos requeridos

5.- Pruebas realizadas para comprobar el correcto funcionamiento del sistema.

4.- Problemas encontrados y su solución.

Enunciado : <u>La gran mayoría de la operativa debería hacerse por ssh.</u>

1. Configuracion de red y servidores



Subdominio FreeIPA/DNS : **1.<nºgrupo>.ff.es.eu.org**

Se mantiene la misma subred con servidores DNS1, DNS2 y NTP construida en prácticas.

Variables :

W **:** nº grupo seleccionado en moodle en Hexadecimal (para MAC e IPv6). ***Pasar a decimal*** para VLAN (máximo 15)

1 Subredes intermedias nuevas : 2001:470:736b:***W*****X0::/60** **(X=1,** en el esquema anterior**)**

2 ***Subredes extremo*** **nuevas :** 2001:470:736b:***WXY::/64*** (con valores establecidos en el esquema anterior)

VLANs : WXY (W en valor decimal)

Z : Designación máquinas específicas, 2001:470:736b:***WXY***::**Z y @** ***MAC*** **VMs qemu :** 52:54:00:0***W:XY:0Z***

* Z=1 para routers interiores para subredes extremas,
* Z=2 para VM2 : servidor controlador ipa1 (maestro)
* Z=3 para VM3 : servidor controlador ipa2 (réplica)
* Z=4 para VM4 : servidor NFS kerberizado

* cliente1 y cliente2 serán configurados con la designación Ipv6 automatica.

* **Subdominios directos DNS** y **FreeIPA** (X correspondiente a cada subred intermedia):

X**.<nºgrupo>.ff.es.eu.org**

** Subdominios inversos DNS alto nivel y DNSs FreeIPA (W : nº grupo, Xsubred intermedia) correspondientes a subredes :*

*2001:470:736b:**W/56***

*2001:470:736b:**WX/60***

* ***Nombres DNS (y de VMs)*** *: orouterW1, orouterW2, ipa1, ipa2, nfs1, cliente1, cliente2*

* ***UUID en xml*** *libvirt de cada VM : últimas cifras* W, X, Y, Z

2. Preparación VM base CentOS

Teneis la imagen VM base *c74.qcow2* (y su *xml* asociado) que podeis obtener desde */misc/usuarios/unai/vms*. Se le ha incluido *puppet*, *ruby* y *vim* (con coloracion sintactica también para puppet y ruby), y el repositorio adicional "*epel*" (necesario para un cierto número de paquetes en CentOS). Usuario/contraseña : root/relativamentelargo

Añadir vuestro usuario en dicha imagen base (comandos useradd, groupadd, usermod, userdel...) y añadirle al grupo *wheel* para darle privilegios root con sudo.

Crear las VMs que necesiteis de CentOS con imagenes diferenciales a partir de ella.

La configuración de vlans se establece en directorio */etc/sysconfig/network-scripts*. Solo necesitais el fichero ifcfg-eth0 (relacionado con la tajeta ethernet física) y teneis que crear un fichero ifcfg-eth0.<nºvlan>. En el tema de configuración de red teneis algunos ejemplos.

Recordar deshabilitar la configuración automática de IPv6 solo en la tajeta de red base (aquí, *eth0*), para que solo tengais comunicación por vlan. Deshabilitarlo con los pasos indicados en el Anexo A.

3. Aspectos de la práctica

Seguir, en todo momento, los datos aportados en el esquema de red inicial y los parámetros indicados en la sección 1, salvo la zona rallada del esquema gráfico. Se van a seguir utilizando el router exterior y los servidores DNS y NTP puestos en marcha en prácticas. En particular, en ellos debeis poner el subdominio DNS inverso adecuado para vuestra subred de alto nivel *2001:470:736b:W/56 y establecer los glue records de DNS necesarios entre este y vuestros subdominios DNS inversos de FreeIPA*.

Configuración para el sistema

Crear el router interior W1, y configurar adecuadamente tanto el anterior router exterior como el router interior W1 para que los paquetes IP se encaminen adecuadamente a las diferentes subredes explicitadas por debajo del segmento de red 2001:470:736b:***W10***::***/60***.

Bajo el router interior W1, crear una primera zona de subredes definida bajo un dominio FreeIPA **1.<nºgrupo>.ff.es.eu.org** constituido por 2 controladores de dominio (maestro y réplica) y 1 máquina servidor NFS kerberizado en una subred. 2 máquinas clientes CentOS definidas para ese dominio FreeIPA en otra subred. Y 2 usuarios creados en el dominio FreeIPA con sus *homes* en el servidor NFS kerberizado con auto montaje. El servidor NFS kerberizado puede ejecutarse sobre otra VM con CentOS.

Todas las máquinas necesitan sincronización de tiempos, también para Kerberos. En los CentOS, utilizar el software "**chrony**" que implementa de forma más práctica el protocolo NTP.

Definir una estrategia de despliegue y puesta en marcha por etapas., añadiendo elementos poco a poco. Comprobar el funcionamiento correcto de cada etapa. Por ekemplo, al poner en marcha un servidor IPA y un cliente, dar de alta y probar una nueva cuenta de usuario en vuestro nuevo dominio IPA.

Tener en cuenta que la operativa de máquinas en dominio IPA implica necesidad de operar continuamente con Kerberos. En particular, para probar el funcionamiento del servicio NFS kerberizado, debeis probar la escritura de ficheros o directorios desde una cuenta de usuario IPA, porque tendra privilegios Kerberos para el dominio IPA, a diferencia de las cuentas de usuario locales que no la tienen.

Configuración de /etc/exports es con formato (hay otro que no es válido):

directorio subbred/subdominio(opciones montaje, incluidas las de kerberización)

Comprobar de forma minuciosa que todos los elementos necesarios de configuración están habilitados.

Los controladores FreeIPA usarán sus propios servicios DNS y NTP para sus subdominios (bien enlazados).

4. Opcional

Poner en marcha 3 servidores GlusterFS (1 VM distinta para cada uno) en configuración de alta disponibilidad (replicacion por quorum) y prestaciones, para sustituir a los servidores NFS en la provisión de directorios home a usuarios. Comprobobar que la caida de un servidor GlusterFS no deja indisponibles los directorios y ficheros que alberga. Recordar que GlusterFS no está kerberizado.

Referencias

Temas : Almacenamiento, Configuración, Seguridad, Integración de servicios.

Redhat :

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/sec-Configure_802_1Q_VLAN_Tagging_Using_the_Command_Line.html

- https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html

- https://access.redhat.com/documentation/en- US/Red_Hat_Enterprise_Linux/7/html/System-Level_Authentication_Guide/index.html

- Documentación Redhat Gluster storage Installation, Administration (versión 3.5).

- Para CentOS 7, teneis explicaciones básicas para Glusterfs 6 en :

https://www.server-world.info/en/note?os=CentOS_7&p=glusterfs6&f=1

Anexo A

Deshabilitar IPv6 en Linux reciente (CentOS,...) :

*En fichero /etc/sysctl.conf (solo deben estar estas entradas activas) :

net.ipv6.conf.eth0.use_tempaddr = 0

net.ipv6.conf.eth0.autoconf = 0

net.ipv6.conf.eth0.accept_ra = 0