AS2 : Proyecto

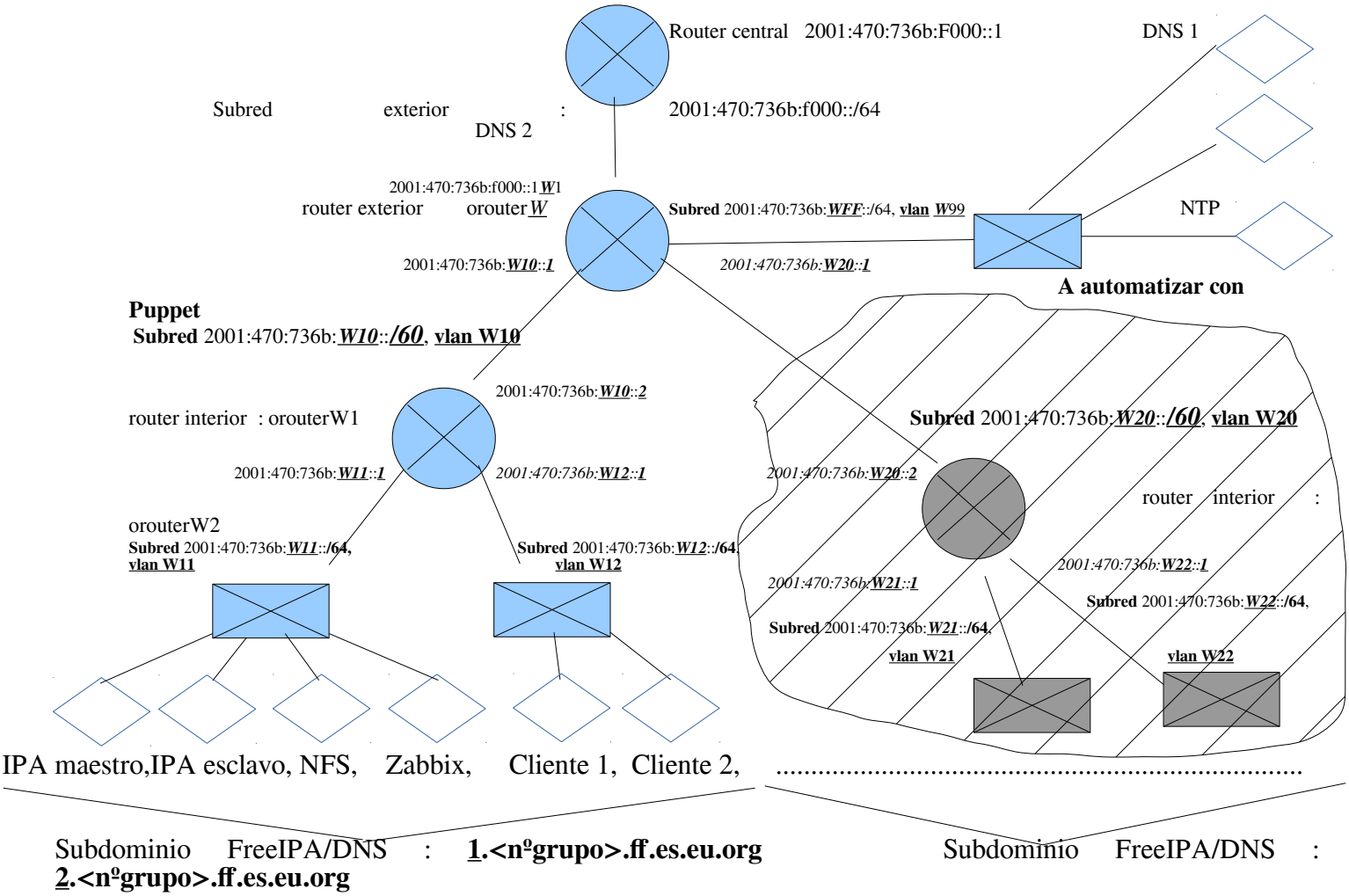
Objetivo : Puesta en marcha de 2 dominios FreeIPA mediante CentOS 7, Ubuntu, Puppet y un entorno de monitorización.

Se deberá **entregar, para cada una de las 2 partes del proyecto y en el tiempo establecido, una memoria** (**y código Puppet en la 2ª parte**) 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



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)

2 Subredes intermedias nuevas : 2001:470:736b:***W*****X0::/60** **(X=1, X=2,** en el esquema anterior**)**

4 ***Subredes extremo*** **nuevas :** 2001:470:736b:***W*****XY::/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
* Z=5 para VM5 : servidor Zabbix

* 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, zabbix1, 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 es un poco diferente a Ubuntu. Ya teneis en el sistema lo necesario. La configuración se establece en directorio */etc/sysconfig/network-scripts*. Solo necesitais el fichero ifcfg-ens3 (relacionado con la tajeta ethernet física) y teneis que crear un fichero ifcfg-ens3.<nºvlan>. En el tema de configuración de red tenesi algunos ejemplos..

Recordar deshabilitar la configuración automática de IPv6 solo en la tajeta de red base (aquí, *ens3*), para que solo tengais comunicación por vlan. Deshabilitarlo con las mismas instrucciones que con Ubuntu en la práctica nº 3.

3. Objetivos del proyecto

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*.

1ª parte : Configuración manual para el sistema en la primera subred

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. Finalmente, habilitar un servidor Zabbix dedicado que monitorice el funcionamiento o parada, el uso de CPU, memoria y disco y el uso de ancho de banda para cada una del resto de máquinas. El servidor NFS kerberizado puede ejecutarse sobre una VM con CentOS. El servidor Zabbix puede ejecutarse sobre una VM con Ubuntu (aunque también está disponible en OpenBSD, FreeBSD y CentOS).

Todas las máquinas necesitan sincronización de tiempos, también para Kerberos. En los linux, podeis 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).

Entrega 1ª parte : antes del 20 de mayo de 2020.

2ª parte : Automatización de configuración y puesta en marcha de 2ª subred

Automatizar la configuración del router interno, del servidor NFSv4, del servidor Zabbix, de clientes ntp, dns, ntp, nfs y zabbix mediante la herramienta u y Puppet ,con modulos . No es necesario automatizar la configuración de los servidores IPA (por excesiva dificultad).

Para ello, adaptar la herramienta "*u*" para que se pueda pasar como parámetro, no un manifiesto sino un fichero tar o similar que contenga todos los modulos y manifiestos necesarios para desplegar la configuración necesario para un conjunto de aplicaciones y sericios en un máquina remotas (o grupos) definidas en el fichero de configuración de "*u*". Estos manifiestos y modulos estarán ya creados en el subdirectorio "*despliegue*" del directorio "*.u*". Podeis construir vuestros modulos, descargar modulos desde el repositorio de puppet : https://forge.puppetlabs.com/ y adaptarlos a vuestras necesidades.

Tener en cuenta que para algunas operaciones necesitareis automatizar un proceso interactivo de autentificación con contrseña para ipa.

Finalmente, utilizar la automatización definida para crear, con rapidez, el segundo segmento de red 2001:470:736b:***W20***::***/60,*** *el* segundo dominio FreeIPA **2.<nºgrupo>.ff.es.eu.org** , bajo un segundo router

interior, con otros 2 controladores en otra subred, 1 servidor NFS kerberizado, 1 servidor Zabbix, 2 máquinas clientes en la cuarta subred y 2 usuarios de dominio.

Entrega 2ª parte : antes del 19 de junio de 2020

4. Opcional

Podeis elegir una o varias cualquiera de ellas. No tienen dependencias entre ellas, aunque algunas puedan combinarse.

a) Definir acuerdos entre los 2 dominio FreeIPA, mediante puppet, para que los usuarios de un dominio puedan entrar en sesión en clientes del otro dominio. Proponer una solución para los homes NFS.

b) Poner en marcha 4 servidores GlusterFS en configuración de alta disponibilidad y prestaciones, mediante puppet, 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

Tema 9 : 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