Instituto de Geofísica
UNAM

VIRTUALIZACIÓN DE SERVIDORES DEL LABORATORIO DE GEODESIA SATELITAL (LAGEOS)

Franco[1a] S.I., Luciano Díaz[2], Gilberto Casillas[1b], Luis Miguel de la Cruz[1c], Miguel Ángel Palacios[1b,], Daniel Rodríguez Osorio[1b].

1a Instituto de Geofísica, LaGeoS, Servicio Magnético.
1b Instituto de Geofísica, Unidad de Cómputo.
1c Instituto de Geofísica, Departamento de Recursos Naturales.
2 Instituto de Ciencias Nucleares, Unidad de Cómputo y Seguridad Informática.

INTRODUCCIÓN

El Laboratorio de Geodesia Satelital (LaGeos) forma parte de los laboratorios institucionales del Instituto de Geofísica. Este laboratorio tiene como objetivo principal proporcionar a los usuarios herramientas e infraestructura de gran nivel para potenciar el uso eficiente e interdisciplinario de los datos GPS dentro del IGef.

Para su operación, el LaGeoS cuenta, actualmente, con dos servidores reales (físicos), uno de los cuales es un servidor de prueba y el otro un Servidor de producción. El desempeño del laboratorio requiere del buen funcionamiento de estos servidores. La instalación y configuración exitosa de dichos servidores ha requerido de la investigación, la recopilación y la organización de mucha información proveniente de diversas fuentes.

Este documento tiene como finalidad describir la metodología utilizada en el LaGeoS para la virtualización de los servidores que se tienen actualmente en operación y de esta manera contar con un banco de conocimientos. El documento constituye una parte de la descripción de infraestructura con la que cuenta el LaGeoS.

Para lograr la virtualización de los servidores, la metodología será descrita desde la instalación y configuración del servidor de producción, al cual llamaremos servidor anfitrión. Después se describirá el proceso de virtualización y, por último se hará una descripción breve de la virtualización, configuración y administración básica de clusters. Toda la información, lista de comandos e instrucciones que se describen en este documento y que se utilizan en el servidor anfitrión, son válidas para un servidor con sistema operativo CentoS 6.9.

1. ESPECIFICACIONES DE LOS SERVIDORES

Las características técnicas de los servidores del LaGeos se resumen en la tabla 1. De estos servidores, el que llevará la mayor carga de trabajo es el servidor de producción. En este servidor se virtualizarán, inicialmente, cinco equipos en donde se realizarán diversos procesos que van desde la adquisición de datos y su procesamiento con diferentes estrategias (programas), hasta funciones propias de un servidor web, entre otros. El servidor anfitrión (¿cual de los 2?) consta de un disco duro de estado sólido (¿de que capacidad?) y 8 discos de 6 TB cada uno. El arreglo de discos de 48 TB

formará parte del arreglo Raid, mientras que el disco de estado sólido se utilizará para instalar el sistema operativo.

Tabla 1: Listado de las características del servidor del LaGeoS.

Nombre	Año de adquisición	Procesador	Memoria RAM	Disco Duros	Interfaz de Red	Tarjetas RAID	Extras
Servidor de prueba	2104	Intel(R) Core(TM) i7-4770 de 8 cores	4 ranuras DIMM totales. 12 GB de memoria (4 GB x 2 y 2 GB x 2)	1 Disco duro SATA de 2 Tb 7200 rpm	Realtek para red LAN. Qualcomm Atheros para wireless.	N/A	Servidor de escritorio. SO Ubuntu 16.04
Servidor de producción	2016	Procesador Intel Xeon E5-2683 V4 de 32 cores	16 ranuras DIMM totales. 128 GB de memoria RAM (32GB x 4), Módulos DDR4 RDIMM ECC a 2400 Mhz.	1 Disco Duro de estado sólido, de 120 GB. Disco SATA-III de 6 Gb/s. 48 TB de capacidad de alamacenamiento (real 28T). Distribuido en 8 discos de 6 TB SAS-III, 7200 rpm (2 discos han sido prestados por el Instituto de Nucleares). 12 bahías para discos SAS-III 12 x 3.5"	Puerto dual para red LAN GbE Intel i350	Tarjeta RAID para discos SATA/SAS; 12 GB/s. LSI Mega RAID cachevault	Servidor de rack 2u. Fuente de poder redundante. S0 Centos 6.0

1.2 DESCARGA DEL SOFTWARE

De acuerdo con las recomendaciones dadas por personal que administra el clúster de servidores del Instituto de Ciencias Nucleares, el sistema operativo que se utilizó fue Centos V. 6.0 . La imagen ISO para instalar el sistema operativo se descargó del sitio:

http://mirror.cc.columbia.edu/pub/linux/centos/6.8/isos/x86_64/

El archivo que se descarga del sitio es:

CentOS-6.8-x86_64-minimal.iso

que corresponde a la instalación mínima del sistema operativo. Una vez que se baja el archivo, se copia a una memoria USB con el comando:

```
sudo dd if=CentOS-6.8-x86_64-minimal.iso of=/dev/sdb1
```

dónde `/dev/sdb1` es el nombre del dispositivo donde se montó la memoria usb al conectarse a la PC. Este nombre lo podemos saber dando el comando *`df -h`*, que nos indica los dispositivos que están montados, el espacio que ocupan y en el sistema de archivos del sistema donde están montados.

1.2 INSTALACIÓN DEL SO

Para instalar el sistema operativo arrancamos la PC desde la memoria que contiene el archivo imagen de instalación de Centos. Para que la computadora reconozca la USB como primera opción de arranque desde la PC presionamos la tecla F11 al momento que la computadora esté corriendo. Si la máquina no arranca desde el USB aun cuando se eligió hacer el arranque desde este dispositivo,

es posible que el USB no esté funcionando correctamente, o bien, que la imagen ISO no se copió correctamente.

Una vez que se reconoce a la USB como el medio de arranque, se carga la imagen de instalación a la computadora y se inicia el proceso de instalación. Durante la instalación llega a un punto donde pregunta que medio utilizará el equipo para realizar la instalación. Dentro de las opciones que presenta la instalación no viene la que corresponde a un medio USB, por lo que seleccionamos la opción Disco duro y en seguida seleccionamos la opción */dev/sdb* (es decir, el sistema reconoce que se utilizara un medio USB en el dispositivo */dev/sdb* conectado al disco duro).

Por otro lado, el modo de instalación que seleccionamos es el modo personalizado. En este modo nos permite borrar las particiones ya existentes en el dispositivo */dev/sda* (disco duro), y volver a crear nuevas particiones. Las particiones que creamos después de haber eliminado las del sistema operativo preexistente de Centos fueron:

Partición	**Tamaño**
/	31 GB
swap	16 GB
/var	16 GB

1.2 CONFIGURACIÓN INICIAL DE LA RED

Para configurar la red del sistema entramos a la sesión de linux y abrimos una terminal de comandos. Dentro de la terminal y como súper usuarios editamos los archivos que se mencionan a continuación. En estos archivos se escriben los parámetros de red que identificarán al servidor: dirección IP, máscara de subred, puerta de enlace y servidores DNS; esta información debe de ser suministrada por el responsable de redes.

El contenido de los archivos que editamos quedaron como se muestra en el recuadro debajo de la ruta de cada archivo junto a su descripción.

/etc/sysconfig/network-scripts/ifcfg-eth0: Características de la interfase de red.

```
DEVICE=eth0
HWADDR=0C:C4:7A:A8:FA:8E # la da por default el sistema
TYPE=Ethernet
ONBOOT=yes  ### Con esta opción la interfase se habilita
NM_CONTROLLED=yes
BOOTPROTO=static ### Se establece que la IP que se otorga es estática.
IPADDR= [dirección IP]*
NETMASK=[máscara de red]*
```

/etc/sysconfig/network: Este archivo es para especificar información acerca de la configuración de la red

```
NETWORKING=yes ### Significa que la red debe ser configurada
HOSTNAME=nandxo ### Nombre del servidor (poderoso en zapoteco)
GATEWAY= [dirección IP de la puerta de enlace]*
```

/etc/resolve.conf: Las direcciones IP del DNS

```
nameserver [dirección IP 1 del DNS]*
nameserver [dirección IP 2 del DNS]*
```

Para aplicar cualquier cambio a la configuración es necesario reiniciar el servicio:

sudo /etc/init.d/network restart

1.2 INSTALACIÓN DE SOFTWARE BÁSICO

En este paso, ya contamos con un usuario, que es el usuario root, con privilegios de administrador, razón por la cual las instalaciones que se harán son como super usuario.

`rpm -qa`→ Este comando nos permite revisar que librerías y programas están instalados.

Por ejemplo:

`rpm -qa | grep openssh` nos dirá si openssh está instalado.

Se instalan o configuran los siguientes programas:

- SELinux: Security-Enhanced Linux (SELinux) es un sistema de control de acceso obligatorio (Mandatory Access Control) basado en la interfaz LSM (Linux Security Modules). En la práctica, el kernel pregunta a SELinux antes de cada llamada al sistema para saber si un proceso está autorizado a realizar dicha operación. Se debe de editar el archivo */etc/selinux/config* para deshabilitar el SELinux; hay que reiniciar el servidor después de está operación:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

- Instalar Extra Packages for Enterprise Linux (EPEL; https://fedoraproject.org/wiki/EPEL):

```
wget http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
wget --no-check-certificate https://getfedora.org/static/0608B895.txt -O epel-key.txt
```

```
wget --no-check-certificate https://getfedora.org/static/0608B895.txt -O epel-key.txt
yum localinstall epel-release-6-8.noarch.rpm
```

- `iftop` programa que viene en EPEL. Sirve para ver y adminsitrar interfases de red.
- `lshw` → para ver el hardware que se encuentra instalado: *yum install lshw*
- `screen` →: permite dejar sesiones abiertas, usar varias teminales o ventanas desde una solo conexión ssh: *yum install screen*
- `iotop` →: Sirve para monitorear el uso de disco: `yum install iotop`. iotop requiere el último Kernel 2.6.18 y Python 2.4 con módulo de ctypes, damos la primera actualización del kernel de Linux con la ayuda del siguiente comando.

  `yum kernel de actualización`

  Luego hay que actualizar Python con el módulo ctypes para iotop paquete. (?)

  `yum install python python-ctypes` Se necesita antes de instalar iotop instalar (?).

2. CONFIGURACIÓN DE ARREGLO RAID

La configuración del RAID se debe de hacer físicamente (no es posible la conexión remota). Para realizar la configuración del RAID se utiliza la interfaz del controlador RAID. Esto se logra durante el arranque del servidor, oprimiendo las teclas *Ctrl+R*. Con esta acción entramos al menú de configuración.

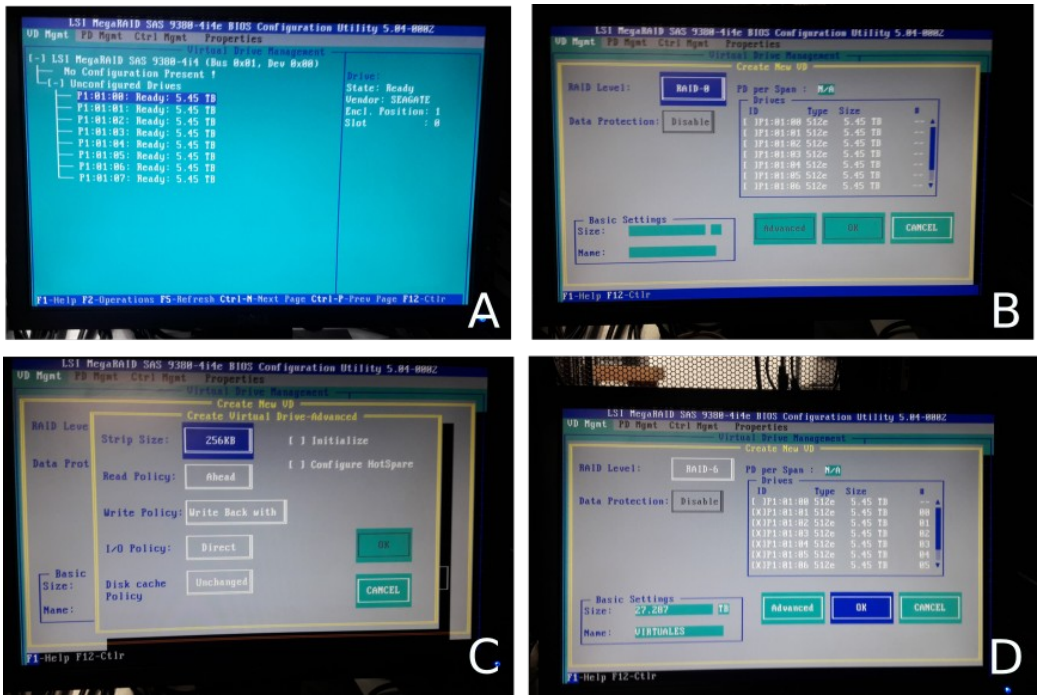

Figura 1: Pantallas de inicio durante la configuración de la tarjeta RAID. 1A: muestra el pantalla de inicio del controlador del RAID. 1B: es la pantalla de inicio para comenzar a crear el nuevo dispositivo virtual. 1C: Configuración de las opciones avanzadas ***"Advanced"*** . 1D: confiugración final del RAID; el nombre de la configuración virtual en nuestro caso es "virtuales". Para más detalles acerca de la configuración, revisar el texto.

En la Figura 1 se muestran la pantalla de entrada de la interfaz (a) y la ventana para crear una nuevo dispositivo virtual (b). La configuración se realiza en la primera ventana VD Magmt (Virtual Device Managment). Los pasos a seguir para realizar la configuración son:

i) Crear un dispositivo virtual. En la opción de ***"No configuration Present"*** (ver Figura 1a para detalles), dar enter. Después de este paso, se despliega una nueva ventana, la cual se muestra en la Figura 1b.

ii) Se define el nivel del RAID. En nuestro caso hemos optado por un RAID6.

iii) Con la barra espaciadora se seleccionan los discos (recuadro del lado derecho de la Figura 1b). Como se menciono anteriormente, en nuestro caso dejaremos un disco de *spare* (de emergencia) y para este caso utilizamos el disco 0. Seleccionamos todos los demás.

iv) Se establece como nombre de la unidad "*VIRTUALES*". En el recuadro inferior izquierdo se muestra el tamaño real del arreglo, *ebn* nuestro caso con 8 discos de 6TB y la configuración descrita, nos queda un espacio real para almacenar datos de 27.8 TB (ver Figura 1c).

v) Las opciones avanzadas *"Advanced"* se dejan las que están por definición, como se muestra en la figura 1d.

2.1 DAR FORMATO AL ARREGLO RAID

El arreglo RAID que creamos en la sección anterior es de varios TB. Para discos mayores a los 2 TB se debe de utilizar el sistema (file system) XFS y no ext4. Para poder utilizar este tipo de sistema (XFS) se necesita la herramienta xfsprogs. Para instalar esta herramienta se utiliza el comando: yum -y install xfsprogs.

Después de instalar xfsprog se debe reiniciar el servidor.

Un detalle importante acerca de XFS es que no es tolerable a fallas por lo que debemos tener un servidor muy confiable (desde el punto de vista de respaldos de suministro de energía eléctrica). El sistema XFS se debe de utilizar en servidores de producción.

Para crear las particiones y dar formato se utilizará el programa parted (yum -y install parted).

3. VIRTUALIZACIÓN

El proceso de virtualización consiste en la emulación, vía software, de algunos recursos tecnológicos: sistema operativo, recursos de red, dispositivos de almacenamiento, etc.

Para empezar la virtualización, hay que cerciorarse de que en el BIOS se ha habilitado la opción de virtualización.

Los pasos a seguir para poder llegar a la virtualización de los servidores son (todo esto se debe de hacer en el servidor anfitrión, servidor físico):

(1) Dar formato al arreglo raid.

(2) Deshabilitar SELinux.

(3) Instalar QEMU. Configurar la cuenta del usuario qemu.

(4) Generar la configuración necesaria para las interfases de red virtual.

(5) Permisos para administrar las interfases de los usuarios.

Para iniciar el proceso de virtualización es necesario instalar varios programas:

bridge-utils: Utilerias para crear interfaces virtuales *bridge* (para más detalle consultar wikipedia).

tunctl: Utileria utilizada para crear y administrar interfaces TUN/TAP. TUN y TAP son los núcleos (kernel) de la red virtual. Estos dispositivos actúan en la capa 3 y 2, respectivamente, de las capas de Redes. En el caso de la virtualización, utilizaremos el dispositivo TAP con el *bridge*.

qemu-kvm & qemu-img: Programas de virtualización. Con estos programas se genera el ambiente para albergar servidores virtuales.

gpxe-roms-qemu: Herramientas que permiten el arranque de las máquinas virtuales por medio de la red.

La instrucción para instalar los programas anteriores es: `yum –y install bridge-utils tunctl qemu-kvm qemu-img gpxe-roms-qemu`

Dar formato al arreglo RAID como se describió en la sección anterior.

3.1 DESHABILITAR SELINUX

SELinux (por sus siglas en inglés de Security-Enhanced Linux) es un sistema de control de acceso obligatorio (Mandatory Access Control) basado en la interfaz LSM (Linux Security Modules). SELinux está definido por default en sistema opertaivo RedHat y CentOS, otros sistemas operativos de linux no necesariamente tienen habilitado por definición este sistema de control.

SELinux puede estar configurado en uno de los tres siguientes estados:

enforcing - Aplica las políticas definidas en el sistema.

permissive - Solo emite advertencias pero no aplica las políticas.

disabled - No se cargan las políticas del sistema.

Para conocer el estado actual de SELinux se utiliza el comando `getenforce`. En caso de que el estado no sea “disabled”, entonces será necesario modificar la configuración para deshabilitar SELinux.

El archivo de configuración es /etc/selinux/config. Para deshabilitar SELinux debe difinirse el valor de la variable SELINUX=disabled. Después de modificar o establecer el valor de esta variable en el archivo de configuración es necesario reiniciar el servidor.

3.2 INSTALAR KVM-QUEMU Y CONFIGURAR LA CUENTA DEL USUARIO QEMU

Para comenzar con el tema de virtualización de servidores, haremos una breve descripción de la aplicación que utilizaremos para tal efecto.

Qemu es una aplicación ampliamente utilizada para crear máquinas virtuales, con diferentes características y sistemas operativos, dentro de un sistema operativo anfitrión.

El proceso de virtualización de servidores consiste en emular un sistema operativo (llamado húesped) dentro de otro (sistema anfitrión) sin tener que particionar el disco duro. La virtualización se hace a partir de los recursos del servidor anfitrión. Con QEMU se pueden emular varios tipos de arquitecturas y tarjetas virtuales.

Una vez que se ha instalado QEMU, es necesario configurar la cuenta de usuario qemu (la cual se genera a instalar **gpxe-roms-qemu**). Este usuario, no tiene un *home* asignado, ni tampoco está habilitado para hacer el *login.* Por tal motivo, hay que modificar las características de este usuario.

Para nuestro caso, hemos decidido que el punto de montaje para todas las máquinas virtuales que se harán en nandxo es: /local/virtuales00. Este punto es el que designamos como el directorio home del usuario qemu.

Para asignar el directorio home al usuario qemu hay que modificar el archivo /etc/passwd. Los pasos que se siguen son:

1. Buscar la línea donde está marcado el usuario qemu.

2. Después de "user:" añadir el punto donde se montará el directorio home. **qemu:x:107:107:qemu user:/local/virtuales00:/bin/nologin**

3. Para permitir que el usuario qemu pueda hacer login, modificar el /bin/nologin/ por el script de arranque. La línea queda así: **qemu:x:107:107:qemu user:/local/virtuales00:/bifrejan/bash**

4. Se salvan los cambios en el archivo /etc/passwd.

5. Crear el archivo de arranque de sesión acorde al script de arranque que se determino (en este caso bash). Para hacer esto se copian las plantillas de /etc/skel/*bash* (estos archivos al ser de sistemas, están ocultos, para verlos usar el comando ls -la *bash*). El genérico de bash está en / etc/bashrc.

6. En el punto de montaje del home de qemu hay que cambiar los permisos: chmod -R qemu:qemu /local/virtuales00

7. Para configurar la red de la máquina virtual se necesitan usar los comandos de brctl y tunctl, los cuales sólo pueden utilizarse por usuarios con privilegios de super usuario (sudo). Para permitir que el usuario qemu pueda utilizar estos comandos hay que utilizar el comando visudo. Este comando abre un archivo en modo de edición utilizando vi. Las modificaciones que hay que hacer son:

   a) Añadir una alias de comando donde se indique que el usuario qemu puede correr los comandos brctl y tunctl. Para lograr esto hay que añadir dos líneas al final de la sección de alias de comando (en ingleś "Command Aliases"):

   #@eml: qemu control

   Cmnd_Alias QEMU = /sbin/ifconfig, /usr/sbin/brctl, /usr/sbin/tunctl

   b) Indicar que cualquier usuario del grupo qemu (solo pertenece a ese grupo el usuario qemu) puede ejecutar cualquier comando si solicitarle contraseña. Para hacer esto se añade una línea en la última sección, justo al final del archivo:

   ## Allows people in group qemu to run all commands without password
   %qemu ALL=(ALL) NOPASSWD: QEMU

3.3 GENERAR LA CONFIGURACIÓN NECESARIA PARA LAS INTERFASES DE RED VIRTUAL:

En está sección, hay que iniciar sesión como usuario qemu, ya que este usuario es el único que puede crear la máquina virtual.

Para entrar en sesión, dado que ya hemos configurado la cuenta para que el usuario qemu pueda conectarse sin autentificación, sólo hay que teclear `qemu`.

Una vez en al cuenta del usuario qemu, comenzaremos con la configuración de la red para las máquina virtuales.

El primer paso es crear el bridge y ligarlo a la interfase de red *real eth0* (en nandxo).

Un bridge es un dispositivo que conecta múltiples segmentos de red. Funciona como capa 1 y/o 2. El bridge conecta o trabaja con las *mac address*.

La instrucción para crear un bridge es:

> `brctl addbr br132`: Con está instrucción se crea el dispositivo bridge br132
>
> `brctl addif br132 eth0`: Se añade el dispositivo eth0 al bridge br132
>
> `ifconfig br132 up`: Se activa o se levanta la interfase br132.
>
> `ifconfig br132 132.248.182.37 netmask 255.255.255.0 up`: Se configura la interfase br132, se la una dirección ip y una máscara de red.
>
> `ifconfig eth0 0.0.0.0 promisc`: Quitarle la dirección ip a la interfase eth0.
>
> `route add default gw 132.248.182.254 br132`: Se añade a la tabla de ruteo el gateway de salida para la interfase br132.

Para garantizar que este bridge exista aun cuando la máquina se reinicie, lo que hacemos es poner estas líneas de comando en un script, el cual se ubica en el home del *root* y se llama setupBRIDGE.sh (/root/setupBRIDGE.sh). Este script debe de tener permisos de ejecución.

Para que se ejecute este script al cargar el sistema, se debe de incluir en el archivo /etc/rc.local. Este script es el último en ejecutarse durante la secuencia de arranque. Es importante que la última tarea que se corra desde rc.local sea la configuración del bridge; por tal motivo, está instrucción debe de estar en la última línea del script *rc.local*.

Una vez que hemos creado el bridge, hay que crear el dispositivo virtual por el cual se conectará. Para hacer esto usamos el comando `tunctl`.

Este comando se utiliza en el script de creación (*install.sh*) y ejecución (*run.sh*) de la máquina virtual, respectivamente. Una breve descripción de estos scripts se hará más adelante.

4 VIRTUALIZACIÓN Y CONFIGURACIÓN DE CLUSTERS

Como ya se mencionó anteriormente, nosotros utilizamos para virtualizar el programa qemu (se describió en la sección 3.2).
Cuando vamos a configurar un cluster, se debe definir que servidor será el nodo maestro y cual o cuales serán los nodos esclavos o de procesamiento.
El procedimiento realizado para la virtualización es el mismo sin importar el nodo del que se trate. Resumiendo lo descrito en el apartado anterior, los pasos para la virtualización son:

1) Crear el disco duro: qemu-img create [nombre_disco] [tamaño] [unidad]
2) Instalar el sistema operativo, utilizando qemu
3) Arrancar el servidor virtual utilizando qemu

4.1 CONFIGURACIÓN DEL NODO MAESTRO

En el nodo maestro, además de realizar las configuraciones que se han descrito anteriormente, se deben de configurar los siguientes servicios:

- DHCP: para otorgar direcciones IP automáticas através de la dirección MAC. `sudo apt-get install isc-dhcp-server`.
- DNSmasq: Para asociar los dominios y las direcciones IP. `apt-get -y install dnsmasq`.
- NIS: Para administrar grupos y usuarios en todos los nodos a partir del nodo maestro. `sudo apt-get -y install nis`.
- NTFS: Para compartir o montar discos. `sudo apt-get install nfs-common`.

El /home debe de ser exportado por *ntfs*.

4.1.2 CONFIGURACIÓN DE USUARIOS

Para compartir los usuarios y servicios entre el nodo maestro y el nodo de procesamiento se utiliza el servicio NIS. Los detalles de configuración del nodo maestros están en el anexo 1.
Este servicio debe de ser instalado tanto en el nodo maestro como en el de procesamiento.

Para crear un nuevo usuario se deben de seguir los siguientes pasos:

```
adduser -u 1200 -m ldg -g 1000 -s /usr/bin/tcsh
```

donde

adduser → es el comando en CentOS, useradd es en ubuntu
-u → user id (se recomienda revisar e archivo /etc/passwd para ver el siguiente id)
1200 → ID del usuario que se va asignar
-m → Para obligar a crear el home del usuario
ldg → User name
-g group id. → Para obligar a que el nuevo usuario pertenezca a un grupo definido.
1000 → ID del grupo que se va asignar
-s → Para asignar un shell de inicio específico
/usr/bin/tcsh → Ubicación y nombre del shell.

Una vez creado el o los nuevos usuarios, hay que actualizar la información en el NIS:

```
/usr/lib/yp/ypinit -m
```

4.1.3 EXPORTAR DISCOS

Como se mencionó anteriormente, los nodos de procesamiento carecen de la partición /home, ya que se asume que compartirán está información con el nodo maestro.
Para lograr esto, la partición home debe ser “compartida” desde el nodo maestro utilizando el sistema NTFS.

Para hacer esto, se debe de añadir el nuevo servidor o nodo de procesamiento en el archivo */etc/exports* y correr la instrucción: `exportfs -rv`

4.2 VIRTUALIZACIÓN DEL NODO ESCLAVO

En el caso del laboratorio, los nodos solo se utilizan para procesar datos. El almacenamiento de los datos está en otro servidor/disco. Por tal motivo, los discos duros son pequeños (100GB, menos no funciona bien el servidor, es muy lento). Por default creamos los servidores con 8 cores y 12GB de memoria RAM.

La partición genérica es:

/swap 12GB
/ 99GB

No existe la partición /home por que esa se monta del nodo maestro.

4.2.1 CONFIGURACIÓN DE LA RED

Como el servido maestro esta configurado como un servidor DHCP, el servidor de procesamiento tomará la dirección IP automáticamente. Para tal efecto, en el nodo maestro, en el archivo de configuración DHCP (*/etc/dhcp/dhcpd.conf*) se deben de incluir las siguientes líneas por cada servidor al que se le quiera otorgar una dirección IP:

```
host hostname.gipsy_lageos.unam.mx {
    hardware ethernet MAC ADDRESS;
    fixed-address direccionIP;
    option host-name "hostname.gipsy_lageos.unam.mx";
}
```

Después de añadir esta línea se tiene que reiniciar el servicio DHCP: `systemctl restart isc-dhcp-server`.

Para asociar el dominio con la dirección IP se utiliza el servicio ***dnsmasq***. Se debe incluir en el **nodo maestro**, en el archivo ***/etc/hosts*** la dirección IP, el nombre del servidor con el dominio y un alias o nombre corto, por ejemplo:

192.168.111.115 satreps.gipsy_lageos.unam.mx satreps
192.168.111.116 ssn.gipsy_lageos.unam.mx ssn

Se reinicia el servicio *dnsmasq*: `sudo systemctl restart dnsmasq`

Estos cambios se ven reflejados en el nodo de procesamiento:
`cat /etc/resolv.conf`

4.2.2 CONFIGURACIÓN DE USUARIOS

Como ya se mencionó, para exportar los usuarios y servicios del nodo maestro al nodo de procesamiento se utiliza el servicio NIS.

El archivo de configuración es ***/etc/yp.conf***. El archivo para usuarios y passwd es: ***/etc/nsswitch.conf*****.** Los detalles de configuración del NIS en el nodo de procesamiento están en el anexo 1.

Confirmar en el archivo ***/etc/defaultdomain*** que se tenga el dominio de la red. Reiniciar el servicio `sudo systemctl restart nis`

Para poder aplicar todos los cambios, hay que **reiniciar o actualizar el servicio NIS** en el **nodo maestro:** `/usr/lib/yp/ypinit –m`

Se debe de crear el nuevo usuario en el nodo maestro (ver sección anterior). Para importar a los usuarios del nodo maestro hacia este nodo usamos `ypcat passwd` y podemos verificar que ya están los nuevos usuarios.

Un paso importante para poder seguir con el siguiente punto, es permitir que los servidores se comuniquen sin necesidad de escribir contraseñas. Para este punto se utiliza el comando `ssh-keygen`.

4.2.3 MONTAR LOS DISCOS EN EL NODO DE PROCESAMIENTO

Como ya se mencionó, las particiones que se crean en el nodo de procesamiento son básicas, ya que se asume que el nodo maestro será el que tenga la información.

Por este motivo, se deben de montar los discos que anteriormente se compartieron (exportaron) en el nodo maestro.

Para montar la partición home del nodo maestro se debe añadir en el archivo */etc/fstab* la línea de monta definitiva:

[dirección IP nodo maestro]:/home /home nfs defaults,_netdev 0 0

Una vez que las lineas de monta automática son añadidas en el archivo */etc/fstab*, se usa el comando `mount /home`.