UDELAR
Regional Este

TALLER DE ADMINISTRACION

DE REDES Y SERVICIOS

APENDICE A

GUÍAS DE ADMINISTRACIÓN Y USUARIOS

Autores:
Juan Güida – Víctor Alem - Pablo García
Aline García - Lorena Gastellú - Celia Dos Santos

Tutores:
Victor Gonzalez - Daniel Viñar

2011

Apéndice A - Instalaciones de software

Índice

1 Instalación básica de Ubuntu Server:

1.1 Procedimiento

1.1.1 Información previa

Esta información debe estar disponible antes de comenzar la instalación.

- Versión de software a instalar: Ubuntu 10.04 LTS "lucid lynx"
- Características de la máquina: marca, modelo, procesador, memoria, disco.
- Nombre de máquina: nombre y dominio.
- Red: <número IP, máscara, gateway, DNSs> o DHCP.
- Particionado: la tabla de particiones como debe quedar.
- Usuarios: nombres de usuarios y su calidad (administrador, usuario no privilegiado), números UID y GID si corresponde.
- Configurar previamente el BIOS de la máquina para que arranque desde el dispositivo en el cual está el instalador de Ubuntu 10.04 LTS "lucid lynx".
- Instalación

1.1.1 En una Instalación gráfica.

1. Elegir lenguaje.
2. Ofrece opciones:
   - Instalar Ubuntu Server.
   - Instalar Ubuntu Enterprise Cloud.
   - Comprobar defectos en el disco.
   - Analizar la memoria.
   - Arrancar desde el primer disco duro.
   - Recuperar un sistema dañado.
3. Elegir región o país.
4. Teclado, ofrece dos opciones:
   - Seleccionar su modelo de teclado de una lista (seleccionar la opción "no" utilizando flechas de dirección y pulsar <enter>).
   - Deducir la disposición del teclado (en esta opción seleccionar la opción "si" utilizando las flechas de dirección y pulsar <enter>, el programa le hará preguntas para configurar su teclado).
5. Configurar la red:
   - Al configurar la red lo primero que el asistente hace es comprobar si tiene acceso a un servidor DHCP. Si detecta algún servidor DHCP en la red se configura automáticamente. A continuación solicita se ingrese el nombre del servidor.
   - Si la configuración automática falla pulsar <enter> en continuar. Se despliegan las siguientes opciones:
     1. Reintentar la configuración automática de la red.
     2. Reintentar la configuración automática de la red indicando un servidor (solicita nombre del servidor DHCP).

3. Configurar la red manualmente (solicita dirección IP, máscara de red, pasarela, direcciones de DNS, nombre de máquina, nombre de dominio)

6. Configurar el reloj: Muestra la zona horaria en base al país o región seleccionado anteriormente. Si es correcta seleccionar "si", de otro modo seleccionar "no" y elegir la zona apropiada de la lista desplegada.
7. Particionado de disco: El asistente de instalación proporciona las siguientes alternativas:
   - Guiado - cambia el tamaño de SCSI1 (0,0,0), partición #1 (sda).
   - Guiado - Utilizar todo el disco.
   - Guiado - Utilizar el espacio libre contiguo más grande.
   - Guiado - Utilizar el disco completo y configurar LVM.
   - Guiado - Utilizar todo el disco y configurar LVM cifrado.
   - Manual (recomendado).
     1. Se despliega lista con discos, particiones y puntos de montaje existentes.
     2. Seleccionar una partición para modificar sus valores, el espacio libre para añadir una partición nueva o un dispositivo para inicializar la tabla de particiones.
     3. Si se trata de un disco duro nuevo, sin tabla de particiones anterior, crear la tabla de particiones seleccionando "si" y pulsar <enter>. El asistente retorna al resumen de particiones.
     4. Seleccionar "espacio libre", se despliegan las siguientes opciones:
        - Crear una partición nueva
        - Particionar de forma automática el espacio libre.
        - Mostrar información de cilindros /Cabezas/Sectores.
     5. Seleccionar "Crear una partición nueva partición y pulsar <enter>.
     6. Ingresar tamaño de la partición.
     7. Seleccionar tipo de la nueva partición (Primaria o Lógica).
     8. Ubicación de la nueva partición (Principio o Final).
     9. En la siguiente pantalla definir: *(Seleccionar con las flechas direccionales el item a establecer y pulsar <enter> para desplegar las opciones)*
        - Utilizar como.... (ext3 recomendado).
        - Punto de montaje.
        - Etiqueta.
        - Bloques reservados.
        - Uso habitual.
        - Marca de arranque.
     10. Luego de configurar la nueva partición seleccionar "Se ha terminado de definir la partición y pulsar enter".
     11. El asistente retorna al resumen de particiones, cosa que ocurrirá cada vez que se cree una nueva partición. Si se desea crear más particiones repetir el procedimiento desde (1) de lo contrario seleccionar "Finalizar particionado y escribir los cambios en el disco" y pulsar <enter>.
     12. Confirmar que se van a escribir los datos en el disco antes de continuar, seleccionar "si" y pulsar <enter>.

8. Configurar usuarios y contraseñas:
    - Ingresar nombre completo para el nuevo usuario, nombre de usuario para la cuenta (será un usuario privilegiado, administrador del sistema) , contraseña.
    - **Recomendación para la contraseña:** Esta debe ser de al menos 8 caracteres, contener letras minúsculas y mayúsculas (menos al principio), algún signo y algún número.
    - Si se quiere cifrar la carpeta personal seleccionar "si" de lo contrario seleccionar "no" y pulsar <enter>.
9. Configurar el gestor de paquetes: Si tiene que usar proxy HTTP para acceder a la red introduzca la información sobre el proxy. En caso contrario dejar en blanco.
10. Seleccionar e instalar programas: Elección de cómo administrar las actualizaciones del sistema, opciones:
    - Sin actualizaciones automáticas. (Las actualizaciones se deberán hacer manualmente con los comandos apt-get update y apt-get upgrade).
    - Instalar actualizaciones de seguridad automáticamente.(Las actualizaciones se realizan automáticamente).
    - Administrar el sistema con Landscape.
11. Selección de programas: Seleccionar los programas que desea instalar de la lista que se despliega.
12. Configuración de Grub-pc: Seleccionar "si" si desea instalar el cargador de arranque Grub en el registro principal de arranque (por lo general no se suele instalar Ubuntu Server junto con otros sistemas operativos, no tendría mucho sentido) de lo contrario seleccionar "no".
13. Terminar la instalación: Extraer el dispositivo de instalación para que el sistema arranque del disco en lugar de reiniciar la instalación. Luego pulsar <enter> en "continuar".

1.2 Servidor SSH

El cliente ssh ya viene instalado por defecto en Ubuntu, no así el servidor ssh.

1.2.1 Instalación:

1. Por línea de comandos:

- Para instalarlo hay que ejecutar:
    - `$ sudo apt-get install openssh-server`

Nota: Es posible que el paquete no se encuentre en los repositorios, para agregarlo hay que actualizar la lista abriendo un terminal y ejecutando el comando:

- `$ sudo apt-get update`

2. **Modo gráfico**

- Ir a: Sistema-> Administración-> Gestor de paquetes synaptic 2. Ingresar en el buscador: openssh-server
- Seleccionar el paquete openssh-server y hacer click en "aplicar"

Nota: Es posible que el paquete no se encuentre en los repositorios, para agregarlo hay que actualizar la lista abriendo un terminal y ejecutando el comando:

- `$ sudo apt-get update`

Después de instalado, para poder configurarlo hay que editar el archivo /etc/ssh/sshd_config Muy recomendado hacerle una copia de respaldo de este archivo antes de modificarlo:

- `$ sudo cp /etc/ssh/sshd_config{,.original}`

El demonio ssh atiende por defecto en el puerto 22, para cambiarlo hay que ir a la linea donde dice:

- `Port 22`

y cambiar el 22 por el puerto que queramos usar.

Para no permitir que se puedan hacer login con el usuario root por ssh hay que cambiar:

- `PermitRootLogin yes`

por:

- `PermitRootLogin no`

Para elegir que usuarios podrán acceder por ssh, hay que agregar la siguiente linea:

- `AllowUsers <usuario1> <usuario2> <usuario3>`

Para que los cambios surtan efecto hay que reiniciar el servidor:

- `$ sudo /etc/init.d/ssh restart`

Para solo recargar el cambio de configuración sin reiniciar el servicio:

- `$ sudo /etc/init.d/ssh reload`

1.2.2 SSH con clave pública-privada

Para generar nuestra clave:

- `$ ssh-keygen -t rsa`

Una vez generada, hay que copiarla al usuario del ordenador remoto con el que queremos mantener la relación de confianza usando el comando ssh-copy-id. Este es un ejemplo del uso con la salida del programa:

- `$ ssh-copy-id usuario_remoto@192.168.0.1`

```
Now try logging into the machine, with "ssh 'usuario_remoto@192.168.0.1'", and
check in: .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

Nota: En caso que nos de este error cuando queramos entrar por ssh: `Agent admitted failure to sign using the key.`

Debemos ejecutar el comando:

- `$ ssh-add`

Nos pedirá el passphrase: `Enter passphrase for /home/usuario/.ssh/id_rsa: Identity added: /home/usuario/.ssh/id_rsa (/home/usuario/.ssh/id_rsa)`

1.2.3 Protejer nuestro servidor SSH

Con denyhosts podremos prevenir el ataque a el servicio o demonio SSH por métodos como fuerza bruta o diccionario. Este después de sucesivos intentos erroneos de logeo por SSH bloquea el acceso a la ip fuente.

Para instalarlo:

- `$ apt-get install denyhosts`

Luego para configurarlo editamos el archivo:

`/etc/denyhosts.conf`

Tiene muchas opciones para configurar, pero las que nos interesan son:

- Purgar las ip bloqueadas después de una hora: PURGE_DENY = 1h
- Ploqueo a intentos de login para usuarios inválidos: DENY_THRESHOLD_INVALID = 3
- Bloqueo a intentos de login para usuarios válidos: DENY_THRESHOLD_VALID = 5
- Bloqueo a intentos de login con el usuario root: DENY_THRESHOLD_ROOT = 1
- Bloqueo a intentos de login con usuarios restringidos: DENY_THRESHOLD_RESTRICTED = 1
- Vuelve a 0 (cero) el contador de intentos fallidos desde una ip cuando el login es válido: RESET_ON_SUCCESS = yes

Luego de terminar de editar el archivo, hay que reinicar el servicio:

- `/etc/init.d/denyhosts restart`

2 Instalación básica de Ubuntu Desktop:

2.1 Procedimiento

2.1.1 Información previa

Esta información debe estar disponible antes de comenzar la instalación:

- Versión de software a instalar: Ubuntu 10.04 i386
- Características de la máquina: marca, modelo, procesador, memoria, disco.
- Nombre de máquina: nombre y dominio.
- Red: <número IP, máscara, gateway, DNSs> o DHCP.
- Particionado: la tabla de particiones como debe quedar.
- Usuarios: nombres de usuarios y su calidad (administrador, usuario no privilegiado), números UID y GID si corresponde.
- Configurar previamente el BIOS de la máquina para que arranque desde el dispositivo en el cual está el instalador de Ubuntu 10.04 i386.

2.1.2 Instalación

Es una Instalación gráfica.

1. Inicio:
   - Ofrece opciones: Probar Ubuntu, Instalar Ubuntu; elegir Instalar.
   - Elegir idioma.

Nota: varía el orden según se instale desde un pendrive o un CD.

2. Zona horaria: Elegir zona horaria correspondiente y continuar.
3. Teclado, ofrece tres opciones:
   - "Opción sugerida" (esto lo toma el programa según la zona horaria elegida anteriormente).
   - "Deducir el mapa del teclado" (en esta opción hacer click en "deducir" y el programa le hará preguntas para configurar su teclado).
   - "Seleccione la suya" (aparece una lista de países y otra de teclados para seleccionarlos manualmente).
   - Aparece un campo de texto para probar la distribución elegida.

Nota: En los siguientes 5 puntos (4, 5, 6, 7 y 8), queda a criterio de cada instalador y cada situación en particular, estos puntos están basados en una instalación con un disco vacío y todo el sistema en una única partición.

4. Preparar espacio en disco, ofrece dos opciones:
   - Borrar y usar el disco entero (en general, No recomendado).
   - Especificar particiones manualmente: opción para generar la tabla de particiones pedida (Avanzado y Recomendado).
5. Preparar particiones: Suele ver el disco como /dev/sda, seleccionarlo, y clickear "Nueva tabla de particiones..." Hacer click en "continuar".
6. Aparecerá un "Espacio libre", seleccionarlo y pulsar en "Añadir".

7. Crear Partición: Aparecerá una ventana en la que hay que establecer los siguientes valores:
    - Tipo de la nueva partición (Primaria o Lógica).
    - Tamaño en MB (elegido por el usuario).
    - Ubicación de la nueva partición (Principio o Fin).
    - Utilizar como... (ext3 recomendado).
    - Punto de montaje (/ en la primera partición, las otras son opcionales).
8. Repetir el paso 6 y luego:
    - Tipo de la nueva partición (Primaria o Lógica).
    - Tamaño en MB (mínimo 3GB).
    - Ubicación de la nueva partición (Principio o Final).
    - Utilizar como... (área de intercambio o "swap").

Click en Adelante.

9. Completar datos personales: nombre usuario, contraseña; será un usuario privilegiado, administrador del sistema; nombre de máquina. Recomendación para la contraseña: Esta debe ser de al menos 8 caracteres, contener letras minúsculas y mayúsculas (menos al principio), algún signo y algún número. Elegir una de las siguientes opciones:
    - Iniciar sesión automáticamente.
    - Solicitar mi contraseña para iniciar sesión (recomendada).
    - Solicitar mi contraseña para iniciar sesión y descifrar mi carpeta personal.
10. Migrar documentos y configuraciones: si es una reinstalación y se conservan datos de usuarios. Siguiente.
11. Verificar los datos. Avanzadas: permite fijar el proxy HTTP de la red. Instalar: comienza la instalación.

Nota: en una oportunidad al reiniciar dio I/O error; quitar CD, Enter finaliza el reinicio, inicia normalmente.

2.1.3 Configuración de red

2.1.3.1. Crear una conexión de red (modo gráfico)

Con Network Manager. Puede invocarse:

- Sobre ícono de red en la barra de tareas, click derecho, Editar las conexiones.
- Menú Sistema, Preferencias, Conexiones de Red.
- En terminal de comandos, ejecutando `nm-connection-editor`.

Permite crear conexiones cableada, inalámbrica, de banda ancha móvil, VPN y DSL.

1. Crear una conexión cableada:
    - Botón Añadir.
    - Dar un nombre adecuado a esta conexión.
    - Si se quiere conectar automáticamente seleccionar "conectar automáticamente": la conexión arranca con la máquina, sin invocación.
    - Ingresar ajustes de Ipv4.
    - Elegir uno de los métodos:

1. Automático (ID del cliente DHCP).
2. Sólo direcciones automáticas (servidor DNS, Dominios de búsqueda, ID del cliente DHCP).
3. Manual (se deberá establecer dirección, máscara de red, puerta de enlace, servidor DNS y Dominios de búsqueda).
4. Sólo enlace local.
5. Compartida con otros equipos.

- Si se quiere que otros utilicen la conexión, marcar "Disponible para todos los usuarios" (requiere privilegios de supervisor).
- Aplicar.

Nota: Para activar o desactivar la conexión: sobre icono de red en la barra de tareas, clic izquierdo, debe mostrar la nueva conexión.

2.1.4 Administración de paquetes

Ajustar repositorios de paquetes Ubuntu.

Los repositorios de paquetes pueden tener diferente respuesta. En general conviene usar repositorios próximos. A la fecha, en Uruguay no hay repositorio Ubuntu, es preciso usar uno de Brasil o Argentina. La carga del servidor y la conectividad son factores decisivos para la elección de un repositorio de paquetes. La Universidad de la República participa de la red CLARA, que da muy buena conectividad hacia otros sitios de la red CLARA, generalmente Universidades.

En el gestor de paquetes Synaptic:

1. Invocar Synaptic: menú Sistema, Administración, Gestor de paquetes Synaptic,
2. Configuración, Repositorios,
   - Descargable de Internet: marcar todo menos Código fuente.
   - Descargar desde: Otro, de Brasil o Argentina.
   - La opción buscar el mejor servidor puede no producir nada, o nada eficiente.

Para todo el sistema, con el archivo `/etc/apt/sources.list`:

1. Preservar el archivo original copiándolo con otro nombre, por ejemplo sources.list.orig.
2. Editar el archivo /etc/apt/sources.list cambiando o incorporando los nuevos respositorios.

Agregar usuarios al sistema:

1. Ir a: Sistemas-> Administración-> Usuarios y grupos.
2. Clickear en "Añadir", ingresar nombre real de usuario y nombre para ingreso del mismo. Aceptar.
3. Establecer contraseña a mano: ingresarla manualmente y repetirla para confirmación. Aceptar.
4. Para agregar más información y modificar privilegios del usuario ir a "Ajustes avanzados".
5. En "tipo de cuenta" seleccionar si el usuario es de Escritorio, Administrador o Personalizado.

3 Instalaciones de servidores DNS

El DNS es un servicio repartido que tiene dos objetivos principales:

- Traducir una dirección canónica en una dirección IP, por ejemplo paloma.taller.curerocha.edu.uy a su IP: 164.73.234.104
- Traducir una dirección IP en una o varias direcciones canónicas, lo que se conoce como traducción inversa.

El "DNS Master" de una zona (por ejemplo taller.curerocha.edu.uy) es el servidor donde se almacena y actualiza la información de los dominios bajo esta zona, y que provee esta información a otros servidores en la red.

Además de un DNS Master es necesario crear un servidor secundario (esclavo), que proporcionará robustez y fiabilidad. Un servidor esclavo es simplemente un servidor de nombres que replica los ficheros de las zonas de un maestro.

Para que un servidor sea DNS Master de una zona, es necesario que el DNS master de la zona de nivel superior le delegue la gestión de dominios (por ejemplo, curerocha.edu.uy es la zona superior de taller.curerocha.edu.uy)

3.1 Master en paloma:

3.1.1 Objetivos:

Creamos un DNS master para las zonas que nos han sido delegadas:

- taller.csic.edu.uy (que nos fue delegada desde CSIC)
- taller.curerocha.edu.uy, que nos fue delegada pos SeCIU, que maneja curerocha.edu.uy

3.1.2 Instalación

Necesitamos BIND y algunos utilitarios:

- `# sudo apt-get install bind9 bind9-doc dnsutils`

3.1.3 Configuración

Los archivos de configuracion del Bind están en `/etc/bind/`

- `$ sudo vi /etc/bind/named.conf.options`

```
// Archivo de configuracion del DNS master de
// taller.curerocha.edu.uy y taller.csic.edu.uy
// acl redesNegadas: define las redes a denegar consultas al servidor DNS
acl redesNegadas {
       0.0.0.0/8; 1.0.0.0/8;
       172.16.0.0/12;
       10.0.0.0/8;
       192.168.0.0/16;
       169.254.0.0/16;
};
options {
       //desactivamos la cache
```

```
        acache-enable no;
        directory "/var/cache/bind";

        //No es necesario forwardear
        //forwarders {
         //    164.73.128.5;
        //     164.73.128.70;
        // };

        //No permitimos las consultas salvo las de nuestro servidor
        allow-query { 127.0.0.1; };
        # allow-query { none; };

        //No permitimos las recusion
        # allow-recursion { none; };
        allow-recursion { 127.0.0.1; };

        //Incluimos las redes de la acl redesNegadas a la lista negra
        blackhole { redesNegadas; };

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

};
```

- `$ sudo vi/etc/bind/named.conf.local`

Editamos este archivo para definir las zonas directas e inversas de nuestro dominio, y los archivos donde estarán las configuraciones de las mismas.

```
//
// Do any local configuration here
//
//Definimos nuestra zona de dominio taller.csic.edu.uy
//Nuestro dns solo va a contestar por esta zona
zone "taller.csic.edu.uy"{
```

```
        type master;
        file "/etc/bind/db.taller.csic.edu.uy";
        allow-query { any;};
        // permitimos transferencia desde nuestro servidor "DNS slave"
        allow-transfer {
                164.73.68.10;
        };
};

zone "taller.curerocha.edu.uy"{
        type master;
        file "/etc/bind/db.taller.curerocha.edu.uy";
        allow-query { any;};
        // permitimos transferencia desde nuestro servidor "DNS slave"
        allow-transfer {
                164.73.68.10;
        };
};

zone "234.73.164.in-addr.arpa"{
        type master;
        file "/etc/bind/db.164.73.234";
        allow-query { any;};
        // permitimos transferencia desde nuestro servidor "DNS slave"
        allow-transfer {
                164.73.68.10;
        };
};

//include "/etc/bind/zones.rfc1918";
```

3.1.4 Los archivos de zonas

Tipos de registros del DNS:

	Tipo	Nombre	Función
Zona	SOA	Start Of Authority	Define una zona representativa del DNS
	NS	Name Server	Identifica los servidores de zona, delega subdominios
Básicos	A	Dirección IPv4	Traducción de nombre a dirección
	AAAA	Dirección IPv6 original	Actualmente obsoleto
	PTR	Puntero	Traducción de dirección a nombre

$TTL: Indica el tiempo de vida (Time To Live) de la información contenida en el fichero. Es decir, el tiempo máximo de validez, tras el cual deberá refrescarse o actualizarse.

@ IN SOA, el registro SOA (Start Of Authority) es siempre el primer recurso en un fichero de zona. El símbolo "@" equivale a la directiva $ORIGIN Este sería el esqueleto de este registro:

```
@ IN SOA <primary-name-server> <hostmaster-email> (
  <serial-number>   ; Se incrementa cuando se modifica el fichero de la zona
  <time-to-refresh> ; Tiempo para los servidores secundarios (esclavos) actualicen los registros
  <time-to-retry>   ; Tiempo para el servidor esclavo antes de solicitar una actualización, si el Master no responde
  <time-to-expire>  ; Si el master no responde antes de que expire este tiempo, el servidor esclavo deja de actuar como servidor de zona
<minimum-TTL> )   ; Time to live negativo
```

- $ sudo vi/etc/bind/db.taller.csic.edu.uy

```
;
; Archivo BIND de definición de zona taller.csic.edu.uy
;
$TTL      86400; 1D
@         IN        SOA       paloma.taller.csic.edu.uy. root.paloma.taller.csic.edu.uy. (
                                2011060903                  ; Serial
                                6H                ; Refresh
                                1D                ; Retry
                                1W                ; Expire
                                10M )    ; Negative Cache TTL
;                               1D )     ; Negative Cache TTL
;
; Servidores de nombres y dirección IP de zona
;
@               IN  NS        paloma.taller.csic.edu.uy.
@               IN  NS        gould.csic.edu.uy.
@                   IN        A         164.73.234.104
;
; Nombres canónicos de servidores e interfaces
;
paloma              IN        A         164.73.234.104
garzon              IN        A         164.73.234.126
;
; Alias a nombres canónicos, para los servicios
;
base-de-datos       IN        CNAME     paloma
bdd                 IN        CNAME     paloma
mediawiki IN        CNAME     paloma
wiki                IN        CNAME     paloma
tikiwiki  IN        CNAME     paloma
$ sudo vi/etc/bind/db.taller.curerocha.edu.uy
;
; Archivo BIND de definición de la zona taller.curerocha.edu.uy
;
$ORIGIN taller.curerocha.edu.uy.
$TTL   86400; 1D
@       IN      SOA     paloma.taller.csic.edu.uy. root.paloma.taller.csic.edu.uy. (
                         2011060909; Serial
                         6H        ; Refresh
                         1D        ; Retry
```

```
                        1W        ; Expire
                        10M  )     ; Negative Cache TTL
;                        1D  )     ; Negative Cache TTL
;
; Servidores de nombres y dirección IP de zona
;
@                   IN NS      paloma.taller.csic.edu.uy.
@                   IN NS      gould.csic.edu.uy.
@                   IN A       164.73.234.104
;
; Nombres canónicos de servidores e interfaces
;
paloma              IN A       164.73.234.104
garzon              IN A       164.73.234.126
;
; Alias a nombres canónicos, para los servicios
;
base-de-datos       IN CNAME paloma
bdd                 IN CNAME paloma
tikiwiki  IN CNAME paloma
wiki                IN CNAME paloma
mediawiki IN CNAME paloma
$ sudo vi/etc/bind/db.164.73.234
;
; Archivo BIND de definición de zona inversa a taller.csic.edu.uy
;
$TTL      86400; 1D
@         IN        SOA       taller.csic.edu.uy. root.taller.csic.edu.uy. (
                               2011060901         ; Serial
                               6H                 ; Refresh
                               1D                 ; Retry
                               1W                 ; Expire
                               1D )               ; Negative Cache TTL
;
@         IN        NS        taller.csic.edu.uy.
@         IN        PTR       taller.csic.edu.uy.
104       IN        PTR       paloma.taller.csic.edu.uy.
126       IN        PTR       garzon.taller.csic.edu.uy.
```

Editamos el archivo `/etc/reslov.conf:`

En este archivo se indica el dominio al que pertenece el ordenador (palabra clave search) y la dirección del servidor de nombres (palabra clave nameserver) al que se debe dirigir. Cuando se intente resolver un nombre que no esté totalmente cualificado se intentará generar un nombre válido añadiendo la entrada de search.

- `$ sudo vi /etc/resolv.conf`

```
search taller.csic.edu.uy
domain taller.csic.edu.uy
nameserver 164.73.128.5
nameserver 164.73.128.70
```

3.2 DNS Resolvedor en Polonio

3.2.1 Objetivos:

1. Crear un DNS master para las zona lan.curerocha.edu.uy (la cual no fue delegada, ya que es solo para consultas internas).
2. Resolver las consultas de las redes internas (10.5.1.0/24, 10.5.2.0/24, 10.5.3.0/24, 10.5.4.0/24 y 10.5.5.0/24).

3.2.2 Instalación:

Necesitamos BIND y algunos utilitarios:

- `# sudo apt-get install bind9 bind9-doc dnsutils`

3.2.3 Configuración:

Los archivos de configuración del Bind están en /etc/bind/

- `$ sudo vi /etc/bind/named.conf.options`

```
// Archivo de configuración del DNS Resolvedor y master de
// lan.curerocha.edu.uy

options {
       //Habilitamos el cache
       acache-enable yes;
       directory "/var/cache/bind";
       // Forwardeamos a los servidores de SeCIU
        forwarders {
              164.73.128.5;
              164.73.128.70;
        };

       allow-query {any;};
       auth-nxdomain no;    # conform to RFC1035
       listen-on-v6 { any; };

};
```

- `$ sudo vi/etc/bind/named.conf.local`

Editamos este archivo para definir las zonas directas e inversas de nuestro dominio,
y los archivos donde estarán las configuraciones de las mismas.

```
//Definimos nuestra zona de dominio lan.curerocha.edu.uy
//Nuestro dns solo va a contestar por estas zonas a la red local

zone "lan.curerocha.edu.uy"{
       type master;
       file "/etc/bind/db.lan.curerocha.edu.uy";
       allow-query { any;};
};


zone "1.5.10.in-addr.arpa"{
       type master;
       file "/etc/bind/db.10.5.1";
       allow-query { any;};
};

zone "2.5.10.in-addr.arpa"{
       type master;
       file "/etc/bind/db.10.5.2";
       allow-query { any;};
};

zone "4.5.10.in-addr.arpa"{
       type master;
       file "/etc/bind/db.10.5.4";
       allow-query { any;};
};

zone "5.5.10.in-addr.arpa"{
       type master;
       file "/etc/bind/db.10.5.5";
       allow-query { any;};
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

3.2.4 Los archivos de Zonas:

Tipos de registros del DNS:

	Tipo	Nombre	Función
Zona	SOA	Start Of Authority	Define una zona representativa del DNS
	NS	Name Server	Identifica los servidores de zona, delega subdominios
Básicos	A	Dirección IPv4	Traducción de nombre a dirección
	AAAA	Dirección IPv6 original	Actualmente obsoleto
	PTR	Puntero	Traducción de dirección a nombre

$TTL: Indica el tiempo de vida (Time To Live) de la información contenida en el fichero. Es decir, el tiempo máximo de validez, tras el cual deberá refrescarse o actualizarse.

@ IN SOA, el registro SOA (Start Of Authority) es siempre el primer recurso en un fichero de zona. El símbolo "@" equivale a la directiva $ORIGIN Este sería el esqueleto de este registro:

```
@ IN SOA <primary-name-server> <hostmaster-email> (
  <serial-number>    ; Se incrementa cuando se modifica el fichero de la zona
  <time-to-refresh>  ; Tiempo para los servidores secundarios (esclavos) actualicen los registros
  <time-to-retry>    ; Tiempo para el servidor esclavo antes de solicitar una actualización, si el Master no responde
  <time-to-expire>   ; Si el master no responde antes de que expire este tiempo, el servidor esclavo deja de actuar como servidor de zona
  <minimum-TTL> )    ; Time to live negativo
```

- $ sudo vi/etc/bind/db.lan.curerocha.edu.uy

```
;
; Archivo BIND de definición de zona lan.curerocha.edu.uy
;
$TTL   360 ; 10M caché positivo
@      IN     SOA    polonio.lan.curerocha.edu.uy. root.polonio.lan.curerocha.edu.uy. (
                      2011060903     ; Serial yyyy/mm/dd/id
                      6H           ; Refresh
                      1D           ; Retry
                      1W           ; Expire
                      10M ) ; Negative Cache TTL
;
@        IN    NS     polonio.lan.curerocha.edu.uy.
@      IN       A     10.5.2.2
polonio       IN       A    10.5.2.2
Equipo01      IN       A      10.5.1.101
Equipo02      IN       A      10.5.1.102
Equipo03      IN       A      10.5.1.103
Equipo04      IN       A      10.5.1.104
Equipo05      IN       A      10.5.1.105
Equipo06      IN       A      10.5.1.106
Equipo07      IN       A      10.5.1.107
Equipo08      IN       A      10.5.1.108
```

```
Equipo09      IN      A      10.5.1.109
Equipo10      IN      A      10.5.1.110
Equipo11      IN      A      10.5.1.111
Equipo12      IN      A      10.5.1.112
Equipo13      IN      A      10.5.1.113
Secretaria01  IN     A      10.5.4.101
Delegados01   IN     A      10.5.5.102
Docentes01    IN     A      10.5.5.103
```

- $ sudo vi/etc/bind/db.10.5.1

```
;
; Archivo BIND de definición de zona inversa 1.5.10.in-addr.arpa
;
$TTL   86400 ; 1D
@      IN     SOA    polonio.lan.curerocha.edu.uy. root.polonio.lan.curerocha.edu.uy. (
                       2011060901  ; Serial yyyy/mm/dd/id
                       6H          ; Refresh
                       1D          ; Retry
                       1W          ; Expire
                       1D )        ; Negative Cache TTL
;
@      IN     NS     polonio.lan.curerocha.edu.uy.
@      IN     PTR    polonio.lan.curerocha.edu.uy.
101    IN     PTR    Equipo01.lan.curerocha.edu.uy.
102    IN     PTR    Equipo02.lan.curerocha.edu.uy.
103    IN     PTR    Equipo03.lan.curerocha.edu.uy.
104    IN     PTR    Equipo04.lan.curerocha.edu.uy.
105    IN     PTR    Equipo05.lan.curerocha.edu.uy.
106    IN     PTR    Equipo06.lan.curerocha.edu.uy.
107    IN     PTR    Equipo07.lan.curerocha.edu.uy.
108    IN     PTR    Equipo08.lan.curerocha.edu.uy.
109    IN     PTR    Equipo09.lan.curerocha.edu.uy.
110    IN     PTR    Equipo10.lan.curerocha.edu.uy.
111    IN     PTR    Equipo11.lan.curerocha.edu.uy.
112    IN     PTR    Equipo12.lan.curerocha.edu.uy.
113    IN     PTR    Equipo13.lan.curerocha.edu.uy.
```

- $ sudo vi/etc/bind/db.10.5.2

```
;
; Archivo BIND de definición de zona inversa 2.5.10.in-addr.arpa
;
$TTL   86400 ; 1D
```

```
@      IN     SOA    polonio.lan.curerocha.edu.uy. root.polonio.lan.curerocha.edu.uy. (
                       2011060901  ; Serial yyyy/mm/dd/id
                       6H          ; Refresh
                       1D          ; Retry
                       1W          ; Expire
                       1D )        ; Negative Cache TTL
;
@      IN     NS     polonio.lan.curerocha.edu.uy.
@      IN     PTR    polonio.lan.curerocha.edu.uy.
2      IN     PTR    polonio.
```

- $ sudo vi/etc/bind/db.10.5.4

```
;
; Archivo BIND de definición de zona inversa 4.5.10.in-addr.arpa
;
$TTL   86400 ; 1D
@      IN     SOA    polonio.lan.curerocha.edu.uy. root.polonio.lan.curerocha.edu.uy. (
                       2011060901  ; Serial yyyy/mm/dd/id
                       6H          ; Refresh
                       1D          ; Retry
                       1W          ; Expire
                       1D )        ; Negative Cache TTL
;
@      IN     NS     polonio.lan.curerocha.edu.uy.
@      IN     PTR    polonio.lan.curerocha.edu.uy.
101    IN     PTR    Secretaria01.lan.curerocha.edu.uy.
```

- $ sudo vi/etc/bind/db.10.5.5

```
;
; Archivo BIND de definición de zona inversa 5.5.10.in-addr.arpa
;
$TTL   86400 ; 1D
@      IN     SOA    polonio.lan.curerocha.edu.uy. root.polonio.lan.curerocha.edu.uy. (
                       2011060901  ; Serial yyyy/mm/dd/id
                       6H          ; Refresh
                       1D          ; Retry
                       1W          ; Expire
                       1D )        ; Negative Cache TTL
;
@      IN     NS     polonio.lan.curerocha.edu.uy.
@      IN     PTR    polonio.lan.curerocha.edu.uy.
```

```
102    IN     PTR    Delegados01.lan.curerocha.edu.uy.
103    IN     PTR    Docentes01.lan.curerocha.edu.uy.
```

Editamos el archivo /etc/reslov.conf

En este archivo se indica el dominio al que pertenece el ordenador (palabra clave search) y la dirección del servidor de nombres (palabra clave nameserver) al que se debe dirigir.

Cuando se intente resolver un nombre que no esté totalmente cualificado se intentará generar un nombre válido añadiendo la entrada de search.

- `$ sudo vi /etc/resolv.conf`

```
search lan.curerocha.edu.uy
domain lan.curerocha.edu.uy
nameserver 127.0.0.1
```

4 Zentyal

4.1 Instalación del Servidor

Zentyal se puede instalar de 2 maneras:

- Imagen pre-instalada (incluye el SO)
- Desde repositorios

En esta documentación solo hablaremos sobre la instalación desde repositorios.

Para hacerlo hay que agregar a `/etc/etc/apt/sources.list` el repositorio:

`deb http://ppa.launchpad.net/zentyal/2.0-contrib/ubuntu lucid main`

Instalamos la firma:

- `$ apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 10E239FF`

Luego de esto actualizamos la base de datos de paquetes:

- `$ apt-get update`

Ahora si podemos instalar Zentyal:

- `$ apt-get install zentyal`

El puerto de escucha lo dejamos por defecto.

Luego de instalado, ingresamos a través de nuestro navegador web a la siguiente dirección:

https://<ip servidor Zentyal>

Ingresamos con nuestro usuario y contraseña del sistema.

La primera vez nos entra en un wizard para agregar las utilidades deseadas, de esta manera él instala un paquete para brindar ciertos servicios. Arriba nos da la opción de "View advanced mode", entramos ahí y nos muestra la lista completa de paquetes a instalar.

Para nuestro servidor de archivos y usuarios necesitamos solo lo siguiente:

- File Sharing
- Printer Shaping
- Users and Groups

Le damos Install, nos muestra la lista de paquetes a instalar (ya agrega solo las dependencias) y luego seleccionamos OK. Esperamos que descargue e instale.

Cuando termina nos pregunta sobre las interfaces de red, cuales son internas y cuales son externas, en nuestro caso solo tenemos interna. Nos va a pedir que le configuremos su interfaz de der, así que la ponemos en static y le agregamos los datos correspondientes.

Ejemplo polonio:

Method: Static

IP address: 10.5.1.254

Netmask: 255.255.255.0

Gateway: 10.5.1.1

Domain Name Server 1: 10.5.1.1

Seleccionamos el servidor en estado: Standalone Server

Y salvamos los cambios.

Aclaración: Cuando se instalan estos servicios, también se instala un servicio de red. Este servicio de red maneja la configuración de la tarjeta de red modificando el archivo /etc/network/interfaces, si editamos este archivo cuando reiniciemos el equipo Zentyal volverá a cambiar la configuración de red por la que tenga guardada. Además los servicios que estén escuchando, manejados por Zentyal, siguen con la configuración de Zentyal y no con la configuración del archivo /etc/network/interfaces.

4.2 Instalación Cliente Zentyal en Ubuntu

Agregar el repositorio:

- Para 10.04:
  - deb http://ppa.launchpad.net/zentyal/desktop/ubuntu lucid main
- Para 10.10:
  - deb http://ppa.launchpad.net/zentyal/desktop/ubuntu maverick main

En:

`/etc/apt/source.list.d/`

En un archivo llamado por ejemplo: zentyal.sources.list

Instalamos la firma:

- `$ apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 10E239FF`

Actualizar e instalamos mediante:

- `$ apt-get update && apt-get install zentyal-desktop`

Durante la instalación, nos va a preguntar sobre LDAP, ignoramos lo que nos pregunte y solo le ponemos la ip del servidor Zentyal: 10.5.2.2

y que no hay un servidor esclavo.

Reiniciamos la máquina para que los cambios surgan efecto.

4.3 Ingresar Usuarios y Grupos en Zentyal

4.3.1 Grupos

Creamos los usuarios en: *Office-> Usuarios y Grupos-> Grupos*. Nos pedirá el nombre del grupo y un comentario sobre el mismo. Si entramos a "Editar" ahí podremos agregar usuarios a dicho grupo y compartir una carpeta para todos los usuarios del mismo. Para acceder a esta carpeta se puede hacer a través de la siguiente dirección:

smb://polonio/<nombre_carpeta>

4.3.2 Usuarios

Antes de crear los usuarios, hay que especificar cual será el shell por defecto. Esto se hace desde *Office-> Usuarios y Grupos-> Opciones de configuración de LDAP -> Shell por defecto*, seleccionamos bash (Este cambio se aplicará únicamente a los usuarios creados a partir de ahora).

Creamos los usuarios en: *Office-> Usuarios y Grupos-> Usuarios* Por defecto se creará una carpeta en /home para nuestro usuario. Para acceder a la carpeta de este usuario lo hacemos a traves de la siguiente ruta:

smb://polonio/<nombre_usuario>

Para establecer parametros de seguridad de validación de los usuarios, en la sección *Office -> Compartir ficheros -> PDC* y dejamos la configuración como se muestra en la siguiente figura

4.4 Configuración

4.4.1 Cambio de idioma y habilitar servicios

En *Core-> System-> General* tenemos la opción de cambiar el lenguaje, agregar usuarios, cambiar el puerto de escucha de Zentyal y el nombre del propio servidor.

Ahora chequeamos que los servicios instalados estén habilitados, esto se hace en *Core-> Estado del módulo*.

4.4.2 Carpetas remotas

Crear los grupos a los que pertenecerán los usuarios en: *Office-> Usuarios y Grupos-> Grupos* Podemos agregar carpetas compartidas para todos los integrantes del grupo, esta carpeta se va a crear en /home/samba/groups/ Para acceder a estas carpetas de forma remota, se puede llegar a través de la siguiente ruta:

smb://polonio/<nombre_carpeta>

Para poder acceder a estos espacios compartidos, deberemos ingresar los siguientes datos:

nombre de usuario: <nombre_usuario>

grupo de trabajo: CURE-ROCHA

contraseña: <contraseña>

Las terminales deberán tener instalado samba, y este debe de tener el valor:CURE-ROCHA en workgroup (/etc/samba/smb.conf).

La configuración de las carpetas compartidas se puede ver en: /etc/samba/smb.conf

4.4.3 Carpetas compartidas

Para crear carpetas compartidas vamos: *Office-> Compartir Ficheros-> Directorios Compartidos* Ahí podremos agregar un nuevo directorio o editar uno ya hecho. Para agregar uno nuevo damos en "Añade nuevo", luego damos el nombre del nuevo recurso compartido, en "Ruta del recurso compartido", si seleccionamos "Directorio bajo Zentyal" esto creará la carpeta en /home/samba/shares/ solo hay que agregar el nombre de la carpeta. Si queremos que se tenga acceso sin autenticación marcamo la opción "Acceso de invitado". Luego de de crearla hay que darle los permisos, esto se hace desde "Control de acceso", luego en "Action" lo editamos, nos da la opción de compartirlo para un usuario en particular o para un grupo de usuarios, con permiso de solo lectura (Read only) o de lectura y escritura (Read and write).

4.5 Modo de uso

4.5.1 Autenticación local con carpeta personal en servidor Zentyal

De esta manera, la autenticación del usuario se hace de forma local y no contra el servidor Zentyal, pero se puede acceder a la carpeta personal guardada en el servidor Zentyal. Para acceder a ella se puede hacer de dos formas. Una forma sería ingresar en el navegador de archivos la dirección de la carpeta (Ctrl + L), ejemplo:

smb://polonio/<nombre_usuario>

Nos solicitará:

Usuario: <nombre_usuario>

Dominio: CURE-ROCHA

Contraseña: <nuestra_contraseña>

De esta forma ya accedemos a nuestra carpeta personal.

Podemos acceder también a carpetas compartidos para un grupo de usuarios. Esto se puede hacer de dos formas:

- A través del navegador de archivos ir a Red-> Red de Windows-> CURE-ROCHA-> POLONIO-> <nombre_carpeta_compartida>
- Ingresar en el navegador de archivos la dirección de la carpeta (Ctrl + L), ejemplo:
    - smb://polonio/<nombre_carpeta_compartida>

4.5.2 Autenticación mediante Zentyal LDAP

Requiere tener instalado Zentyal-Desktop. Hay tres formas de uso:

1. Autenticación mediante Zentyal LDAP: la base de datos de usuario está guardada únicamente en el servidor Zentyal y si se tiene una cuenta en él se podrá logear desde cualquier máquina en la red.
2. Auto-configuración en la máquina cliente por los servicios provisto desde Zentyal (mail, samba, Jabber, VoIP, ...): la primera vez que se logea en la máquina esta crea el directorio home con la pre-configuración apropiada.
3. Perfiles itinerantes (Roaming profiles): los datos en el directorio home son sincronizados desde el servidor para poder trabajar con sus archivos desde cualquier máquina de la red, mantiene una copia local te los mismos.

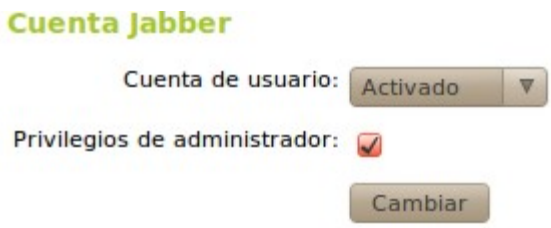
Las que se implementaron son las dos primeras.

4.6 Configuración de Jabber

Para configurar la cuenta de chat ingresamos como administrador a la página de Zentyal y vamos a: *Core -> Gestión de software -> Componentes Zentyal* y en este menú seleccionamos el componente Jabber e instalamos.

Luego de instalado, en el menú a la izquierda, aparecerá en la sección de "Communications" una entrada para Jabber donde se podrá setear los parámetros de configuración.

Para activar usuarios vamos a -> Office -> Usuarios y Grupos -> Usuarios. Aquí editamos el usuario que queremos activar, en la sección de cuentas de Jabber activamos esto y le damos privilegios de administración. Presionamos en cambiar y guardamos los cambios.



Nota: La activación de los usuarios puede demorar unos minutos.

Nota: Esto configura una cuenta jabber, debe configurarse un cliente de mensajería instantánea, ej. Empathy.

5 Instalación y configuración OpenLDAP

5.1 Instalación

Para instalar OpenLDAP serán necesarios los paquetes slapd y ldap-utils, para instalar:

- `$ aptitude install slapd ldap-utils`

Luego lanzamos los siguientes comandos

- `$ ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif`
- `$ ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif`
- `$ ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif`

Creamos el archivo con la configuración para luego acceder a ldap

- `$ mkdir ldapLaburo`
- `$ cd ldapLaburo`
- `$ vi datos_base_slapd`

Editamos el archivo datos_base_slapd, un ejemplo es el siguiente:

```
root@paloma:~/ldapLaburo# cat datos_base_slapd.ldif
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb

# Database settings
dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=ldap,dc=curerocha,dc=edu,dc=uy
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=ldap,dc=curerocha,dc=edu,dc=uy
olcRootPW: secreto
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
```

```
olcAccess: to attrs=userPassword by dn="cn=admin,dc=ldap,dc=curerocha,dc=edu,dc=uy" write
by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=ldap,dc=curerocha,dc=edu,dc=uy" write by * read
```

Le cambiamos el nombre:

- `$ mv datos_base_slapd datos_base_slapd.ldif`

Y ejecutamos el siguiente comando:

- `$ ldapadd -Y EXTERNAL -H ldapi:/// -f datos_base_slapd.ldif`

Creamos datos_frontend_slapd.ldif

- `$ vi datos_frontend_slapd.ldif`

y le agregamos la siguiente información:

```
root@paloma:~/ldapLaburo# cat datos_frontend_slapd.ldif
# Create top-level object in domain
dn: dc=ldap,dc=curerocha,dc=edu,dc=uy
objectClass: top
objectClass: dcObject
objectclass: organization
o: CURE Rocha
dc: ldap
description: Directorio LDAP del CURE

# Admin user.
dn: cn=admin,dc=ldap,dc=curerocha,dc=edu,dc=uy
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: secreto

dn: ou=gente,dc=ldap,dc=curerocha,dc=edu,dc=uy
objectClass: organizationalUnit
ou: gente

dn: ou=groupos,dc=ldap,dc=curerocha,dc=edu,dc=uy
objectClass: organizationalUnit
ou: groupos

dn: uid=victor,ou=gente,dc=ldap,dc=curerocha,dc=edu,dc=uy
objectClass: inetOrgPerson
objectClass: posixAccount
```

```
objectClass: shadowAccount
uid: victor
sn: Alem
givenName: Víctor
cn: Víctor Alem
displayName: Víctor Alem
uidNumber: 1000
gidNumber: 10000
userPassword: secreto1
gecos: Víctor Alem
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
postalCode: 31000
l: Toulouse
o: Example
mobile: +33 (0)6 xx xx xx xx
homePhone: +33 (0)5 xx xx xx xx
title: System Administrator
postalAddress:
initials: VA
Confirmamos que todo este correcto con:
$ ldapadd -x -D cn=admin,dc=curerocha,dc=edu,dc=uy -W -f datos_frontend_slapd.ldif
```

5.2 Convertir del Viejo archivo de configuración slapd.conf al formato cn=config

Aquí explicaré con un ejemplo de como agregar los schemas de GOsa.

Para realizar esta tarea creamos el archivo slapd_convert.conf con el siguiente contenido:

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/openldap.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/misc.schema
include         /etc/ldap/schema/trust.schema


include         /etc/ldap/schema/samba3.schema
```

```
include         /etc/ldap/schema/gosystem.schema
include         /etc/ldap/schema/gofon.schema
include         /etc/ldap/schema/goto.schema
include         /etc/ldap/schema/goto-mime.schema
# Note: before 2.6.5 this file was named gosa+samba3.schema
include         /etc/ldap/schema/gosa-samba3.schema
include         /etc/ldap/schema/gofax.schema
include         /etc/ldap/schema/openssh.schema
include         /etc/ldap/schema/goserver.schema
include         /etc/ldap/schema/fai.schema
include         /etc/ldap/schema/dnszone.schema
include         /etc/ldap/schema/rfc2739.schema
include         /etc/ldap/schema/kolab2.schema
include         /etc/ldap/schema/apple.schema
include         /etc/ldap/schema/nagios.schema
include         /etc/ldap/schema/phpgwaccount.schema
include         /etc/ldap/schema/pureftpd.schema
include         /etc/ldap/schema/phpscheduleit.schema
include         /etc/ldap/schema/pptp.schema
include         /etc/ldap/schema/openxchange.schema
include         /etc/ldap/schema/dhcp.schema
```

Luego ejecutamos el siguiente comando.

- `$ slaptest -f slapd_convert.conf -F /usr/local/etc/openldap/slapd.d`

Luego le cambiamos los permisos a todos los archivos del directorio /etc/ldap/slapd.d/cn=config/cn=schema/ con el siguiente comando.

- `$ chown openldap:openldap /etc/ldap/slapd.d/cn=config/cn=schema/*`

Esto sería lo necesario para que quede GOsa funcionando.

5.3 Phpldapadmin

5.3.1 Instalación

- `$ apt-get install phpldapadmin`

Hacemos un respaldo de la configuración por defecto y editamos el archivo config.php

$ cp /etc/phpldapadmin/config.php /etc/phpldapadmin/config.php.orig

$ vi /etc/phpldapadmin/config.php

En este archivo editar las siguientes lineas:

```
$ldapservers->SetValue($i,'server','name','My LDAP Server');  // The name to display

$ldapservers->SetValue($i,'server','host','127.0.0.1');  // Address of the LDAP server

$ldapservers->SetValue($i,'server','base',array('dc=ldap,dc=curerocha,dc=edu,dc=uy'));  //
Base dn

$servers->setValue('login','bind_id','cn=admin,dc=ldap,dc=curerocha,dc=edu,dc=uy');
```

Entramos por web https://ip_servidor/phpldapadmin e ingresamos el password configurado en el ldap.

6 Gosa

6.1 Introducción

Esta página cuenta y quiere dejar huella de la experiencia que no pudimos completar en el taller por falta de tiempo, pero creemos es un buen "frontend" para tal vez impelementar en próximas ediciones del Taller de Administración de Redes y Servicios como plataforma para una gestión completa de la red del CURE.

6.2 Requisitos Previos

Para instalar GOsa es necesario instalar lo siguiente:

- Apache
- PHP
- MySQL
- LDAP

Nota: Para instalar LDAP, recomiendo leer las siguientes referencias:

- https://oss.gonicus.de/labs/gosa/wiki/DocumentationInstallingGOsa
- https://help.ubuntu.com/10.04/serverguide/C/openldap-server.html
- http://taller.curerocha.edu.uy/mediawiki/index.php/Instalaci%C3%B3n_y_configuraci%C3%B3n_OpenLDAP

6.3 Instalación GOsa

Para instalar GOsa lo primero es agregar la fuente a los repositorios, para esto creamos el archivo /etc/apt/source.list.d/gosa.source.list con la siguiente linea:

deb http://oss.gonicus.de/pub/gosa/debian-etch/ ./

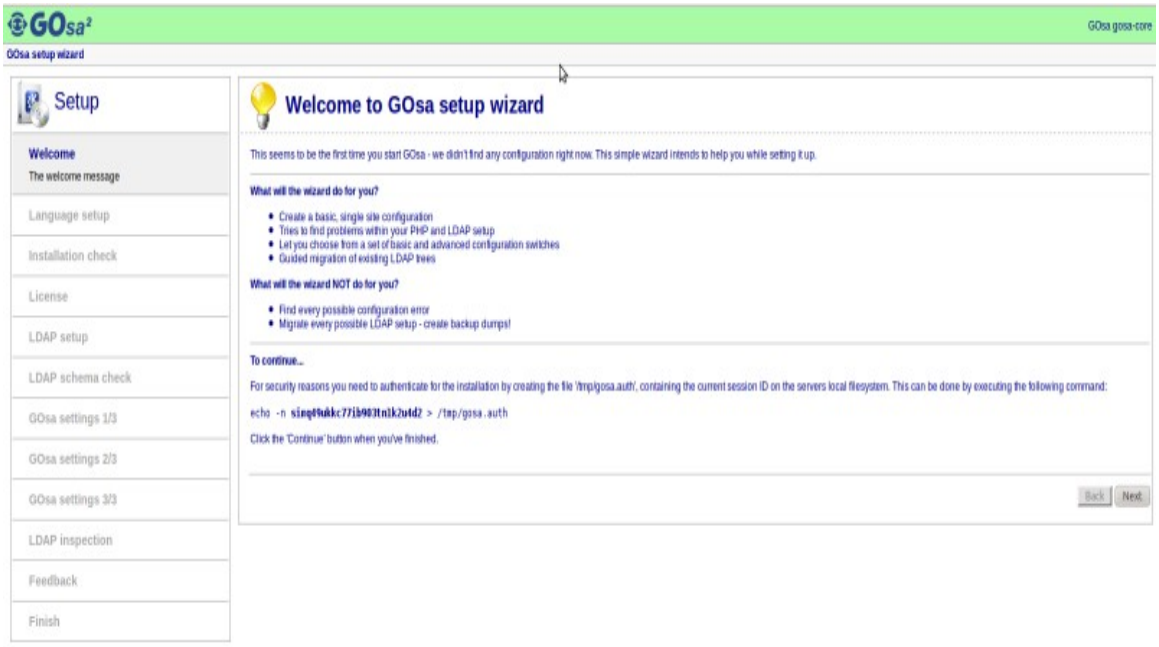
Luego, desde **aptitude** instalamos los paquetes necesarios. Este punto es lo que habría que exporar un poco más, por falta de tiempo instalé todos los paquetes de GOsa y sus plugins, pero no debería ser necesario...

Nota: Nosotros instalamos en Ubuntu 10.04 LTS y se precisa una versión de GOsa superior a la 2.5, la debian squeeze no anduvo pero la etch si. Leer: https://oss.gonicus.de/labs/gosa/wiki/InstallingGOsa

6.4 Configuración GOsa

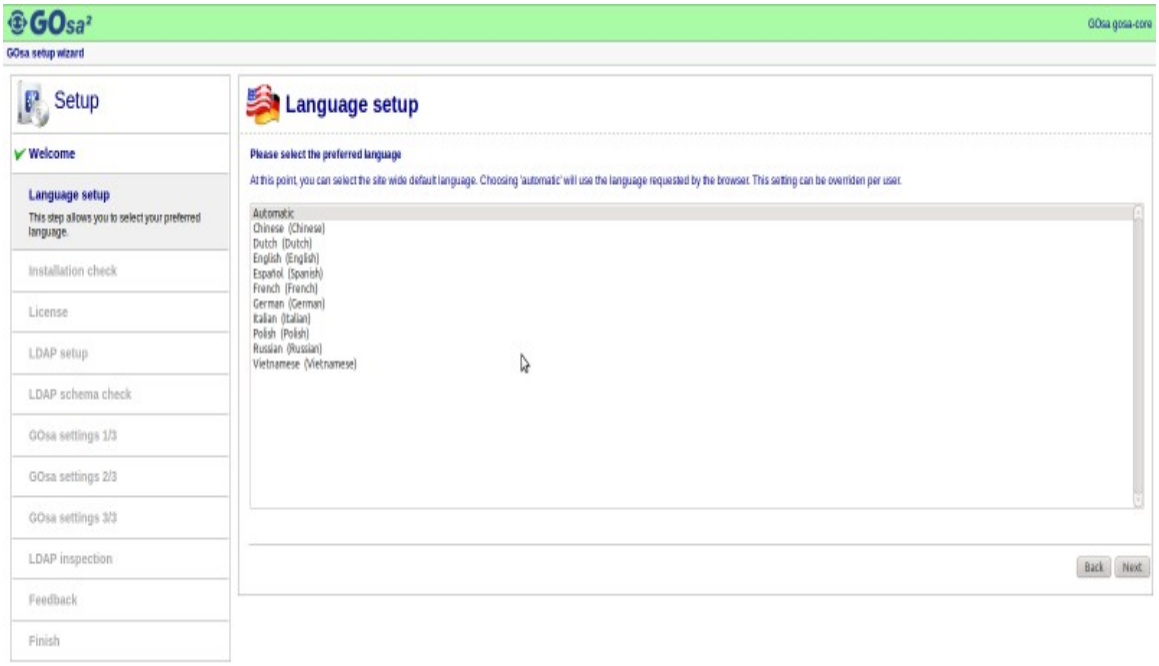
Luego de instalados los paquetes, ingresamos vía web a https://servidor/GOsa y se inicia el setup.

6.4.1 Paso 1: Bienvenida Setup



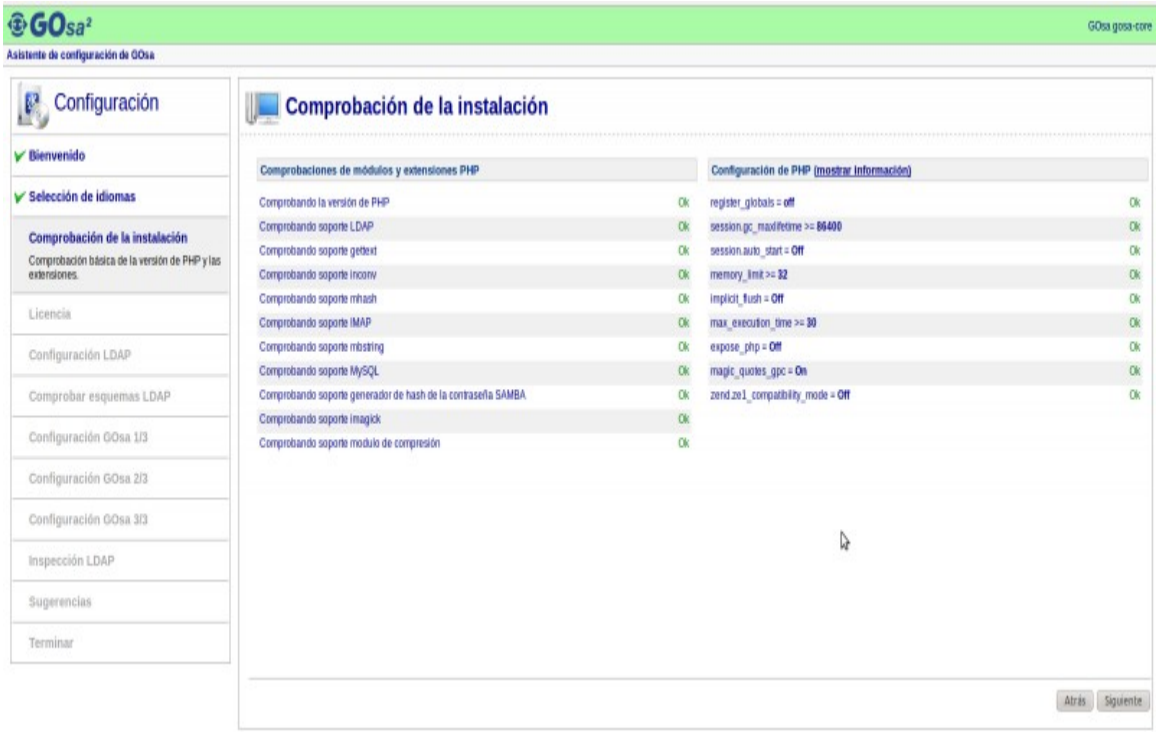
En este paso debemos ejecutar el comando que nos muestra en la página.

6.4.2 Paso 2: Lenguaje



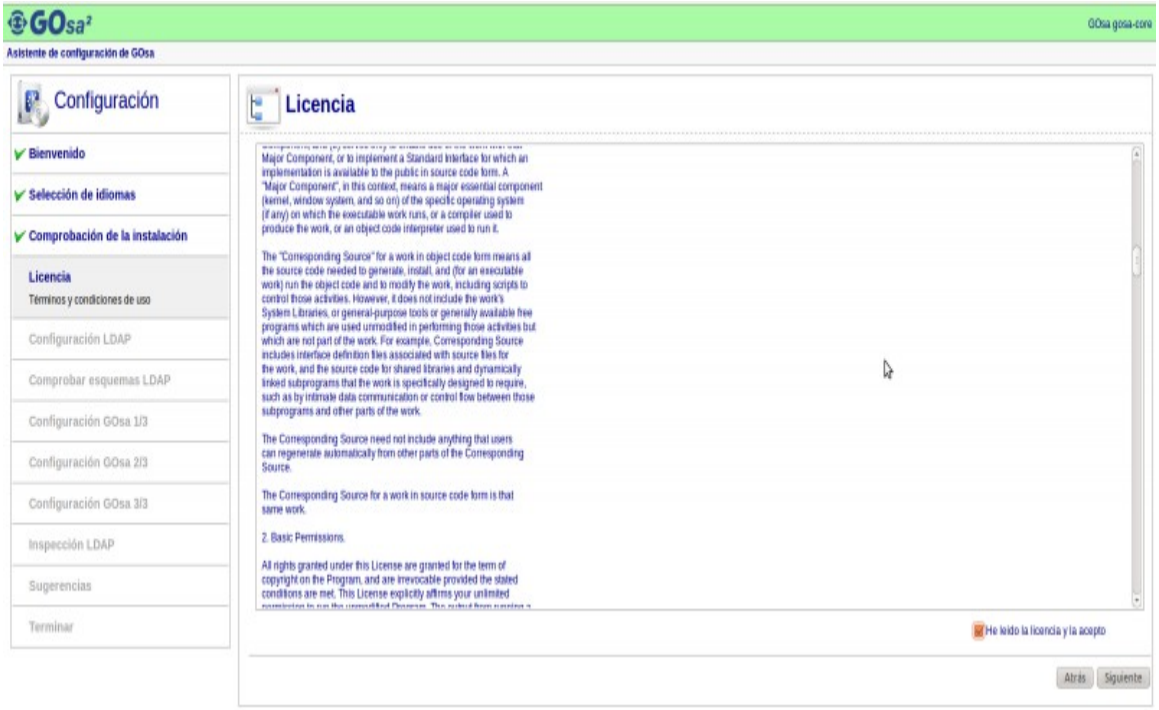
Elegir el idioma deseado.

6.4.3 Paso 3: Comprobación de la instalación



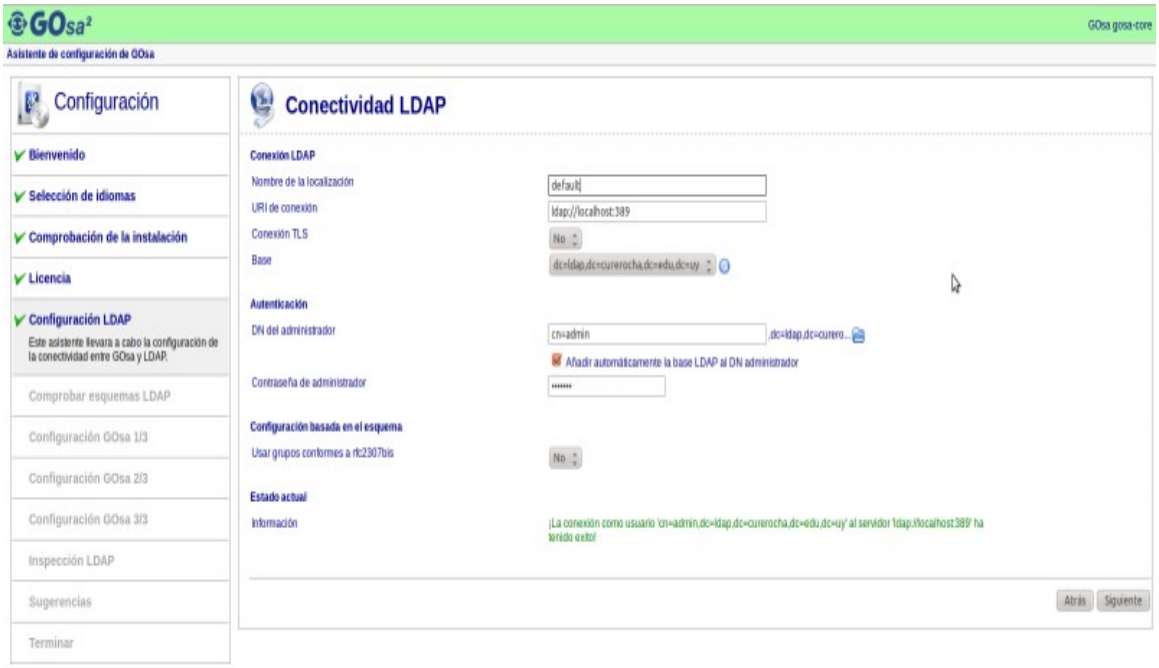
Chequeamos que esté todo bien y seguimos, de lo contrario hacer los cambios pertinentes.

6.4.4 Paso 4: Licencia



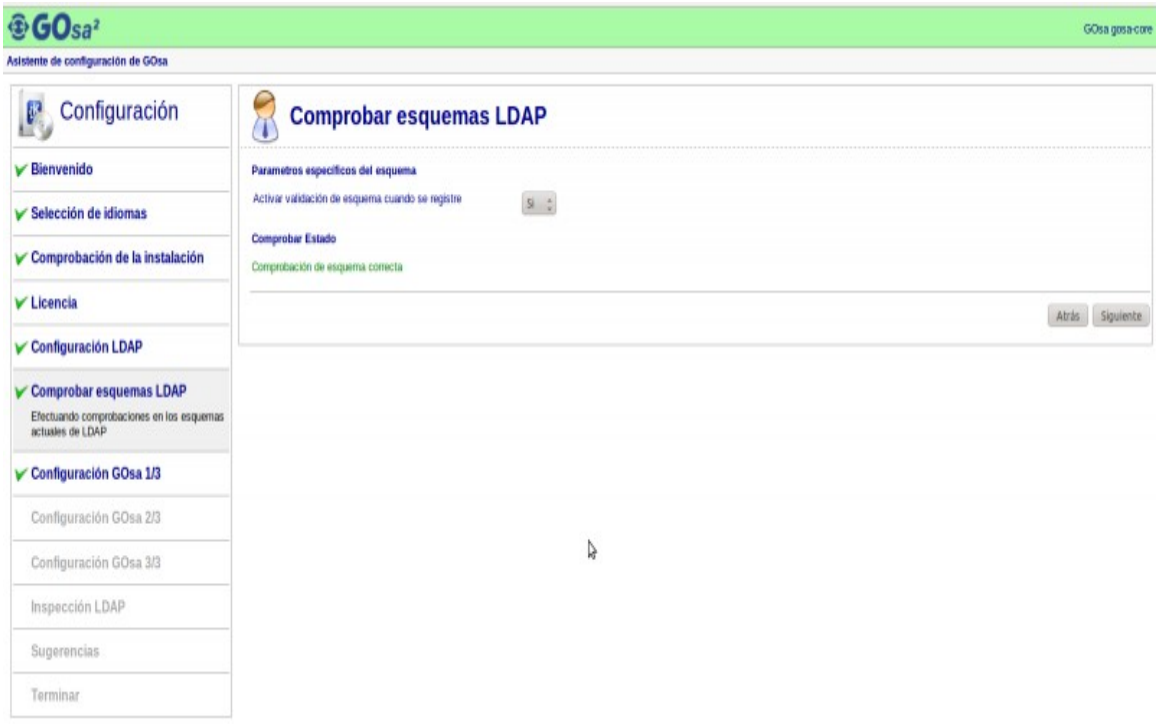
Leemos detenidamente todo el documento y seguimos...

6.4.5 Paso 6: Conectividad LDAP



En este paso hay que escribir la configuración de LDAP.

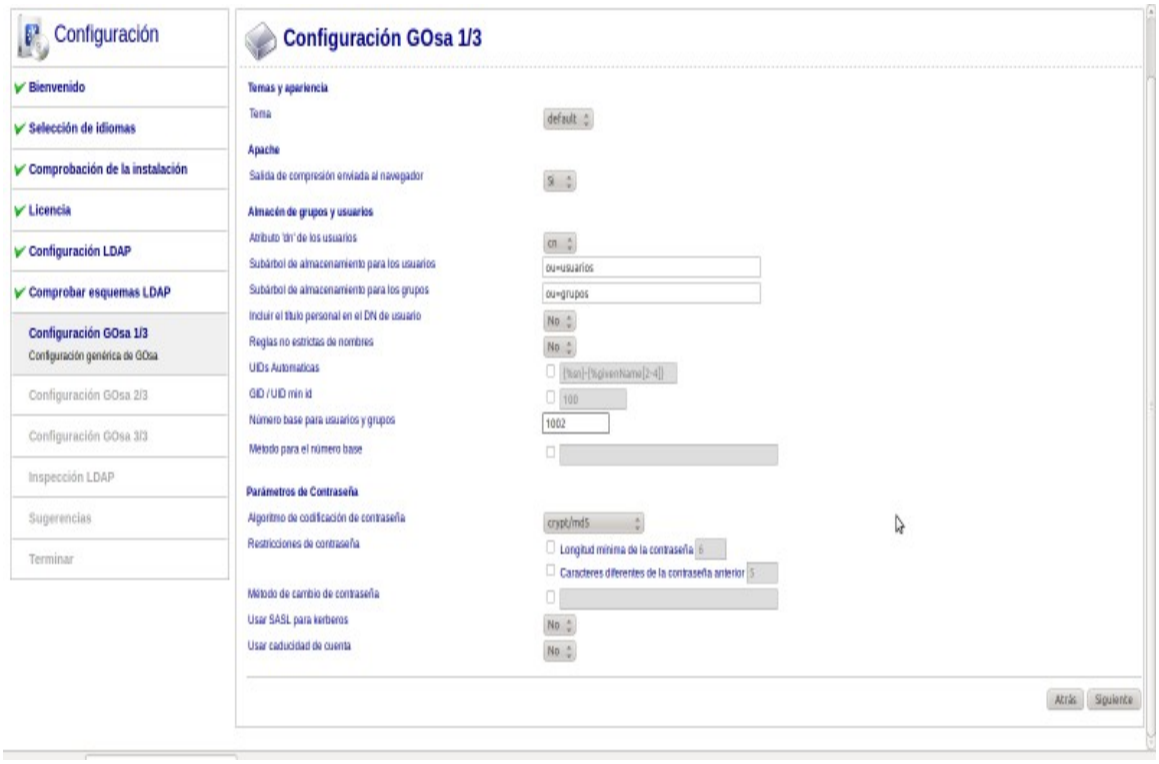
6.4.6 Paso 7: Comprobación de Esquemas



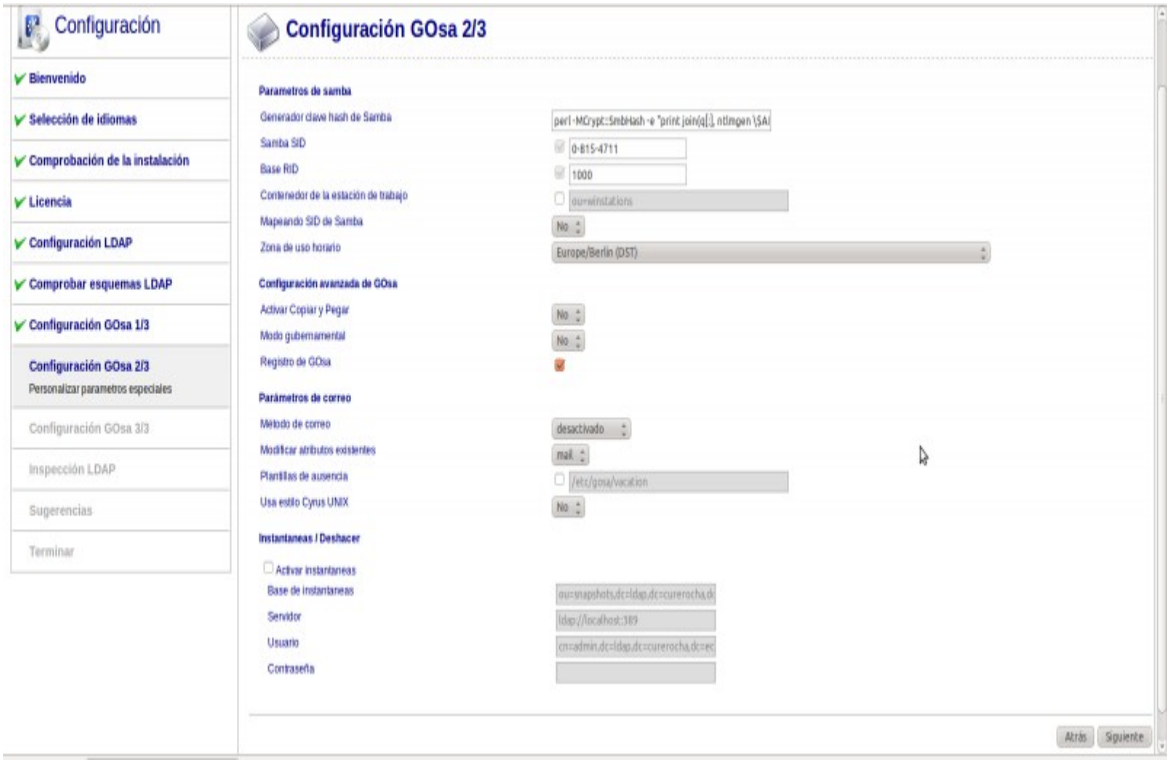
Este paso puede dar errores porque hay que tener el LDAP funcionando bien, por más información de cómo agregar los schemas para GOsa aquí.

6.4.7 Paso 8: Configuración GOsa 1/3

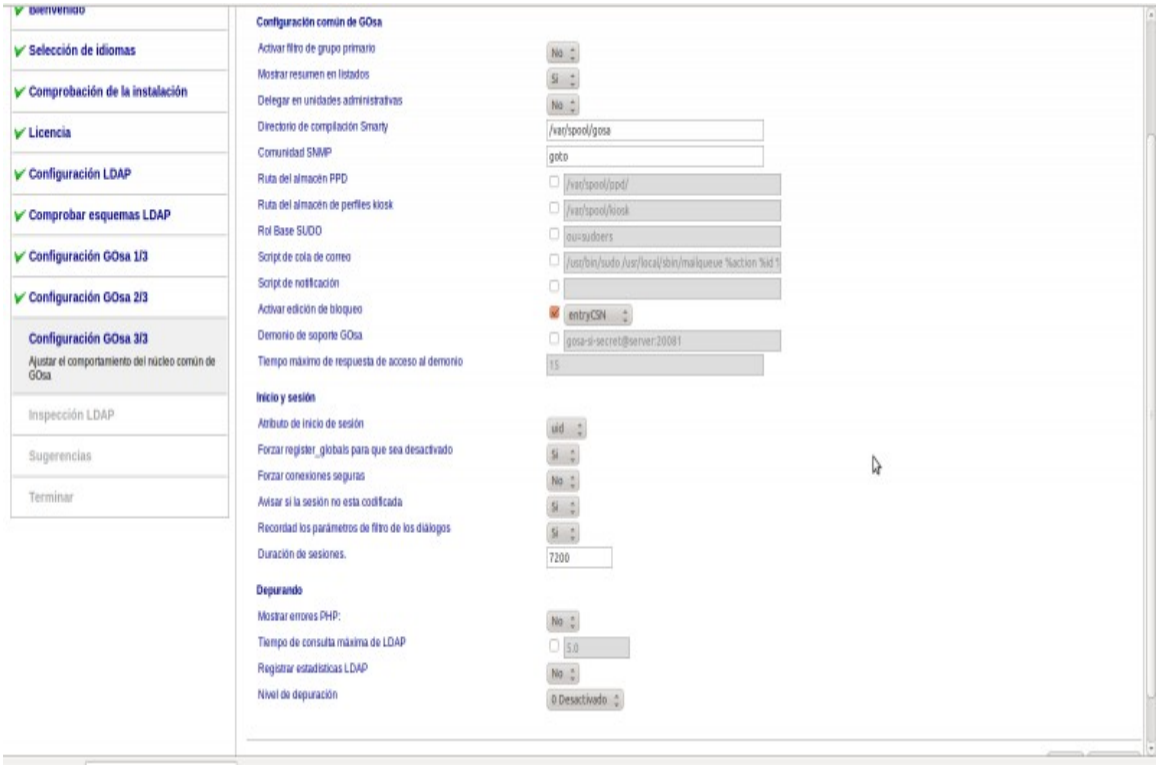
En los siguientes tres pasos, seleccionar las caracteristicas de GOsa deseadas.



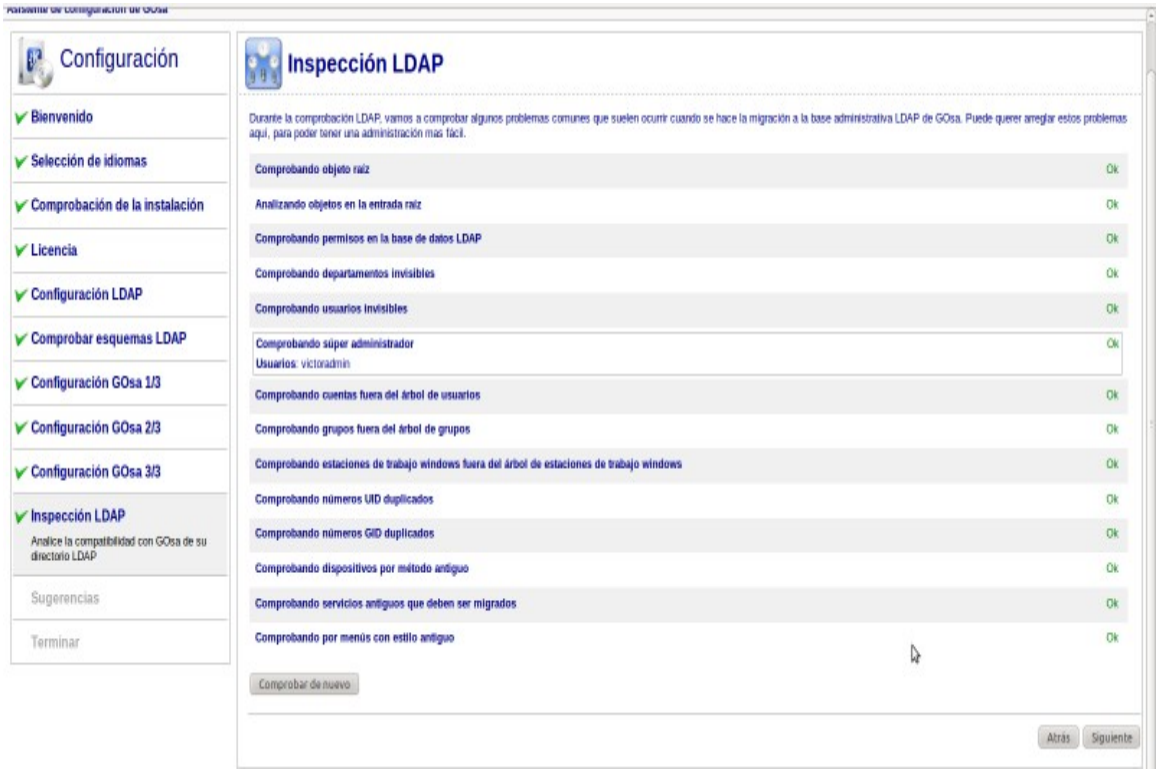
6.4.8 Paso 9: Configuración GOsa 2/3



6.4.9 Paso 10: Configuración GOsa 3/3



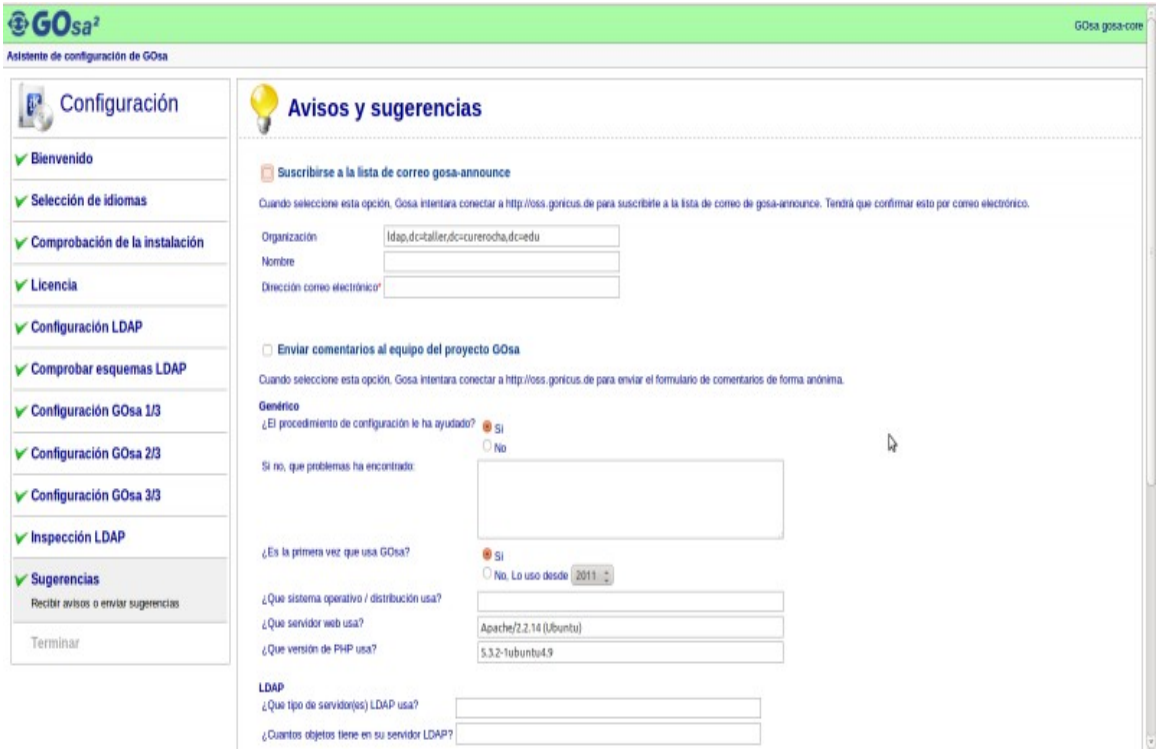
6.4.10 Paso 11: Inspección LDAP



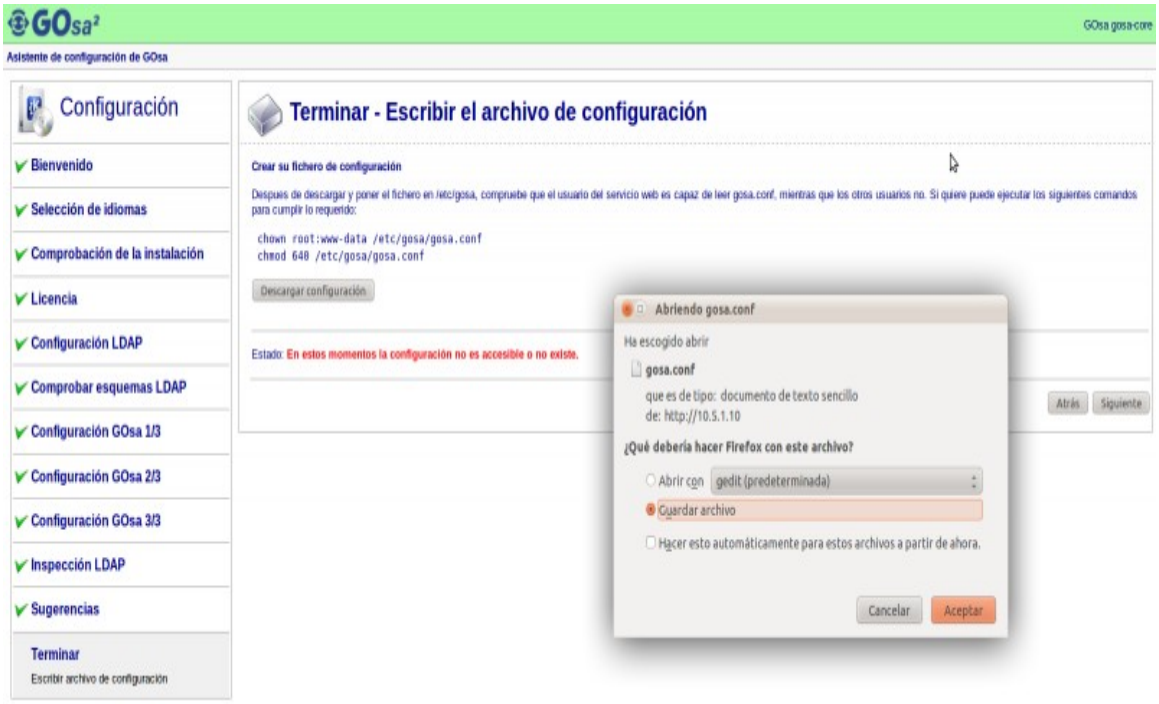
Aquí la aplicación web nos da la posibilidad de, en caso de error, corregirlo y crear la cuenta de administrador de GOsa. Corregir los errores sí los hay y continuar.

6.4.11 Paso 12: Avisos y sugerencias

Esta es una parte opcional.



6.4.12 Paso 13: Terminar la instalación



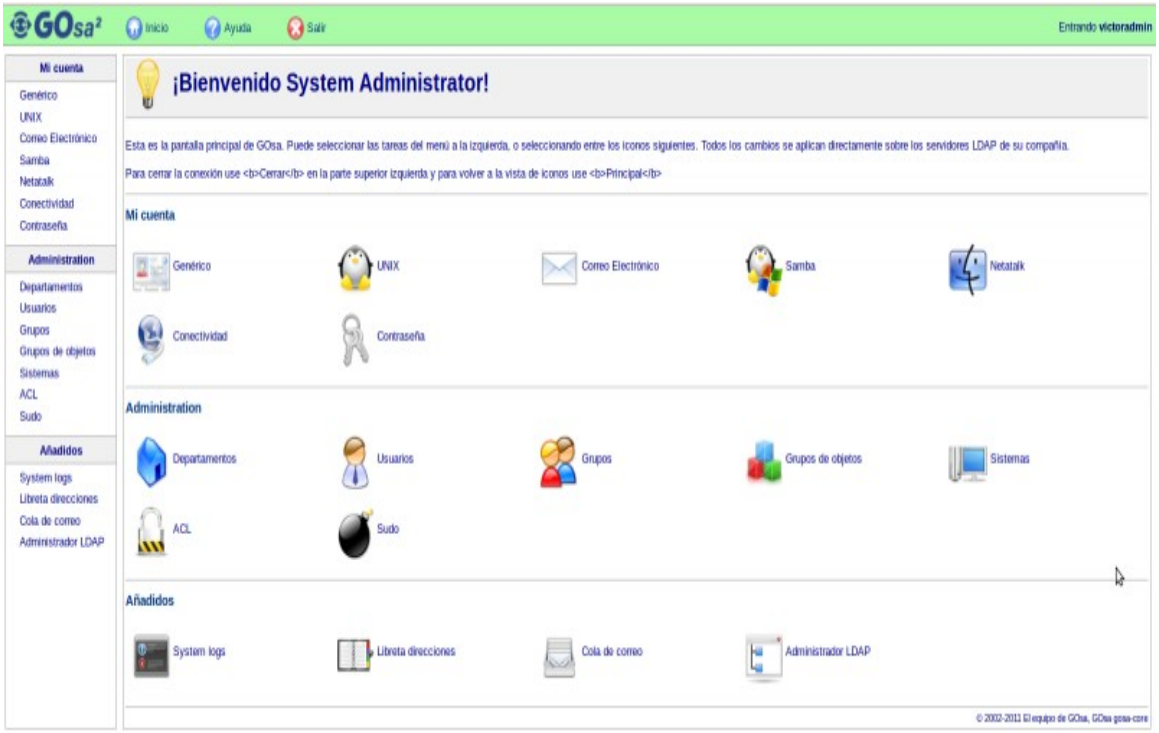
En este paso hay que descrgar el archivo y luego copiarlo en el directorio de GOsa y derle los siguientes permisos:

- `$ chown root:www-data /etc/gosa/gosa.conf`
- `$ chmod 640 /etc/gosa/gosa.conf`

6.5 Pantalla de login

Ingresar con el usuario administrador de GOsa.

6.6 Pantalla de bienvenida GOsa



Hasta aquí llegó la exploración de GOsa que por falta de tiempo no lo pudimos implementar en los servidores del CURE.

7 Apache2 – Servidor Web

Servidores web en GNU/linux: el principal y más conocido: apache pero también: lighthttpd, cherokee, ...

Utilizaremos apache2 (denominado así en debian/ubuntu porque cohabita(ro)n las versiones 1.3.x (apache) y 2.x (apache2)

7.1 Estructura de directorios de Apache2

Organización de /etc/apache2:

- /etc/apache2/apache2.conf: archivo principal de configuración,
- /etc/apache2/ports.conf: declaración de uso de VirtualHosts y puertos de escucha
- /etc/apache2/conf.d/ carpeta de configuraciones específicas a módulos u otros paquetes que utilizan apache
- /etc/apache2/sites-available: definición de "sitios" VirtualHosts. aquí, inicialmente hay un sitio llamado "default", que responderá a cualquier solicitud.
- /etc/apache2/sites-enabled: "sitios" activados (enlaces simbólicos a la precedente carpeta)

7.2 Instalación

- `$ aptitude install apache2`

Primer prueba: desde un navegador visitar la página: http://servidor.apache/ donde "servidor.apache" es la IP del servidor, o un nombre de domínio que resuelve a ésta. (si el servidor tiene un navegador, puede sar: http://localhost/)

Debemos entonces ver aparecer una página de prueba: "It works!"

7.3 Algunos comandos útiles de Apache2

Utilitarios de administración de sitios:

- `a2ensite` (por "apache2 enable site"): activación de los sitios disponibles,
- `a2dissite`: desactivación de los sitios.

Podemos, por ejemplo, crear un nuevo sitio creando un archivo /etc/apache2/sites-available/mi_sitio, a partir del archivo /etc/apache2/sites-available/default

Si queremos que este sitio sólo responda a cierto dominio que resuelve en ese servidor (y no a la IP o a otro dominio), agregamos en la sección <VirtualServer *:80> una directiva:

- `ServerName www.mi_servidor.org`

Se pueden personalizar las directivas existentes y/o agregar muchas otras. Debemos finalmente activar el sitio:

- `a2ensite mi_sitio`

Y re-cargar la configuración:

- `/etc/init.d/apache2 reload`

Otros utilitarios similares existen para los módulos.

- `a2enmod`: habilitación de un módulo apache,
- `a2dismod`: deshabilitación de un módulo apache,

Apache ya viene compilado con diferentes módulos. Por ejemplo, para habilitar apache en https: `a2enmod ssl`

Esto requerirá, además, un certificado válido y la configuración de un sitio en https. Un certificado autofirmado se puede obtener instalando ssl-cert, y un sitio activando:

- `a2ensite default-ssl`
- `as2enmod`, sin parámetro, muestra la lista de módulos disponibles.

Además de las dependencias, existen varios paquetes adicionales ligados a apache, a menudo a través de módulos: libapache2-mod-XXX, por ejemplo PHP: libapache2-mod-php5

Apache se utiliza a menudo en una configuración "LAMP": Linux Apache MySQL PHP. Es necesario instalar además:

`libapache2-mod-php5` (que incluye php5 en dependencia)

`mysql-server`

`php-mysql`

7.3.1 Objetivos

1. Redirigir por default a la página principal de mediawiki con el módulo "rewrite" de apache
2. Crear "vhosts" para la base de datos, mediawiki y tikiwiki (modificando previamente el DNS-apache)

7.3.2 Software

- Apache2

7.3.3 Procedimientos

7.3.4 Redirigir por default a la página principal de mediawiki con el módulo "rewrite" de apache

Para lograr esto, editamos el archivo /etc/apache2/sites-enabled/000-default y agregar el siguiente módulo:

```
<IfModule mod_rewrite.c>
     RewriteEngine on
     RewriteRule ^/$ /mediawiki [R]
</IfModule>
```

7.4 Crear "vhosts" para la base de datos, mediawiki y tikiwiki

- vhost para la base de datos y redirección por default a mediawiki:

Queremos ingresar a la base de datos sólo por https y si los usuarios entran por http se rediriga a https. Para esto crearemos dos sitios, uno base-de-datos (vhost en el puerto 80) y otro base-de-datos-ssl (vhost por default en el puerto 443), en el primero unicamente redirigiremos a https y en el último haremos la redirección a mediawiki. Editemos /etc/apache2/sites-enabled/base-de-datos y agrequemos la siguiente linea para redirigir en forma permanente a https:

- `Redirect permanent / https://base-de-datos.taller.curerocha.edu.uy/`

Y agregamos un NameServer y algunos ServerAlias

`ServerName base-de-datos.taller.curerocha.edu.uy`

`ServerAlias base-de-datos.taller.csic.edu.uy bdd.taller.curerocha.edu.uy`

Con esto iremos directamente a base-de-datos-ssl (vhost en el puerto 443), ahora configuremos este sitio editando /etc/apache2/sites-enabled/base-de-datos-ssl y agregando lo siguiente:

```
# Ponemos el alias en https solamente
Alias /base-de-datos /usr/share/phpmyadmin


<IfModule mod_rewrite.c>
     RewriteEngine On
     RewriteRule ^/$ /base-de-datos/ [R]
</IfModule>
```

- vhost para tikiawiki

En el vhost (y en el DNS) definimos ServerName y ServerAlias

```
ServerName tikiwiki.taller.curerocha.edu.uy
ServerAlias tikiwiki.taller.csic.edu.uy
```

- vhost para mediawiki

Procedemos de la misma manera que con tikiwiki respecto a los ServerName y los ServerAlias. Además hagamos alguna redirección poniendo lo siguiente en el archivo /etc/apache2/sites-enable/mediawiki

```
ServerName wiki.taller.curerocha.edu.uy
ServerAlias wiki.taller.csic.edu.uy mediawiki.taller.curerocha.edu.uy
mediawiki.taller.csic.edu.uy


DocumentRoot /var/www/


RewriteEngine on
RewriteCond%{HTTP_HOST}  !^wiki\.taller\.curerocha\.edu\.uy [NC]
RewriteCond%{HTTP_HOST}  !^$
RewriteRule ^/(.*)         http://wiki.taller.curerocha.edu.uy/$1 [R]
RewriteRule ^/$ /mediawiki [R]
```

7.5 DNS-apache

Para que funcionen los vhosts del apache, hay que agregar las zonas correspondientes. Editar el archivo /etc/bind/db.taller.curerocha.edu.uy como el siguiente:

```
; Archivo BIND de definición de la zona taller.curerocha.edu.uy
;
$ORIGIN taller.curerocha.edu.uy.
;;; acortamos los TTL mientras hacemos pŕuebas!
; $TTL   86400 ; 1D
$TTL   360 ; 10M
@       IN      SOA     paloma.taller.csic.edu.uy. root.paloma.taller.csic.edu.uy. (
                         2011060909 ; Serial
                         6H         ; Refresh
                         1D         ; Retry
                         1W         ; Expire
```

```
                        10M  )      ; Negative Cache TTL
;                        1D  )      ; Negative Cache TTL
;
; Servidores de nombres y dirección IP de zona
;
@            IN NS   paloma.taller.csic.edu.uy.
@            IN NS   gould.csic.edu.uy.
@            IN A    164.73.234.104
;
; Nombres canónicos de servidores e interfaces
;
paloma       IN A    164.73.234.104
garzon       IN A    164.73.234.126
;
; Alias a nombres canónicos, para los servicios
;
base-de-datosIN CNAME paloma
bdd                IN CNAME paloma
tikiwiki     IN CNAME paloma
wiki               IN CNAME paloma
mediawiki    IN CNAME paloma
```

8 MySQL

MySQL es un software libre (en un esquema de licenciamiento dual) de gestión de bases de datos relacional, multihilo y multiusuario.

8.1 Requisitos Prévios

- Apache2
- PHP (Instalación: aptitude install php5)

8.2 Instalación MySQL

- `$ apt-get install mysql-server`

Generar contraseña para MySQL:

```
$ apt-get install pwgen
```

```
$ pwgen 16 -y
```

La clave se guardará en /root/adminSysCure/MySQL.txt

8.3 Instalación phpmyadmin

- `$ apt-get install phpmyadmin`

Comentar el alias para que no entre por el nombre por default (http://servidor.com/phpmyadmin)

Editar el archivo /etc/phpmyadmin/apache.conf comentando la linea:

```
Alias /phpmyadmin /usr/share/phpmyadmin
```

Manejaremos mejor este tema con vhosts (ver: Apache2)

Instalación de openssl y ssl-cert;

- `$ apt-get install openssl ssl-cert`

Crear los certificados:

- `$ a2enmod ssl`
- `$ mkdir /etc/apache2/ssl`
- `$ /usr/sbin/make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/apache.pem`

Creamos el sitio base-de-datos-ssl y base-de-datos (más información en Apache2).

Habilitamos los sitios

- `$ a2ensite base-de-datos-ssl`
- `$ a2ensite base-de-datos`

Reiniciamos apache

- `$ service apache2 restart`

9 Configuraciones de “Garzón”

9.1 Instalación de OPENWRT

Usamos la distribución OPENWRT 10.03.1. Se puede descargar desde el sitio de OpenWRT: http://wiki.openwrt.org/toh/tp-link/tl-wr1043nd|#oem.easy.installation

De esta manera obtenemos mucha mas funcionalidad y versatilidad.

1. Mediante la interfaz web, que viene con defecto con el router, en la opción de "Firmware Upgrade" tenemos la opción de actualizar su firmware por OPENWRT.
2. Luego de cargada el firmware de OPENWRT, reiniciamos el router.
3. Con el nuevo firmware cargado, desde una consola entramos por telnet para darle una contraseña al usuario root (único usuario del firmware):
   - `$ telnet 192.168.1.1`
   - `$ passwd`
   - `$ exit`
4. Por consola no volvemos a logear pero por ssh:
   - `$ ssh root@192.168.1.1`
5. Ahora tenemos que editar la configuración de red por defecto, esto lo hacemos editando: /etc/config/network, y lo dejamos de la siguiente forma:

```
config 'interface' 'loopback'
   option 'ifname' 'lo'
   option 'proto' 'static'
   option 'ipaddr' '127.0.0.1'
   option 'netmask' '255.0.0.0'

config 'interface' 'wan'
   option 'ifname' 'eth0.1'
   option 'proto' 'static'
   option 'ipaddr' '164.73.234.126'
   option 'netmask' '255.255.255.128'
   option 'defaultroute' '0'
   option 'peerdns' '0'
   option 'gateway' '164.73.234.1'
   option 'dns' '164.73.128.5 164.73.128.70'

config 'switch'
   option 'name' 'rtl8366rb'
   option 'reset' '1'
   option 'enable_vlan' '1'

option 'device' 'rtl8366rb'
```

```
	option 'vlan' '1'
	option 'ports' '0 5t'

config 'switch_vlan'
	option 'device' 'rtl8366rb'
	option 'vlan' '2'
	option 'ports' '1 5t'

config 'switch_vlan'
	option 'device' 'rtl8366rb'
	option 'vlan' '3'
	option 'ports' '2 5t'

config 'switch_vlan'
	option 'device' 'rtl8366rb'
	option 'vlan' '4'
	option 'ports' '3 5t'

config 'switch_vlan'
	option 'device' 'rtl8366rb'
	option 'vlan' '5'
	option 'ports' '4 5t'

config 'interface' 'dmz'
	option 'proto' 'static'
	option 'ifname' 'eth0.2'
	option 'ipaddr' '10.5.2.1'
	option 'netmask' '255.255.255.0'
	option 'defaultroute' '0'
	option 'peerdns' '0'

config 'interface' 'lan1'
	option 'proto' 'static'
	option 'ifname' 'eth0.3'
	option 'ipaddr' '10.5.1.1'
	option 'netmask' '255.255.255.0'
	option 'defaultroute' '0'
	option 'peerdns' '0'

config 'interface' 'lan2'
	option 'proto' 'static'
	option 'ifname' 'eth0.4'
	option 'netmask' '255.255.255.0'
```

```
        option 'defaultroute' '0'
        option 'peerdns' '0'
        option 'ipaddr' '10.5.4.1'

config 'interface' 'lan3'
        option 'proto' 'static'
        option 'ifname' 'eth0.5'
        option 'netmask' '255.255.255.0'
        option 'defaultroute' '0'
        option 'peerdns' '0'
        option 'ipaddr' '10.5.5.1'

config 'alias' 'legacy'
        option 'proto' 'static'
        option 'interface' 'lan1'
        option 'ipaddr' '10.5.1.252'
        option 'netmask' '255.255.255.0'

config 'interface' 'wlan'
        option 'proto' 'static'
        option 'ipaddr' '10.5.3.1'
        option 'netmask' '255.255.255.0'
        option 'defaultroute' '0'
        option 'peerdns' '0'
        option 'ifname' 'wlan0'
```

Para trabajar más facil, paramos y deshabilitamos el firewall, para después de configurado volver a habilitarlo.

Lo hacemos mediante los comandos:

- `$ /etc/init.d/firewall disable`
- `$ /etc/init.d/firewall stop`

Para chequear que quedó deshabilitado:

- `$ iptables –L`

9.2 DHCP en OPENWRT

Network->DHCP

Ahí agregamos una entrada nueva por cada zona distinta donde queremos dar el servicio de DHCP

Elejimos:

- Interfaz: la interfaz por donde queremos que se de el servicio de DHCP, ejemplo: wlan
- Start: a partir de que ip empieza a entregar (sólo el último octeto), ej: 2 (empieza a entregar a partir de la xxx.xxx.xxx.2)

- Limit: última ip que entrega no incluida (sólo el último octeto), ej: 100 (última a entregar xxx.xxx.xxx.99)
- Leasetime: tiempo que recervará la ip entregada para la misma mac, ej: 5h (5 horas) ó 20m (20 minutos)
- Dynamic DHCP: si no está marcado, solo entregará ips a las mac que tengan recervada una ip, Static Leases (se muestra en el siguiente punto).
- DHCP-Options:
    - 3,xxx.xxx.xxx.xxx -> para asignar un gateway distinto al de por defecto
    - 6,xxx.xxx.xxx.xxx -> para asignar un DNS distinto al de por defecto
    - 15,dominio -> para asignar un nombre de dominio
- Static Leases: se puede hacer que el servidor DHCP siempre entregue la misma ip a la misma mac, esto se hace agregando un nombre, la dirección mac y la ip a asignar.

Para reinicar el servicio de dhcp:

- `/etc/init.d/dnsmasq stop`
- `/etc/init.d/dnsmasq start`

Agrego una muestra del archivo /etc/config/dhcp:

```
config 'dnsmasq'
	option 'domainneeded' '1'
	option 'boguspriv' '1'
	option 'filterwin2k' '0'
	option 'localise_queries' '1'
	option 'rebind_protection' '1'
	option 'rebind_localhost' '1'
	option 'local' '/lan/'
	option 'domain' 'lan'
	option 'expandhosts' '1'
	option 'nonegcache' '0'
	option 'authoritative' '1'
	option 'readethers' '1'
	option 'leasefile' '/tmp/dhcp.leases'
	option 'resolvfile' '/tmp/resolv.conf.auto'

config 'dhcp' 'wan'
	option 'interface' 'wan'
	option 'ignore' '1'
	option 'dynamicdhcp' '0'

config 'dhcp' 'lan1'
	option 'start' '2'
	option 'limit' '250'
	option 'leasetime' '5h'
	option 'dynamicdhcp' '1'
	option 'interface' 'lan1'
```

```
	list 'dhcp_option' '3,10.5.1.1' # de esta forma se puede asignar la gateway, sino se
	asigna por defecto

	list 'dhcp_option' '6,200.40.30.245' # de esta forma se puede asignar el DNS, sino se
	asigna por defecto, si son mas de uno, agregar una coma y la IP del otro servidor DNS
	(6,200.40.30.245,200.40.220.245).


config 'host'

	option 'name' 'Equipo8'

	option 'mac' '00:22:68:58:b4:66'

	option 'ip' '10.5.1.8'


config 'dhcp' 'wlan'

	option 'interface' 'wlan'

	option 'start' '2'

	option 'limit' '100'

	option 'leasetime' '1h'
```

Aclaración: toda la configuración de DHCP va en este archivo y NO en /etc/config/dnsmasq y tampoco en /etc/ethers. NO es recomendable tocar estos archivos y tampoco editar /etc/dhcp, usar la interfaz web. Siempre hacer un respado de la configuración del router antes de cambiar algo, System->Backup y restore opción Create backup

9.3 Wi-Fi en OpenWRT

Para agregar ssl se instala el paquete luci-ssl, después de instalar hay que reinicar el router. Tenemos que crear una interfaz para la red inalámbrica:

Network->Interface

Creamos una interfaz, llamada por ejemplo wlan, luego entramos para editarla

Protocol: Static

Interface: wlan0

y le asignamos su ip y máscara.

Ahora vamos al firewall:

Firewall->Zone

Agregamos la zona wlan, le asignamos la network wlan, aceptamos el tráfico entrante y saliente y rechazamos el forwarding.

Firewall->Traffic Control

Agregamos:

Source: wlan

Destination: wan

Para así dar salida a la wifi a internet.

Para habilitar la tarjeta inalambrica hay que ir a:

Network->Wifi->RADIO0

Ahí le marcamos la opción de: "enable"

Ahora hay que configurar el DHCP, en:

Network->DHCP

Ahí agregamos una entrada nueva por cada zona distinta donde queremos dar el servicio de DHCP

Elejimos:

- Interfaz: wlan
- Start: a partir de que ip empieza a entregar (sólo el último octeto), ej: 2 (empieza a entregar a partir de la xxx.xxx.xxx.2)
- Dynamic DHCP: si no está marcado, solo entregará ips a las mac que tengan recervada una ip, Static Leases (se muestra en el siguiente punto).
- Limit: última ip que entrega no incluida (sólo el último octeto), ej: 100 (última a entregar xxx.xxx.xxx.99)
- Leasetime: tiempo que recervará la ip entregada para la misma mac, ej: 5h (5 horas) ó 20m (20 minutos)
- DHCP-Options:
  - 3,xxx.xxx.xxx.xxx -> para asignar un gateway distinto al de por defecto
  - 6,xxx.xxx.xxx.xxx -> para asignar un DNS distinto al de por defecto
  - Static Leases: se puede hacer que el servidor DHCP siempre entregue la misma ip a la misma mac, esto se hace agregando un nombre, la dirección mac y la ip a asignar.

Para reinicar el servicio de dhcp:

- `/etc/init.d/dnsmasq stop`
- `/etc/init.d/dnsmasq start`

Agrego una muestra del archivo /etc/config/dhcp:

```
config 'dnsmasq'
 option 'domainneeded' '1'
 option 'boguspriv' '1'
 option 'filterwin2k' '0'
 option 'localise_queries' '1'
 option 'rebind_protection' '1'
 option 'rebind_localhost' '1'
 option 'local' '/lan/'
 option 'domain' 'lan'
 option 'expandhosts' '1'
 option 'nonegcache' '0'
 option 'authoritative' '1'
 option 'readethers' '1'
 option 'leasefile' '/tmp/dhcp.leases'
 option 'resolvfile' '/tmp/resolv.conf.auto'

 config 'dhcp' 'wan'
 option 'interface' 'wan'
 option 'ignore' '1'
```

```
 option 'dynamicdhcp' '0'


 config 'dhcp' 'lan1'
 option 'start' '2'
 option 'limit' '250'
 option 'leasetime' '5h'
 option 'dynamicdhcp' '1'
 option 'interface' 'lan1'
 list 'dhcp_option' '3,10.5.1.1' # de esta forma se puede asignar la gateway, sino se
asigna por defecto
 list 'dhcp_option' '6,200.40.30.245' # de esta forma se puede asignar el DNS, sino se
asigna por defecto, si son mas de uno, agregar una coma y la IP del otro servidor DNS
(6,200.40.30.245,200.40.220.245).


 config 'host'
 option 'name' 'Equipo8'
 option 'mac' '00:22:68:58:b4:66'
 option 'ip' '10.5.1.8'


 config 'dhcp' 'wlan'
 option 'interface' 'wlan'
 option 'start' '2'
 option 'limit' '100'
 option 'leasetime' '1h'
```

Aclaración: toda la configuración de DHCP va en este archivo y NO en /etc/config/dnsmasq y tampoco en /etc/ethers. NO es recomendable tocar estos archivos y tampoco editar /etc/dhcp, usar la interfaz web. Siempre hacer un respado de la configuración del router antes de cambiar algo, System->Backup y restore opción Create backup

10 Firewall

10.1 Firewalls a implementar

Tendremos 3 firewalls en la red:

- Garzón
- Paloma
- Polonio

10.1.1 Garzón

En garzón implementamos las siguientes zonas:

- internet: wan
- laboratorio: lan1
- inalámbrica: wlan
- dmz interna: dmz
- secretaría: lan2
- públicas: lan3

Ninguna zona puede enviar tráfico a las demás zonas, salvo casos particulares que veremos más adelante.

Se implementa un nat saliente para la zona wan.

10.1.1.1. Reglas Avanzadas

10.1.1.1.1 Reglas para acceder desde la lan1 (Laboratorio) a polonio

Reglas para acceder desde la a lan1 a la web de administración de Zentyal (Zentyal-lan1-web):

- Origen: lan1
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 443
- Acción: ACCEPT

Reglas para autenticación de usuarios en Zentyal (Zentyal-lan1-389):

- Origen: lan1
- Destino: dmz
- Protocolo: TCP+UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 389
- Acción: ACCEPT

Reglas para acceder a carpetas compartidas (Zentyal-lan1-445):

- Origen: lan1
- Destino: dmz
- Protocolo: TCP+UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 445
- Acción: ACCEPT

Reglas para acceder a cambiar contraseña (Zentyal-lan1-8888):

- Origen: lan1
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 8888
- Acción: ACCEPT

Reglas para acceder por ssh a Polonio (Zentyal-lan1-ssh):

- Origen: lan1
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 22
- Acción: ACCEPT

Reglas para obtener información de DNS en Plonio (Zentyal-lan1-DNS):

- Origen: lan1
- Destino: dmz
- Protocolo: UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 53
- Acción: ACCEPT

10.1.1.1.2 Reglas para acceder desde la DMZ Externa a la DMZ Interna (Polonio)

Reglas (DMZ externa a DMZ interna):

- Origen: wan
- Destino: dmz
- Dirección de origen: 164.73.234.0/25
- Dirección de destino: 0.0.0.0/0
- Acción: ACCEPT

10.1.1.1.3 Reglas para acceder desde la lan2 (Secretaría) a polonio

Reglas para acceder desde la a lan2 a la web de administración de Zentyal (Zentyal-lan2-web):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 443
- Acción: ACCEPT

Reglas para autenticación de usuarios en Zentyal (Zentyal-lan2-389):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP+UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 389
- Acción: ACCEPT

Reglas para acceder a carpetas compartidas (Zentyal-lan2-445):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP+UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 445
- Acción: ACCEPT

Reglas para acceder a cambiar contraseña (Zentyal-lan2-8888):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 8888
- Acción: ACCEPT

Reglas para acceder por ssh a Polonio (Zentyal-lan2-ssh):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 22
- Acción: ACCEPT

Reglas para obtener información de DNS en Plonio (Zentyal-lan2-DNS):

- Origen: lan2
- Destino: dmz
- Protocolo: UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 53
- Acción: ACCEPT

10.1.1.1.4 Reglas para acceder desde la lan3 (Docentes y públicas) a polonio

Reglas para autenticación de usuarios en Zentyal (Zentyal-lan3-389):

- Origen: lan3
- Destino: dmz
- Protocolo: TCP+UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 389
- Acción: ACCEPT

Reglas para acceder a carpetas compartidas (Zentyal-lan3-445):

- Origen: lan3
- Destino: dmz
- Protocolo: TCP+UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 445
- Acción: ACCEPT

Reglas para acceder a cambiar contraseña (Zentyal-lan3-8888):

- Origen: lan3
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 8888
- Acción: ACCEPT

Reglas para obtener información de DNS en Plonio (Zentyal-lan3-DNS):

- Origen: lan3
- Destino: dmz
- Protocolo: UDP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 53
- Acción: ACCEPT

10.1.1.1.5 Reglas para acceder desde la wlan (Wi-Fi) a las carpetas compartidas en Polonio

Reglas para acceder por ssh a Polonio (Zentyal-lan2-ssh):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 445
- Acción: ACCEPT

Reglas para acceder por ssh a Polonio (Zentyal-lan2-ssh):

- Origen: lan2
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 389
- Acción: ACCEPT

Reglas para acceder a cambiar contraseña (Zentyal-wlan-8888):

- Origen: wlan
- Destino: dmz
- Protocolo: TCP
- Dirección de destino: 10.5.2.2
- Puerto de destino: 8888
- Acción: ACCEPT

10.1.2 Paloma

Se utilizó la aplicación Firewall Builder para contruir las reglas de iptables, que luego fue exportada al servidor Paloma. Por mas información sobre Firewall Builder ir al siguiente http://www.fwbuilder.org/4.0/docs/users_guide/ link.

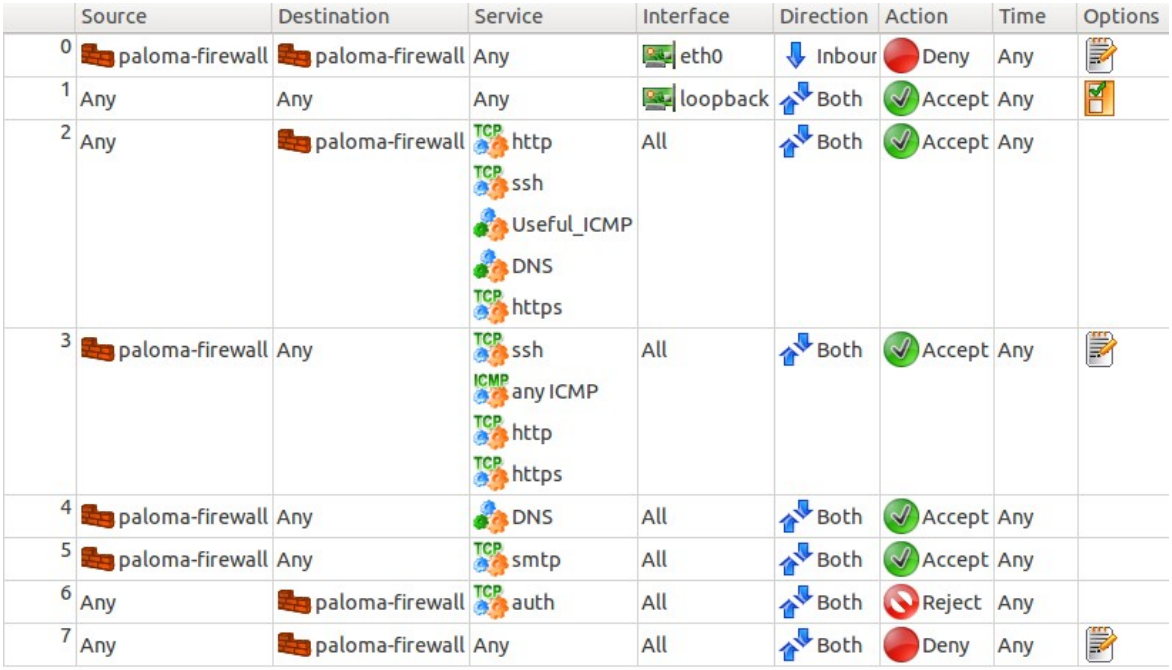
Las reglas que se permitirán entrantes serán:

- http
- https
- ssh
- ICMP
- DNS

Las reglas salientes que se permitirán serán:

- ssh
- ICMP
- http
- https
- DNS
- smtp
- NTP

Se adjunta captura de las reglas aplicadas:



	Source	Destination	Service	Interface	Direction	Action	Time	Options
0	paloma-firewall	paloma-firewall	Any	eth0	Inbour	Deny	Any	
1	Any	Any	Any	loopback	Both	Accept	Any	
2	Any	paloma-firewall	http ssh Useful_ICMP DNS https	All	Both	Accept	Any	
3	paloma-firewall	Any	ssh any ICMP http https	All	Both	Accept	Any	
4	paloma-firewall	Any	DNS	All	Both	Accept	Any	
5	paloma-firewall	Any	smtp	All	Both	Accept	Any	
6	Any	paloma-firewall	auth	All	Both	Reject	Any	
7	Any	paloma-firewall	Any	All	Both	Deny	Any	

10.1.3 Polonio

Se utilizó la aplicación Firewall Builder para contruir las reglas de iptables, que luego fue exportada al servidor Polonio. Por mas información sobre Firewall Builder ir al siguiente [http://www.fwbuilder.org/4.0/docs/users_guide/ link].

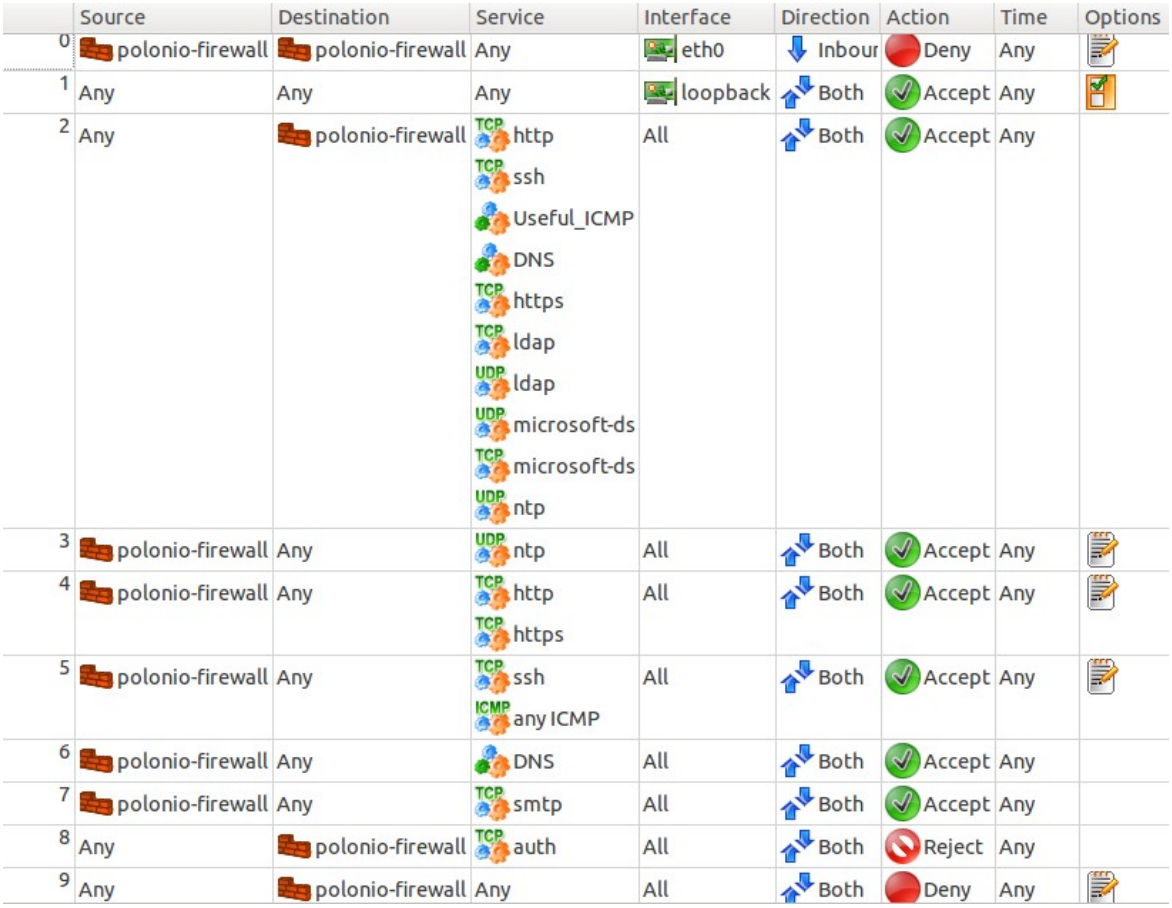
Las reglas que se permitirán entrantes serán:

- http
- https
- https-8888
- ssh
- ICMP
- DNS
- LDAP UDP
- LDAP TCP
- microsoft-ds UDP
- microsoft-ds TCP
- NTP

Las reglas salientes que se permitirán serán:

- ssh
- ICMP
- http
- https
- DNS
- smtp
- NTP

Se adjunta captura de las reglas aplicadas:



	Source	Destination	Service	Interface	Direction	Action	Time	Options
0	polonio-firewall	polonio-firewall	Any	eth0	Inbour	Deny	Any	
1	Any	Any	Any	loopback	Both	Accept	Any	
2	Any	polonio-firewall	TCP http TCP ssh Useful_ICMP DNS TCP https TCP ldap UDP ldap UDP microsoft-ds TCP microsoft-ds UDP ntp	All	Both	Accept	Any	
3	polonio-firewall	Any	UDP ntp	All	Both	Accept	Any	
4	polonio-firewall	Any	TCP http TCP https	All	Both	Accept	Any	
5	polonio-firewall	Any	TCP ssh ICMP any ICMP	All	Both	Accept	Any	
6	polonio-firewall	Any	DNS	All	Both	Accept	Any	
7	polonio-firewall	Any	TCP smtp	All	Both	Accept	Any	
8	Any	polonio-firewall	TCP auth	All	Both	Reject	Any	
9	Any	polonio-firewall	Any	All	Both	Deny	Any	

Se guardará una copia de seguridad, de las configuracines en /root de Paloma

10.2 Referencias

http://www.fwbuilder.org/4.0/docs/users_guide/

http://wiki.openwrt.org/doc/uci/firewall

11 Correo electrónico -Postfix-

11.1 Postfix

Postfix es un servidor de correo de software libre / código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail. Objetivo por el que implementamos postfix: Hay que tener un agente de correo configurado y funcionando para el envío de estado del sistema del servidor mediante logwatch.

11.2 Instalación de Postfix

Para poder instalar nuestro servidor de correo Postfix:

- `$ sudo apt-get install postfix`

Antes de terminar de instalar los paquetes se ejecuta el asistente de configuración de postfix, solamente hay que dar enter y seleccionar sin configuración.

11.3 Configuración de Postfix para que envío correo

En el archivo de configuración /etc/postfix/main.cf hay que completar con la siguiente información:

```
myorigin = tu_dominio.com
mydomain = $myorigin
myhostname = nombre_de_maquina.$mydomain
mydestination = $mydomain, $myhostname, localhost.$mydomain, localhost
relayhost = # Cuando no tiene nada este campo, es la propia máquina quien envía
inet_interfaces = all
home_mailbox = Mail/ # Hay que crear este directorio
```

Ejemplo de archivo /etc/postfix/main.cf ya configurado:

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
readme_directory = no
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
```

```
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.
myhostname = paloma.taller.csic.edu.uy
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = paloma.taller.csic.edu.uy, localhost.taller.csic.edu.uy, , localhost
relayhost =
mynetworks = 127.0.0.0/8::ffff:127.0.0.0?/104::1?/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
home_mailbox = Mail/
```

Comandos útiles:

- `$ /etc/init.d/postfix start`
- `$ /etc/init.d/postfix stop`
- `$ /etc/init.d/postfix restart`

11.4 Software

"Logwatch": analizador de estado del sistema.

11.4.1 Instalación de Logwatch

- `$ apt-get install logwatch`

11.4.2 Configuración

Logwatch guarda la información por defecto en el directorio /usr/share/logwatch/default.conf/ , pero este directorio no es necesario modificarlo ya que logwatch también se fija en /etc/logwatch/ y sobrescribe la configuración por defecto. Por lo tanto, directamente creamos el siguiente archivo: /etc/logwatch/conf/logwatch.conf en este vamos a hacer nuestras modificaciones personales, si queremos nuevamente la configuración por defecto, basta con borrar este archivo. Ejemplo de /etc/logwatch/conf/logwatch.conf:

```
# archivo /etc/logwatch/conf/logwatch.conf #
# Para que logwatch nos mande un reporte por mail
Output = mail
# Con esto elegimos el formato del reporte (text, html...)
Format = html
# Dirección de destino del reporte
```

```
MailTo = tu_correo@tu_servidor.com
# Remitente del reporte
MailFrom = logwatch
# Dia que quiero el reporte (Yesterday, Today, all)
Range = Yesterday
# De que servicios quiero recibir reportes
Service = all
```

Con esto hacemos que cada vez que ejecutemos el comando "logwatch" recibamos un mail con el reporte. Para recibir diariamente sin tener que ingresar a la máquina vamos a editar el archivo /etc/cron.daily/00logwatch y agregamos la siguiente línea:

```
/usr/sbin/logwatch --mailto tu_correo@tu_servidor.com
```

Guardamos los cambios y listo, recibiremos todos los días un reporte de logwatch.

12 NFS

NFS (Network File System) es un procolo que permite a un sistema compartir directorios y archivos con otros sistemas a través de la red. Usando NFS, los usuarios y los programas pueden acceder a archivos en sistemas remotos casi como si fueran archivos locales.

12.1 Servidor

12.1.1 Instalación

- `$ apt-get install nfs-kernel-server`

12.1.2 Configuración

Para configurar los direcctorios a compartir, se añaden al archivo /etc/exports de la siguiente forma:

/<directorio> <ip o red> (ro,no_root_squash)

- /<directorio> ruta del directorio que se va a compartir, ejmplo: /home
- <ip o red> ip o red a quién se le dará acceso, ejemplo:
- 10.5.1.1 para compartirlo solo con esta máquina
- 10.5.1.1/24 para la red 10.5.1.0
- (ro,sync,no_root_squash) son los permisos:
- ro: sólo lectura
- rw: lectura y escritura

no_root_squash: hará que los usuarios administradores de los clientes tengan también los permisos vigentes de root sobre nfsd

Por más información ver la páqina man (man exports(5))

Para iniciar el servidor NFS:

- `$ /etc/init.d/nfs-kernel-server start`

Puertos que usa NFS Hay que tener abiertos en el firewall los puertos: 111, 2049 y 32771.

12.2 Cliente

12.2.1 Instalación

Si no se dispone del cliente NFS, se puede instalar de la siguiente manera:

- `$ apt-get install nfs-common`

Montar manualmente

Para montar manualmente una carpeta compartida en otra máquina, se hace mediante el comando:

- `$ mount <equipo_remoto>:/<directorio_compartido> /<directorio_local>`

El directorio local debe de existir antes de querer montarle la carpeta compartida.

Montar automáticamente

Para esto hay que editar el archivo fstab:

- `$  vi /etc/fstab`

y agregar la siguiente linea:

```
<equipo_remoto>:/<directorio_compartido> /<directorio_local> nfs
rsize=8192,wsize=8192,timeo=14,intr
```

Para probar la configuración, hay que usar el comando:

- `$ mount /<directorio_local>`

13 Samba

El cliente samba viene instalado por defecto en Ubuntu, no así el servidor samba.

13.1 Instalación

Para instalar el servidor samba:

- `$ apt-get install samba`

Instalar interfaz gráfica

Interfaz gráfica para el samba:

- `$ apt-get install system-config-samba`

13.2 Configuración

Para configurar samba hay que editar el archivo /etc/samba/smb.conf. Lo primero es configurar correctamente el grupo de trabajo, buscando y editando la siguiente linea:

```
[global]
workgroup = WORKGROUP
```

Cambiando WORKGROUP por nuestro grupo de trabajo.

Luego agregamos la carpeta que queremos compartir:

```
[public]
comment = Public Folder
path = /home/public
public = no
writable = yes
create mask = 0777
directory mask = 0777
```

Explicación de las sentencias anteriores:

- comment: comentario sobre el recurso compartido
- path: direcotorio compartido
- public: si es o no de acceso público
- writable: si es de sólo lectura o si es de lectura y escritura
- create mask:
- directory mask:

Aclaración: debemos darle a la carpeta del sistema que compartimos, los permisos necesarios para que el usuario que use samba pueda leer y/o escribir en ella. Ejemplo:

- `$ chmod 777 /home/public`

Para autenticar el usuario (del sistema), descomentar la linea:

```
security = user
```

ó sustituirla por:

```
security = SHARE
```

para que quede compartida sin autenticación de usuario

Luego de terminar los cambios reiniciamos el servidor samba:

- `$ /etc/init.d/smbd restart`

13.3 Acceso a las carpetas compartidas

Desde Windows

Desde Windows colocamos en la barra de direcciones de alguna ventana: \\<ip_equipo_remoto>\<carpeta_compartida>

Desde Linux

Desde Linux (que tenga instalado el paquete samba-client) abrimos una carpeta y colocamos en la barra de direcciones: smb://<ip_equipo_remoto>/<carpeta_compartida>/

14 DokuWiki

DokuWiki es un wiki principalmente orientado a la creación de documentación de cualquier tipo. Está destinado a equipos de desarrolladores, grupos de trabajo y pequeñas compañías. Tiene una sintaxis sencilla pero potente que asegura que los archivos de datos se puedan leer desde fuera del wiki y facilita la creación de textos estructurados. Toda la información se guarda en archivos de texto plano, no necesita ninguna base de datos.

14.1 Requisitos de instalación:

- Servidor de páginas web con soporte de PHP: preferiblemente apache2 aunque se admiten otras alternativas.
- PHP versión 5.1.2 o superior. Las versiones más recientes desde el año 2009 han abandonado el soporte para PHP 4.
- Se recomienda disponer de las extensiones gráficas GD2 incluidas con determinadas versiones de PHP.

14.2 Instalación:

1. Descargar la última versión de dokuwiki
   - `wget http://www.splitbrain.org/_media/projects/dokuwiki/dokuwiki-2011-05-25a.tgz`
2. Descomprimir el archivo
   - `$ sudo tar -vxzf dokuwiki-2011-05-25a.tgz`
3. Crear una carpeta con el contenido del dokuwiki
   - `$ sudo mv dokuwiki-2011-05-25a dokuwiki`
4. Mover dicha carperta a /var/www
   - `$ sudo mv dokuwiki /var/www/dokuwiki`
5. Cambiarle los permisos de configuración para que se pueda correr el script
   - `$ sudo chmod a+w /var/www/dokuwiki/conf/`

Nota: puede que necesite más permisos de en /var/www/dokuwiki/data, por ejemplo en pages, attic, media, meta, cache, locks, index, tmp.

14.3 Configurar apache

1. Crear una entrada en el archivo /etc/apache2/sites-available:
   - `cp /etc/apache2/sites-available/default /etc/apache2/sites-available/dokuwiki`
2. Editar el archivo /etc/apache2/sites-available/dokuwiki
   - `$ sudo vi /etc/apache2/sites-available/dokuwiki` Y modificar la línea:
     - Modificando: `Documentroot /var/www` a `Documentroot /var/www/dokuwiki`
     - Luego desde el directorio /etc/apache2/ ejecutar el siguiente comando:
       - `$ sudo a2ensite dokuwiki`
     - Esto activa el servicio dokuwiki creando una entrada para el mismo en /etc/apache2/sites-enabled
   - Reiniciar el servicio apache:
     - `$ sudo /etc/init.d/apache2 restart`

Para verificar que se instaló correctamente ir a: http://taller.curerocha.edu.uy/dokuwiki

15 MediaWiki

15.1 Requisitos Previos

Para poder instalar Mediawiki es necesario disponer de:

- Apache2
- PHP5
- MySQL

15.2 Instalación

1. Descargar la última versión de Mediawiki desde la página oficial de mediawiki:
   http://download.wikimedia.org/mediawiki/1.16/mediawiki-1.16.5.tar.gz
2. Descomprimir el archivo:
   sudo tar -vxzf mediawiki-1.16.5.tar.gz
3. Renombrar la carpeta:
   sudo mv mediawiki-1.16.5 mediawiki
4. Colocar el directorio mediawiki en el directorio /var/www/:
   sudo mv mediawiki /var/www/mediawiki
5. Para correr el script de instalación, el directorio /var/www/mediawiki/config debe tener permisos de escritura (sólamente para el proceso de instalación):
   sudo chmod a+w /var/www/mediawiki/config/

15.3 Configurar Apache

1. crear una entrada en /etc/apache2/sites-available/:
   cp /etc/apache2/sites-available/default /etc/apache2/sites-available/mediawiki
2. Editar el archivo creado:
   sudo vi /etc/apache2/sites-aviable/mediakiki
   Modificando Documentroot /var/www a Documentroot /var/www/tikiwiki
3. Luego desde el directorio /etc/apache2/ ejecutar el siguiente comando:
   sudo a2ensite mediawiki
   Esto activa el servicio mediawiki creando una entrada para el mismo en /etc/apache2/sites-enabled
4. Reiniciar el servicio apache:
   sudo /etc/init.d/apache2 restart
5. Ya podemos ingresar por la web (http://taller.curerocha.edu.uy/mediawiki) para culminar con la instalación.

15.4 Captchas

- Configuración de captchas para mediawiki:
- Primero hay que descargar la extensión ConfirmEdit para la versión de mediawiki instalada (archivo tar.gz).
- Descomprimir el archivo descargado en la carpeta "extension" del directorio de instalación de mediawiki.

En el archivo de configuración de mediawiki (LocalSettings.php) agregar la siguiente linea:

```
$ require_once( "$IP/extensions/ConfirmEdit/ConfirmEdit.php" );
```

16 Tikiwiki

16.1 Requisitos Previos

Para poder instalar esta wiki es necesario tener funcionando Apache2, PHP5 y MySQL

- sudo apt-get update
- sudo apt-get upgrade
- sudo tasksel

Seleccionar la opción de LAMP, les pedirá la clave de MySQL.

16.1.1 Instalación

Descargar la última versión de Tikiwiki:

- sudo wget http://softlayer.dl.sourceforge.net/sourceforge/tikiwiki/tikiwiki-3.1.tar.gz

Descomprimir el archivo:

- `$ sudo tar -xvzf tikiwiki-3.1.tar.gz`
- `$ sudo mv tikiwiki-3.1 tikiwiki`
- `$ sudo mv tikiwiki /var/www/tikiwiki`
- `$ cd /var/www/tikiwiki`
- `$ sudo sh setup.sh`

Desplegara la siguiente información:

```
User (www-data):
Group (www-data):
Multi ():
Checking dirs:
backups ... ok.
db ... ok. dump ... ok.
img/wiki ... ok.
img/wiki_up ... ok.
img/trackers ... ok.
modules/cache ... ok.
temp ... ok.
temp/cache ... ok.
templates_c ... ok.
templates ... ok.
styles ... ok.
maps ... ok.
whelp ... ok.
mods ... ok.
files ... ok.
tiki_tests/tests ... ok.
lib/Galaxia/processes ... ok.
Fix global perms ... chowned ... done. Fix special dirs ... done.
```

16.2 Configurar Apache

- `$ sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-available/tikiwiki`
- `$ sudo vi /etc/apache2/sites-available/tikiwiki`

Modificar `Documentroot /var/www` a `Documentroot /var/www/tikiwiki`

- `cd /etc/apache2/`
- `a2ensite tikiwiki`
- `$ sudo /etc/init.d/apache2 restart`

16.3 Creación de la base de datos para Tikiwiki:

- Acceder a Phpmyadmin: https://base-de-datos.taller.curerocha.edu.uy/
- Loguearse
- Solapa Base de datos
- Crear nueva base de datos con el nombre Tikiwiki
- Acceder a la wiki: http://tikiwiki.taller.curerocha.edu.uy/
- A partir de acá hay una guía para la configuración de la wiki
- Sera necesario además instalar un servidor de correo como postfix
- Link Wiki: http://tikiwiki.taller.curerocha.edu.uy/
- Ingresar con el susuario admin
- La contraseña esta en paloma: /root/adminSysCure/Tikiwiki.txt
- Y pueden luego crearse su usuario

17 Respaldos en Servidores Paloma y Polonio

17.1 Crear partición para respaldos.

Los respaldos se realizaron en los segundos discos de cada servidor, (/dev/sdb).

Crear Volúmenes Físicos (PV)

Para poder usar un dispositivo de almacenamiento con el LVM lo primero es inicializarlo, para ello se usa el comando seguido del nombre del dispositivo o los dispositivos de bloques a inicializar. Así, si queremos inicializar el segundo disco, podríamos usar el comando:

```
$ pvcreate /dev/sdb
```

```
Physical volume "/dev/sdb" successfully created
```

17.1.1 Crear Grupos de Volúmen (VG)

Una vez que tenemos inicializados el volúmen físico (o varios volúmenes) hay que crear un Grupo de Volúmen, de está forma se obtiene algo así como un área de almacenamiento cuya capacidad es la suma de las capacidades de todos los Volúmenes Físicos que lo forman. Para crear un nuevo Grupo de Volúmen se emplea el comando vgcreate, con el primer parámetro se especifica el nombre que tendrá el Grupo de Volúmen, a continuación, se indica la lista de Volúmenes Físicos que formarán el Grupo de Volúmen. Básicamente, la sintaxis es la siguiente:

```
vgcreate nombre_del_vg volúmen_físico [volúmen_físico ...]
```

Ejemplo:

```
vgcreate respaldos /dev/sdb
```

17.1.2 Crear Volúmenes Lógicos (LV)

Una vez dispongamos de un Grupo de Volúmen, es hora de distribuir su espacio en Volúmenes Lógicos sobre los que poder crear sistemas de archivos. Para crear un Volúmen Lógico se emplea el comando lvcreate, su sintaxis es la siguiente:

```
lvcreate {-L/--size tamaño} {-n/--name nombre_del_lv} nombre_del_vg
```

Con la opción -L o --size se especifica el tamaño que tendrá el Volúmen Lógico, si no se especifica ningún sufijo, se asumirá que es en megabytes, los sufijos que se pueden usar son: K para kilobytes, M para megabytes, G para gigabytes y T para terabytes. La opción -n o –name sirve para establecer el nombre que tendrá el Volúmen Lógico, si no se especificase un nombre entonces se establecería uno del tipo lvol#, donde # es número interno asignado al Volúmen Lógico. El último parámetro que hay que indicarle al comando es el Grupo de Volúmen donde se creará el Volúmen Lógico.

Ejemplo:

```
lvcreate -L 100G -n paloma respaldos
```

Por cada Volúmen Lógico que tengamos, se creará un dispositivo dentro de que estará compuesto por el nombre del Grupo de Volúmen, un guión y el nombre del Volúmen Lógico, por ejemplo, si el Grupo de Volúmen se llama respaldos y la Volúmen Lógico que hemos creado se llama paloma, entonces se creará el dispositivo /dev/mapper/respaldos-paloma. Por otro lado, también se creará un enlace simbólico con la forma /dev/grupo_de_volúmen/volúmen_lógico, en el caso del ejemplo, se llamaría: /dev/respaldos/paloma.

Crear un sistema de archivos en un Volúmen Lógico

Una vez que tenemos un Volúmen Lógico, podemos usar su dispositivo como un dispositivo de bloques en el que crear un sistema de archivos. Ejemplo, para crear un sistema de archivos ext3 en el Volúmen Lógico perteneciente al servidor de paloma:

```
mkfs.ext4 /dev/mapper/respaldos-paloma
```

Fichero /etc/fstab

Este fichero indica como montar cada dispositivo y de qué configuración utilizar. Lista los discos y particiones disponibles. Aquí debemos agregar una nueva entrada para nuestra nueva partición, para que el sistema lo lea cada vez que se inicia. La sintaxis de este fichero es la siguiente:

```
<dispositivo> <punto_de_montaje> <sistema_de_archivos> <opciones> <dump-freq> <pass-num>
```

Ejemplo:

```
/dev/mapper/respaldos-paloma /respaldos  ext4   defaults     0 2
```

Montar partición

Para montar la nueva partición primero tenemos que crear la carpeta donde queremos montarla:

```
$ mkdir respaldos
```

Luego montar la partición en el directorio:

```
$ mount /dev/mapper/respaldos-polonio /respaldos
```

17.2 Respaldos.

Se creó un script con el fin de respaldar la información de que contienen los servidores (paloma y polonio). Cada servidor guardará un respaldo de si mismo y una copia del respaldo del otro servidor, obteniendo así más seguridad en caso de fallas en el sistema.

Procedimiento

1. Creación de usuario 'respaldo' para realizar los backups y agregado del mismo al grupo admin:

   ```
   $ adduser respaldo admin
   ```

2. Agregar la siguiente línea al archivo /etc/sudoers para permitir al usuario 'respaldo' que utilize sudo sin ingresar contraseña, ya que el script se va a ejecutar automáticamente y varios de los comandos que lo componen necesitan que le usuario tenga privilegios de administrador:

   ```
   respaldo ALL=NOPASSWD: ALL
   ```

3. Generar una clave pública para el usuario respaldo y copiarla en el otro servidor para que el usuario respaldo pueda hacer scp de un servidor al otro para copiar sus archivos de respaldo.
   En la primer línea generamos la clave y en la segunda la copiamos en el otro servidor

   ```
   respaldo@paloma$ ssh-keygen -t rsa -C "respaldo"

   ssh-copy-id respaldo@10.5.2.2
   ```

4. Crear el script, este está ubicado en /home/respaldo, y fue nombrado respaldo.sh, tanto el de paloma como el de polonio son esencialmente lo mismo, varían dependiendo de las necesidades de cada servidor que cosas respaldar, a continuación se muestra el script creado para el servidor paloma, es igual al de polonio pero agregando respaldo a las base de datos:

   ```
   #!/bin/sh
   #
   #Realizar backup de mysql como usuario root, a todas la bases de datos existentes, y
   #guardar la salida en el archivo /respaldos/respaldo_db.sql.
   sudo mysqldump -uroot -pRuvdansh7jun --all-databases > /respaldos/respaldo_db.sql
   #
   #Generar un archovo tar del archivo respaldo_db.sql.
   sudo tar -zcvf /respaldos/respaldo_db_$(date +%d%m%y).tgz /respaldos/*.sql
   #
   #Respaldar el directorio /etc/apache2
   sudo cp -r /etc/apache2/ /respaldos/respaldo_apache2/
   ```

```
#Respaldar el directorio /etc/bind
sudo cp -r /etc/bind/ /respaldos/respaldo_bind/
#Respaldar el directorio /home
sudo cp -r /home/ /respaldos/respaldo_home/
#Respaldar el directorio /var/www
sudo cp -r /var/www/ /respaldos/respaldo_www/
#
#
#Generar un archivo tar con todos los directorios de respaldo generados
anteriormente.
sudo tar -zcvf /respaldos/respaldo_arch_$(date +%d%m%y).tgz
/respaldos/respaldo_apache2/ /respaldos/respaldo_bind/ /respaldos/respaldo_home/
/respaldos/respaldo_www/
#
#Borrar las carpetas.
sudo rm -r /respaldos/respaldo_www/ /respaldos/respaldo_apache2/
/respaldos/respaldo_bind/ /respaldos/respaldo_home/  /respaldos/respaldo_db.sql
#
#
#Buscar los archivos que tengan mas de 2 dias y eliminarlos.
sudo find -name '*.tgz' -type f -mtime +2 -exec rm -f {} \;
#
#
#Crear un tar con todos los respaldos del día para enviar a polonio
sudo tar -zcvf /respaldos/paloma_$(date +%d%m%y).tgz
respaldos/respaldo_arch_* /respaldos/respaldo_db_*
#
#Copiar el respaldo al servidor polonio vía scp
scp respaldo@localhost:/respaldos/paloma_*    respaldo@10.5.2.2:/respaldos/paloma/
```

5. Agregar una entrada en el fichero crontab para que el script se ejecute automáticamente en un horario en el que estimamos que la red no está siendo utilizada. El usuario encargado de ejecutar el script es 'respaldo':

```
#sudo crontab -e
# m h  dom mon dow   command
15 2 * * * /home/aline/respaldo.sh respaldo
```