TFC GNU/Linux

I-FORMA.COM

01/2012

Alejandro Ripoll Hoyos

Contenido

1. Introducción

En este proyecto llevaremos a cabo el diseño y la implantación de una arquitectura de sistemas basados en GNU/Linux.

Para ello, tomaremos como caso de estudio la solicitud de una hipotética empresa cliente y detallaremos el proceso de diseño e implementación de forma que la infraestructura final satisfaga todos los requerimientos iniciales.

En este apartado introductorio presentamos el caso de estudio, así como los requerimientos y el alcance del proyecto. Como último punto se incluye la planificación temporal inicial.

1.1. Caso de estudio

I-forma.com, una microempresa de nueva creación dedicada a la formación online, nos ha solicitado el diseño y la implantación de la infraestructura informática de su oficina. En dicha oficina trabajarán cinco administrativos, un coordinador y un informático encargado de las tareas de soporte y mantenimiento de la infraestructura.

La oficina dispone de una línea ADSL simétrica con dirección *ip* fija que utilizará tanto para el acceso a los servicios externos como para el acceso a internet desde la propia oficina. El resto de equipos e infraestructura de red se adquirirán de acuerdo a la arquitectura de sistemas propuesta.

1.1.1. Requerimientos funcionales

A través del análisis de requerimientos del cliente hemos obtenido la siguiente lista de requerimientos funcionales:

- Servicio web accesible desde el exterior que hospede la plataforma de tele-formación y la web informativa de la empresa. También desean disponer de estadísticas de uso de ambos sitios web.
- Servicio de correo electrónico con antivirus y antispam para correo interno y comunicación con los alumnos.
- Estaciones de trabajo para cada uno de los trabajadores de la empresa con autenticación centralizada.
- Directorio de trabajo compartido.
- Acceso web externo al correo electrónico. Esto resulta necesario para que los tutores dispongan de una cuenta de correo de la empresa para la comunicación con los alumnos.

- Servicio de impresión compartida desde cualquier estación de trabajo. Se dispondrá de una impresora laser conectada al equipo del coordinador.

1.1.2. Requerimientos de seguridad y continuidad del negocio

A través del análisis de requerimientos del cliente hemos obtenido la siguiente lista de requerimientos de seguridad y continuidad del negocio:

- Navegación web restringida para el personal administrativo excepto a un listado de sitios autorizados.
- El acceso de los tutores al correo electrónico vía web debe limitarse mediante certificados cliente ssl. Dichos certificados serán emitidos por la propia empresa y se revocarán tras la fecha de finalización del curso.
- La administración remota de los servidores y equipos de trabajo sólo será accesible desde el puesto de trabajo del infórmatico.
- Los permisos del directorio de trabajo compartido deben ser configurables en base a usuarios y grupos.
- Se deben realizar copias de seguridad diarias del directorio de trabajo compartido y el correo electrónico para recuperación en caso de desastre.
- Los cortes de servicio en la plataforma de tele-formación deben reducirse al mínimo al tratarse de un servicio crítico para el negocio. Por ello será necesario disponer de un sistema de alta disponibilidad.
- Se deben definir los planes de contingencia en caso de caída de cualquiera de los equipos de la infraestructura.

1.1.3. Requerimientos económicos

Al tratarse de una nueva empresa el presupuesto inicial es limitado por lo que se debe reducir, en la medida de lo posible, el gasto en infraestructura y licencias.

1.1.4. Otros requerimientos

Toda la infraestructura debe diseñarse de forma que resulte escalable en caso de crecimiento de la empresa, definiendo además el plan a seguir en los siguientes supuestos:

- Mayor número de trabajadores.
- Mayor espacio de almacenamiento compartido.
- Mayor número de usuarios en la plataforma de tele-formación.

1.2. Alcance del proyecto

Diseñar la infraestructura informática teniendo en cuenta las especificaciones del cliente y sus requerimientos. Deberemos identificar las necesidades implícitas (servidores, infraestructura de comunicaciones, necesidades de impresión), definir las políticas de seguridad tanto internas (quién tiene acceso y a qué), como externas (firewall, DMZ's, conexiones seguras,…).

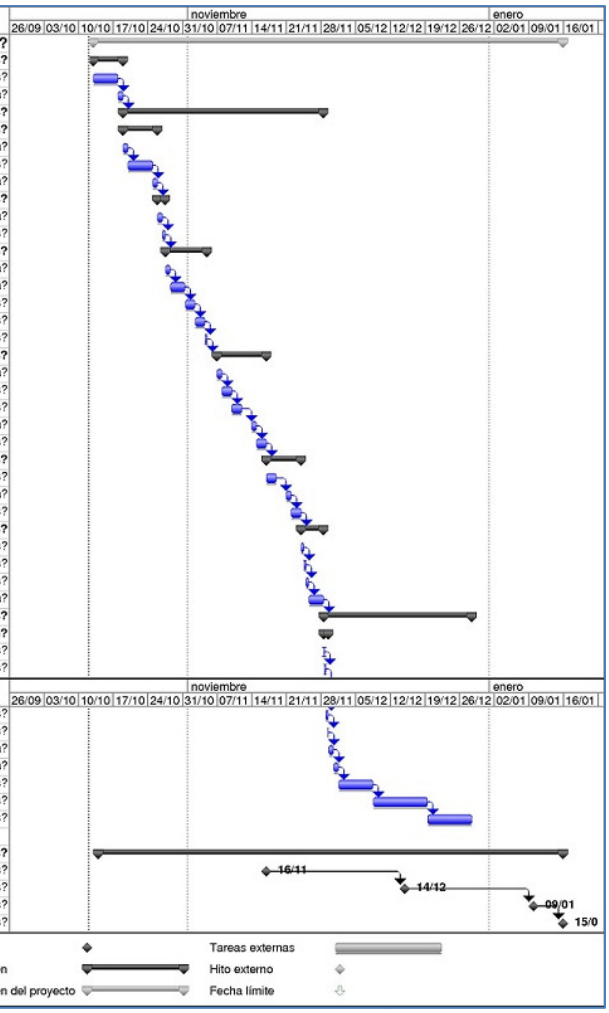
Planificaremos todo el proceso de implantación del sistema en sus distintas fases (diseño, desarrollo, despliegue).

Estableceremos las políticas de mantenimiento del entorno y las tareas necesarias (rotado de ficheros de log, copias de seguridad,…).

1.3. Planificación inicial

El proyecto seguirá la siguiente planificación temporal:

Id	Nombre de tarea	Duración
0	**Proyecto TFC**	**67 días?**
1	**Análisis y diseño**	**4 días?**
2	Diseño de la infraestructura	3 días?
3	Selección de SO y software base	1 día?
4	**Implantación**	**28,5 días?**
5	**Implantación inicial**	**5 días?**
6	Creación de máquinas virtuales	1 día?
7	Instalación de SO	3 días?
8	Configuración de red	1 día?
9	**Instalación del firewall**	**1,5 días?**
10	Definición de reglas de acceso	1 día?
11	Instalación del servidor de hora	0,5 días?
12	**Instalación del servidor corporativo**	**6,5 días?**
13	Instalación del servicio dns	1 día?
14	Instalación del servicio de almacenamiento compartido	1 día?
15	Instalación del servicio ldap	2 días?
16	Instalación del servicio proxy	2 días?
17	Instalación de la entidad certificadora interna	0,5 días?
18	**Instalación del servidor web**	**8 días?**
19	Instalación de software base	1 día?
20	Instalación de la plataforma de tele-formación	2 días?
21	Instalación de la web informativa	2 días?
22	Instalación del sistema de generación de estadísticas de uso	1 día?
23	Configuración de alta disponibilidad	2 días?
24	**Instalación del servidor de correo electrónico**	**5 días?**
25	Instalación de software base	2 días?
26	Instalación y configuración del sistema de antispam y antivirus	1 día?
27	Instalación de servicio webmail	2 días?
28	**Instalación de los puestos de trabajo**	**2,5 días?**
29	Integración con ldap	0,5 días?
30	Configuración del correo electrónico	0,5 días?
31	Configuración del almacenamiento compartido	0,5 días?
32	Configuración de impresora compartida	1 día?
33	**Post-Implantación**	**22 días?**
34	**Tareas de mantenimiento**	**1 día?**
35	Copia de seguridad del correo electrónico	0,25 días?
36	Copia de seguridad del directorio compartido	0,25 días?
37	Copia de seguridad de la base de datos	0,25 días?
38	Rotado y compresión de ficheros de log	0,25 días?
39	Propuestas para para ampliación de la infraestructura	1 día?
40	Definición de planes de contingencia	1 día?
41	Pruebas	5 días?
42	Revisión de la documentación	7 días?
43	Realización del video de presentación	7 días?
44		
45	**PECS**	**66 días?**
46	PEC2	24 días?
47	PEC3	20 días?
48	PEC4	18 días?
49	PEC5	4 días?



Proyecto: Proyecto TFC
Fecha: mié 12/10/11

Tarea · División · Progreso · Hito · Resumen · Resumen del proyecto · Tareas externas · Hito externo · Fecha límite

2. Diseño

En esta fase del proyecto se definen todos los elementos que conformarán la infraestructura informática y servirá como modelo de cara a la implementación.

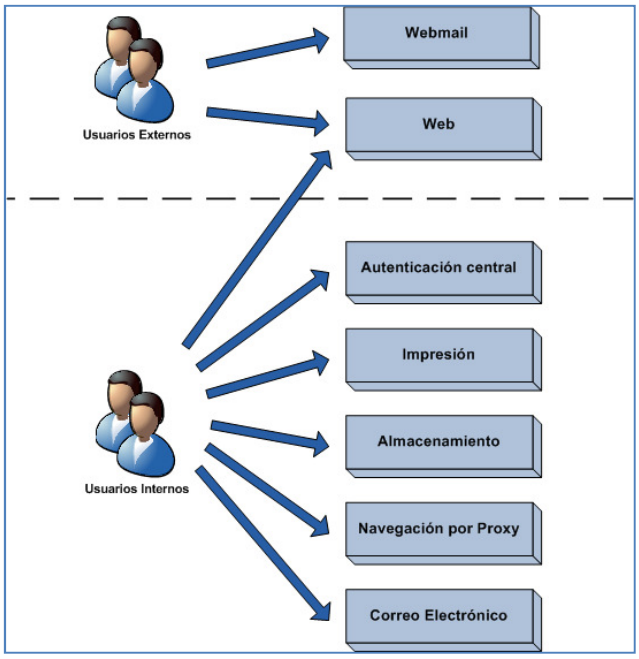
En primer lugar, hemos analizado los requerimientos del cliente para obtener un listado de servicios a implementar. A continuación hemos definido la arquitectura y la estructura física de la red y, por último, seleccionamos el software a utilizar y el estándar de nombres y direcciones de red.

2.1. Arquitectura de servicios

A través del análisis de los requerimientos del cliente obtenemos una lista de servicios, así como el tipo de usuario (interno o externo) que requiere acceso al mismo.[1]

Utilizaremos esta información para disponer los servicios en distintas redes de acuerdo al tipo de accesos.

Ilustración 1 - Arquitectura de servicios



[1] No aparecen representados en el esquema los servicios que, aunque no han sido especificados por el cliente, resultan necesarios para el buen funcionamiento de la infraestructura como el servicio de sincronización horaria o el de resolución de nombres local.

2.2. Arquitectura de red

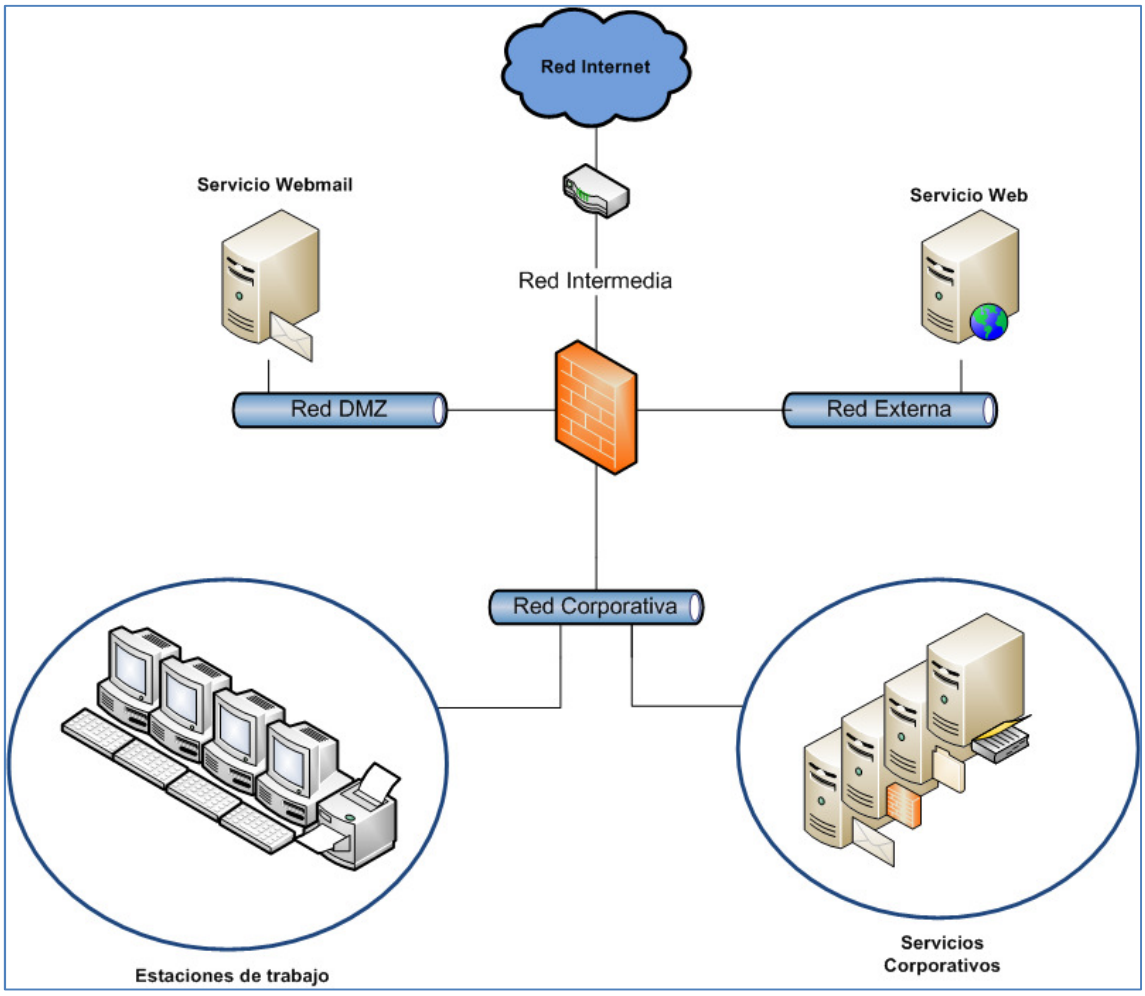
A la vista de la arquitectura de servicios, necesitaremos situar los servicios en, al menos, dos redes diferentes, en base al tipo de usuarios que accederán a ellos. Llamaremos a estas redes Red Externa y Red Corporativa.

El servicio de webmail requiere consideraciones especiales ya que, a pesar de ser utilizado por usuarios externos, se realizarán conexiones desde el mismo hacia el servicio de correo corporativo. Por razones de seguridad, situaremos este servicio en una nueva red a la que llamaremos Red DMZ.

Para la conexión entre las diferentes redes se configurará un servidor que realizará las tareas de enrutamiento y control de accesos (cortafuegos). Definiremos también la Red Intermedia como la que une el router ADSL y el cortafuegos, y la Red Internet en la que englobaremos cualquier dirección externa a nuestra red.

En el siguiente esquema puede observarse la estructura lógica de red:

Ilustración 2 - Arquitectura de red

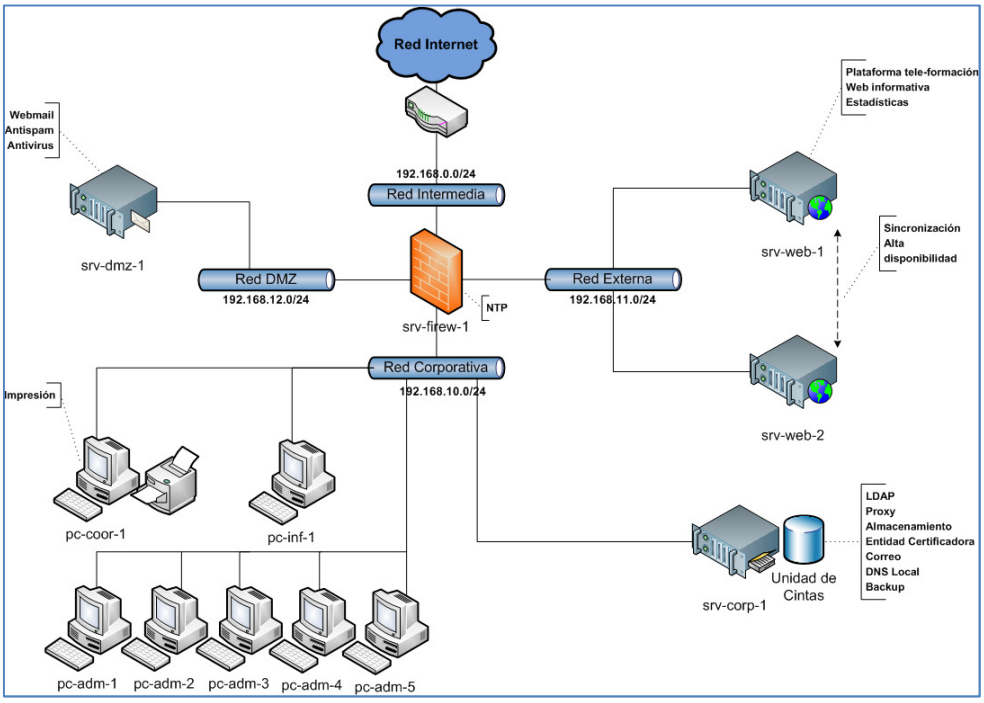


2.3. Distribución física de la infraestructura

Tras el diseño preliminar de la arquitectura de servicios y de red pasamos ahora a definir la distribución física de los diferentes dispositivos y equipos. Utilizando como base la arquitectura de red del apartado anterior hemos situado los servidores y estaciones de trabajo y distribuido los distintos servicios.

El siguiente esquema muestra la arquitectura completa:

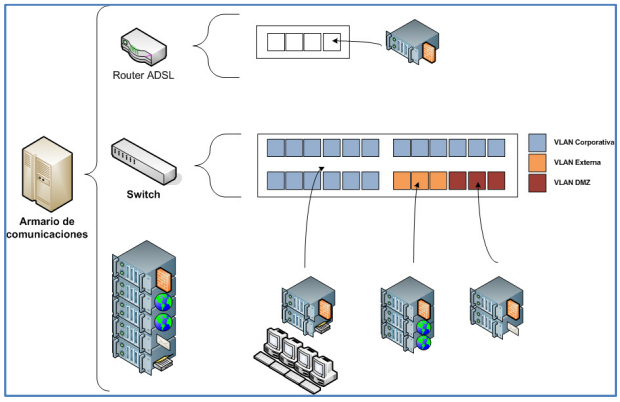
Ilustración 3 - Esquema de red



En la ilustración 4 puede observarse la disposición física de los equipos en el armario de comunicaciones, así como el esquema de conexiones de red.

Hemos asignado los puertos del *switch* a distintas *VLANS* [2] para cada red de modo que podamos simular una separación física sin necesidad de utilizar dispositivos diferentes para ello.

Ilustración 4 - Esquema de conexiones



[2] http://es.wikipedia.org/wiki/VLAN

2.4. Estándar de nombres y direcciones de red

A modo de referencia, definimos el estándar a seguir para los nombres y direcciones de red que se usarán durante la implantación.

En primer lugar, hemos seleccionado rangos de direcciones privadas de clase C para cada una de las redes (tabla 1).

Tabla 1 - Direcciones de red

Red	Dirección de red
Intermedia	192.168.0.0/24
Corporativa	192.168.10.0/24
Externa	192.168.11.0/24
DMZ	192.168.12.0/24

Dentro de la red corporativa designamos también distintos rangos de direcciones según el tipo de equipo. Esta separación será tan sólo administrativa, con el fin de facilitar la gestión (tabla 2).

Tabla 2 - Subredes administrativas

Grupo	Rango de direcciones
Servidores corporativos	192.168.10.1 – 192.168.10.9
Informaticos	192.168.10.10 – 192.168.10.19
Coordinadores	192.168.10.20 – 192.168.10.29
Administrativos	192.168.10.30 – 192.168.10.254

Por último, definimos la política a seguir en los nombres de equipo. Todos ellos seguirán el siguiente formato: TIPO-FUNCION-NODO.DOMINIO[3]

Tabla 3 - Nombres y direcciones de red

Dispositivo	Dirección de red	Nombre de host
Router ADSL	192.168.0.1/24 1.2.3.4 (ip pública)	dev-router-1.i-forma.local
Cortafuegos	192.168.0.2/24 192.168.10.1/24 192.168.11.1/24 192.168.12.1/24	srv-firew-1.i-forma.local
Servidor DMZ	192.168.12.2/24	srv-dmz-1.i-forma.local
Servidor Web 1	192.168.11.2/24	srv-web-1.i-forma.local
Servidor Web 2	192.168.11.3/24	srv-web-2.i-forma.local
Servidor Corporativo	192.168.10.2/24	srv-corp-1.i-forma.local
PC Informatico 1	192.168.10.10/24	pc-inf-1.i-forma.local
PC Coordinador 1	192.168.10.20/24	pc-coor-1.i-forma.local
PC Administrativo 1	192.168.10.30/24	pc-adm-1.i-forma.local
PC Administrativo 2	192.168.10.31/24	pc-adm-2.i-forma.local
PC Administrativo 3	192.168.10.32/24	pc-adm-3.i-forma.local
PC Administrativo 4	192.168.10.33/24	pc-adm-4.i-forma.local
PC Administrativo 5	192.168.10.34/24	pc-adm-5.i-forma.local

[3] En ocasiones haremos referencia a los equipos omitiendo el dominio ya que, en todos los casos, este será i-forma.local.

2.5. Elección de sistema operativo y software base

Como sistema operativo hemos optado por distribuciones GNU/Linux de la rama RedHat. En concreto utilizaremos *Fedora* para las estaciones de trabajo y *CentOS* para los servidores. Estas distribuciones presentan una serie de ventajas:

- Estabilidad.
- Disponibilidad de software.
- Documentación.
- Continuidad en las actualizaciones.
- Libre uso.

Fedora
Sitio web: http://fedoraproject.org/es/
Distribución GNU/Linux para estación de trabajo.

CentOS
Sitio web: http://www.centos.org/
Distribución GNU/Linux para servidor.

Como software base utilizaremos exclusivamente proyectos de software libre:

Netfilter – iptables
Sitio web: http://www.netfilter.org/projects/iptables/
Filtrado de paquetes.

Apache HTTP Server
Sitio web: http://httpd.apache.org/
Servidor web.

PHP
Sitio web: http://www.php.net/
Lenguaje scripting para sitios web dinámicos.

MySQL
Sitio web: http://www.mysql.com/
Motor de bases de datos.

Drupal
Sitio web: http://drupal.org.es/
Gestor de contenidos en lenguaje PHP.

Moodle
Sitio web: http://moodle.org/
Plataforma de tele-formación en lenguaje PHP.

AWStats
Sitio web: http://awstats.sourceforge.net/
Generador de estadísticas de acceso.

DRBD
Sitio web: http://www.drbd.org/
RAID en red.

Heartbeat
Sitio web: http://linux-ha.org/
Alta disponibilidad.

OpenSSL
Sitio web: http://www.openssl.org/
Librería SSL.

OpenLDAP
Sitio web: http://www.openldap.org/
Servicio de directorio LDAP.

Squid
Sitio web: http://www.squid-cache.org/
Servicio de proxy.

Bind
Sitio web: http://www.isc.org/software/bind
Servicio de resolución de nombres.

Postfix
Sitio web: http://www.postfix.org/
Servicio de correo (SMTP).

Cyrus-sasl
Sitio web: http://www.cyrusimap.org/
Autenticación SMTP.

Dovecot
Sitio web: http://dovecot.org/
Servicio POP3/IMAP.

Roundcube
Sitio web: http://roundcube.net/
Servicio webmail en PHP.

ClamAV
Sitio web: http://www.clamav.net/
Antivirus.

SpamAssassin
Sitio web: http://spamassassin.apache.org/
Antispam.

3. Implantación inicial

En esta fase, realizamos las tareas comunes a toda la infraestructura y aquellas que son un prerrequisito para las fases posteriores, como la instalación del sistema operativo o la configuración de red. Las tareas realizadas son las siguientes:

- Creación de registros DNS externos.
- Configuración del router ADSL.
- Instalación de sistema operativo en servidores y estaciones de trabajo.
- Configuración de red.

Una vez completadas estas tareas dispondremos de una arquitectura de sistemas, con un sistema operativo funcional en cada uno de ellos, así como la configuración de red necesaria para la comunicación entre estos sistemas. También creamos en esta fase los registros dns externos y el reenvío de puertos en el router ADSL que serán necesarios para el acceso externo a los servicios.

3.1. Registros DNS externos

Para el acceso a los servicios desde el exterior necesitamos configurar los registros dns del dominio i-forma.com. Supondremos que la gestión del dominio y sus servidores autoritativos están alojados en un proveedor de servicios externo.

Creamos los registros de tipo A apuntando a nuestra dirección ip pública y los alias necesarios para el acceso a todos los servicios. Asimismo necesitaremos un registro de tipo MX para la recepción de correo electrónico[4].

Por último, creamos un registro SPF[5] para especificar la lista de direcciones *ip* autorizadas a enviar correos electrónicos con un remitente de nuestro dominio. La comprobación o no de estos registros (y por lo tanto su efectividad) depende del servidor de correo electrónico receptor, pero su uso está lo bastante extendido como para que resulte interesante configurarlo.

Tabla 4 - Registros DNS externos

Registro	Tipo	Valor
@	A	1.2.3.4
www	A	1.2.3.4
correo	CNAME	www
webmail	CNAME	www
cursos	CNAME	www
@	MX 10	correo
@	TXT	"v=spf1 mx ~all"

[4] http://es.wikipedia.org/wiki/Domain_Name_System#Tipos_de_registros_DNS
[5] http://es.wikipedia.org/wiki/Sender_Policy_Framework

Con el fin de evitar problemas en el envío de correo al exterior, será necesario configurar un registro de resolución dns inversa para nuestra *ip* pública de modo que la resolución directa e inversa de la misma coincida. Muchos proveedores de correo electrónico incorporan esta comprobación como medida antispam por lo que resulta casi obligatorio para evitar que dichos envíos se rechacen. La creación de este registro debe solicitarse a nuestro proveedor de red.

Tabla 5 - Resolución inversa de la ip pública.

Registro	Tipo	Valor
4	PTR	correo.i-forma.com.

3.2. Configuración router ADSL

Necesitamos realizar dos cambios de configuración en el router ADSL. En primer lugar, debemos añadir rutas estáticas para las redes internas para permitir la comunicación. Esto es necesario ya que, para el router, la red intermedia que lo une con el cortafuegos es la única visible.[6]

Las tres rutas estáticas a añadir en el router para la comunicación con las redes internas serían las siguientes:

Tabla 6 - Rutas estáticas.

Destino	Máscara	Puerta de enlace
192.168.10.0	255.255.255.0	192.168.0.2
192.168.11.0	255.255.255.0	192.168.0.2
192.168.12.0	255.255.255.0	192.168.0.2

Al añadir estas rutas se hace posible la comunicación del router al resto de redes enrutando dichos paquetes a través del cortafuegos.

En segundo lugar, configuraremos el reenvío de puertos en el router ADSL para el acceso externo a los servicios. Cualquier acceso a los puertos 25, 80, 443 y 8443 en la *ip* pública del router será reenviado mediante un NAT de entrada al dispositivo que hospeda ese servicio.[7]

Tabla 7 - Reenvío de puertos.

Puerto público	Puerto privado	Destino	Servicio
25	25	192.168.12.2	SMTP
80	80	192.168.11.10	Web
443	443	192.168.11.10	Web (HTTPS)
8443	443	192.168.12.2	Webmail (HTTPS)

[6] Otra alternativa hubiera sido resolverlo mediante el uso de reglas de NAT en el cortafuegos.

[7] Podemos deshabilitar el acceso externo a los servicios en cualquier momento eliminando estas reglas de reenvio.

3.3. Instalación inicial de los servidores

Como sistema operativo para los servidores se ha optado por la distribución CentOS GNU/Linux. Esta distribución está orientada a equipos servidores en entornos empresariales y es compatible a nivel binario con RedHat Enterprise Linux. Los medios para la instalación de CentOS están disponibles para su descarga desde cualquiera de los repositorios oficiales.[8] Para el proyecto hemos seleccionado la versión CentOS 6 de 64 bits.

Una vez descargado el fichero de imagen lo instalaremos en todos los equipos servidor:

- *srv-firew-1.i-forma.local*
- *srv-web-{1..2}.i-forma.local*
- *srv-dmz-1.i-forma.local*
- *srv-corp-1.i-forma.local*

Realizamos una instalación por defecto de la distribución a excepción de los siguientes puntos:

- Idioma y teclado español.
- Perfil "Basic Server" (sin entorno gráfico).
- Modificar el particionado en *srv-web-{1..2}.* Añadiremos una partición dedicada para base de datos la cual se dejará sin formatear ni montar en el sistema de ficheros.

Tras completar la instalación accedemos al sistema para deshabilitar *selinux* e *iptables* y limitar el acceso ssh al mismo en el fichero hosts.allow. Para ello debemos ejecutar los siguientes comandos y modificar los ficheros de configuración.

Comandos 1 - Deshabilitar iptables.

```
# service iptables stop
# chkconfig iptables off
```

Configuración 1 - SELinux y hosts.allow.

```
/etc/selinux/config
/etc/hosts.allow
```

[8] http://www.centos.org/modules/tinycontent/index.php?id=30

3.4. Instalación inicial de las estaciones de trabajo

Para los equipos cliente hemos seleccionado la distribución orientada a estaciones de trabajo de la rama RedHat: Fedora. Esta distribución es de libre uso y los medios de instalación están disponibles desde su página oficial.[9] Descargamos la versión Fedora 15 de 32 bits y la instalamos en las estaciones de trabajo.

- *pc-adm-{1..5}.i-forma.local*
- *pc-inf-1.i-forma.local*
- *pc-coor.i-forma.local*

Durante la instalación se nos obliga a crear un usuario local que eliminaremos una vez se integré el sistema con LDAP. Tras completar la instalación debemos acceder al sistema para deshabilitar selinux e iptables y limitar el acceso ssh al mismo mediante hosts.allow.

Comandos 2 - Deshabilitar iptables.

```
# service iptables stop
# chkconfig iptables off
```

Configuración 2 - SELinux y hosts.allow.

```
/etc/selinux/config
/etc/hosts.allow
```

3.5. Configuración de red

Para la configuración de red modificamos los siguientes parámetros en cada uno de nuestros equipos:

- Nombre de host, dirección IP y máscara de red siguiendo lo especificado en el estándar de nombres y direcciones.
- Puerta de enlace: La interfaz correspondiente del firewall, o el router en el caso de srv-firew-1.
- Servidor DNS: El servidor corporativo srv-corp-1 (192.168.10.2). También configuraremos la variable search con valor "i-forma.local" para que puedan resolverse los nombres locales con o sin el dominio.[10]

Se listan a continuación los ficheros de configuración que han sido modificados en cada equipo.

[9] http://fedoraproject.org/es/get-fedora-options#formats

[10] En el caso de srv-corp-1 el servidor de nombres será localhost.

Configuración 3 - Configuración de red de srv-firew-1.

```
/etc/resolv.conf
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/ifcfg-eth1
/etc/sysconfig/network-scripts/ifcfg-eth2
/etc/sysconfig/network-scripts/ifcfg-eth3
```

Configuración 4 - Configuración de red de srv-corp-1, srv-dmz-1 y srv-web-{1..2}.

```
/etc/resolv.conf
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
```

Configuración 5 - Configuración de red de pc-inf-1, pc-coor-1 y pc-adm-{1..5}.

```
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-p3p1
```

Una vez completados todos los cambios debemos reiniciar el servicio network para aplicarlos usando el siguiente comando:

Comandos 3 - Reiniciar servicio network.

```
# service network restart
```

Para finalizar activamos el reenvío de paquetes en srv-firew-1 modificando el valor de net.ipv4.ip_forward en el fichero /etc/sysctl.conf y recargando la configuración:

Comandos 4 - Activar reenvío de paquetes.

```
# vi /etc/sysctl.conf
# sysctl -p
```

Podemos comprobar que la comunicación entre las redes es correcta utilizando el comando ping.

4. Implantación del cortafuegos

El cortafuegos o *firewall* es un elemento clave de nuestra red en el que implementaremos la política de accesos a nivel de red en nuestra infraestructura.

El primer paso para el diseño de un cortafuegos es definir la política base del mismo la cual puede ser permisiva (se permiten todos los accesos excepto los denegados explícitamente) o restrictiva (se prohíben todos los accesos excepto los explícitamente habilitados). En nuestro caso optaremos por una política restrictiva ya que nos ofrece un mayor control y seguridad.

A continuación creamos un listado con todos los accesos necesarios y, por último, lo implementamos en el servidor srv-firew-1 utilizando reglas de iptables.

4.1. Definición de reglas de acceso

En base a los requerimientos del cliente y de los diferentes servicios podemos identificar el siguiente conjunto de accesos que deben ser habilitados. Al estar utilizando una política restrictiva cualquier acceso no especificado aquí será denegado por el cortafuegos.

Tabla 8 - Reglas de acceso a los servicios externos.

Desde	Hacia	Interfaz	Tipo
Red intermedia	192.168.10.10:80	eth0	FORWARD
Red intermedia	192.168.10.10:443	eth0	FORWARD
Red intermedia	srv-dmz-1:443	eth0	FORWARD
Red intermedia	srv-dmz-1:25	eth0	FORWARD

Tabla 9 - Reglas de acceso para resolución DNS.

Desde	Hacia	Interfaz	Tipo
Red Externa	srv-corp-1:53 (UDP)	eth2	FORWARD
Red DMZ	srv-corp-1:53 (UDP)	eth3	FORWARD
srv-firew-1	srv-corp-1:53 (UDP)	*	OUTPUT
srv-corp-1	*:53 (UDP)	eth1	FORWARD

Tabla 10 - Reglas de acceso para sincronización horaria.

Desde	Hacia	Interfaz	Tipo
*	srv-firew-1:123 (UDP)	*	INPUT
srv-firew-1	*:123 (UDP)	*	OUTPUT

Tabla 11 - Reglas de acceso para SSH.

Desde	Hacia	Interfaz	Tipo
pc-inf-1	srv-firew-1:22	eth1	INPUT
srv-corp-1	srv-firew-1:22	eth1	INPUT
pc-inf-1	Red DMZ:22	eth1	FORWARD
pc-inf-1	Red Externa:22	eth1	FORWARD
srv-corp-1	Red DMZ:22	eth1	FORWARD
srv-corp-1	Red Externa:22	eth1	FORWARD

Tabla 12 - Reglas de acceso para Webmail.

Desde	Hacia	Interfaz	Tipo
srv-dmz-1	srv-corp-1:143	eth3	FORWARD

Tabla 13 - Reglas de acceso para reenvío SMTP.

Desde	Hacia	Interfaz	Tipo
srv-dmz-1	srv-corp-1:25	eth3	FORWARD
Red Externa	srv-corp-1:25	eth2	FORWARD
srv-dmz-1	*:25	eth3	FORWARD
srv-corp-1	*:25	eth1	FORWARD

Tabla 14 - Reglas de acceso para navegación del proxy.

Desde	Hacia	Interfaz	Tipo
srv-corp-1	*:80	eth1	FORWARD
srv-corp-1	*:443	eth1	FORWARD

Tabla 15 - Reglas de acceso para actualización del antivirus.

Desde	Hacia	Interfaz	Tipo
srv-dmz-1	*:80	eth3	FORWARD

4.2. Configuración de iptables

Procederemos ahora a implementar la política de accesos mediante reglas de iptables. Para ello creamos un script en /root/firewall-red.sh en el servidor srv-firew-1 que contenga todos los comandos necesarios. De esta forma resultará más fácil realizar modificaciones posteriores. El script está dividido en varias secciones:

1. Declaración de variables.

```
# Redes
red_int=192.168.0.0/24
red_corp=192.168.10.0/24
red_dmz=192.168.12.0/24
red_ext=192.168.11.0/24

# Servidores
serv_webmail=192.168.12.2
serv_corp=192.168.10.2
serv_web=192.168.11.10

# Clientes
pc_inf=192.168.10.10
```

2. Eliminar reglas existentes.

```
# Eliminar todas las reglas de todas las cadenas
iptables --flush
iptables -t nat --flush
```

3. Política restrictiva por defecto.

```
# Politicas por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

4. Permitir accesos locales y conexiones establecidas.

```
# Permitir retornos
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

### Conexiones establecidas
# Acepta paquetes de conexiones ya establecidas o derivadas de una conexion ya
establecida
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

5. Política de accesos.

```
### Servicios externos
# Acepta paquetes de solicitud de conexion http,https,stmp y 443
iptables -A FORWARD -i eth0 -p tcp --sport 1024: -d $serv_web --dport 80 -m state --
state NEW -j ACCEPT
iptables -A FORWARD -i eth0 -p tcp --sport 1024: -d $serv_web --dport 443 -m state --
state NEW -j ACCEPT
iptables -A FORWARD -i eth0 -p tcp --sport 1024: -d $serv_webmail --dport 25 -m state -
-state NEW -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -p tcp --sport 1024: -d $serv_webmail --dport 443 -m state
--state NEW -j ACCEPT

### DNS
# Acepta consultas dns (udp) desde la red dmz y la red externa al servidor corporativo
iptables -A FORWARD -i eth2 -d $serv_corp -p udp --sport 1024: --dport 53 -j ACCEPT
iptables -A FORWARD -i eth3 -d $serv_corp -p udp --sport 1024: --dport 53 -j ACCEPT
# Acepta consultas dns desde el firewall al servidor corporativo
iptables -A OUTPUT -d $serv_corp -p udp --sport 1024: --dport 53 -j ACCEPT
# Acepta consultas dns desde el servidor corporativo al exterior
iptables -A FORWARD -i eth1 -p udp --sport 1024: --dport 53 -j ACCEPT

### NTP
# Acepta accesos al servicio ntp desde cualquier red
iptables -A INPUT -p udp --sport 123 --dport 123 -j ACCEPT
# Acepta accesos desde el firewall a servidores ntp externos
iptables -A OUTPUT -p udp --dport 123 -j ACCEPT

### SSH
# Acepta conexiones ssh al firewall desde pc-inf-1
iptables -A INPUT -i eth1 -s $pc_inf -d $fw_corp -p tcp --sport 1024: --dport 22 -j
ACCEPT
iptables -A INPUT -i eth1 -s $serv_corp -d $fw_corp -p tcp --sport 1024: --dport 22 -j
ACCEPT
# Acepta conexiones ssh a cualquier servidor desde pc-inf-1
iptables -A FORWARD -i eth1 -s $pc_inf -d $red_dmz -p tcp --sport 1024: --dport 22 -j
ACCEPT
iptables -A FORWARD -i eth1 -s $pc_inf -d $red_ext -p tcp --sport 1024: --dport 22 -j
ACCEPT
# Acepta conexiones ssh desde el servidor corporativo a cualquier servidor de la dmz y
la red externa
iptables -A FORWARD -i eth1 -s $serv_corp -d $red_dmz -p tcp --sport 1024: --dport 22 -
j ACCEPT
iptables -A FORWARD -i eth1 -s $serv_corp -d $red_ext -p tcp --sport 1024: --dport 22 -
j ACCEPT

### IMAP
# Acepta conexiones al servicio imap desde el servidor de webmail al servidor
corporativo
iptables -A FORWARD -i eth3 -s $serv_webmail -d $serv_corp -p tcp --sport 1024: --dport
143 -j ACCEPT

### Reenvio SMTP
# Acepta conexiones al servicio smtp desde srv-dmz-1 al servidor corporativo
iptables -A FORWARD -i eth3 -s $serv_webmail -d $serv_corp -p tcp --sport 1024: --dport
25 -j ACCEPT
# Acepta conexiones al servicio smtp desde srv-web-1 y srv-web-2 al servidor
corporativo
iptables -A FORWARD -i eth2 -s $red_ext -d $serv_corp -p tcp --sport 1024: --dport 25 -
j ACCEPT

### Salida SMTP
# Permite envio de correos al exterior desde serv_corp y serv_webmail
iptables -A FORWARD -i eth3 -s $serv_webmail -p tcp --sport 1024: --dport 25 -j ACCEPT
iptables -A FORWARD -i eth1 -s $serv_corp -p tcp --sport 1024: --dport 25 -j ACCEPT

### Navegacion externa desde el proxy
iptables -A FORWARD -i eth1 -s $serv_corp -p tcp --sport 1024: --dport 80 -j ACCEPT
iptables -A FORWARD -i eth1 -s $serv_corp -p tcp --sport 1024: --dport 443 -j ACCEPT

### Actualizacion del antivirus
iptables -A FORWARD -i eth3 -s $serv_webmail -p tcp --sport 1024: --dport 80 -j ACCEPT
```

Una vez completado el script habilitamos iptables con estos comandos:

Comandos 5 - Activar servicio iptables.

```
# chkconfig iptables on
# service iptables start
```

Ejecutamos el script y guardamos los datos con iptables save:

Comandos 6 - Aplicar política de accesos iptables.

```
# /root/firewall-red.sh
# service iptables save
```

Para cualquier cambio posterior en los accesos no tendríamos más que modificar el script y volver a ejecutar los dos últimos pasos. [11]

4.3. Deshabilitar firewall

En caso de que desearamos deshabilitar el cortafuegos de forma temporal por alguna razón, podríamos hacerlo ejecutando el siguiente comando, que habilitaría todos los accesos hasta el próximo reinicio del servidor:

Comandos 7 - Parar el servicio iptables.

```
# service iptables stop
```

Para habilitar nuevamente el cortafuegos debemos iniciar el servicio iptables:

Comandos 8 - Iniciar servicio iptables.

```
# service iptables start
```

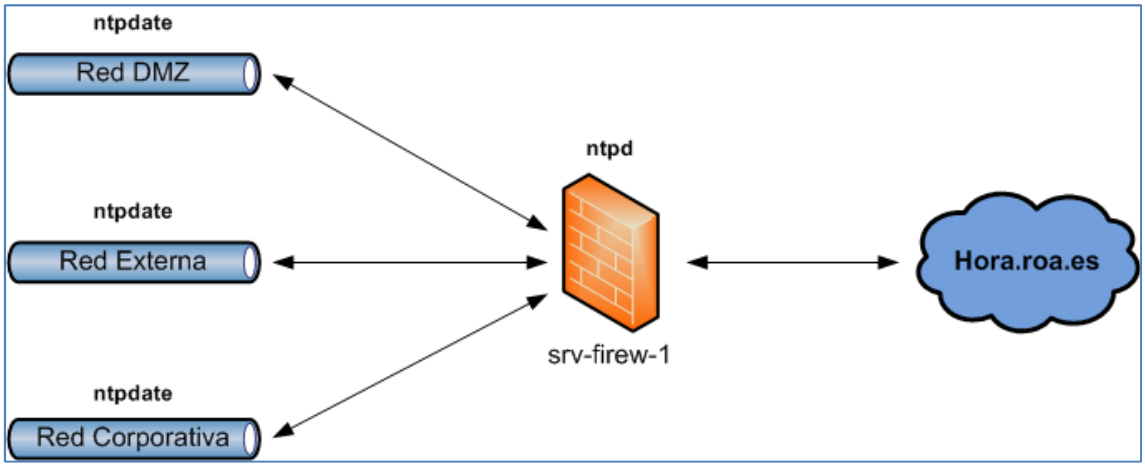
[11] Durante la instalación del resto de servidores el firewall estará deshabilitado ya que necesitaremos acceso al exterior desde los mismos para la instalación de algunos paquetes.

5. Implantación del servicio de sincronización horaria

La sincronización horaria entre todos los dispositivos de nuestra red resulta imprescindible cuando estamos trabajando con servicios en red. Una forma efectiva de asegurar esta sincronización es mediante la utilización del servicio ntp y, en sistemas GNU/Linux concretamente, utilizando el servicio ntpd y la herramienta ntpdate.

Configuraremos el servicio ntpd en srv-firew-1, que se sincronizará con el servidor de hora ROA, la hora oficial de España.[12] El resto de dispositivos utilizarán ntpdate para sincronizarse con srv-firew-1.

Ilustración 5 - Estructura del servicio de sincronización horaria.



5.1. Instalación y configuración del servidor

Los pasos para la configuración del servicio ntpd en srv-firew-1 serán los siguientes:

- Modificación del fichero de configuración ntp.
- Sincronización manual con el servidor de hora ROA.
- Activación del servicio.

En el fichero de configuración /etc/ntp.conf eliminaremos las referencias a los servidores por defecto y añadiremos hora.roa.es como servidor principal. A continuación forzamos la sincronización manual.[13]

Comandos 9 - Sincronización manual con hora ROA.

```
# ntpdate hora.roa.es
```

[12] http://es.wikipedia.org/wiki/Hora_ROA

[13] Esto es necesario ya que, en el caso de que exista una gran diferencia entre ambos, ntpd no efectuará la sincronización.

Por último, iniciamos el servicio ntpd y lo configuramos con arranque automático:

Comandos 10 - Iniciar servicio ntpd.

```
# service ntpd start
# chkconfig ntpd on
```

5.2. Instalación y configuración de los clientes

Una vez iniciado ntpd en el cortafuegos, configuramos el resto de sistemas para sincronizarse con él usando la herramienta ntpdate. Para ello modificamos el fichero de configuración /etc/ntp.conf, seleccionando como servidor la interfaz del cortafuegos situada en la misma red que el equipo.[14] Configuramos una tarea programada que ejecute ntpdate cada hora:

Comandos 11 - Tarea programada ntpdate.

```
# vi /etc/cron.hourly/ntpdate.cron
service ntpdate start
# chmod 755 /etc/cron.hourly/ntpdate.cron
```

[14] Esta ip siempre coincidirá con la puerta de enlace para dicho sistema.

6. Implantación del servicio de resolución de nombres

El servicio de resolución de nombres traduce nombres en direcciones de red y resulta imprescindible en cualquier infraestructura informática. En nuestra infraestructura hemos utilizado dos dominios distintos:

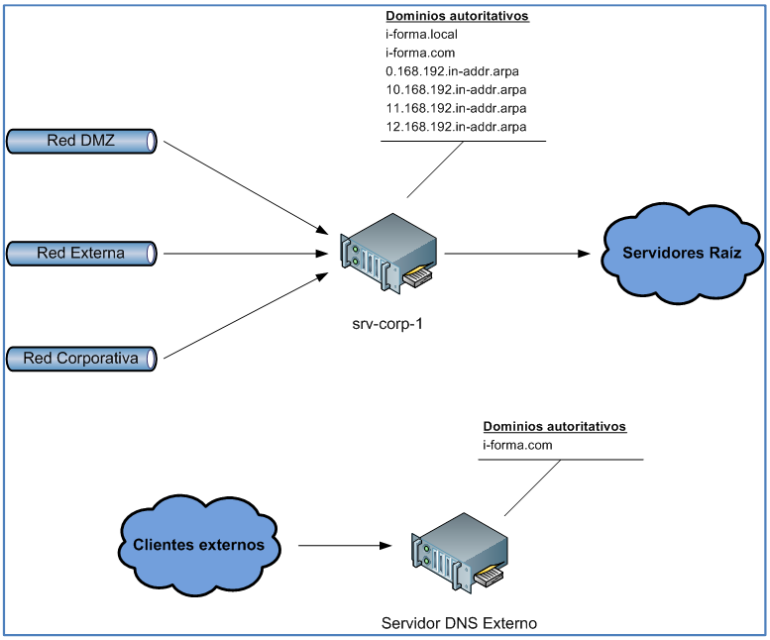
- **i-forma.com**: Para referirnos a servicios externos. Resuelto por un servidor dns externo.
- **i-forma.local**: Para referirnos a servicios y sistemas internos.

Como servidor DNS utilizamos Bind el cual instalaremos en srv-corp-1. No será necesaria ninguna modificación adicional en los clientes ya que se realizaron como parte de la configuración de red inicial. En caso de que nuestro servidor DNS reciba una consulta de un dominio del cual no es servidor autoritativo la reenviará directamente a los servidores raíz.[15] El servidor DNS corporativo realizará las siguientes funciones:

- Resolución del dominio i-forma.local.
- Resolución local del dominio i-forma.com.
- Resolución inversa de las redes internas.
- Servidor DNS para todos los sistemas.

Al resolver de forma local el dominio i-forma.com podemos evitar que los accesos desde la red corporativa a los servicios externos se realicen a través de la ip pública. [16]

Ilustración 6 - Estructura del servicio de resolución de nombres.



[15] http://es.wikipedia.org/wiki/Servidor_Ra%C3%ADz

[16] Una alternativa hubiera sido implementarlo mediantes reglas de NAT en el cortafuegos.

6.1. Instalación y configuración del servidor

La implantación del servicio se realizará en los siguientes pasos:

- Instalación de paquetes rpm.
- Configuración.
- Creación de ficheros de zona.
- Activación del servicio.

El primer paso consiste en instalar el paquete rpm de bind[17]:

Comandos 12 - Instalación rpm bind.

```
# yum -y install bind
```

Seguidamente, modificamos el fichero /etc/named.conf para definir cuáles serán nuestros dominios autoritativos y permitir las consultas dns desde el resto de sistemas. A continuación creamos los ficheros de zonas que contienen la definición de los registros para cada uno de los dominios autoritativos:

Configuración 6 - Ficheros de zona DNS.

```
/var/named/i-forma.local.zone
/var/named/i-forma.com.zone
/var/named/0.168.192.in-addr.arpa.zone
/var/named/10.168.192.in-addr.arpa.zone
/var/named/11.168.192.in-addr.arpa.zone
/var/named/12.168.192.in-addr.arpa.zone
```

Además de la resolución directa e inversa del cada sistema se han creado algunos registros que permiten el acceso a los servicios utilizando un nombre descriptivo:

Tabla 16 - Registros DNS.

Dominio	Registro	Tipo	Valor
i-forma.local	impresion	CNAME	pc-coor-1
i-forma.local	ldap	CNAME	srv-corp-1
i-forma.local	proxy	CNAME	srv-corp-1
i-forma.local	fichero	CNAME	srv-corp-1
i-forma.local	mail	CNAME	srv-corp-1
i-forma.com	www	A	192.168.11.10
i-forma.com	webmail	A	192.168.12.2
i-forma.com	cursos	A	192.168.11.10
i-forma.com	estadisticas	A	192.168.11.10

Por último, se puede iniciar el servicio named y configurarlo con arranque automático:

Comandos 13 - Iniciar servicio named.

```
# chkconfig named on
# service named start
```

[17] Será necesario añadir temporalmente un servidor dns externo a /etc/resolv.conf, de lo contrario no podríamos resolver el nombre de los repositorios.

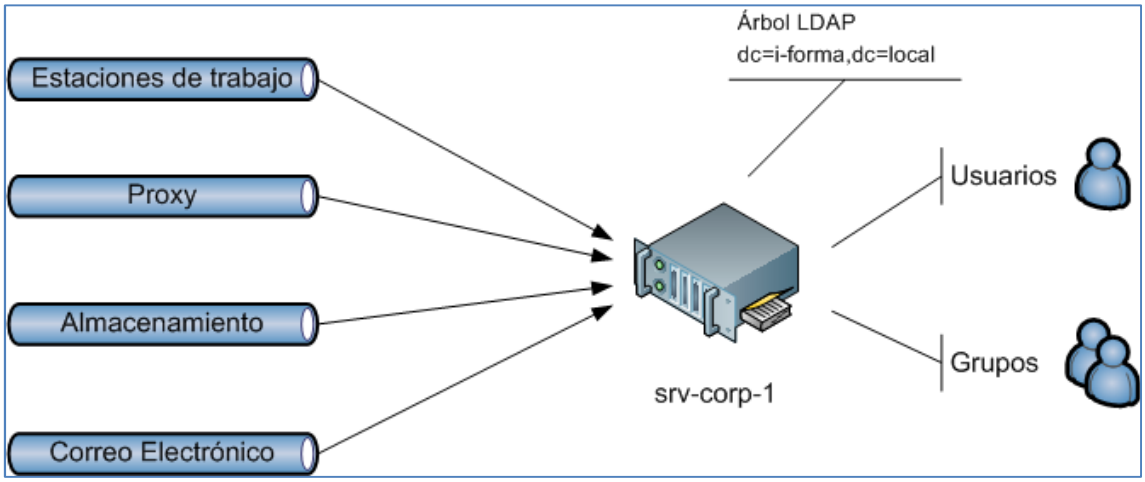
7. Implantación del servicio de directorio

El servicio de directorio permite crear una estructura de usuarios y grupos que usaremos para centralizar la autenticación y permisos de los siguientes servicios:

- Autenticación en las estaciones de trabajo
- Almacenamiento compartido
- Proxy
- Correo electrónico

Para su implementación utilizamos openldap el cual instalamos en srv-corp-1. Una vez completada la instalación, integramos las estaciones de trabajo con ldap. La integración del resto de servicios se realizará durante la instalación de los mismos.

Ilustración 7 - Estructura del servicio LDAP.



7.1. Instalación y configuración del servidor

Los pasos a seguir para la instalación de openldap son los siguientes:

- Instalación de paquetes rpm
- Configuración del servicio
- Creación de usuarios y grupos locales
- Migración
- Integración del servidor corporativo con autenticación ldap

En primer lugar instalamos todos los paquetes rpm necesarios desde los repositorios oficiales de CentOS utilizando yum:

Comandos 14 - Instalación rpms servidor ldap.

```
# yum -y install openldap-clients openldap-servers migrationtools nss-pam-ldapd
```

A continuación, eliminamos los ficheros de configuración existentes y editamos el fichero principal slapd.conf para modificar la raíz del árbol ldap y el usuario administrador. Para generar la password de dicho usuario utilizamos el comando slappasswd:

Comandos 15 - Configuración servidor LDAP.

```
# cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
# rm -rf /etc/openldap/slapd.d/
# slappasswd
# vi /etc/openldap/slapd.conf
```

Tras configurarlo ya podemos iniciar el servicio slapd:

Comandos 16 - Inicio del servicio slapd.

```
# service slapd start
# chkconfig slapd on
```

Ahora crearemos los usuarios y grupos en el sistema para después migrarlos a LDAP usando los scripts incluidos en el paquete migrationtools:

Comandos 17 - Creación de usuarios y grupos.

```
# groupadd informaticos
# groupadd administrativos
# groupadd coordinadores
# useradd informatico1 -g informaticos
# useradd coordinador1 -g coordinadores
# useradd administrativo1 -g administrativos
# useradd administrativo2 -g administrativos
# useradd administrativo3 -g administrativos
# useradd administrativo4 -g administrativos
# useradd administrativo5 -g administrativos
```

Editamos migrationtools/mígrate_common.ph para especificar nuestro dominio ldap, y a continuación, ejecutamos mígrate_base.pl, migrate_group.pl y mígrate_passwd.pl para convertir los usuarios y grupos locales a un fichero ldif importable en openldap mediante el comando ldapadd:

Comandos 18 - Migración de usuarios y grupos a LDAP.

```
# vi /usr/share/migrationtools/mígrate_commom.ph
# mkdir /root/LDAP
# cd /root/LDAP
# /usr/share/migrationtools/mígrate_base.pl > base.ldif
# ldapadd -x -W -D 'cn=Manager,dc=i-forma,dc=local' -h 127.0.0.1 -f base.ldif
# /usr/share/migrationtools/migrate_group.pl /etc/group group.ldif
# /usr/share/migrationtools/migrate_passwd.pl /etc/passwd passwd.ldif
# ldapadd -x -W -D 'cn=Manager,dc=i-forma,dc=local' -h 127.0.0.1 -f group.ldif
# ldapadd -x -W -D 'cn=Manager,dc=i-forma,dc=local' -h 127.0.0.1 -f passwd.ldif
```

Por último configuraremos el propio servidor corporativo para utilizar la autenticación ldap ya que será necesario después para la gestión de permisos del almacenamiento compartido. Para ello ejecutamos el comando "setup", seleccionamos "Utilizar autenticación ldap" entre las opciones de autenticación y modificamos los siguientes ficheros de configuración:

Configuración 7 - Integración de srv-corp-1 con LDAP.

```
/etc/nsswitch.conf
/etc/openldap/ldap.conf
/etc/nslcd.conf
/etc/sysconfig/authconfig
/etc/pam.d/password-auth
/etc/pam.d/system-auth
```

También necesitaremos iniciar el servicio nslcd:

Comandos 19 - Iniciar servicio nslcd.

```
# chkconfig nslcd on
# service nslcd start
```

Para comprobar que la integración con ldap ha sido correcta podemos utilizar el comando getent. La salida del comando debería mostrar por duplicado las entradas de los usuarios y grupos exportados a ldap.

Comandos 20 - Comprobar integración con LDAP.

```
# getent passwd
```

Una vez comprobado, eliminamos los usuarios y grupos locales que creamos al comienzo.

7.2. Instalación y configuración de los clientes

Para la integración de las estaciones de trabajo con ldap debemos instalar los paquetes rpm necesarios y, después, modificar varios ficheros de configuración de forma similar a la integración del servidor corporativo. Para comenzar, instalamos los paquetes rpm desde el repositorio:

Comandos 21 - Instalación rpm cliente LDAP.

```
# yum install openldap-clients nss_ldap
```

Y a continuación, ejecutamos el comando "setup", seleccionamos "Utilizar autenticación ldap" entre las opciones de autenticación y modificamos los siguientes ficheros de configuración:

Configuración 8 - Configuración del cliente LDAP.

```
/etc/nsswitch.conf
/etc/sysconfig/authconfig
/etc/pam.d/password-auth
/etc/pam.d/system-auth
```

En los ficheros de configuración de pam hemos añadido una llamada al módulo mkhomedir que se encarga de crear el directorio de trabajo de un usuario en caso de que no exista.

Una vez comprobemos que la integración es correcta podemos eliminar el usuario local "admin" creado durante la instalación inicial del sistema.

7.3. Gestión de usuarios y grupos LDAP

Para añadir un nuevo usuario a ldap debemos crear un fichero ldif con el siguiente formato:

Configuración 9 - Fichero LDIF para creación de nuevos usuarios.

```
dn: uid=<nombreUsuario>,ou=People,dc=i-forma,dc=local
uid: <nombreUsuario>
cn: <nombreUsuario>
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}<passwordCifrada>
shadowLastChange: 15318
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: <UID>
gidNumber: <GID>
homeDirectory: /home/<nombreUsuario>
```

En caso de querer crear un nuevo grupo el formato a seguir sería este:

Configuración 10 - Fichero LDIF para creación de nuevos grupos.

```
dn: cn=<nombreGrupo>,ou=Group,dc=i-forma,dc=local
objectClass: posixGroup
objectClass: top
cn: <nombreGrupo>
userPassword: {crypt}x
gidNumber: <GID>
```

A continuación, importamos el fichero ldif utilizando el comando ldapadd:

Comandos 22 - Importar un fichero LDIF.

```
# ldapadd -a -x -D 'cn=Manager,dc=i-forma,dc=local' -W -f fichero.ldif
```

Para mostrar una lista de todo el contenido de nuestro árbol ldap podemos realizar una consulta al mismo utilizando el comando ldapsearch:

Comandos 23 - Listar contenido del árbol LDAP.

```
# ldapsearch -h localhost -x -b 'dc=i-forma,dc=local'
```

8. Implantación del servicio de almacenamiento compartido

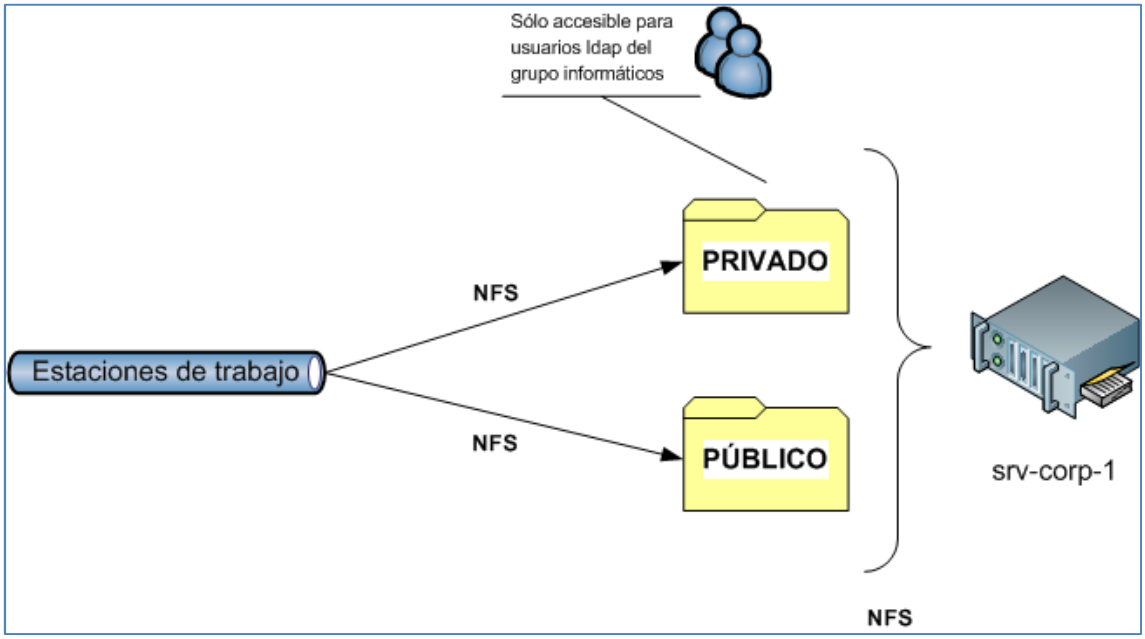
Tal como se especificaba en los requerimientos funcionales del proyecto debemos disponer de directorios de almacenamiento compartido accesibles desde todas las estaciones de trabajo y con permisos configurables en base a usuarios y grupos. Para su implementación haremos uso de los siguientes elementos:

- Directorios exportados mediante NFS
- Integración con LDAP
- Permisos del sistema de ficheros ext4.

De este modo, hemos creado los directorios a compartir en el servidor corporativo, asignamos permisos en base a usuarios y grupos de ldap y los exportaremos mediante nfs para ser montados en todas las estaciones de trabajo.

A modo de ejemplo crearemos los directorios "publico", accesible por todos los usuarios; y "privado", sólo accesible a los usuarios del grupo informaticos.

Ilustración 8 - Estructura del servicio de almacenamiento compartido.



8.1. Instalación y configuración del servidor

Llevamos a cabo la instalación en los siguientes pasos:

- Instalación de paquetes rpm.
- Creación de directorios.
- Configuración.
- Activación del servicio.

En primer lugar instalamos el paquete nfs-utils mediante yum:

Comandos 24 - Instalación rpm de nfs.

```
# yum -y install nfs-utils
```

A continuación, creamos los directorios que se exportarán via NFS y asignamos los permisos adecuados.

Comandos 25 - Creación directorios compartidos.

```
# mkdir /ALMACENAMIENTO
# cd /ALMACENAMIENTO
# mkdir publico
# mkdir privado
# chgrp informaticos privado
# chmod 777 publico
# chmod 770 privado
```

Ahora modificamos el fichero de configuración /etc/exports para que estos directorios sean accesibles desde el resto de la red corporativa. Por último, iniciamos todos los servicios necesarios:

Comandos 26 - Inicio servicios servidor nfs.

```
# chkconfig rpcbind on
# chkconfig nfslock on
# chkconfig nfs on
# service rpcbind start
# service nfslock start
# service nfs start
```

8.2. Instalación y configuración de los clientes

Los pasos para el montaje de los directorios en los equipos cliente son los siguientes:

- Instalación de paquetes rpm.
- Activación de servicios.
- Configuración.
- Montaje de los directorios compartidos.

En primer lugar, instalamos el paquete rpm nfs-utils:

Comandos 27 - Instalación rpm nfs cliente.

```
# yum -y install nfs-utils
```

En segundo lugar, iniciamos todos los servicios requeridos:

Comandos 28 - Inicio services cliente nfs.

```
# chkconfig rpcbind on
# chkconfig rpcidmapd on
# chkconfig nfslock on
# chkconfig netfs on
# service rpcbind start
# service rpcidmapd start
# service nfslock start
# service netfs start
```

A continuación, creamos los directorios vacios en los que se montarán las carpetas compartidas y editamos /etc/fstab [18] para que se monten automáticamente en el arranque:

Comandos 29 - Montaje de almacenamiento compartido.

```
# mkdir /home/publico
# mkdir /home/privado
# vi /etc/fstab
# mount -a
```

8.3. Modificación de permisos de un directorio o fichero

Para modificar los permisos en el directorio compartido no tendríamos más que modificarlos en el servidor corporativo, utilizando para ello la gestión de permisos del sistema de ficheros ext4. Esto puede hacerse mediante los comandos chown, chgrp y chmod.

En caso de que se deseen definir unos permisos más complejos (por ejemplo permitir el acceso sólo a algunos usuarios determinados dentro de un grupo ldap) puede usarse el sistema de acls.[19]

[18] Hemos añadido la opción soft al punto de montaje para que el sistema siga su arranque normal en caso de caída del servidor nfs. En este caso los directorios deberían montarse manualmente una vez el servicio nfs se haya restablecido.

[19] http://centos.org/docs/5/html/Deployment_Guide-en-US/s1-acls-setting.html

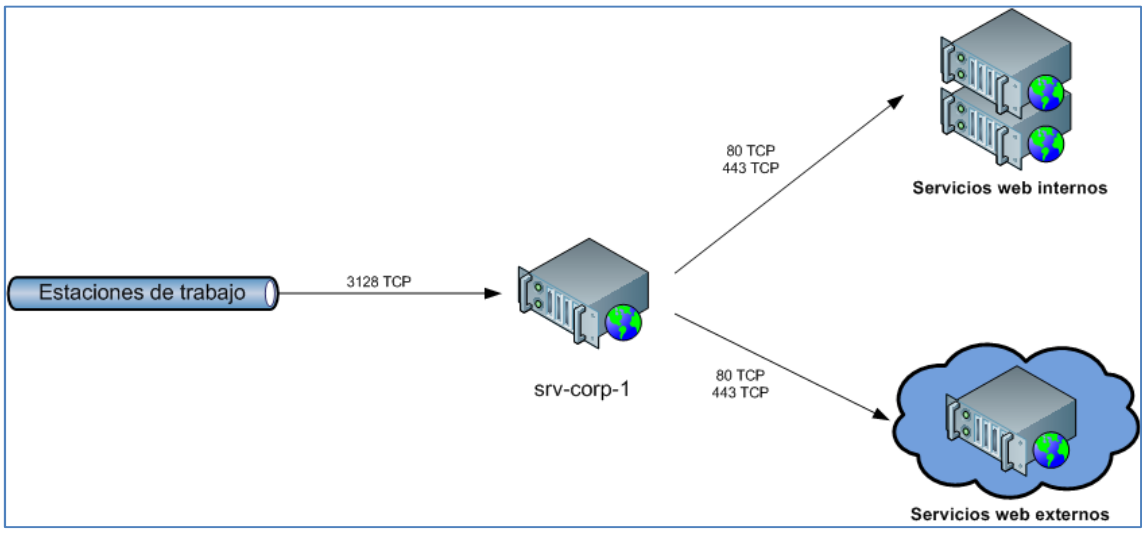
9. Implantación del servicio de proxy

El servicio de proxy nos permite configurar un servidor que haga las funciones de intermediario en la navegación web desde las estaciones de trabajo. Esto nos permitirá aplicar distintas políticas de acceso en base al grupo LDAP al que pertenezca un usuario.

Para la implementación del servicio de proxy utilizamos Squid, el cual se instalará en el servidor corporativo. Integramos squid con nuestro servicio ldap de forma que, tal como se especifica en los requerimientos del proyecto, los usuarios del grupo administrativos sólo tengan permitido el acceso web a una lista de sitios determinada.

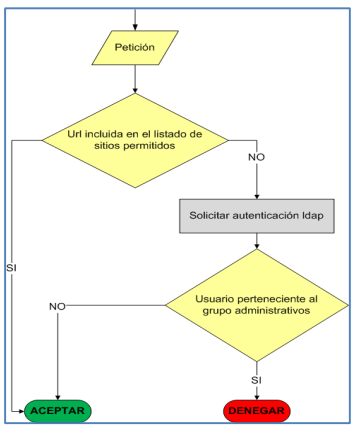
Como se observa en el siguiente diagrama, todos los accesos web (tanto a los servicios internos como a los externos) se realizarán a través del proxy. Al no tratarse de un servicio de proxy transparente necesitaremos configurar la url del servicio proxy en cada una de las estaciones de trabajo.

Ilustración 9 - Estructura del servicio de proxy.



Para cada petición que el servicio de proxy reciba se comprobará la lista de sitios permitidos y si el usuario pertenece al grupo administrativos. En la ilustración 10 aparece un diagrama de flujo con el proceso completo de evaluación de una petición.

Ilustración 10 - Comprobaciones de acceso del servicio proxy.



9.1. Instalación y configuración del servidor

Llevamos a cabo la instalación de squid en srv-corp-1 en tres pasos:

- Instalación de paquetes rpm.
- Configuración.
- Activación del servicio.

En primer lugar, instalamos el paquete rpm squid desde los repositorios de CentOS utilizando yum:

Comandos 30 - Instalación rpm de Squid.

```
# yum -y install squid
```

A continuación, editamos el fichero de configuración del servicio situado en /etc/squid/squid.conf para habilitar el acceso desde la red local al servicio, integrarlo con autenticación ldap y especificar nuestra política de accesos y el listado de sitios permitidos. Por último, activaremos el servicio utilizando los siguientes comandos:

Comandos 31 - Inicio del servicio Squid.

```
# chkconfig squid on
# service squid start
```

9.2. Configuración de los clientes

La configuración en cada uno de los clientes difiere según el navegador. En el navegador Mozilla Firefox, por ejemplo, dicha configuración está situada dentro del menú de preferencias en "Avanzado" => "Red" => "Configuración".

En cualquier caso, los datos de configuración manual del proxy serían los siguientes:

- Servidor Proxy: proxy.i-forma.local
- Puerto: 3128
- Servicios: HTTP y HTTPS

9.3. Modificar lista de sitios permitidos

En el caso de que deseemos modificar la lista de sitios permitidos, deberíamos actualizar el valor de la variable sitiospermitidos del fichero /etc/squid/squid.conf. Una vez modificada, debemos recargar la configuración del servicio ejecutando el siguiente comando:

Comandos 32 - Recarga de configuración de squid.

```
# service squid reload
```

10. Implantación de la entidad certificadora interna

Dentro de los requerimientos de seguridad del proyecto se nos solicitaba que, para el acceso al servicio de webmail, fuera necesario un certificado SSL cliente.

Con objeto de implementar estas restricciones crearemos una entidad certificadora interna que usaremos para expedir los certificados cliente. Tanto para la creación de la entidad certificadora como para la de los certificados se utilizarán las librerías openssl.

10.1. Instalación y configuración

Seguimos estos pasos para la creación de una entidad certificadora:

- Instalación de paquetes rpm.
- Creación de entidad certificadora.
- Creación del fichero de restricciones.

En primer lugar, instalamos mediante yum el paquete rpm openssl:

Comandos 33 - Instalación rpm OpenSSL.

```
# yum -y install openssl
```

A continuación, ejecutamos los comandos para generar el certificado y la llave privada de nuestra entidad certificadora:

Comandos 34 - Creación de entidad certificadora.

```
# mkdir /root/CA && cd /root/CA
# openssl req -x509 -newkey rsa:2048 -keyout cakey.pem -out cacert.pem
```

Por último, crearemos el fichero de restricciones que utilizaremos para generar los certificados cliente. En este fichero se especifican los permisos extendidos del certificado de forma que sólo pueda usarse como certificado ssl cliente:

Comandos 35 - Fichero de permisos extendidos.

```
# vi constraint
basicConstraints=critical,CA:FALSE
extendedKeyUsage = clientAuth
```

10.2. Creación de un certificado SSL cliente

Para generar un nuevo certificado cliente nos situaremos en el directorio de la entidad certificadora y ejecutaremos los siguientes comandos:

Comandos 36 - Creación de un certificado SSL cliente.

```
# openssl genrsa -des3 -passout pass:<PASS> -out <USUARIO>.key 2048
# openssl req -new -key <USUARIO>.key -passin pass:<PASS> -subj "/DC=I-
Forma/C=ES/CN=<USUARIO>" -out <USUARIO>.req
# openssl x509 -CA cacert.pem -CAkey cakey.pem -CAcreateserial -req -in <USUARIO>.req -
days <DIAS_VALIDEZ> -extfile contraint -sha1 -out <USUARIO>.pem
# openssl pkcs12 -export -in <USUARIO>.pem -inkey <USUARIO>.key -certfile cacert.pem -
out <USUARIO>.p12
```

De esta forma, generaremos un fichero p12 que incluye tanto el certificado como su clave privada. Este fichero se enviará al cliente junto con las instrucciones de instalación del mismo.

A la hora de firmar un certificado se introduce el periodo de validez, de este modo controlaremos que los certificados sólo puedan ser usados hasta la fecha de finalización del curso.

10.3. Importar certificado SSL en el navegador

La importación de certificado p12 en el navegador se realizará de forma distinta dependiendo del navegador usado. En el caso de Mozilla Firefox, este se puede importar a través del menú de preferencias en el apartado “Avanzado” => “Cifrado” => “Ver certificados” => “Sus certificados”.

11. Implantación del servicio web

Dentro del servicio web englobaremos tres sitios con distintas funciones:

- Plataforma de tele-formación (cursos.i-forma.com)
- Web informativa (www.i-forma.com).
- Estadísticas de acceso (estadísticas.i-forma.com).

Todos los sitios se servirán desde un mismo servidor web accesible desde el exterior, aunque el acceso a las estadísticas se limitará a las direcciones de la red corporativa mediante configuración. Implementaremos cada uno de los diferentes sitios mediante gestores de contenido ya existentes.

- Plataforma de tele-formación: Moodle
- Web informativa: Drupal
- Estadísticas: AWStats

Como software base para los servidores web hemos optado por la configuración más común de entre las soportadas por estas plataformas:

- Servidor web: Apache
- Contenido dinámico: PHP
- Base de datos: MySQL

Para la alta disponibilidad configuramos un cluster activo-pasivo con los servidores srv-web-1 y srv-web-2 y el uso de las siguientes tecnologías:

- DRBD, para la replicación de la base de datos.
- Rsync, para la replicación de los ficheros web.
- Heartbeat, para la alta disponibilidad.

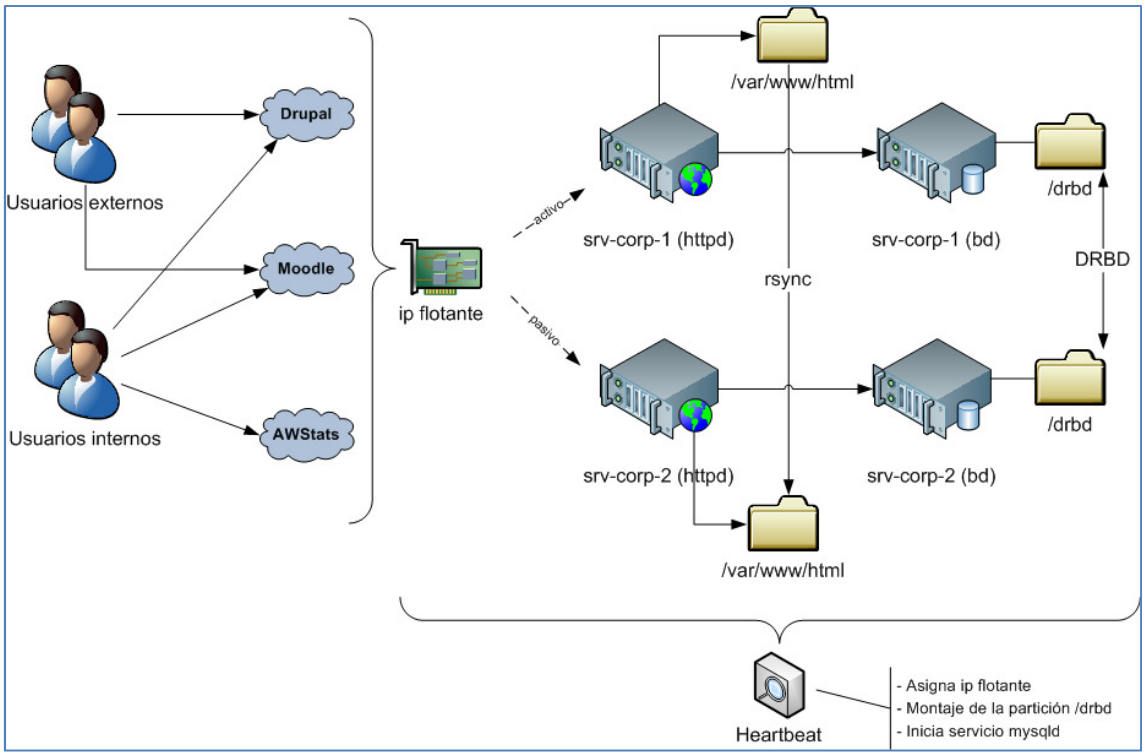
Mediante DRBD tendremos un raid espejo de la partición de la base de datos a nivel de red de forma que ambos nodos siempre contengan exactamente la misma información. Una tarea programada realizará la sincronización de los ficheros de la web entre ambos nodos cada minuto y, por último, el servicio heartbeat se encargará de configurar la ip flotante del cluster y de mantener los servicios corriendo en el nodo activo.

Los pasos a seguir para la implantación del servicio web con alta disponibilidad son los siguientes:

- Instalación y configuración de DRBD.
- Configuración rsync.
- Instalación y configuración de software base.
- Instalación y configuración de heartbeat.
- Instalación de Moodle.
- Instalación de Drupal.
- Instalación de AWStats.

En el siguiente esquema se muestra la estructura del servicio web:

Ilustración 11 - Estructura del servicio web.



11.1. Instalación y configuración de DRBD

La implantación de DRBD se realizará en los siguientes pasos:

- Instalación de paquetes rpm.
- Configuración.
- Activación del servicio.
- Preparación del volumen.

Una vez completados, podremos montar el dispositivo drbd y hacer uso de él de forma que la replicación resulte transparente para el usuario y el resto de las aplicaciones.

En primer lugar, necesitamos instalar el paquete drbd y el módulo del kernel para el soporte de estos dispositivos. Dichos paquetes rpm no se encuentran disponibles aun en los repositorios oficiales de CentOS 6 por lo que serán descargados desde un repositorio externo.[20]

Comandos 37 - Instalación rpm DRBD.

```
# rpm -Uvh http://dl.atrpms.net/el6-x86_64/atrpms/stable/drbd-kmdl-2.6.32-
220.2.1.el6.x86_64-8.3.11-31.el6.x86_64.rpm
# rpm -Uvh http://dl.atrpms.net/el6-x86_64/atrpms/stable/drbd-8.3.11-31.el6.x86_64.rpm
```

[20] http://bugs.centos.org/view.php?id=5030

Debemos asegurarnos de que el módulo coincide exactamente con nuestra versión y revisión del kernel, que podemos comprobar mediante el comando uname.

Una vez instalados, pasamos a configurar los parámetros de drbd y del nuevo volumen drbd0 que crearemos. Deben especificarse los nodos implicados así como la partición usada. En nuestro caso, se tratará de la partición extra que creamos en la instalación inicial de los servidores srv-web-1 y srv-web-2. Debemos editar los siguientes ficheros de configuración para reflejar estos datos:

Configuración 11 - Configuración DRBD.

```
/etc/drbd.d/global_common.conf
/etc/drbd.d/main.res
```

Para la activación del servicio ejecutamos los siguientes comandos en ambos nodos:

Comandos 38 - Activación del servicio DRBD.

```
# drbdadm create-md main
# mkdir /drbd
# mkdir /var/lib/drbd
# chkconfig drbd on
# service drbd start
```

Por último, forzamos la replicación y le damos formato ext4 al nuevo volumen drbd0. Para ello ejecutaremos estos comandos en el servidor srv-web-1:

Comandos 39 - Replicación DRBD.

```
# drbdsetup /dev/drbd0 primary -o
# mkfs.ext4 /dev/drbd0
```

Al marcar el nodo 1 como primario con el comando drbdsetup se iniciará la replicación a nivel de bit de las particiones.[21] Puede comprobarse el estado de la replicación en cualquier momento ejecutando el siguiente comando:

Comandos 40 - Comprobar estado del servicio DRBD.

```
# service drbd status
```

[21] La replicación puede tardar varios minutos dependiendo de tamaño de la partición.

11.2. Configuración de la sincronización de ficheros web

Configuramos la replicación periódica de los ficheros de la web situados en /var/www/html entre srv-web-1 y srv-web-2. Para ello utilizaremos la herramienta rsync.

Necesitamos, en primer lugar, configurar llaves ssh de forma que sea posible autenticar desde srv-web-1 a srv-web-2 sin necesidad de usar password. Para ello ejecutamos los siguientes comandos:

Comandos 41 - Configurar autenticación ssh con clave pública.

```
En srv-web-1:
# ssh-keygen
# scp /root/ssh/id_rsa.pub srv-web-2:/root/

En srv-web-2:
# mkdir /root/.ssh
# mv /root/id_rsa.pub /root/.ssh/authorized_keys
```

Una vez completado creamos una tarea programada en srv-web-1 que sincronize el contenido del directorio cada minuto:

Comandos 42 - Tarea programada rsync.

```
# vi /etc/cron.d/rsync_web
* * * * * root rsync -a --delete /var/www/html/ srv-web-2.i-forma.local:/var/www/html/
```

11.3. Instalación y configuración de software base

Los pasos para la instalación y configuración del software base son los siguientes:

- Instalación de paquetes rpm.
- Configuración.
- Activación de servicios.
- Securización de la base de datos.

Necesitamos instalar los paquetes rpm de apache, mysql y php; así como una serie de módulos php para drupal y moodle:

Comandos 43 - Instalación rpm software base servidor web.

```
# yum -y install httpd mysql mysql-server php php-mysql mod_ssl php-mbstring php-xmlrpc
php-gd php-soap php-intl php-xml
```

Creamos ahora el directorio /etc/httpd/sites.d/ que contendrá los ficheros de configuración específicos para cada uno de los sitios web:

Comandos 44 - Directorio de configuración de los sitios web.

```
# mkdir /etc/httpd/sites.d/
```

Modificamos los ficheros de configuración de apache y mysql para habilitar los hosts virtuales por nombre [22] y modificar la ruta de los datos de mysql de forma que use la partición drbd:

Configuración 12 - Apache y MySQL.

```
/etc/httpd/conf/httpd.conf
/etc/my.cnf
```

A continuación, iniciamos los servicios apache y mysql (este último sólo en el nodo primario):

Comandos 45 - Inicio servicios web y base de datos.

```
# chkconfig httpd on
# service mysqld start
# service httpd start
```

Por último, mejoramos la seguridad de la instalación de mysql con la herramienta mysql_secure_installation con la que asignamos una contraseña para el usuario root, eliminamos los datos de prueba y bloqueamos el acceso remoto como administrador a la base de datos:

Comandos 46 - Mejora de la seguridad de MySQL.

```
# /usr/bin/mysql_secure_installation
```

Una vez completado podemos parar el servicio mysql ya que el sistema de alta disponibilidad se encargará de iniciarlo cuando sea necesario.

11.4. Instalación y configuración de Heartbeat

El servicio heartbeat se encargá de monitorizar en todo momento el estado de cada nodo y llevar a cabo las acciones necesarias para mantener activo el servicio en el nodo primario, o iniciarlo en el secundario en caso de caída. En concreto, las acciones que realizará heartbeat son las siguientes:

- Asignación de la ip flotante al nodo activo.
- Configurar nodo maestro para el volumen DRBD.
- Montaje de la partición /drbd.
- Inicio del servicio MySQL.

[22] http://en.wikipedia.org/wiki/Virtual_hosting#Name-based

Los pasos a seguir para la instalación y configuración de heartbeat son los siguientes:

- Instalación del repositorio EPEL.
- Instalación de paquetes rpm.
- Configuración.
- Activación del servicio.

El paquete rpm de heartbeat no está disponible, a día de hoy, en los repositorios oficiales de CentOS 6 por lo que, para su instalación añadimos el repositorio EPEL[23].

Comandos 47 - Instalación de rpm de heartbeat desde repositorio EPEL.

```
# rpm -Uvh http://download.fedora.redhat.com/pub/epel/6/x86_64/epel-release-6-
5.noarch.rpm
# yum -y --enablerepo=epel install heartbeat
```

A continuación modificamos los ficheros de configuración de heartbeat y creamos el script /etc/ha.d/resource.d/mysql[24].

Configuración 13 - Heartbeat.

```
/etc/ha.d/ha.cf
/etc/ha.d/haresources
/etc/ha.d/authkeys
/etc/ha.d/resource.d/mysql
```

Algunos de estos ficheros necesitan permisos específicos:

Comandos 48 - Permisos de los ficheros de configuración de heartbeat.

```
# chmod 600 /etc/ha.d/authkeys
# chmod 755 /etc/ha.d/resource.d/mysql
```

Por último, iniciamos el servicio heartbeat con los siguientes comandos:

Comandos 49 - Iniciar servicio heartbeat.

```
# chkconfig heartbeat on
# service heartbeat start
```

En este momento ya tendremos el servicio web funcional en el nodo primario (srv-web-1) y toda la configuración necesaria para la alta disponibilidad por lo que procederemos a la instalación de los distintos sitios web.

[23] http://fedoraproject.org/wiki/EPEL/es

[24] http://dev.mysql.com/doc/mysql-ha-scalability/en/ha-heartbeat-drbd.html

11.5. Instalación y configuración de la plataforma de tele-formación

Instalamos el sitio web de moodle que realizará las funciones de plataforma de tele-formación. Los pasos de la instalación son los siguientes:

- Descarga de Moodle.
- Configuración de la base de datos.
- Creación del directorio moodledata.
- Configuración web.
- Instalador web.

En primer lugar, descargamos la última versión estable de Moodle desde su página web oficial. Descomprimimos dicho paquete y lo movemos al directorio web /var/www/html.

Comandos 50 - Descarga e instalación de Moodle.

```
# mkdir /root/INSTALL && cd /root/INSTALL
# wget http://download.moodle.org/download.php/direct/stable22/moodle-latest-22.tgz
# tar -xvzf  moodle-latest-22.tgz
# mv  moodle /var/www/html/
```

A continuación nos conectamos utilizando el cliente MySQL para crear la base de datos y el usuario para Moodle. El usuario tendrá permisos exclusivamente sobre dicha base de datos:

Comandos 51 - Creación de usuarios y base de datos de Moodle.

```
# mysql -u root -p
mysql> CREATE DATABASE moodle;
mysql> GRANT ALL ON moodle.* TO 'moodleuser'@'localhost' IDENTIFIED BY 'password';
mysql> ALTER DATABASE moodle DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
mysql> quit
```

Seguidamente, creamos el directorio moodledata que alojará los ficheros que se suban a la plataforma. Por razones de seguridad, se nos recomienda que dicho directorio esté situado en una ruta distinta de la web para que no sea directamente accesible. Debemos otorgar al servicio httpd permisos de escritura sobre este directorio:

Comandos 52 - Creación de moodledata.

```
# mkdir /var/www/html/moodledata
# chown -R apache:apache /var/www/html/moodledata
```

Creamos el fichero de configuración /etc/httpd/sites.d/moodle.conf que contendrá el nombre del sitio y la ruta de ficheros web y logs. Recargamos la configuración del servicio httpd para aplicar estos cambios:

Comandos 53 - Reinicio de apache.

```
# service httpd restart
```

Por último, accedemos con un navegador a la dirección http://cursos.i-forma.com/install.php que iniciará el asistente de instalación via web de Moodle. El asistente comprobará que cumplimos los requisitos necesarios para la instalación y solicitará los datos de conexión a la base de datos. Una vez se haya completado, podremos acceder a la plataforma de tele-formación en cualquier momento a través de la url http://cursos.i-forma.com.

11.6. Instalación y configuración de la web informativa

Instalamos Drupal como gestor de contenidos para la web informativa. La instalación se realiza mediante el instalador web, pero, al igual que en la instalación de Moodle, serán necesarios algunos pasos previos.

- Descarga de Drupal.
- Configuración PHP.
- Configuración de Drupal.
- Configuración web.
- Instalador web.

En primer lugar, descargamos la última versión estable de Drupal desde su web oficial y la descomprimimos bajo el directorio /var/www/html.

Comandos 54 - Descarga e instalación de Drupal.

```
# cd /root/INSTALL
# wget http://ftp.drupal.org/files/projects/drupal-7.10.tar.gz
# tar -xvzf drupal-7.10.tar.gz
# mv drupal-7.10 /var/www/html
# cd /var/www/html && ln -s drupal-7.10 drupal
# chown -R root:root /var/www/html/drupal-7.10
```

A continuación, debemos modificar algunos parámetros de php en su fichero de configuración por la forma en que Drupal gestiona las sesiones web:

Configuración 14 - PHP

```
/etc/php.ini
```

Nos conectamos con el cliente MySQL para la creación de la base de datos de drupal y un usuario con permisos sobre ella:

Comandos 55 - Creación de usuario y base de datos de Drupal.

```
# mysql -u root -p
mysql> CREATE DATABASE drupal;
mysql> GRANT ALL ON drupal.* TO 'drupaluser'@'localhost' IDENTIFIED BY 'password';
```

Modificamos el fichero de configuración de drupal settings.php para definir los parámetros de conexión a nuestra base de datos en la variable $databases y el nombre del sitio web en $base_url:

Comandos 56 - Configuración Drupal.

```
# cp /var/www/html/drupal/sites/default/default.settings.php
/var/www/html/drupal/sites/default/settings.php
# vi /var/www/html/drupal/sites/default/settings.php
```

Descargamos el paquete de traducción al español:

Comandos 57 - Traducción al español de Drupal.

```
# cd /var/www/html/drupal/profiles/standard/translations/
# wget http://ftp.drupal.org/files/translations/7.x/drupal/drupal-7.10.es.po
```

Creamos el directorio donde drupal almacenará los ficheros subidos y damos al servicio web permisos de escritura sobre el mismo:

Comandos 58 - Directorio de datos de Drupal.

```
# mkdir /var/www/html/drupal/sites/default/files
# chown -R apache:apache /var/www/html/drupal/sites/default/files
```

Crearemos el fichero /etc/httpd/sites.d/drupal.conf definiendo el nombre y rutas de ficheros y de log del sitio web. Necesitaremos también habilitar la directiva AllowOverride ya que drupal hace uso de ficheros .htaccess para reglas de reescritura de urls. Recargaremos estos cambios en el servicio con el siguiente comando:

Comandos 59 - Reinicio del servicio web.

```
# service httpd restart
```

Una vez completados estos pasos accederemos al instalador web a través de la url http://www.i-forma.com/install.php en el cual se comprobarán los requerimientos de instalación y se creará el contenido inicial de la base de datos.

Una vez finalizado el asistente tendremos disponible el sitio web informativo a través de la url http://www.i-forma.com.

11.7. Instalación y configuración de sistema de estadísticas

Para la generación de estadísticas de los accesos realizados a la web informativa y la plataforma de tele-formación utilizaremos el programa AWStats. Este paquete proporciona unos scripts en lenguaje Perl que analizan los logs del servicio web y generan estadísticas de uso. Los pasos para la instalación y configuración de AWStats serán los siguientes:

- Descarga de AWStats.
- Creación de perfiles.
- Configuración web.
- Generación de estadísticas.

En primer lugar, descargamos la última versión estable de AWStats desde su web oficial:

Comandos 60 - Descarga e instalación de AWStats.

```
# cd /root/INSTALL
# wget http://prdownloads.sourceforge.net/awstats/awstats-7.0.tar.gz
# tar -xvzf awstats-7.0.tar.gz
# mv awstats-7.0 /usr/local/awstats
# chown -R root:root /usr/local/awstats
```

A continuación, generamos un perfil de estadísticas inicial mediante el comando awstats_configure.pl:

Comandos 61 - Creación de perfil de estadísticas.

```
# chown -R root:root /usr/local/awstats
# cd /usr/local/awstats/tools/
# ./awstats_configure.pl
Do you want me to build a new AWStats config/profile
file (required if first install): y
Your web site, virtual server or profile name: www.i-forma.com
```

Esto creará un perfil por defecto en el directorio /etc/awstats/. Realizamos una copia del mismo para el sitio cursos.i-forma.com y modificamos en ambos ficheros las variables referentes a la ruta de los logs (LogFile) y nombre del sitio (SiteDomain):

Comandos 62 - Configuración de perfiles de estadísticas.

```
# cp /etc/awstats/awstats.www.i-forma.com.conf /etc/awstats/awstats.cursos.i-
forma.com.conf
# vi /etc/awstats/awstats.www.i-forma.com.conf
# vi /etc/awstats/awstats.cursos.i-forma.com.conf
```

A continuación, creamos el sitio web y su fichero de configuración dentro del directorio sites.d:

Comandos 63 - Configuración del sitio web de AWStats.

```
# mkdir /var/www/html/estadísticas
# vi /etc/httpd/sites.d/awstats.conf
# service httpd restart
```

Por último, creamos el fichero en el que se almacenarán las estadísticas generadas y configuramos una tarea programada para la actualización diaría:

Comandos 64 - Tarea programada AWStats.

```
# mkdir /var/lib/awstats
# vi /etc/cron.daily/awstats
/usr/local/awstats/tools/awstats_updateall.pl now
# chmod 755 /etc/cron.daily/awstats
```

Una vez completada la instalación, podemos acceder a las estadísticas de uso a través de las siguientes urls[25]:

- http://estadisticas.i-forma.com/www
- http://estadisticas.i-forma.com/cursos

11.8. Actualizar estadísticas de acceso web

Las estadísticas web están configuradas para actualizarse cada día pero, en caso de que deseemos actualizarlas en otro momento, tan sólo debe ejecutarse el siguiente comando en srv-web-1:

Comandos 65 - Actualizar estadísticas de sitios web.

```
# /usr/local/awstats/tools/awstats_updateall.pl now
```

[25] Se han configurado reglas de redirección para que no sea necesario usar la url completa.

12. Implantación del servicio de correo electrónico

La infraestructura del servicio de correo electrónico estará compuesta por los siguientes elementos:

- Servicio de correo para los trabajadores de la empresa.
- Pasarela de correo antispam/antivirus para el correo externo.
- Acceso externo al correo electrónico via web (Webmail).

Dichas funciones se repartirán entre dos servidores distintos:

- Servidor corporativo: Servicio de correo
- Servidor DMZ: Pasarela de correo y servicio webmail.

Para la implementación hemos seleccionado la siguiente lista de software base:

- MTA: Postfix
- Servidor POP3/IMAP: Dovecot
- Autenticación SMTP: Cyrus
- Antivirus: ClamAV + Amavis
- Antispam: SpamAssassin + Amavis
- Servidor web: Apache + PHP
- Base de datos: MySQL
- Servicio webmail: Roundcube
- Sistema de listas negras (RBL): Spamhaus

En las ilustraciones 12 y 13 se muestra la estructura del servicio de correo.

Ilustración 12 - Estructura del servicio de correo.

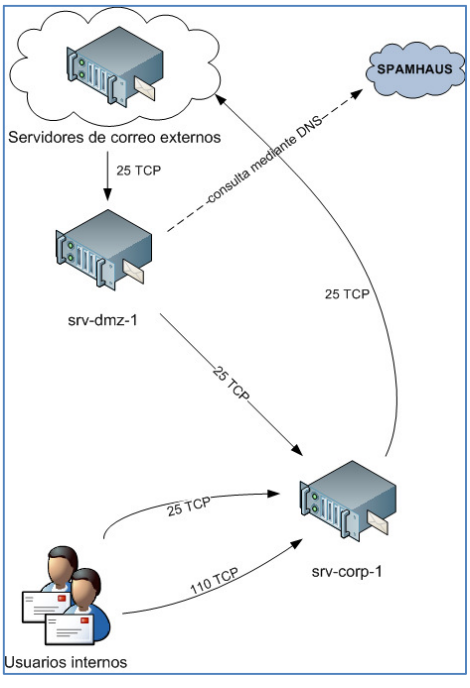
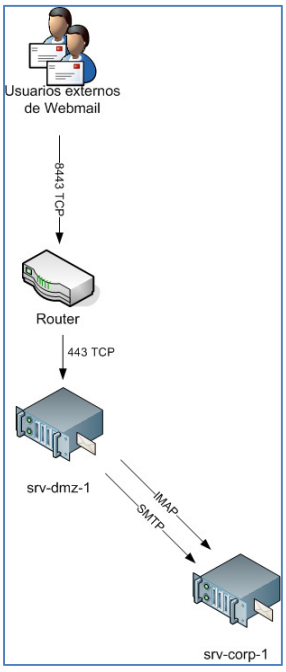


Ilustración 13 - Estructura del servicio de webmail.



Ante la llegada de un nuevo mensaje desde un servidor externo a la pasarela se realizan una serie de comprobaciones para decidir si este será o no reenviado hacia el servidor corporativo:

- El servidor chequea la pertenencia a la lista negra spamhaus[26] de la dirección ip de la que procede el correo. En caso de afirmativo dicho correo se rechazará.
- Se envía el correo al servicio intermedio amavisd.
- Se analizan los ficheros adjuntos del mensaje en busca de virus utilizando clamav.
- Se analiza el mensaje mediante el servicio spamassassin y se le asigna una puntuación de spam.
- En base a la puntuación otorgada a un mensaje será reenviado, rechazado o marcado como spam añadiendo la etiqueta "*** SPAM ***" al asunto del mismo.

Realizamos la implantación del servicio de correo en las siguientes fases:

- Instalación y configuración del servicio de correo corporativo.
- Instalación y configuración de la pasarela de correo.
- Instalación y configuración del servicio de webmail.
- Configuración de los clientes.

12.1. Instalación y configuración del servidor de correo corporativo

Para la instalación de servidor de correo corporativo seguimos los siguientes pasos:

- Instalación de paquetes rpm.
- Configuración de postfix.
- Configuración de dovecot.
- Configuración de Cyrus.
- Activación del servicio.

En primer lugar, instalamos todos los paquetes rpm necesarios utilizando yum:

Comandos 66 - Instalación rpm del servidor de correo corporativo.

```
# yum -y install postfix dovecot cyrus-sasl cyrus-sasl-ldap
```

Modificamos la configuración de postfix editando los siguientes ficheros:

Configuración 15 - Postfix.

```
/etc/postfix/master.cf
/etc/postfix/main.cf
```

[26] http://www.spamhaus.org/

De este modo, definimos que postfix permita accesos desde el resto de la infraestructura y la autenticación para el envío de correo. A continuación, configuraremos dovecot modificando los siguientes ficheros para integrarlo con ldap y definir algunos de los parámetros del servicio:

Configuración 16 - Dovecot

```
/etc/dovecot/dovecot.conf
/etc/dovecot/conf.d/10-mail.conf
/etc/dovecot/conf.d/10-ssl.conf
/etc/dovecot/dovecot-ldap.conf.ext [27]
/etc/dovecot/conf.d/10-auth.conf
```

Editamos los ficheros de configuración del servicio cyrus para integrar la autenticación con ldap:

Configuración 17 - Cyrus-sasl

```
/etc/saslauthd.conf
/etc/sysconfig/saslauthd
```

El último paso consistirá en iniciar los servicios y configurarlos con arranque automático:

Comandos 67 - Inicio de servicios del servidor de correo corporativo.

```
# service postfix start
# chkconfig postfix on
# chkconfig dovecot on
# service dovecot start
# chkconfig saslauthd on
# service saslauthd start
```

12.2. Instalación y configuración de la pasarela de correo

Realizamos la instalación de la pasarela de correo siguiendo los siguientes pasos:

- Instalación de paquetes rpm.
- Configuración de postfix.
- Configuración de clamav.
- Configuración de amavis.
- Activación del servicio.

Algunos de los paquetes rpm que necesitaremos no están disponibles aun en los repositorios oficiales de CentOS 6 por lo que antes configuraremos el repositorio EPEL.

Comandos 68 - Instalación de paquetes rpm para la pasarela de correo.

```
# rpm -Uvh http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-
5.noarch.rpm
# yum -y install postfix clamav clamav-db clamd spamassassin amavisd-new
```

[27] Utilizando como plantilla el fichero /usr/share/doc/dovecot-2.0.9/example-config/conf.d/auth-ldap.conf.ext

Para la configuración de postfix debemos modificar los siguientes ficheros:

Configuración 18 - Postfix.

```
/etc/postfix/main.cf
/etc/postfix/master.cf
/etc/postfix/mailertable
/etc/postfix/relay_domains
```

Los ficheros mailertable y relay_domains deben convertirse al formato usado por postfix. Para esto ejecutamos los siguientes comandos:

Comandos 69 - Convertir ficheros mailertable y relay_domains.

```
# postmap /etc/postfix/mailertable
# postmap /etc/postfix/relay_domains
```

Modificamos el fichero de configuración de clamav para deshabilitar los sockets TCP ya que, en su lugar, utilizaremos sockets fichero[28].

Configuración 19 - ClamAV.

```
/etc/clamd.conf
```

Forzamos la actualización inicial de la base de datos de virus ejecutando este comando:

Comandos 70 - Actualizar base de datos de virus de ClamAV.

```
# /usr/bin/freshclam –v
```

Modificamos el fichero de configuración de amavis:

Configuración 20 - Amavis.

```
/etc/amavis/amavisd.conf
```

Como último paso, iniciaremos los servicios y los configuraremos con arranque automático:

Comandos 71 - Inicio de servicios de la pasarela de correo.

```
# chkconfig clamd on
# chkconfig spamassassin on
# chkconfig amavisd on
# chkconfig clamd.amavisd on
# chkconfig postfix on
# service spamassassin start
# service clamd start
# service clamd.amavisd start
# service amavisd start
# service postfix start
```

[28] http://es.wikipedia.org/wiki/Socket_de_Internet#Variantes

12.3. Instalación y configuración del servicio de correo web

Realizamos la implantación del servicio de webmail en los siguientes pasos:

- Instalación de paquetes rpm.
- Activación del servicio.
- Securización de MySQL.
- Descarga de Roundcube.
- Configuración de la base de datos.
- Configuración web y PHP.
- Instalador web.
- Configuración autenticación SSL cliente.

En primer lugar, instalamos el software base necesario mediante yum:

Comandos 72 - Instalación rpms del servicio webmail.

```
# yum -y install mysql mysql-server php php-mysql httpd mod_ssl php-xml php-mbstring
php-intl php-mcrypt libmcrypt
```

Iniciamos los servicios y los configuramos con arranque automático:

Comandos 73 - Inicio de servicios de webmail.

```
# chkconfig mysqld on
# chkconfig httpd on
# service mysqld start
# service httpd start
```

Mejoramos la seguridad de la instalación de mysql ejecutando la herramienta mysql_secure_installation:

Comandos 74 - Opciones de seguridad de MySQL.

```
# /usr/bin/mysql_secure_installation
```

A continuación, descargamos la última versión estable de Roundcube desde su web oficial y la descomprimimos en /var/www/html. Modificamos también los permisos de los directorios temp y logs en los que el servidor web necesitará permisos de escritura:

Comandos 75 - Descarga e instalación de Roundcube.

```
# mkdir /root/INSTALL && cd /root/INSTALL
# wget
http://downloads.sourceforge.net/project/roundcubemail/roundcubemail/0.6/roundcubemail-
0.6.tar.gz?r=http%3A%2F%2Froundcube.net%2Fdownload&ts=1323715054&use_mirror=kent
# tar -xvzf roundcubemail-0.6.tar.gz
# mv roundcubemail-0.6 /var/www/html/roundcube
# chown -R root:root /var/www/html/roundcube
# cd /var/www/html/roundcube
# chown -R apache:apache temp logs
```

Nos conectamos mediante el cliente MySQL y creamos la base de datos y el usuario de roundcube:

Comandos 76 - Creación de usuario y base de datos de Roundcube.

```
# mysql –u root –p
mysql> CREATE DATABASE roundcube;
mysql> GRANT ALL ON roundcube.* TO 'roundcubeuser'@'localhost' IDENTIFIED BY
'password';
mysql> quit;
```

Ejecutaremos el script sql incluido en roundcube para crear la estructura inicial de la base de datos:

Comandos 77 - Importar base de datos inicial.

```
# mysql –u root –p –D roundcube < /var/www/html/roundcube/SQL/mysql.initial.sql
```

Modificamos los ficheros de configuración de apache y php para deshabilitar los accesos por el puerto 80, definir el sitio web y marcar "Europe/Madrid" como zona horaria de php al tratarse de un requisito de roundcube.

Configuración 21 - Apache y PHP.

```
/etc/httpd/conf/httpd.conf
/etc/httpd/conf.d/ssl.conf
/etc/php.ini
```

Reiniciamos el servicio web para aplicar dichos cambios:

Comandos 78 - Reinicio del servidor web.

```
# service httpd restart
```

Como último paso, accedemos con un navegador a https://webmail.i-forma.com/installer para iniciar el asistente de instalación via web. Se solicitarán los datos de acceso al servicio smtp, imap y los datos de acceso a base de datos.[29] Una vez completado el asistente de instalación, podemos acceder al correo electrónico via web a través de la url https://webmail.i-forma.com desde la red corporativa o usando https://webmail.i-forma.com:8443 en el caso de los usuarios externos.

Para forzar la autenticación SSL de los clientes debemos copiar la clave pública de nuestra entidad certificadora interna al servidor DMZ y añadir las siguientes directivas en el fichero de configuración ssl.conf de apache:

Comandos 79 - Configuración SSL cliente.

```
# vi /etc/httpd/conf.d/ssl.conf
SSLCACertificateFile   <RUTA>/cacert.pem
SSLVerifyClient require
```

[29] Por razones de seguridad debemos eliminar el directorio "installer" una vez finalizada la instalación.

12.4. Configuración de los clientes

Para el acceso de los clientes al servicio de correo podemos utilizar cualquier cliente de correo y configurar en el mismo los datos de acceso a la cuenta. En nuestro caso, utilizaremos el cliente por defecto incluido en GNOME llamado Evolution.

Los datos de configuración para una cuenta serían los siguientes:

- Servidor: mail.i-forma.local
- Tipo de cuenta: POP
- Habilitar autenticación SMTP.

13. Implantación del servicio de impresión compartida

Para implementar el servicio de impresión compartida utilizaremos el propio servicio de impresión del sistema llamado cups. Para ello sólo serán necesarios dos cambios:

- Permitir accesos remotos en el servidor cups del equipo de la impresora.
- Añadir la impresora en las estaciones de trabajo como impresora de red.

13.1. Configuración del equipo conectado a la impresora

Debemos modificar el fichero de configuración del servicio cups para permitir los accesos remotos al mismo en el equipo que posea la impresora. Para ello iniciaremos sesión en pc-coor-1 a través de ssh y editaremos el siguiente fichero:

Configuración 22 - Servicio CUPS.

```
/etc/cups/cupsd.conf
```

Para aplicar estos cambios debemos reiniciar el servicio cupsd:

Comandos 80 - Reinicio del servicio CUPS.

```
# service cups restart
```

13.2. Configuración de los equipos remotos

Para añadir la impresora de red en el resto de estaciones de trabajo utilizamos el asistente gráfico. Para iniciarlo podemos ejecutar el siguiente comando:

Comandos 81 - Abrir asistente gráfico de configuración de impresoras.

```
# system-config-printer
```

A continuación seleccionaremos "Impresora de red" buscando por el nombre impresion.i-forma.local.

14. Tareas de mantenimiento

Para el buen funcionamiento de una infraestructura informática se requiere realizar una serie de tareas de mantenimiento. A continuación se describirán dos de ellas:

- Copias de seguridad.
- Rotado y compresión de logs.

14.1. Copias de seguridad

Para evitar pérdida de datos y facilitar las tareas de recuperación en caso de caída se deben realizar copias de seguridad periódicas. Para el caso de nuestra infraestructura se propone realizar copias de seguridad del correo electrónico, directorios de almacenamiento compartido, ficheros web, bases de datos y ficheros de configuración relevantes.

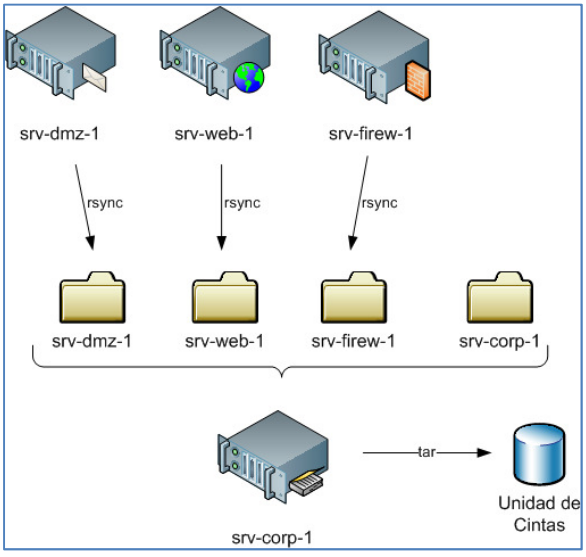
Para la realización de la copia de seguridad de las bases de datos configuraremos una tarea programada diaria en los servidores web y el servidor dmz que genera un backup en formato sql mediante el comando mysqldump.

Comandos 82 - Copia de seguridad de la base de datos.

```
# mysqldump -u root -p --all-databases > /var/backup/mysql.`date +%d`.sql
# gzip -f  /var/backup/mysql.`date +%d`.sql
```

Como servidor de backup utilizaremos el servidor corporativo el cual cuenta con una unidad de cintas magnéticas. Sincronizaremos mediante rsync todos los directorios y ficheros necesarios y volcaremos dicho contenido a cinta utilizando el comando tar. Para ello, será necesario configurar la autenticación ssh con clave pública entre srv-corp-1 y el resto de servidores de la infraestructura.

Ilustración 14 - Estructura del sistema de copias de seguridad.



Definimos un calendario de copias de seguridad:

- El primer lunes de cada mes se utilizará la cinta etiquetada como MENSUAL.
- El resto de lunes se utilizará la cinta etiquetada como SEMANAL.
- De martes a domingo la copia de seguridad se realizará en la cinta etiquetada como DIARIA.
- Una vez al año se realizará una copia de seguridad en una cinta ANUAL que se guardará indefinidamente.

Los directorios y ficheros a sincronizar para cada servidor serían los siguientes:

Configuración 23 - Backup de srv-dmz-1.

```
/var/www/html/
/var/log/httpd/
/var/backup/

/etc/selinux/config
/etc/hosts.allow
/etc/resolv.conf
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/ntp.conf
/etc/postfix/
/etc/clamd.conf
/etc/amavis/
/etc/httpd/conf/
/etc/httpd/conf.d/
/etc/php.ini
```

Configuración 24 - Backup de srv-web-1.

```
/var/www/html/
/var/log/httpd/
/var/backup/
/var/lib/awstats/

/etc/selinux/config
/etc/hosts.allow
/etc/resolv.conf
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/awstats/
/etc/ntp.conf
/etc/drbd.d/
/etc/httpd/conf/
/etc/httpd/conf.d/
/etc/httpd/sites.d/
/etc/my.cnf
/etc/ha.d/
/etc/php.ini
/etc/cron.daily/awstats
```

Configuración 25 - Backup de srv-firew-1.

```
/root/firewall-red.sh

/etc/selinux/config
/etc/hosts.allow
/etc/resolv.conf
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/ifcfg-eth1
/etc/sysconfig/network-scripts/ifcfg-eth2
/etc/sysconfig/network-scripts/ifcfg-eth3
/etc/sysctl.conf
/etc/ntp.conf
```

Configuración 26 - Backup de srv-corp-1.

```
/var/spool/mail
/var/named/
/ALMACENAMIENTO/
/var/lib/ldap/
/root/CA/
/root/LDAP/

/etc/selinux/config
/etc/hosts.allow
/etc/resolv.conf
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/ntp.conf
/etc/named.conf
/etc/openldap/
/etc/nsswitch.conf
/etc/nslcd.conf
/etc/sysconfig/authconfig
/etc/pam.d/
/etc/exports
/etc/squid/
/etc/postfix/
/etc/dovecot/
/etc/saslauthd.conf
/etc/sysconfig/saslauthd
```

14.2. Rotado y compresión de logs

Modificamos los ficheros de configuración de apache en srv-web-{1..2} y srv-dmz-1 para que, en lugar de directamente a un fichero, los logs se envíen al script rotatelogs. Este script los almacenará en un fichero de log con la fecha anexa. Las directivas de configuración para habilitar esto son las siguientes:

Configuración 27 - Rotado de logs de apache.

```
CustomLog "|/usr/sbin/rotatelogs logs/NOMBRE_access_log.%Y-%m-%d" combined
ErrorLog "|/usr/sbin/rotatelogs logs/NOMBRE_error_log.%Y-%m-%d"
```

Para ahorrar espacio en disco también comprimiremos los ficheros de log con más de un mes de antigüedad mediante una tarea en /etc/cron.daily:

Comandos 83 - Tarea programada de borrado de logs.

```
# find /var/log/httpd/ -mtime +30 -exec gzip -f {} \;
```

15. Ampliación de la infraestructura

Entre los requerimientos del cliente se encuentra el estudio de amplicaciones futuras en la infraestructura y el plan de acción a seguir para cada uno de los siguientes supuestos.

15.1. Mayor número de trabajadores

En el caso de un aumento significativo en el número de estaciones de trabajo la primera limitación que nos encontraríamos sería la falta de puertos disponibles en el switch. El plan de acción en este caso pasaría por la adquisición de nuevos switches dedicados para la red corporativa los cuales se conectarían, a su vez, a los puertos de VLAN corporativa del switch principal.

15.2. Mayor espacio de almacenamiento compartido

En caso de requerir una mayor cantidad de espacio de almacenamiento compartido los pasos a seguir serían los siguientes:

- Adquisición de nuevos discos duros.
- Instalación de los nuevos discos en el servidor srv-corp-1.
- Añadir los discos al volumen group vg_srvcorp1
- Incrementar el tamaño del volumen lógico lv_root

Los dos últimos pasos pueden realizarse mediante los comandos de administración de lvm o mediante la interfaz gráfica system-config-lvm. Al estar utilizando discos lógicos no requieren de corte de servicio y son del todo transparentes de cara al usuario y al resto de aplicaciones del sistema.

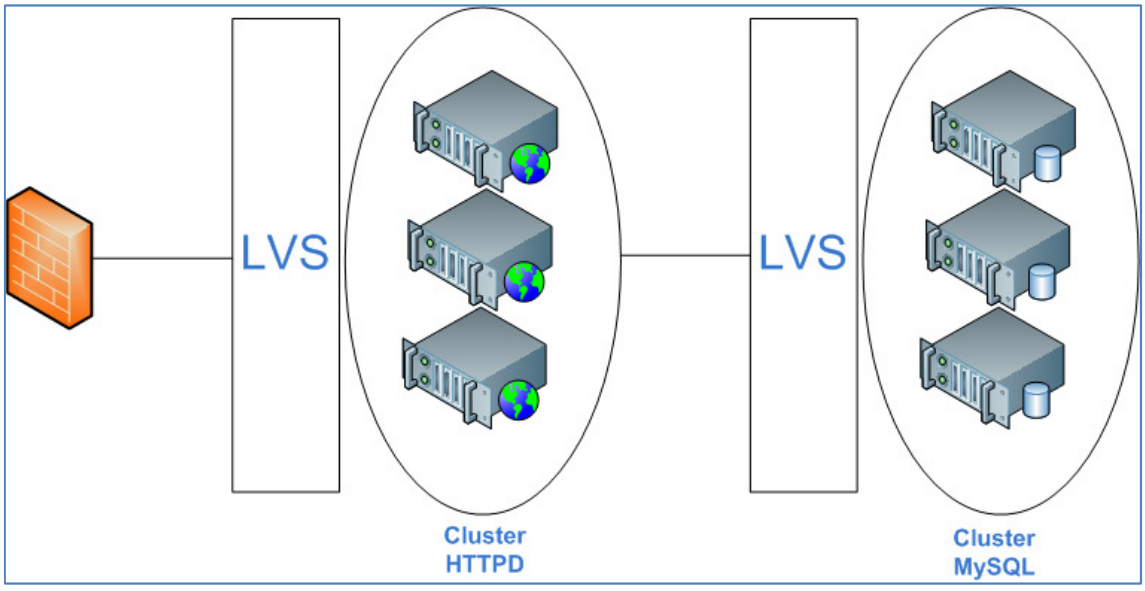
15.3. Mayor número de usuarios en la plataforma de tele-formación

Ante un incremento considerable en el tráfico de la plataforma de tele-formación podríamos encontrarnos con problemas de rendimiento en el servidor web. En caso de que estos problemas de rendimiento se deban a una falta de capacidad de proceso debemos plantear una nueva arquitectura de estos servicios:

- Convertir el cluster activo-pasivo en un cluster activo-activo.
- Alojar la base de datos en un cluster MySQL dedicado.
- Situar balanceadores de carga delante del cluster web y el cluster de base de datos.

Con esta nueva arquitectura se podrían añadir tantos nodos como sea necesario sin necesidad de corte de servicio con lo que estaríamos mejorando el rendimiento así como la alta disponibilidad del servicio.

Ilustración 15 - Estructura de arquitectura en cluster propuesta.



16. Planes de contingencia

Entre los requerimientos del proyecto se incluía la definición de los planes de contingencia ante caídas de cualquier de los elementos de la infraestructura. Para cada uno de ellos indicaremos el impacto del mismo en el servicio y el plan a seguir para restaurarlo.

16.1. Caída del switch

- Impacto: Corte total de todos los servicios tanto internos como externos.
- Plan de acción: Sustitución del switch.

16.2. Caída del router ADSL

- Impacto: Corte de todos los servicios externos así como los servicios internos que requieran acceso al exterior.
- Plan de acción: Sustitución del router ADSL.

16.3. Caída del cortafuegos

- Impacto: Corte de todos los servicios externos así como los servicios internos que requieran salida al exterior. El resto de servicios de la red corporativa pueden seguir operando con normalidad.
- Plan de acción: Sustitución del servidor cortafuegos y recuperación de los ficheros de configuración desde la copia de seguridad.

16.4. Caída del servidor corporativo

- Impacto: Corte de todos los servicios internos excepto la impresión compartida y corte del servicio de webmail.
- Plan de acción: Sustitución del servidor corporativo y recuperación de ficheros desde la copia de seguridad.

16.5. Caída del servidor DMZ

- Impacto: Corte del servicio de correo electrónico via web y de la recepción de correo del exterior.
- Plan de acción: Sustitución del servidor dmz y recuperación de ficheros desde la copia de seguridad.

16.6. Caída del servidor web

- Impacto: Corte del servicio web en caso de caída de ambos nodos. Sin impacto en caso de caída de un solo nodo.
- Plan de acción: Sustitución del nodo afectado y recuperación de ficheros de configuración desde la copia de seguridad. En caso de caída del nodo primario deben actualizarse manualmente las estadísticas web con los accesos realizados al nodo secundario.

17. Bibliografía

A continuación se referencian las fuentes de documentación consultadas durante la realización del proyecto, tanto documentación oficial como tutoriales de terceros.

17.1. Documentación oficial

Iptables: http://www.netfilter.org/documentation/index.html

Apache: http://httpd.apache.org/docs/2.2/

PHP: http://www.php.net/manual/es/

MySQL: http://dev.mysql.com/doc/

RoundCube: http://trac.roundcube.net/wiki

Postfix: http://www.postfix.org/documentation.html

Drupal: http://drupal.org/handbooks

Moodle: http://docs.moodle.org/22/en?lang=en

OpenSSL: http://www.openssl.org/docs/apps/openssl.html

Dovecot: http://wiki2.dovecot.org/

OpenLDAP: http://www.openldap.org/doc/admin24/

Squid: http://www.squid-cache.org/Doc/config/

AwStats: http://awstats.sourceforge.net/docs/index.html

Bind: http://www.isc.org/software/bind/documentation

Ntpd: http://www.ntp.org/documentation.html

NFS: http://nfs.sourceforge.net/

DRBD: http://www.drbd.org/docs/about/

Rsync: http://rsync.samba.org/ftp/rsync/rsync.html

Heartbeat: http://www.linux-ha.org/doc/users-guide/users-guide.html

Cyrus: http://www.cyrusimap.org/docs/cyrus-sasl/2.1.23/

Amavis: http://www.ijs.si/software/amavisd/#doc

Cups: http://www.cups.org/documentation.php

17.2. Tutoriales

http://www.encuentroalternativo.com/mysql-alta-disponibilidad-usando-drbd-heartbeat/

http://dev.mysql.com/doc/refman/5.0/en/ha-heartbeat-drbd.html

http://dev.mysql.com/doc/refman/5.0/en/replication-howto.html

http://houseoflinux.com/high-availability/building-a-high-available-file-server-with-nfs-v4-drbd-8-3-and-heartbeat-on-centos-6/

http://rm-rf.es/ldap-openldap-instalacion-y-configuracion-i/

http://www.techrockdo.com/linux/centos-6-authentication-to-active-directory-part-1

http://wiki.contribs.org/Client_Authentication:Fedora

http://linux-cd.com.ar/manuales/rh9.0/rhl-rg-es-9/s1-nfs-client-config.html

http://www.server-world.info/en/note?os=CentOS_6&p=nfs

http://linux.die.net/man/8/squid_ldap_group

http://workaround.org/squid-ldap

http://docs.moodle.org/22/en/Installing_Moodle

http://drupal.org.es/manuales/instalacion

http://www.alcancelibre.org/staticpages/index.php/como-postfix-tls-y-auth

http://linuxwiki.riverworth.com/index.php?title=LDAP_Authentication#Cyrus_LDAP

http://wiki.dovecot.org/AuthDatabase/LDAP/AuthBinds

http://trac.roundcube.net/wiki/Howto_Install

http://www.vicente-navarro.com/blog/2008/01/13/backups-con-rsync/

http://rm-rf.es/como-securizar-un-servidor-ssh/