

# **Servicios básicos en servidores**

## **Práctica 2 ASORC**

- **Jimena Escobar Bermúdez**
- **Benjamín Soro López**
- **Julio Granados Barros**
- **Francisco González Aguilar**

- **Introducción**
- **Sistemas operativos**
  - **Windows Server 2012**
    - Licencia
    - Particionamiento
    - Arranque y parada de servicios
    - GYGWIN + OpenSSH
      - Acceso SSH mediante clave RSA
    - Servidor VNC
    - Remote Desktop
    - Active Directory
    - Servidor DNS
    - Dynamic DNS-No-IP.org
    - Servidor DHCP
      - DHCP con DNS
    - Compartir archivos
    - Servidor de Impresión
    - Merak
    - Servidor FTP
    - Herramienta de virtualización: VMWare
  - **Slackware 14.0**
    - Licencia
    - Gestión del particionamiento
    - Arranque y parada de servicios
    - Servidor SSH
      - Acceso SSH mediante clave RSA
    - Servidor VNC - TightVNC
    - Determinación IP estática
    - XDMCP
    - FreeNX
    - OpenLDAP
    - Servidor DNS
    - Dynamic DNS-No-IP.org
    - Servidor DHCP
      - DHCP con DNS
    - NFS
    - Sendmail
    - Servidor FTP
  - **Debian Server**
    - Licencia
    - Particionado
    - Arranque y Parada
    - Servidor SSH
    - Servidor VNC - TightVNC
    - XDMCP
    - FreeNX
    - Servidor DNS
    - Servidor DHCP

- DHCP con DNS
  - Dynamic DNS-No-IP.org
  - Servidor NFS
  - Samba
  - CUPS
  - VSFTP
  - VMWare Server
  - LDAP
  - WINE
- **Solaris**
    - Licencia
    - Servicio SSH
    - Servicio SCP
    - Servicio SFTP
    - Servicio VNC
    - Terminal Server
    - Rdesktop
    - XDMCP
    - FreeNX
    - DHCP
    - SAMBA
  - **CentOS**
    - Licencia
    - Particionado
    - Arranque y parada de servicios
    - VNC
    - XDMCP
    - FreeNX
    - Servicio DHCP
    - NFS
    - Samba/SMB
    - Servidor FTP
    - Emulación de otro sistema operativo: Wine
  - **PCBSD**
    - Licencia
    - Particionado
    - Arranque y parada
    - Problemas surgidos

# Introducción

---

Ha continuación se va a explicar la configuración de una serie de servicios en un servidor.

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Los temas de estudio y servicios que se van a configurar son los siguientes:

- **Licencias:** contrato que agrupa una serie de cláusulas en las que se recogen unos términos y condiciones referentes al uso del sistema operativo.
- **Particionado:** forma en la que se va a distribuir la memoria de la máquina.
- **Arranque y parada de servicios:** gestión de los servicios ofrecidos por un servidor así como de sus runlevels.
- **Administración remota:**
  - **SSH (Secure SHell):** nombre de un protocolo y del programa que lo implementa. Sirve para acceder a máquinas remotas a través de una red manejando las mismas a través de un intérprete de comandos
  - **SFTP (Secure File Transfer Protocol):** protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable. Se utiliza comúnmente con SSH para proporcionar seguridad a los datos.
  - **SCP (Secure Copy):** medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo SSH.
  - **VNC (Computación Virtual en Red):** programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente y de forma gráfica a través de un ordenador cliente. También llamado software de escritorio remoto.
- **Terminal Services:**
  - **XDMCP (X Display Manager Control Protocol):** protocolo utilizado en redes para comunicar un ordenador servidor que ejecuta un sistema operativo con un gestor de ventanas basado en X-Window, con el resto de clientes que se conectarán a éste con propósitos interactivos.
  - **FreeNX:** programa que realiza conexiones remotas X11 muy rápidas usando SSH, lo que permite a los usuarios acceder a escritorios

remotos de Linux o Unix incluso bajo conexiones lentas como las realizadas con módem.

- **Servidor de Directorio:** aplicación que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.
- **Gestión de Usuarios:**
  - **Local:** sistema de gestión y autenticación a nivel local que utiliza varios ficheros para la comprobación de la autenticidad del usuario.
  - **NIS (Network Information Service):** protocolo de servicios de directorios cliente-servidor para el envío de datos de configuración en sistemas distribuidos tales como nombres de usuarios y hosts entre computadoras sobre una red.
  - **LDAP (Lightweight Directory Access Protocol):** protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
- **Servicio DNS (Domain Name System):** sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red con el propósito de poder localizar y direccionar estos equipos mundialmente.
- **Servicio DHCP (Dynamic Host Configuration Protocol):** protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
- **Unión DNS+DHCP:** permite la actualización dinámica de direcciones según concesión.
- **Servidor de archivos:** servidor cuya función es permitir el acceso remoto a archivos almacenados en él o directamente accesibles a través de él.
  - **NFS (Network File System):** protocolo de nivel de aplicación, según el Modelo OSI. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.
  - **SAMBA:** implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows.

- **SMB (Server Message Block)**: protocolo de red que permite compartir archivos, impresoras y otros recursos entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.
- **Servidor de Impresión**: servidor que conecta una impresora a la red para que cualquier máquina pueda acceder a ella e imprimir trabajos sin depender de otra.
- **Servidor de Correo**: servidor encargado de la gestión y distribución de emails.
- **Servidor FTP (File Transfer Protocol)**: protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.
- **Emulación de otro sistema operativo**: software que permite ejecutar programas en una plataforma con diferente hardware o sistema operativo para el cual fueron escritos originalmente. A diferencia de un simulador, que sólo trata de reproducir el comportamiento del programa, un emulador trata de modelar de forma precisa el dispositivo de manera que este funcione como si estuviese siendo usado en el aparato original.
- **Virtualización**: software que permite crear una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.
- **Paravirtualización**: software que aporta un sistema operativo origen sobre el cual se pueden virtualizar todos los demás.

# Sistemas operativos

---

## Windows Server 2012

### Licencia

Microsoft CLUF

### Particionamiento

Unidad C: para albergar el sistema operativo, tamaño 30GB

Unidad D: para albergar el Internet Information Services, tamaño 5GB

Unidad E: para albergar el servidor FTP, tamaño 10GB

### Parada y arranque de Servicios

Acceder a Panel de Control > Herramientas Administrativas > Servicios.

### GYGWIN + OpenSSH

Acceder a <http://cygwin.com/install.html> y descargar el instalador.

Comenzar con la instalación y marcar la opción de “Install from Internet” para que descargue el contenido necesario > Siguiente.

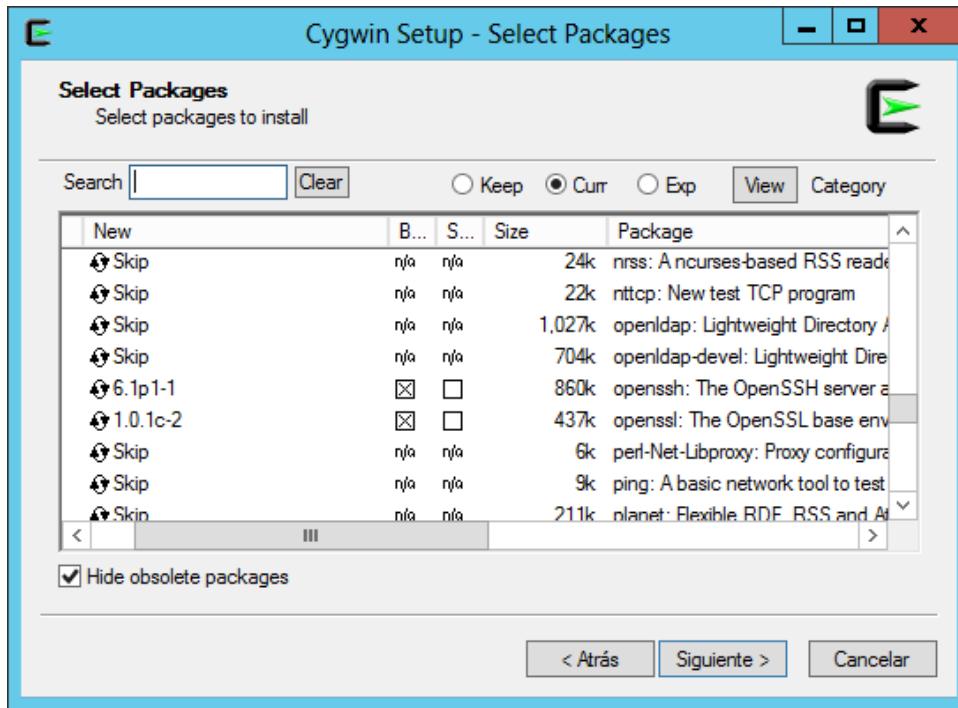
Colocar como directorio raíz “C:\cygwin” y dejar la opción de para todos los usuarios marcada > Siguiente.

Como directorio de paquetes local, colocar también la dirección “C:\cygwin” que se bajen los paquetes necesarios > Siguiente.

Elegir la opción de conexión a internet, por defecto “Direct Connection” > Siguiente.

De la lista de mirrors mostrada, elegir uno cualesquiera > Siguiente.

Desplegar la categoría “Net” y buscar OpenSSH y OpenSSL. Hacer click en el “Skip” de ambos para ver la versión a instalar > Siguiente.



Click en siguiente para resolver las dependencias que hayan.

Cuando termine de instalar todas las dependencias necesarias y los paquetes seleccionados, se podrá añadir un ícono en el Escritorio, por defecto se dejará marcado > Finalizar.

## Configurar SSH

Acceder al Escritorio y “Ejecutar como administrador” el acceso directo a Cygwin.

Para configurar el servidor SSH, escribir “ssh-host-config” y cuando solicite la separación de privilegios, elegir “Yes”.

Cuando solicite si crear una cuenta local llamada “sshd”, seleccionar “Yes”.

Cuando solicite instalar sshd como servicio, seleccionar “Yes”.

Como valor para el demonio, colocar el valor 7.

Al ser un Windows Server, la cuenta System no se puede utilizar, por tanto se debe crear una cuenta con privilegios suficientes, la configuración ofrece el usuario “cyg\_server”.

Cuando solicite cambiar el nombre, colocar “No” y cuando pida crear dicha cuenta colocar “Yes”.

Colocar una contraseña para el nuevo usuario, la contraseña debe cumplir las políticas de restricción del Servidor.

Reintroducida la contraseña, se completará la instalación y ya se podrá poner en marcha el servidor SSH con el comando “net start sshd”.

## Comprobación del servidor con cliente SSH

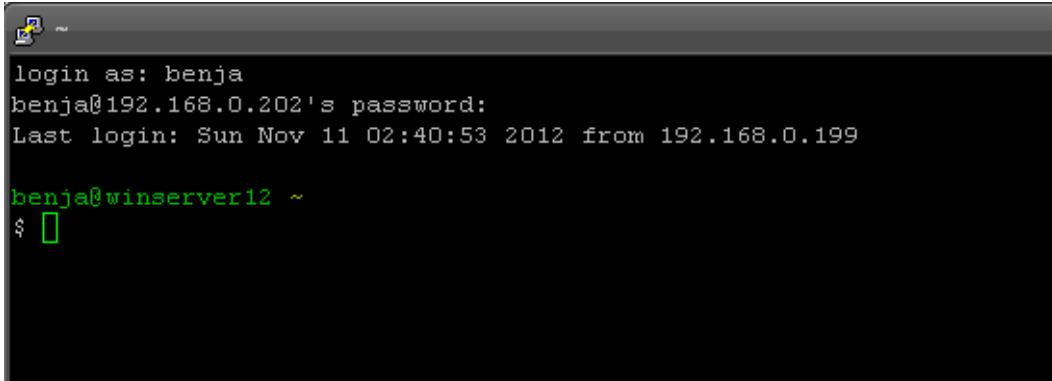
Antes de abrir un cliente ssh, es necesario abrir el puerto 22 en el Firewall.

Para ello, Panel de Control > Firewall de Windows > Configuración avanzada > Reglas de entrada > Nueva regla.

La regla es un Puerto > TCP, Local específico: 22 > Permitir la conexión > Aplicar la regla a los tres perfiles > Proporcionan un nombre a la regla > Finalizar.

Abrir un cliente SSH, colocar dirección y puerto del servidor. Si todo va bien, solicitará un usuario y contraseña, válido cualquier usuario del servidor o del Dominio.

Después de introducir la contraseña, se tendrá acceso al sistema mediante SSH.



```
benja@winserver12 ~
```

The screenshot shows a terminal window with a dark background and light-colored text. It displays a successful SSH login session. The text includes:

- "login as: benja"
- "benja@192.168.0.202's password:"
- "Last login: Sun Nov 11 02:40:53 2012 from 192.168.0.199"
- "benja@winserver12 ~"
- "\$ █"

### Acceso SSH mediante clave RSA

Editar el fichero /etc/sshd\_config y descomentar la línea “RSAAuthentication yes” y “Protocol 2”.

Reiniciar el servicio con “net stop ssh” y “net start ssh” o mediante Servicios de Windows.

En el cliente SSH que se quiera conectar con el servidor debe generar el par de claves RSA:

#### Linux

Ejecutar “ssh-keygen -t rsa” y guardar en la carpeta por defecto, en caso que exista sobreescribir.

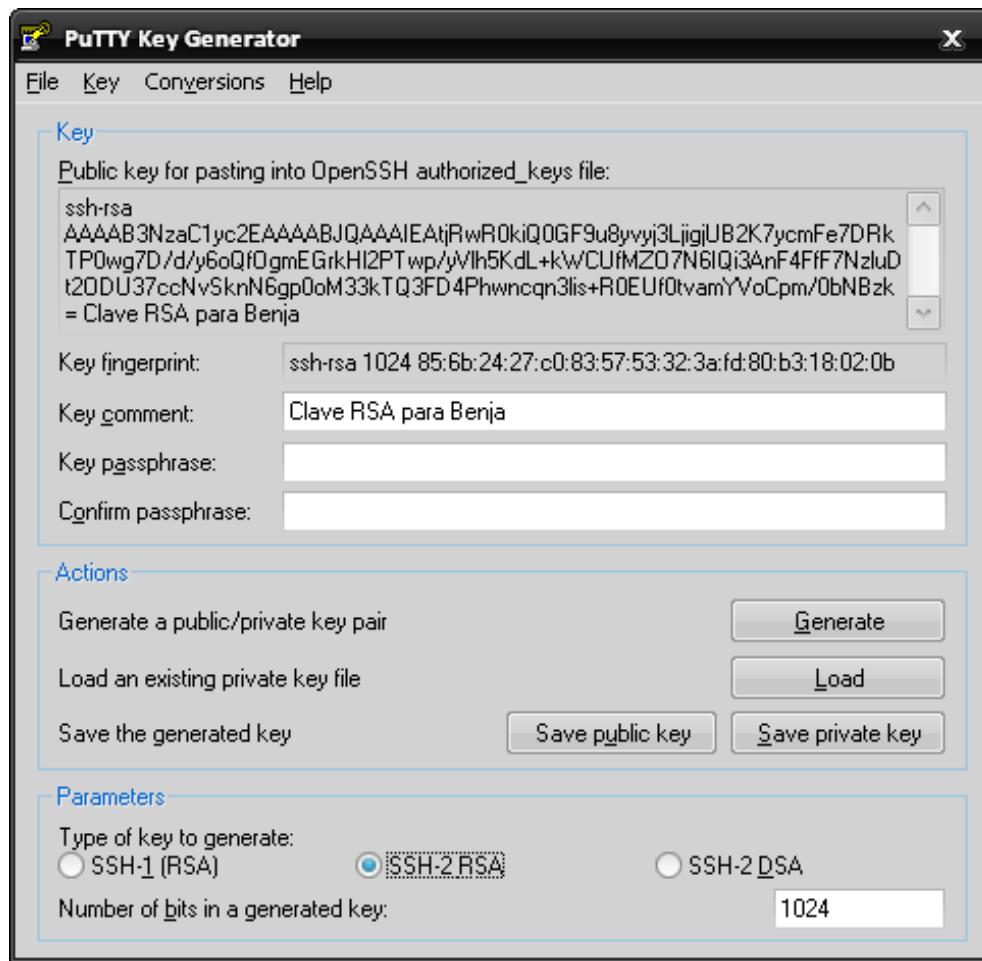
No introducir nada como “passphrase”.

Generada la clave pública, mediante SCP se envía la clave pública “id\_rsa.pub” al servidor SSH “scp ./ssh/id\_rsa.pub usuario@winserver12:~” que se guardará en el \$HOME.

En el servidor SSH, acceder al lugar de la clave pública y ejecutar: “cat id\_rsa.pub >> .ssh/authorized\_keys” para que añada la clave a la lista de claves autorizadas. Ahora en el cliente se podrá conectar con el usuario mediante SSH sin necesidad de introducir ninguna contraseña.

#### Windows

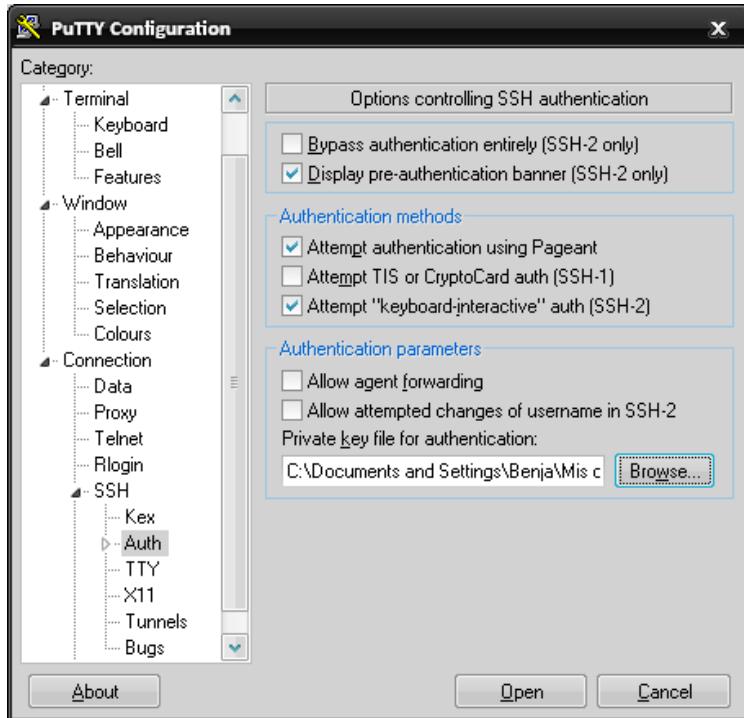
Descargar el programa “puttygen”, y generar una clave RSA para SSH-2. Colocar un comentario de clave descriptivo.



Copiar la clave pública e introducirla en “.ssh/authorized\_keys” del usuario que queramos conectarnos.

Introducir la clave mediante una conexión con el programa WinSCP o a través de Putty, pegando el código en la terminal.

Conectarse con el servidor SSH con Putty y con la clave RSA:



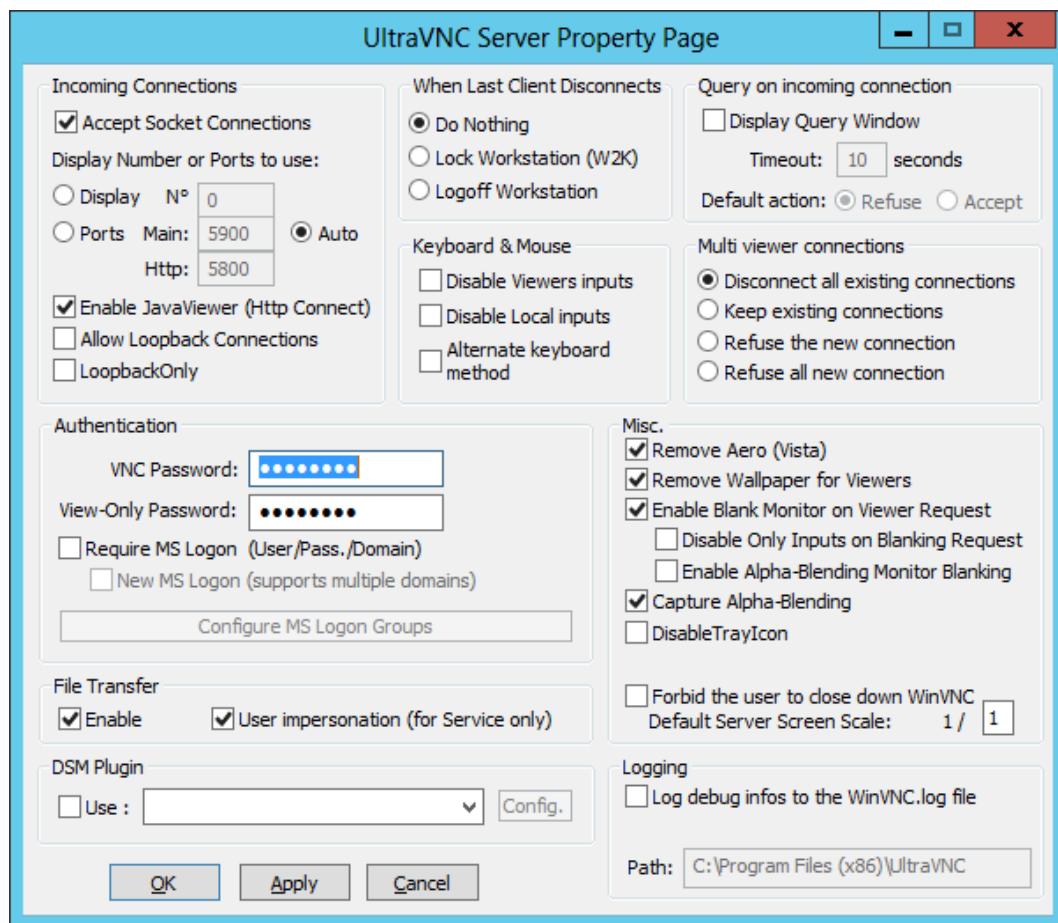
## Servidor VNC

Windows no incorpora un servidor VNC de forma nativa, por tanto hay que recurrir a programas de terceros para poder establecer un servidor VNC.

Acceder a <http://www.uvnc.com/downloads/ultravnc.html> para descargar una combinación de servidor VNC, cliente y muchas características más durante la instalación.

Seleccionar las opciones adecuadas para el servidor: modo silencioso y instalar como servicio, se recomienda esta última dado que el servidor VNC arrancará como servicio cada vez que el servidor inicie.

Una vez instalado el servidor VNC, requiere configuración para permitir el acceso:

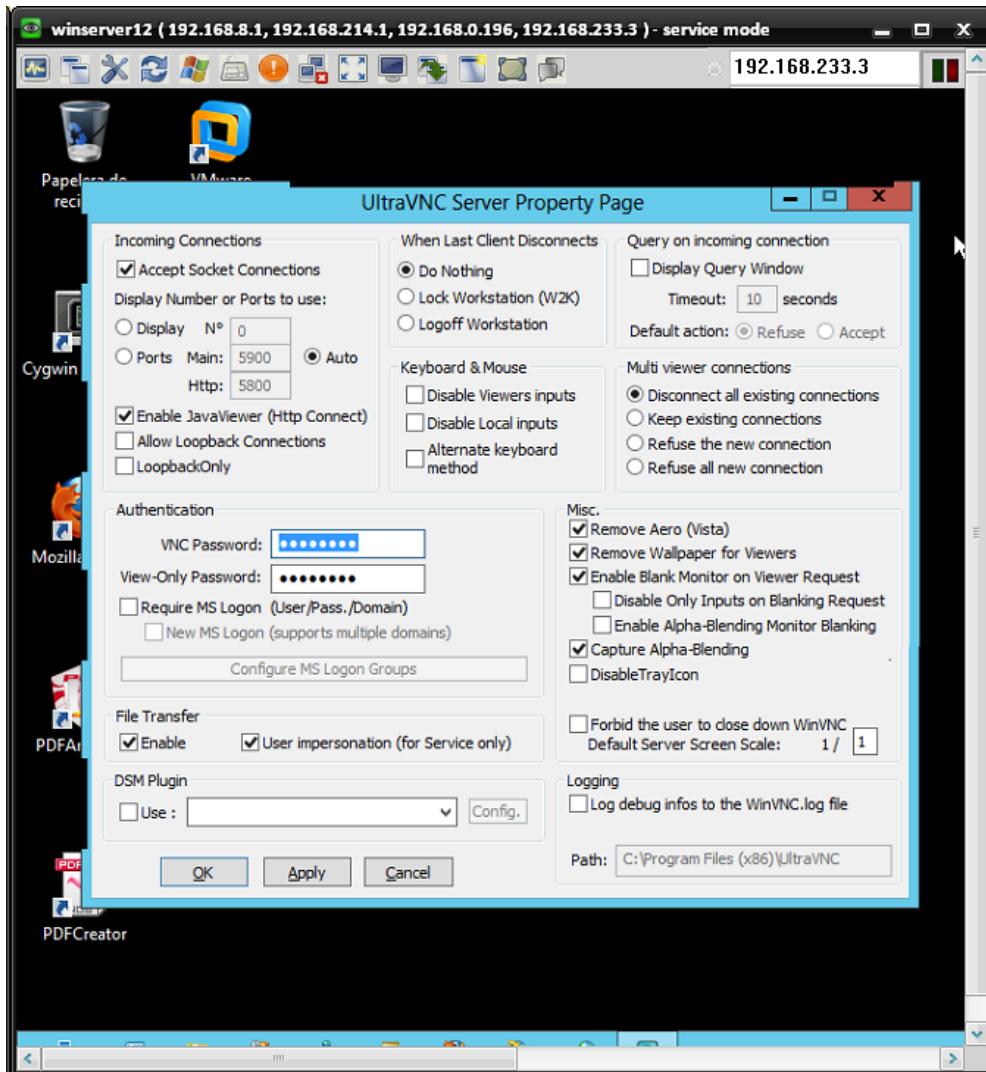


Se debe configurar la contraseña de acceso, si se permite la transferencia de archivos y configurar las múltiples opciones el resto de secciones.

### Cliente VNC

Descargar el mismo paquete que en el servidor pero durante la instalación sólo marcar el Cliente VNC.

Instalado, se introduce la IP del servidor VNC y durante la conexión se introduce la contraseña introducida en el Panel de administración del servidor VNC.



## Remote Desktop (Terminal Service)

Panel de Administrador del servidor > Administrar > Agregar roles y características > Dejar opciones por defecto > Siguiente > Siguiente > Siguiente.

Marcar “Servicios de Escritorio remoto” > Siguiente.

Marcar “Host de sesión de Escritorio remoto” > Siguiente > Instalar.

## Active Directory

En panel de Administrador del servidor > Menu Administrar -> Agregar roles y características

Tipo de instalación -> Instalación basada en características o en roles

Seleccionar el servidor local

Roles de servidor -> Servicios de dominio de Active Directory y aceptar las características incluidas

Confirmar los siguientes pasos e instalar.

## Configuración Active Directory

Seleccionar AD DS en el panel izquierdo del Administrador del servidor

Hacer click sobre el botón de notificaciones y seleccionar la opción de “Promocionar este servidor a controlador de dominio”.

- Promoción a controlador de dominio
- Añadir un nuevo bosque y especificar el nombre del dominio, siguiente.
- Incluir las características de servidor DNS y especificar contraseña para la recuperación de los Servicios de Directorio, siguiente.
- Ignorar el mensaje de aviso de DNS, siguiente.
- Especificar el nombre del dominio NetBIOS, siguiente.
- Comprobar que las rutas de la base de datos, logs y Sysvol son correctas, siguiente.
- Realizar la comprobación de prerequisitos, instalar.
- El equipo se reinicia sin dar aviso alguno para completar la instalación.

### **Comprobación Controlador de Dominio funcionando**

Cuando se reinicie el equipo, el nombre del Controlador de Dominio debe aparecer junto al nombre del usuario y el acceso a sus credenciales debe realizarse contra el controlador.

### **Puesta en marcha Active Directory**

En el panel de Administrador de Servidor > Herramientas > Centro de administración active Directory > Click servidor local

### **Creación Unidad organizativa**

Panel derecho > Nuevo > Unidad organizativa

Rellenar los datos que se consideren sobre la unidad organizativa, aceptar.

### **Creación Usuario**

En la nueva unidad organizativa, Panel derecho > Nuevo > Usuario

Rellenar los datos referentes al usuario e incluirlo en los grupos que se considere, aceptar.

### **Servidor DNS**

En panel de Administrador del servidor > Menu Administrar -> Agregar roles y características

Tipo de instalación -> Instalación basada en características o en roles

Seleccionar el servidor local

Roles de servidor -> Servidor DNS y aceptar las características incluidas

Confirmar los siguientes pasos e instalar.

### **Configuración Servidor DNS**

Seleccionar DNS en el panel izquierdo del Administrador del servidor

Menú Herramientas > DNS

### **Añadir registros al dominio principal**

DNS > (NombreServer) > Zonas de búsqueda directa > (dominio)

Creadas por defecto los registros tipo NS y A correspondientes al servidor

Añadir los registros que se consideren

### **Configuración de los reenviadores**

DNS > (NombreServer) > Reenviadores

Añadir las ip's de los servidores DNS para resolver consultas que el servidor DNS local no pueda resolver

Editar > Añadir 8.8.8.8 y 8.8.4.4 como servidores a reenviar.

### Configuración de los servidores raíz

Por defecto el servidor DNS ya contiene la información de los distintos servidores raíz a los cuales acceder cuando los servidores configurados como reenviadores no están disponibles.

### Comprobacion servidor DNS funcionando

DNS > (NombreServer) > Click derecho > Ejecutar nslookup

Escribir google.com y comprobar que se obtiene la dirección ip correspondiente.

### Posibles problemas

Asegurarse que el servidor DNS sobre el que se está realizando la petición es el local.

En Centro de Redes y recursos compartidos > Seleccionar las conexiones disponibles > Propiedades > Protocolo de Internet versión 4 > Configuración manual servidor DNS > Anotar 127.0.0.1

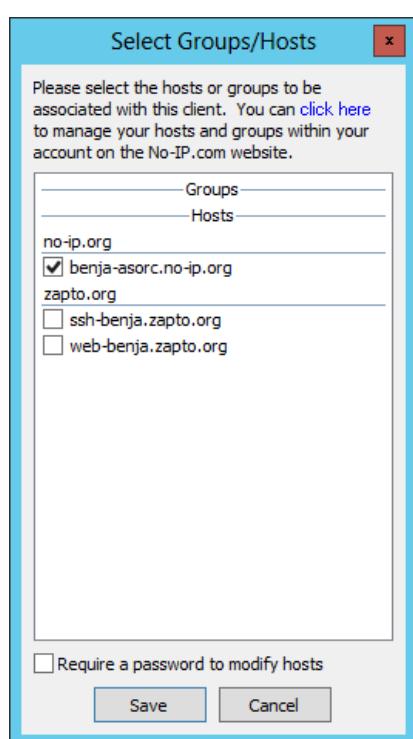
Aceptar y mediante consola, realizar una consulta DNS a través de nslookup.

### Dynamic DNS - No-IP.org

Para instalar un servicio que controle el cambio de IP externa, hay que acceder a la web no-ip.org, registrar una cuenta y añadir el primer hostname.

Una vez registrados, se deberá descargar el cliente que controle los cambios de IP externa.

Con el cliente instalado se deberá elegir qué host o grupo asociar a dicho cliente:



Una vez seleccionado, el cliente comenzará la monitorización del estado de la IP externa, cuando se detecte un cambio será notificado a la Web del servicio no-ip.org.

## Servidor DHCP

En panel de Administrador del servidor > Menu Administrar -> Agregar roles y características

Tipo de instalación -> Instalación basada en características o en roles

Seleccionar el servidor local

Roles de servidor -> Servidor DHCP y aceptar las características incluidas

Confirmar los siguientes pasos e instalar.

## Configuración Post-instalación

Usar las credenciales de Administrador para autorizar DHCP en Active Directory, confirmar.

## Configuración Servidor DHCP

Seleccionar DHCP en el panel izquierdo del Administrador del servidor

Menú Herramientas > DHCP

### Añadir nuevo ámbito

DHCP > (nombreServidor) > IPv4 > Click último ícono barra de navegación

Siguiente > Especificar nombre de ámbito > Definir el intervalo de IP a asignar >

Siguiente

Completar o dejar en blanco la lista de direcciones a excluir > Siguiente

Especificar el tiempo deseado en la duración de la Concesión de una dirección IP, 3 días recomendable > Siguiente

Marcar opción de “Configurar las opciones de DHCP ahora” > Siguiente

Especificar la dirección IP del enrutador, puede ser la IP del propio servidor >

Siguiente

Especificar el servidor DNS primario, colocar direcciones IP de los servidores DNS a utilizar > Siguiente

Especificar el servidor WINS con la dirección IP del servidor local para peticiones de clientes Windows > Siguiente

Seleccionar “Activar este ámbito ahora” > Siguiente > Finalizar

## Habilitar Sincronización DHCP con DNS

DHCP > (nombreServidor) IPv4 > Propiedades del Ámbito > Pestaña DNS

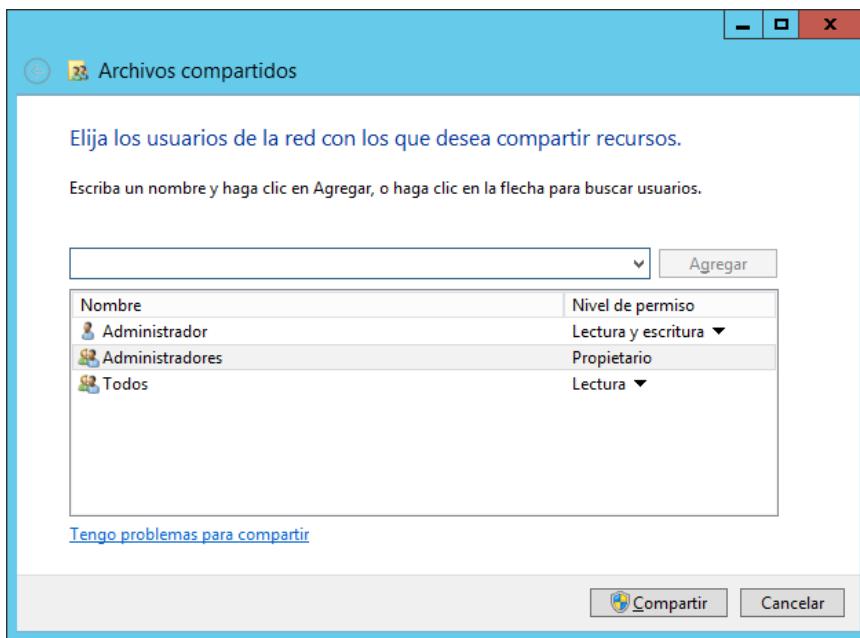
Marcar “Habilitar actualizaciones DNS dinámicas de acuerdo con la siguiente configuración” y “Actualizar siempre dinámicamente registros DNS A y PTR”.

Marcar “Descartar registros A y PTR cuando se elimine la concesión”.

## Compartir Archivos

Crear una carpeta en cualquier lugar del sistema > segundo botón botón del ratón > Compartir con > Uso compartido avanzado.

Definir los permisos para grupos y usuarios y Compartir:



### Acceso al recurso compartido

Acceder a Mi PC > Herramientas > Conectar a unidad de red > Seleccionar unidad y acceso compartido:



Finalizar y en base a los permisos definidos en la compartición del recurso se podrá crear o leer los archivos que contenga el recurso.

### Servidor de Impresión

Panel de Administrador del servidor > Administrar > Agregar roles y características > Dejar opciones por defecto > Siguiente > Siguiente > Siguiente.

En Roles de Servidor > Marcar Servicios de impresión y documentos > Agregar características > Siguiente > Siguiente.

En la sección de Servicios de rol > Marcar sólo la opción “Servidor de impresión” > Instalar.

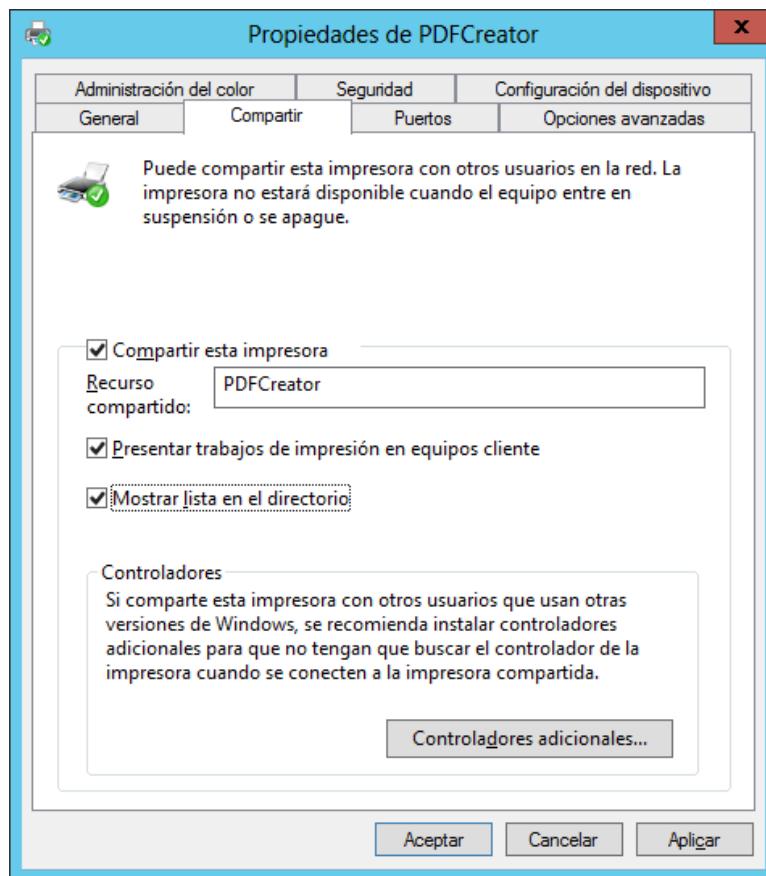
## Configuración y acceso a la Impresora

Herramientas Administrativas > Administración de impresión > Desplegar

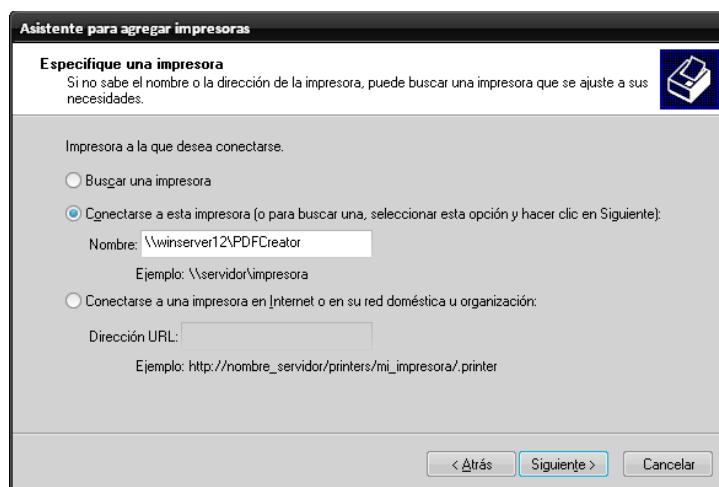
Servidores de impresión y el el servidor local.

Seleccionar la impresora deseada > Administrar uso compartido.

Compartir la impresora y mostrar lista en el directorio:



Dado el nombre del servidor y de la impresora, añadir la impresora a cualquier cliente:



Seguir con el asistente para que se descarguen los controladores de la impresora y finalizar el asistente.

## **Merak**

Acceder a la página oficial <http://www.icewarp.es/descargas/>, llenar el formulario de contacto y se enviará un correo con el enlace mediante el cual se puede descargar el programa.

Durante la instalación se selecciona el modo de instalación básico, ya que es suficiente con una instalación para un soporte de al menos 500 cuentas.

Se deberá especificar el nombre de host, dominio primario, una cuenta de administrador y una contraseña segura.

Finalizado el asistente se podrá entrar al Panel de Administración de Merak.

### Configuración Merak

Se necesita la creación de registros MX, A y SRV en el servidor DNS para agrupar las cuentas del Active directory con Merak:

DNS

Correo (MX) 'benjaw12.es':

No hay registros de DNS

SmartDiscover (SRV) '\_autodiscover.\_tcp.benjaw12.es':

No hay registros de DNS

SmartDiscover (A) 'autodiscover.benjaw12.es':

No hay registros de DNS

WebDAV (SRV) '\_caldav.\_tcp.benjaw12.es':

No hay registros de DNS

WebDAV (SRV) '\_caldavs.\_tcp.benjaw12.es':

No hay registros de DNS

WebDAV (SRV) '\_carddav.\_tcp.benjaw12.es':

No hay registros de DNS

WebDAV (SRV) '\_carddavs.\_tcp.benjaw12.es':

No hay registros de DNS

Mensajería instantánea (SRV) '\_xmpp-server.\_tcp.benjaw12.es':

No hay registros de DNS

Mensajería instantánea (SRV) '\_xmpp-client.\_tcp.benjaw12.es':

No hay registros de DNS

iSchedule (SRV) '\_ischedule.\_tcp.benjaw12.es':

No hay registros de DNS

SPF (TXT) 'benjaw12.es':  
No hay registros de DNS

Es necesario añadir una nueva cuenta de usuario, en Cuenta > Crear nuevo > Usuario

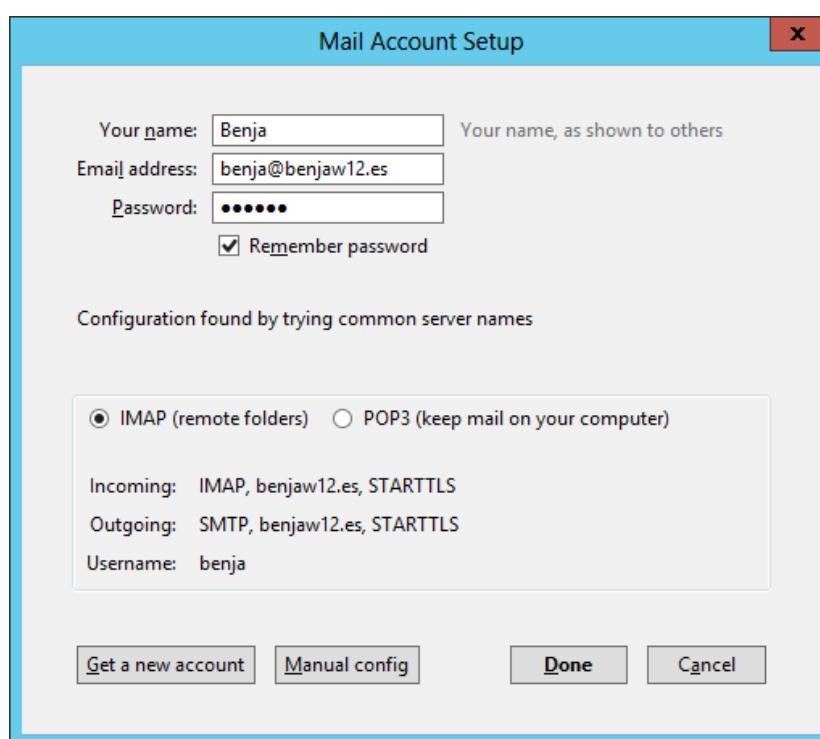
### Comprobación Merak

Merak incluye un cliente de Correo Administración Web, pero para ello debe estar instalado y configurado el IIS.

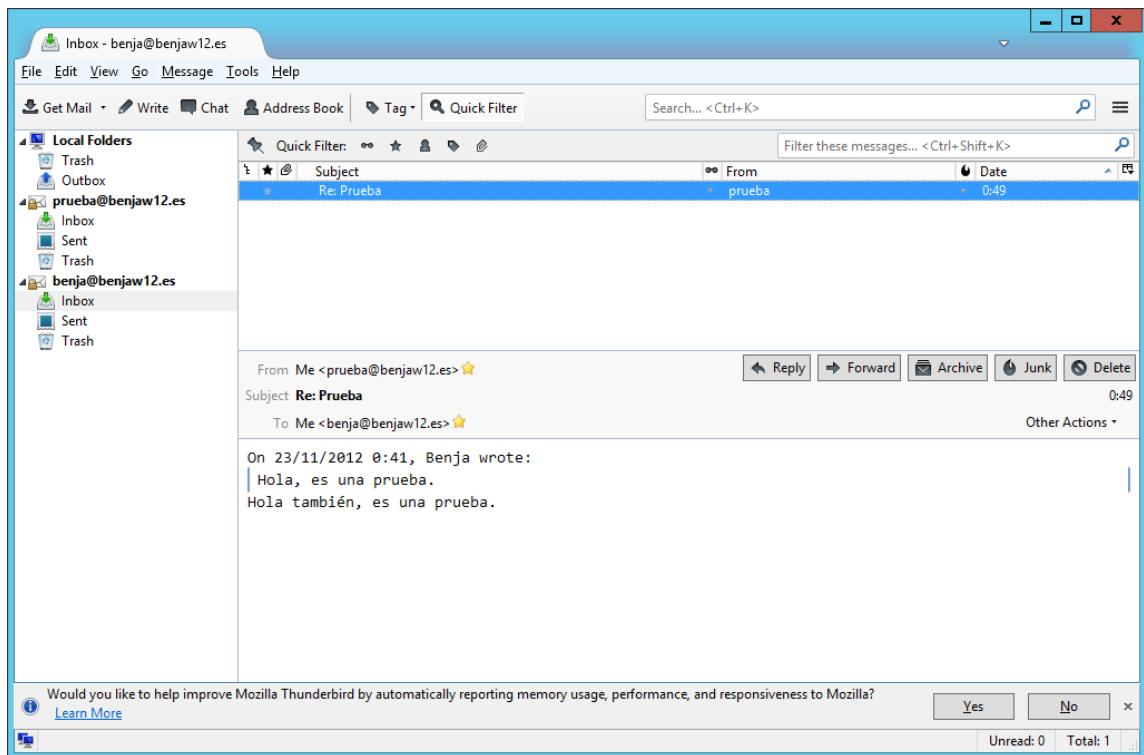
Por ello se utilizará otro cliente de correo para comprobar el funcionamiento de Mekar.

Se utilizará el Cliente Thunderbird, un cliente que permitirá comprobar gran parte de las funcionalidades que incorpora Merak.

Introducir los datos del usuario anteriormente creado y se comprobará la validez del usuario:



Aceptamos, y enviamos un email de prueba a un usuario cualquiera.  
En este caso se ha respondido el mensaje enviado a un usuario de prueba para comprobar que ambas cuentas pueden enviar y recibir:

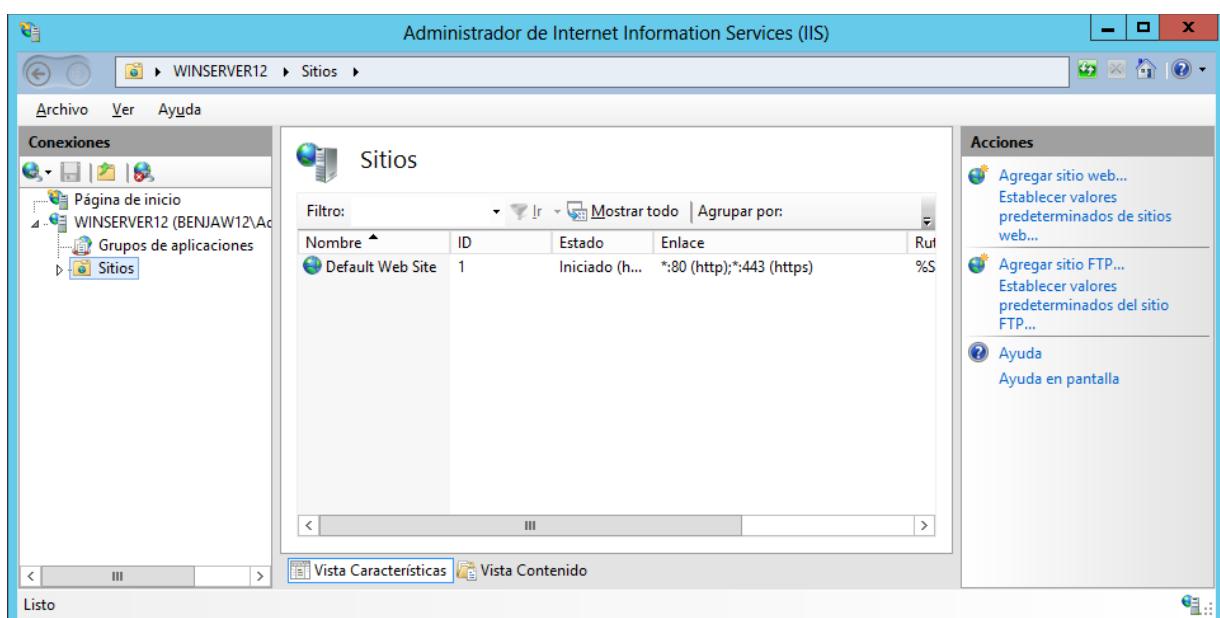


## Servidor FTP

Panel de Administrador del servidor > Administrar > Agregar roles y características  
> Dejar opciones por defecto > Siguiente > Siguiente > Siguiente.  
En Roles de Servidor > Desplegar el Rol Servidor Web > Marcar Servidor FTP >  
Siguiente > Siguiente > Instalar.

## Añadir sitio a servidor FTP

Acceder al Administrador de IIS > desplegar el servidor > seleccionar sitios.



Hacer click sobre “Agregar sitio FTP” y en el asistente indicar los datos del servidor

## FTP.

En la pantalla de “Configuración de enlaces y SSL” elegir la IP y puerto o dejar “Todas las no asignadas” por defecto.

Dejar marcada la opción de “Iniciar sitio FTP automáticamente” y en el apartado SSL, seleccionar “Sin SSL”.

En la siguiente pantalla de autenticación y autorización, marcar “Básica”, permitir el acceso a “Roles o grupos de usuarios especificados” > especificar “Administradores” o el grupo que se desee y marcar tanto la opción de Leer como Escribir > Finalizar.

## Posibles problemas

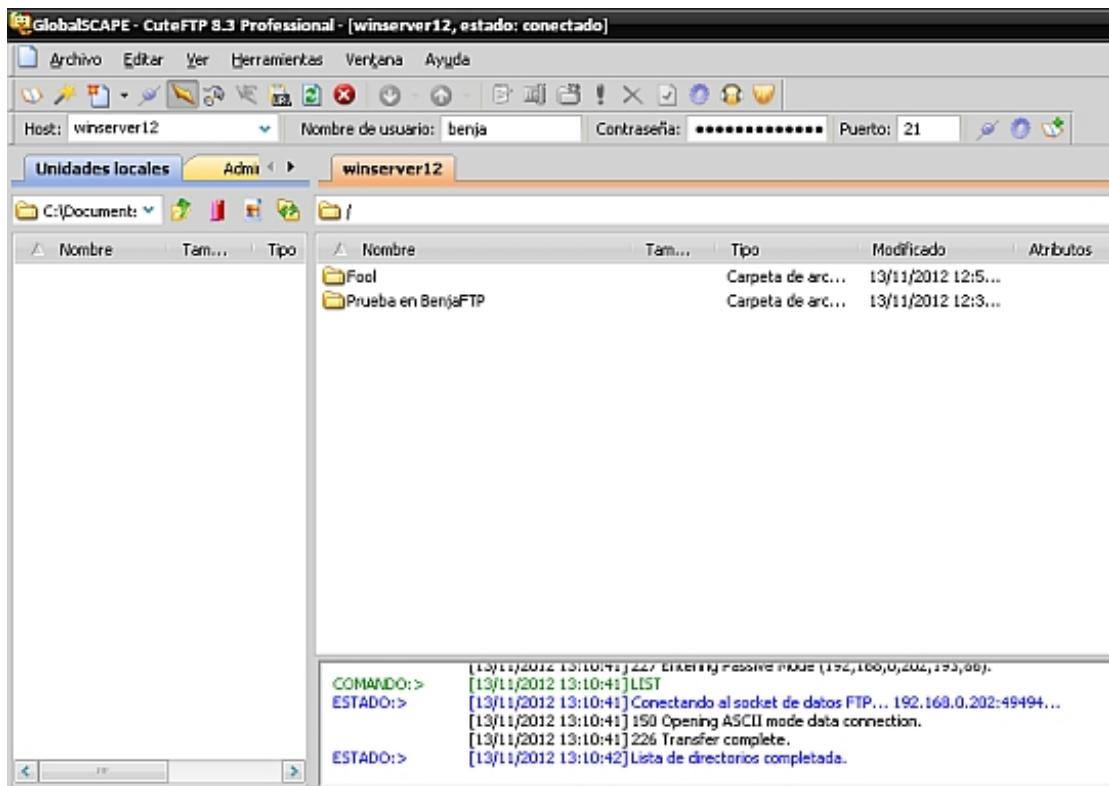
Verificar que se han creado las reglas oportunas para permitir el tráfico entrante y saliente en el Firewall.

Acceder a “Firewall de Windows con seguridad avanzada” y comprobar las reglas sobre FTP. Si no existen reglas se deben crear dos reglas que permitan el tráfico por el puerto 21 entrante y el 20 saliente.

## Comprobación acceso a Servidor FTP

Desde cualquier cliente FTP, realizar una petición al servidor mediante su IP o nombre e introducir un usuario que pertenezca al grupo de Administradores:





## Herramientas de Virtualización: VMware

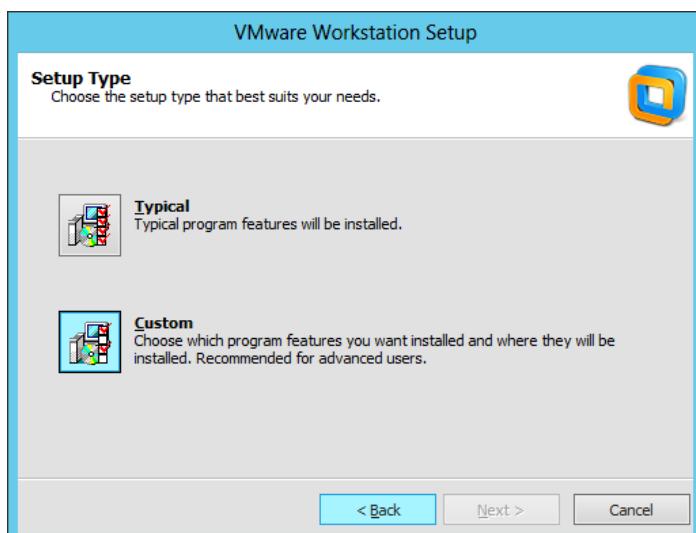
Acceder a la página Web de [vmware.com](http://vmware.com), registrarse y validar la cuenta.

\*No se recomienda instalar VMware Server en un controlador de dominio de Windows, por ese motivo se recomienda a continuación otro producto.

Acceder a la sección de Productos y Descargas y seleccionar “VMware Workstation”.

Proceder a su descarga y posterior instalación.

Durante la instalación, seleccionar Instalación personalizada:



Sólo Marcar la opción “Enhanced Keyboard Utility” para permitir el soporte al

teclado Español.

En la pantalla de introducción del puerto de escucha del servicio, por defecto 443, colocar un puerto diferente en caso que el **IIS** esté activo en el servidor para evitar un conflicto en la conexión.

Desmarcar tanto la opción de “Check for product updates on startup” como “Help improve VMware Workstation” y comenzar con la instalación.

Introducir la clave solicitada en la versión de prueba y finalizar la instalación.

## Slackware 14.0

### Licencia

GPL

### Gestión del particionamiento

Durante el proceso de instalación se deben definir las particiones que se considere con las herramientas que se proporcionan durante la instalación.

Para este caso, se han definido tres particiones más la del Swap:

- Una partición que se sitúa en root “/”
- Una segunda que se sitúa en usr “/usr”
- Una tercera que se sitúa en var “/var”

Esta gestión permite aislar toda la paquetería, programas y contenido de las aplicaciones de la configuración del sistema, archivos temporales y archivos personales.

### Parada y arranque de servicios

Slackware posee su sistema de scripts de inicio y parada de servicios alojado en “/etc/rc.d”. El fichero “/etc/rc.d/rc.local” contiene las directivas para los servicios que inicien después de que los servicios del sistema hayan iniciado.

En “/etc/rc.d/rc.[4 | 6 | S | M]” se encuentran los scripts de inicio de los servicios para los modos gráficos, multiusuarios y monousuario

### Servidor SSH

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search ssh” e instalando los paquetes que corresponden al servidor SSH.

### Configuración SSH

Editar el fichero “/etc/ssh/sshd\_config” y descomentar la línea “RSAAuthentication yes” y “Protocol 2”. Para permitir la versión 2 del protocolo y permitir autenticación con certificados RSA.

### Reiniciar el servicio

Para reflejar los cambios realizados en la configuración, ejecutar “/etc/rc.d/rc.sshd stop” y “/etc/rc.d/rc.sshd start”.

Realizar un restart está orientado a actualizar la configuración cuando un

Administrador ha accedido y no se quiere que se corte la conexión

### Acceso SSH mediante clave RSA

En el cliente SSH que se quiera conectar con el servidor debe generar el par de claves RSA:

#### Linux

Ejecutar “ssh-keygen -t rsa” y guardar en la carpeta por defecto, en caso que exista sobreescribir.

No introducir nada como “passphrase”.

Generada la clave pública, mediante SCP se envía la clave pública “id\_rsa.pub” al servidor SSH “scp ./ssh/id\_rsa.pub usuario@winserver12:~” que se guardará en el \$HOME.

En el servidor SSH, acceder al lugar de la clave pública y ejecutar: “cat id\_rsa.pub >> .ssh/authorized\_keys” para que añada la clave a la lista de claves autorizadas.

Ahora en el cliente se podrá conectar con el usuario mediante SSH sin necesidad de introducir ninguna contraseña.

#### Windows

Descargar el programa “puttygen”, y generar una clave RSA para SSH-2. Colocar un comentario de clave descriptivo.

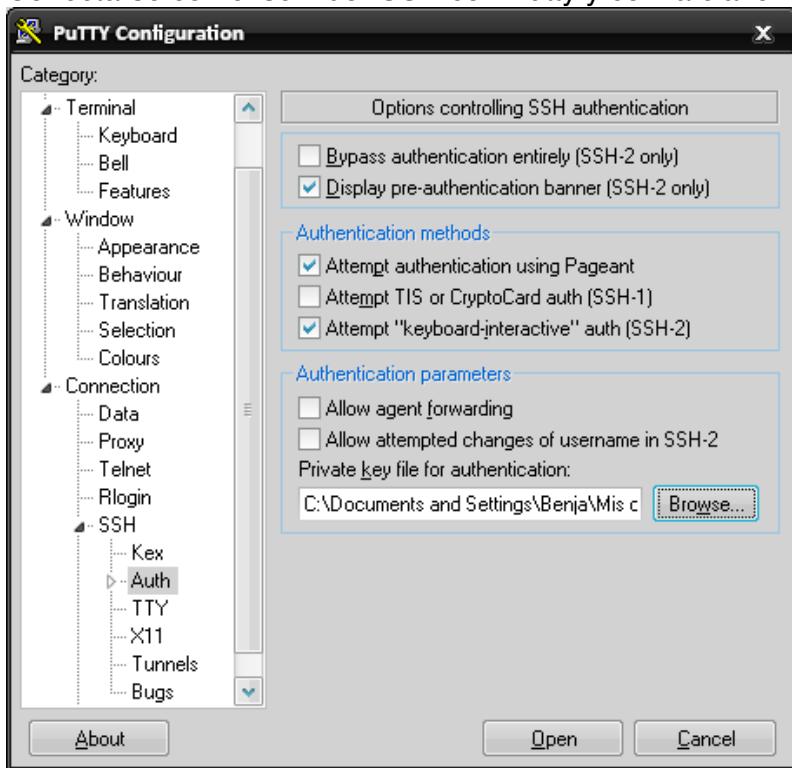


Copiar la clave pública e introducirla en “.ssh/authorized\_keys” del usuario que

queramos conectarnos.

Introducir la clave mediante una conexión con el programa WinSCP o a través de Putty, pegando el código en la terminal.

Conectarse con el servidor SSH con Putty y con la clave RSA:



## Servidor VNC - TightVNC

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search vnc” e instalando los paquetes que corresponden al servidor VNC.

En la configuración por defecto, VNC no creará los archivos de configuración por usuario, por tanto se tiene que ejecutar para el usuario que quiera ser accedido vía VNC: “vncserver”

Se introduce una clave para acceder con el usuario actual y no se introduce una contraseña para el modo “view-only”.

VNC creará los archivos de configuración para ese usuario en su home y además se especificará en qué pantalla está disponible, por defecto la 1 (:1).

En el archivo “.vnc/xstartup” se encuentra la configuración de la visualización, resolución, colores, etc.

Cada vez que se modifique ese fichero es necesario reiniciar el servicio VNC. Para ello hay que dotar de permisos 755 al demonio de VNC. “chmod 755 /etc/rc.d/rc.vncservers”

Y ejecutar: “/etc/rc.d/rc.vncservers restart”

## Arranque de usuario por defecto

Editar el fichero “`/etc/rc.d/rc.vncservers.conf`” y descomentar la última línea añadiendo el usuario con que se accederá vía VNC.  
Reiniciar el servicio: “`/etc/rc.d/rc.vncservers restart`”

### Añadir el VNC al arranque de servicios

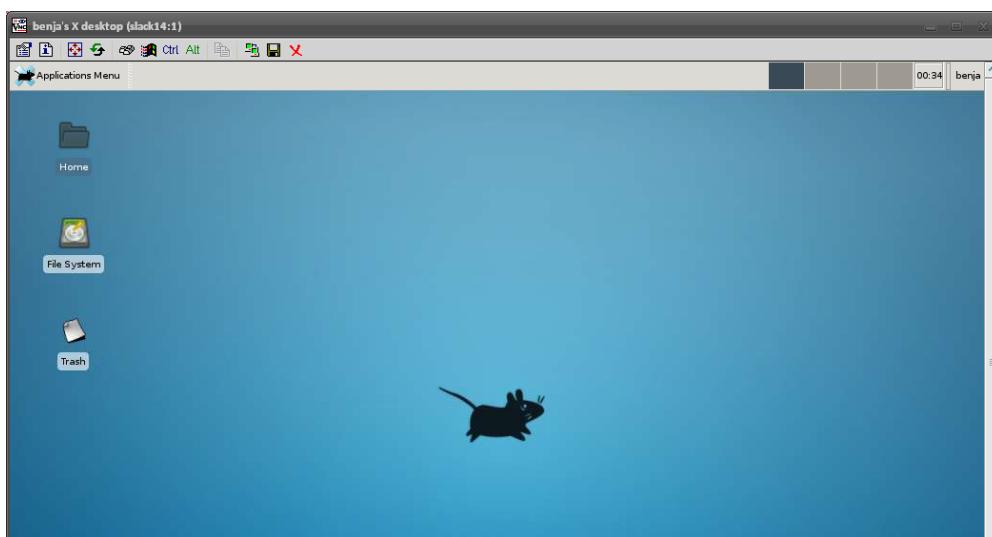
Añadir el siguiente código al final del archivo “`/etc/rc.d/rc.local`”:

```
# Start VNC server
# If you do not wish this to be executed here then comment it out,
# and the installer will skip it next time.
if [ -x /etc/rc.d/rc.vncservers ]; then
    /etc/rc.d/rc.vncservers start
fi
```

Cada vez que inicie la máquina se creará una sesión VNC para el usuario que se haya especificado en el archivo .conf.

### Acceso mediante VNCViewer

Se puede acceder mediante un cliente en Windows, Linux o una interfaz en Java (<http://www.tightvnc.com/download-old.php>)



### Determinación IP estática

En Slackware se puede realizar el proceso de dos formas:

- Sencilla: ejecutar “netconfig” para ejecutar el asistente de configuración.
- Compleja: editar los distintos ficheros de configuración de los interfaces.

Se ha elegido la opción compleja para familiarizarse con la estructura que utiliza el sistema y por la utilización de un segundo interfaz de red.

Se utilizará una interfaz con direccionamiento IP estático y el otro con direccionamiento por DHCP.

Como usuario root, editar el fichero “`/etc/rc.d/rc.inet1.conf`” y para cada interfaz colocar los datos necesarios. Para la situación arriba planteada:

```

# Config information for eth0:
IPADDR[0]="192.168.X.X"
NETMASK[0]="255.255.255.0"
USE_DHCP[0]="no"
DHCP_HOSTNAME[0]="""

# Config information for eth1:
IPADDR[1]=""
NETMASK[1]=""
USE_DHCP[1]="yes"
DHCP_HOSTNAME[1]="""

```

Al utilizar DHCP en un interfaz, no es necesario especificar una dirección por defecto:

```

# Default gateway IP address:
GATEWAY=""

```

### **Reiniciar la red**

Para que se reflejen los cambios anteriores es necesario reiniciar la red:  
“/etc/rc.d/rc.inet1 restart”

### **XDMCP**

En Slackware ya posee de forma nativa soporte para XDMCP, pero por defecto viene desactivado.

### **Activar XDMCP**

Editar el archivo “/etc/X11/xdm/xdm-config” y comentar la línea (añadir un ! delante) que contenga: “*DisplayManager.requestPort: 0*”  
Así se permite la escucha de peticiones XDMCP.

Editar el archivo “/etc/X11/xdm/Xaccess” y quitar el comentario de la línea: “*#\* #any host can get a login window*”  
Para permitir que todos los usuario pueda ver la pantalla de logeo.

Cambiar al runlevel gráfico de la máquina, editando el archivo “/etc/inittab” y cambiando: *id:3:initdefault:* por *id:4:initdefault:*

### **Acceder vía XDMCP**

En un cliente Linux con el servidor X instalado, ejecutar: “*X -query IP\_HOST :1*”

### **FreeNX**

Para Slackware es necesario la descarga de los archivos fuente:

<http://www.nomachine.com/select-package.php?os=linux&id=1>

Seleccionar los paquetes acorde con la arquitectura del procesador.

Se deben descargar: el nodo, el servidor y el cliente.

Mover los archivos descargados a “/usr” y descomprimirlos.

Crear los siguientes directorios en “/etc/init.d”: “*mkdir /etc/init.d/rc{0,2,3,5,6}.d*”

Instalar el nodo y el servidor: “*/usr/NX/scripts/setup/nxnode --install suse*” y

`"/usr/NX/scripts/setup/nxserver --install suse"`

### **Configuración FreeNX**

**\*\*Bug en el archivo de comprobación de claves de SSH**

El fichero de configuración de SSH (`"/etc/ssh/sshd_config"`) hay una línea que marca el fichero para comprobar el acceso por clave mediante SSH (`"AuthorizedKeysFile .ssh/authorized_keys"`). Pero en el home de NX, (`"/usr/NX/home/nx/.ssh"`) no existe ese fichero, por tanto una posible solución es renombrar el fichero `"/usr/NX/home/nx/.ssh/ authorized_keys2"`:  
`"mv /usr/NX/home/nx/.ssh/ authorized_keys2 /usr/NX/home/nx/.ssh/ authorized_keys"`.

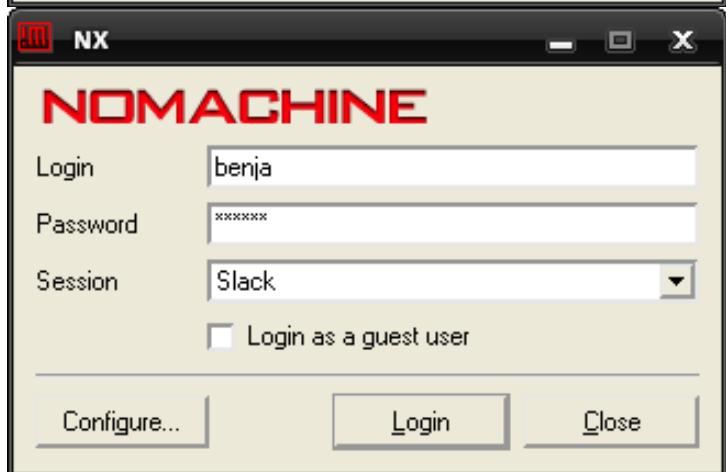
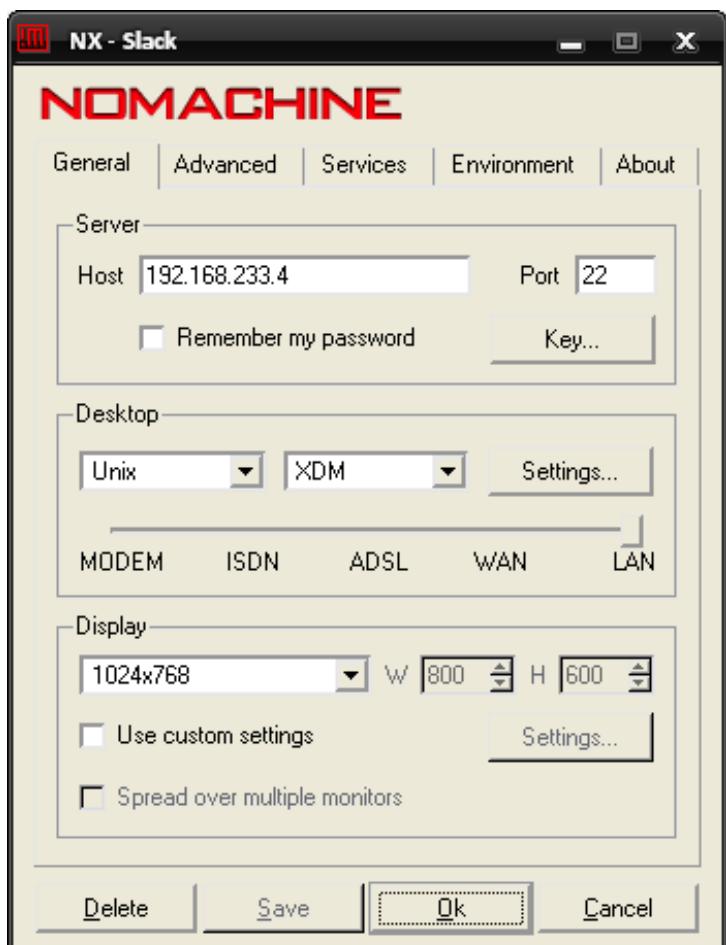
Cambiar los permisos de los archivos del home:

```
chown nx:root /usr/NX/home/nx/.ssh/authorized_keys  
chmod 0644 /usr/NX/home/nx/.ssh/authorized_keys  
chown nx:root /usr/NX/home/nx/.ssh/default.id_dsa.pub  
chmod 0644 /usr/NX/home/nx/.ssh/default.id_dsa.pub
```

### **Acceso con cliente NX**

Descargar un cliente para Windows: [http://www.nomachine.com/download-package.php?Prod\\_Id=3835](http://www.nomachine.com/download-package.php?Prod_Id=3835)

Seguir los pasos del asistente y finalmente la configuración de conexión con el servidor NX estará lista:





## OpenLDAP

Acceder a <http://www.openldap.org/software/download/> y obtener la última versión.

Descomprimir el paquete bajado, acceder al directorio creado y ejecutar:

`./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var`

Después ejecutar “`make depend`”, “`make`” y “`make install`”

Crear el script del servicio, crear el archivo “`rc.openldap`” en “`/etc/rc.d/`” y añadir lo siguiente:

```
#!/bin/bash

bin="/usr/libexec/slapd"
host="192.168.233.4"
port="389"
pid_file="/var/run/slapd/slapd.pid"

function start_slapd {
echo "Starting slapd: $bin"
$bin -h ldap://$host:$port
}

function stop_slapd {
if [[ -f $pid_file ]]; then
    kill -15 `cat $pid_file`
    sleep 2
fi}
```

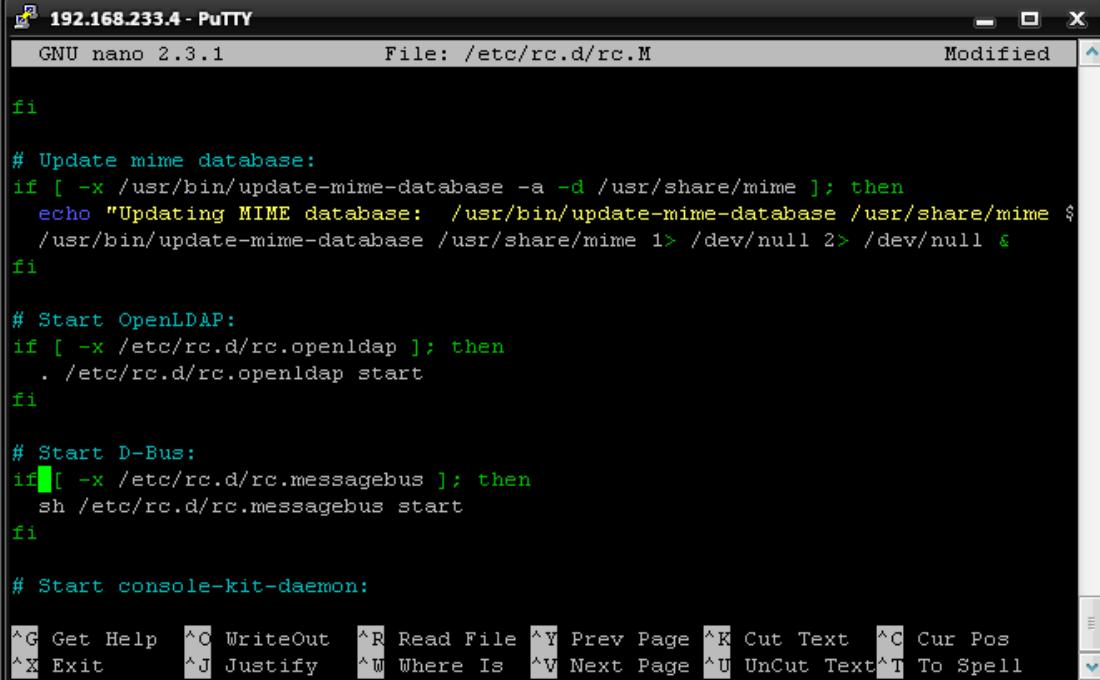
```

}

if [[ $1 == "start" ]]; then
    start_slapd
fi

```

Dotar al script de permisos de ejecución: “`chmod +x /etc/rc.d/rc.openldap`”  
 Abrir el fichero “`/etc/rc.d/rc.M`” y buscar la sección de código sobre LDAP, copiarla y pegarla justo antes de la sección sobre D-Bus:



```

192.168.233.4 - Putty
GNU nano 2.3.1          File: /etc/rc.d/rc.M          Modified

fi

# Update mime database:
if [ -x /usr/bin/update-mime-database -a -d /usr/share/mime ]; then
    echo "Updating MIME database: /usr/bin/update-mime-database /usr/share/mime $"
    /usr/bin/update-mime-database /usr/share/mime 1> /dev/null 2> /dev/null &
fi

# Start OpenLDAP:
if [ -x /etc/rc.d/rc.openldap ]; then
    ./etc/rc.d/rc.openldap start
fi

# Start D-Bus:
if [ -x /etc/rc.d/rc.messagebus ]; then
    sh /etc/rc.d/rc.messagebus start
fi

# Start console-kit-daemon:

```

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
 ^X Exit ^J Justify ^W Where Is ^V Next Page ^U Uncut Text ^T To Spell

## Configuración OpenLDAP

Modificar el archivo “`/etc/openldap/slapd.conf`” con lo siguiente:

```

# SCHEMES
include      /etc/openldap/schema/core.schema
include      /etc/openldap/schema/cosine.schema
include      /etc/openldap/schema/inetorgperson.schema
include      /etc/openldap/schema/nis.schema

# ACL
include      /etc/openldap/acl.conf

# DATABASE
database    bdb
directory   /var/lib/ldap/example.com

# GENERIC
pidfile    /var/run/slapd/slapd.pid
argsfile   /var/run/slapd/slapd.args
suffix     "dc=example,dc=com"

```

```
rootdn      "cn=ldapadmin,dc=example,dc=com"
rootpw      {SSHA}MWyKewM8KHu22/4SdiYYuyXEoAjrZEoQ
loglevel    256
sizelimit   unlimited
```

Cambiar *example* y *com* por el dominio que se prefiera. La contraseña es temporal, más tarde se definirá una en concreto.

Crear el archivo de las ACLS (“/etc/openldap/acl.conf”) y agregar:

```
access to attrs=userPassword
by self write
```

```
by * auth
```

```
access to dn.base=""
by * read
```

```
access to * by self write
by * read
```

Crear el directorio especificado en el archivo de configuración y copiar la base de datos de ejemplo:

```
mkdir -p /var/lib/ldap/example.com
cp /var/lib/openldap-data/DB_CONFIG.example
/var/lib/ldap/example.com/DB_CONFIG
```

Crear el directorio para los PIDfiles del demonio:

```
mkdir /var/run/slapd/
```

Crear la contraseña para root de LDAP:

```
slappasswd
New password:
Re-enter new password:
{SSHA}MWyKewM8KHu22/4SdiYYuyXEoAjrZEoQ
```

Colocar todo el string en el archivo “/etc/openldap/slapd.conf” en la directiva *rootpw*

Editar el la configuración del Syslog “/etc/syslog.conf” para separar los mensajes de LDAP a un log diferente:

```
# LDAP
local4.* <- tab -> /var/log/ldap.log
```

```
touch /var/log/ldap.log
chmod 644 /var/log/ldap.log
```

```
/etc/rc.d/rc.syslog restart
```

Intentar lanzar slapd: “/usr/libexec/slapd -h ldap://192.168.233.4:389”

Ahora se debería ver algo como esto en el ldap.log:

```
tail -f /var/log/ldap.log
Nov 17 18:09:11 slack14 slapd[3572]: @(#) $OpenLDAP: slapd 2.4.33 (Nov 17
2012 14:31:37) $ ^lroot@slack14:/root/openldap-2.4.33/servers/slapd
Nov 17 18:09:11 slack14 slapd[3573]: bdb_monitor_db_open: monitoring disabled;
configure monitor database to enable
Nov 17 18:09:11 slack14 slapd[3573]: slapd starting
```

Y comprobar también que realmente está en ejecución:

```
pgrep -fl slapd
3573 /usr/libexec/slapd -h ldap://192.168.233.4:389
```

### **Configuración Cliente**

Editar el fichero de configuración “/etc/openldap/ldap.conf” y crear un enlace simbólico:

```
BASE dc=example,dc=com
URI ldap://192.168.1.70:389
ln -s /etc/openldap/ldap.conf /etc/ldap.conf
```

### **Creación del árbol de información de dominio**

Crear un archivo cualquiera y añadir, cambiando los datos de dominio por los que se prefieran:

```
dn: dc=benjaSlack14,dc=es
o: benjaSlack14
dc: benjaSlack14
objectClass: dcObject
objectClass: organization
```

```
dn: ou=groups,dc=benjaSlack14,dc=es
objectClass: top
objectClass: organizationalUnit
ou: Groups
```

```
dn: cn=users,ou=groups,dc=benjaSlack14,dc=es
objectClass: top
objectClass: posixGroup
gidNumber: 101
cn: users
```

```
dn: ou=users,dc=benjaSlack14,dc=es
```

```
objectClass: top
objectClass: organizationalUnit
ou: Users

dn: uid=benja,ou=users,dc=benjaSlack14,dc=es
cn: Benjamin Soro
sn: Soro
givenName: Benja
uid: benja
uidNumber: 1000
gidNumber: 100
homeDirectory: /home/benja
loginShell: /bin/bash
gecos: Normal User
mail: benja@benjaSlack14.es
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
userPassword:
```

Añadir la información de organización a LDAP: "`ldapadd -x -W -D 'cn=ldapadmin,dc=benjaSlack14,dc=es' -f basic_dit.ldif`"

Falta añadir la contraseña al usuario creado anteriormente:

```
"ldappasswd -x -W -D 'cn=ldapadmin,dc=benjaSlack14,dc=es' -S 'uid=benja,ou=users,dc=benjaSlack14,dc=es""
```

### **Instalación Linux-PAM**

```
wget http://pkgs.fedoraproject.org/repo/pkgs/pam/Linux-PAM-1.1.1.tar.bz2/9b3d952b173d5b9836cbc7e8de108bee/Linux-PAM-1.1.1.tar.bz2
```

```
tar xfj Linux-PAM-1.1.1.tar.bz2
cd Linux-PAM-1.1.1
./configure --prefix=/usr --disable-static --enable-shared
make
make install
```

### **Instalación Módulo Ldap\_pam**

```
wget http://www.padl.com/download/pam_ldap.tgz
```

```
tar xfz pam_ldap.tgz
cd pam_ldap-*
./configure --prefix=/ --libdir=/lib --mandir=/usr/man --disable-static --enable-shared
make
make install
```

### **Comprobación Módulo Ldap\_pam**

```
ls /lib/security/*ldap*
/lib/security/pam_ldap.so
```

### **Instalación NSS\_LDAP**

```
wget http://www.padl.com/download/nss_ldap.tgz
```

```
tar xfz nss_ldap.tgz
cd nss_ldap-
export PATH=$PATH:./
./configure --prefix=/ --libdir=/lib --mandir=/usr/man --disable-static --enable-shared
make
make install
```

### **Añadir LDAP a nsswitch.conf**

*Editar “/etc/nsswitch.conf” y añadir “ldap” a las siguientes líneas:*

```
passwd:      files ldap
shadow:      files ldap
group:       files ldap
```

### **Comprobación LDAP**

Si todo ha ido correcto, ejecutar “getent passwd” debería dar el nombre del usuario añadido a LDAP anteriormente.

### **Recompilación de Shadow para soporte PAM**

Acceder a <http://slackbuilds.org/mirror/slackware/slackware-14.0/source/a/shadow/> y descargar el paquete fuente y el archivo .SlackBuild

Editar el archivo .SlackBuild y añadir “--with-libpam” a la sección:

```
./configure \
--prefix=/usr \
--sysconfdir=/etc \
--mandir=/usr/man \
--docdir=/usr/doc/shadow-$VERSION \
--disable-shared \
--without-libcrack \
--with-libpam \
--build=$ARCH-slackware-linux
```

Guardar y ejecutar: “sh shadow.SlackBuild”

Comprobar que el paquete creado en temporal contenga los el bin su y login:

```
tar tfv /tmp/shadow-4.1.4.3-i486-7.txz | grep bin
...
-rws--x--x root/root 36913 2011-11-12 14:00 bin/su
-rwxr-xr-x root/root 43720 2011-11-12 14:00 bin/login
```

Quitar el antiguo Shadow e instalar el nuevo:

```
removepkg shadow  
...  
installpkg /tmp/shadow-4.1.4.3-i486-7.txz
```

### Mecanismo de autenticación

Crear un nuevo directorio para guardar los mecanismos actuales, ya que se utilizarán otros más precisos:

```
mkdir /etc/pam.d/orig  
mv /etc/pam.d/* /etc/pam.d/orig
```

Crear la siguiente lista de mecanismos:

*En “/etc/pam.d/login”*

```
auth      include    common-auth  
account   include    common-account  
session   include    common-session
```

*En “/etc/pam.d/common-auth”*

```
auth      sufficient pam_unix.so  
auth      sufficient pam_ldap.so use_first_pass  
auth      required  pam_deny.so
```

*En “/etc/pam.d/common-account”*

```
account  sufficient pam_unix.so  
account  sufficient pam_ldap.so  
account  required  pam_permit.so
```

*En “/etc/pam.d/common-password”*

```
password sufficient pam_unix.so  
password sufficient pam_ldap.so  
password required  pam_deny.so
```

*En “/etc/pam.d/common-session”*

```
session  sufficient pam_mkhomedir.so skel=/etc/skel umask=0022  
session  sufficient pam_unix.so  
session  sufficient pam_ldap.so  
session  required  pam_deny.so
```

### Prueba de Login

Ejecutar login e intentar acceder como “root”.

\*En caso que aparezca una lista de mensajes de configuration error, deshabilitarlos en “/etc/login.defs” en la línea:

```
#FAILLOG_ENAB      yes
```

Si funciona todo correcto, salir y probar con un usuario de LDAP:

```

nobody:x:99:99:nobody::/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
benja:x:1000:1001::/home/benja:/bin/bash
nx:x:998:998::/usr/NX/home/nx:/usr/NX/bin/nxserver
benja:x:1000:100:Normal User:/home/benja:/bin/bash
pepito:x:1001:100:Extra User:/home/pepito:/bin/bash
root@slack14:/etc/openldap# login pepito
configuration error - unknown item 'LASTLOG_ENAB' (notify administrator)
configuration error - unknown item 'MAIL_CHECK_ENAB' (notify administrator)
configuration error - unknown item 'OBSCURE_CHECKS_ENAB' (notify administrator)
configuration error - unknown item 'PORTTIME_CHECKS_ENAB' (notify administrator)
configuration error - unknown item 'QUOTAS_ENAB' (notify administrator)
configuration error - unknown item 'MOTD_FILE' (notify administrator)
configuration error - unknown item 'FTMP_FILE' (notify administrator)
configuration error - unknown item 'NOLOGINS_FILE' (notify administrator)
configuration error - unknown item 'ENV_HZ' (notify administrator)
configuration error - unknown item 'PASS_MIN_LEN' (notify administrator)
configuration error - unknown item 'SU_WHEEL_ONLY' (notify administrator)
configuration error - unknown item 'PASS_CHANGE_TRIES' (notify administrator)
configuration error - unknown item 'PASS_ALWAYS_WARN' (notify administrator)
configuration error - unknown item 'CHFN_AUTH' (notify administrator)
configuration error - unknown item 'ENVIRON_FILE' (notify administrator)
Password:
pepito@slack14:~$ 

```

Para que los usuarios de LDAP puedan ejecutar “passwd” y “su” hay que definir mecanismos también para ellos:

*En “/etc/pam.d/passwd”*

<i>auth</i>	<i>include</i>	<i>common-auth</i>
<i>account</i>	<i>include</i>	<i>common-account</i>
<i>password</i>	<i>include</i>	<i>common-password</i>

*En “/etc/pam.d/su”*

<i>auth</i>	<i>sufficient</i>	<i>pam_rootok.so</i>
<i>auth</i>	<i>include</i>	<i>common-auth</i>
<i>account</i>	<i>include</i>	<i>common-account</i>
<i>session</i>	<i>include</i>	<i>common-session</i>

## Instalación LDAP Account Manager

Requisitos:

- Apache instalado
- PHP5 instalado y habilitado
- Módulos LDAP instalados y habilitados: *authnz\_ldap\_module* y *ldap\_module*

Descargar el Source code de <https://www.ldap-account-manager.org/lamcms/releases>, extraer el contenido y copiarlo a: “*cp -r . /var/www/htdocs/lam/*”

Acceder al nuevo lugar: “*cd /var/www/htdocs/lam/config*” y copiar los ficheros de

ejemplo: “*cp config.cfg\_sample config.cfg*” y “*cp lam.conf\_sample lam.conf*”  
Cambiar el propietario a Apache: “*chown -R apache.apache /var/www/htdocs/lam*”

Acceder mediante un navegador Web a la dirección del servidor/lam para acceder al panel de acceso:

User name Manager  
Password   
Language Español (España)

---

LDAP server ldap://localhost:389  
Server profile lam

Hacer click sobre el enlace de Configuración de la esquina superior derecha:



Click sobre Edit servers, introducir la contraseña que es “lam”.

Ahora se tiene acceso a toda la configuración del LDAP del servidor, configurar todos los datos según estén en el servidor LDAP.

Volver al panel central de login e introducir la contraseña del root del LDAP para acceder al panel de gestión de nodos del árbol LDAP:

ID de usuario	Nombre
1	Benja
2	Pepito

## Servidor DNS

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search bind” e instalando los paquetes que corresponden al servidor DNS.

### Lanzar el servicio

Como la instalación de BIND en Slackware ya crea los archivos de configuración para Localhost por defecto, queda lanzar el servicio.

Primero dar permisos de ejecución al demonio, “chmod 755 /etc/rc.d/rc.bind” y después lanzar el servicio “/etc/rc.d/rc.bind start”.

### Configuración BIND

Acceder al archivo “/etc/named.conf” y en la sección Options comprobar si existe una subsección “Forwarders”, si no añadir:

```
forward first;
forwarders {
  8.8.8.8;
  8.8.4.4;
};
```

### Creación de Zona

Acceder a “/var/named/caching-example” y copiar el fichero de localhost de ejemplo a la carpeta padre: “cp localhost.zone ..../nombreZona.zone”.

Acceder a la carpeta padre y editar la nueva zona:

```

$TTL 86400
$ORIGIN nombreZona.
@           1D IN SOA  @ root (
        43          ; serial (d. adams)
        3H          ; refresh
        15M         ; retry
        1W          ; expiry
        1D )        ; minimum

        1D IN NS   @
        1D IN A    192.168.X.X
www      IN A    192.168.X.X

```

Se puede definir el prefijo “www” para acceder al servidor Web que será configurado más tarde.

Guardar el archivo y editar el archivo “/etc/named.conf” para añadir la nueva zona.  
Comprobar que la zona ha sido correctamente creada: “named-checkzone nombreZona /var/named/nombreZona.zone”  
Añadir la nueva zona creada al archivo “/etc/named.conf”:

```

zone "nombreZona" IN {
    type master;
    file "nombreZona.zone";
    allow-update { none; };
};

```

Comprobar que el archivo es correcto: “named-checkconf /etc/named.conf”.

### **Dynamic DNS - No-IP.org**

Para instalar un servicio que controle el cambio de IP externa, hay que acceder a la web no-ip.org, registrar una cuenta y añadir el primer hostname.  
Si ya se realizó con otra instalación, descargar sólo el cliente para Linux.

Al estar en Slackware, hay que descomprimir y compilar el paquete. Dentro de la carpeta: “make”. Cuando termine: “make install”  
Si se poseen múltiples interfaces, solicitará a qué interfaz asociar la conexión.  
Se solicitará el usuario y contraseña de no-ip.  
Se solicitará sobre qué cuenta se quiere estar actualizado.  
Añadir el intervalo de consulta por defecto.  
En la opción de ejecutar alguna cosa cuando la actualización sea completada, poner que No.  
Lanzar el programa “noip2”.

Para opciones de configuración del cliente o añadir un script al inicio para que ejecute automáticamente “noip2”, consultar el archivo LEEME.PRIMERO.

### **Servidor DHCP**

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search dhcp” e instalando los paquetes que corresponden al servidor DHCP.

### Configurar servidor DHCP

Como el archivo de configuración “/etc/dhcpd.conf” está vacío, para tener las primeras impresiones de las directivas del servidor, hay que copiar el fichero de ejemplo que DHCP proporciona en su documentación.

Ejecutar: “cp /usr/doc/dhcp-VERSION/examples/dhcpd.conf /etc/dhcpd.conf”

Editar el fichero “/etc/dhcpd.conf”, quitar todo el contenido y adaptar a las necesidades lo siguiente:

```
# Use this to enable / disable dynamic dns updates globally.  
#ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;  
  
# A slightly different configuration for an internal subnet.  
subnet 192.168.233.0 netmask 255.255.255.0 {  
    range 192.168.233.150 192.168.233.200;  
    option domain-name-servers 192.168.233.4, 192.168.233.3;  
    option domain-name "benjaSlack14.es";  
    option routers 192.168.233.4;  
    option broadcast-address 192.168.233.255;  
    option subnet-mask 255.255.255.0;  
    default-lease-time 600;  
    max-lease-time 7200;  
}
```

Guardar y ejecutar el demonio del servidor DHCP.

En caso que no esté, hay que crear el script de inicio que debe estar en “/etc/rc.d/”.

Copiar el siguiente código script, cambiando los interfaces necesarios en la variable DHCPD\_OPTIONS:

```
#!/bin/sh  
#  
#/etc/rc.d/rc.dhcpd  
# This shell script takes care of starting and stopping the ISC DHCPD service  
  
# Put the command line options here that you want to pass to dhcpcd:  
DHCPD_OPTIONS="-q eth0 eth1"  
  
[ -x /usr/sbin/dhcpcd ] || exit 0  
  
[ -f /etc/dhcpd.conf ] || exit 0  
  
start() {  
    # Start daemons.  
    echo -n "Starting dhcpcd: /usr/sbin/dhcpcd $DHCPD_OPTIONS "  
    /usr/sbin/dhcpcd $DHCPD_OPTIONS
```

```

        echo
    }
stop() {
    # Stop daemons.
    echo -n "Shutting down dhcpcd: "
    killall -TERM dhcpcd
    echo
}
status() {
PIDS=$(pidof dhcpcd)
if [ "$PIDS" == "" ]; then
    echo "dhcpcd is not running!"
else
    echo "dhcpcd is running at pid(s) ${PIDS}."
fi
}
restart() {
    stop
    start
}

# See how we were called.
case "$1" in
start)
    start
;;
stop)
    stop
;;
restart)
    stop
    start
;;
status)
    status
;;
*)
    echo "Usage: $0 {start|stop|status|restart}"
;;
esac
exit 0

```

Dentro de “/etc/rc.d” ejecutar “cat > rc.dhcpcd” y pegar el contenido copiado anteriormente y presionar Ctrl+D para guardar el contenido.

Es necesario cambiar los permisos al archivo creado: “chmod 755 rc.dhcpcd”  
Iniciar el servicio: “/etc/rc.d/rc.dhcpcd start”

### **Comprobar el funcionamiento de DHCP**

Ejecutar: “/etc/rc.d/rc.dhcpcd status” y debe mostrar que el servidor DHCP está funcionando.

En caso contrario revisar el archivo “/var/log/syslog” para comprobar los errores cometidos.

### **Habilitar Sincronización DHCP con DNS**

Generar una clave para establecer una sincronización segura, ejecutar: “dnssec-keygen -r /dev/urandom -a HMAC-MD5 -b 128 -n USER DHCP\_UPDATER”

Para ver y copiar la clave generada, ejecutar: “cat Kdhcp\_updater.\*.private|grep Key”

Editar el fichero “/etc/named.conf” y añadir el código:

```

key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;

    # Important: Replace this key with your generated key.
    # Also note that the key should be surrounded by quotes.
    secret "CLAVE";
};

```

Y para cada zona que quiera ser actualizada, cambiar “*allow-update { none; };*” por “*allow-update { key DHCP\_UPDATER; };*”

Editar el fichero “/etc/dhcpd.conf” y cambiar la línea “*#ddns-update-style none;*” por (*cambiando el servidor de nombres*):

```

ddns-update-style interim;
ignore client-updates;
ddns-domainname "benjaSlack14.es.";
ddns-rev-domainname "in-addr.arpa.";

```

Añadir también:

```

key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;

    # Important: Replace this key with your generated key.
    # Also note that the key should be surrounded by quotes.
    secret "CLAVE";
};

zone benjaSlack14.es. {
    primary 127.0.0.1;
    key DHCP_UPDATER;
}

zone 233.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    key DHCP_UPDATER;
}

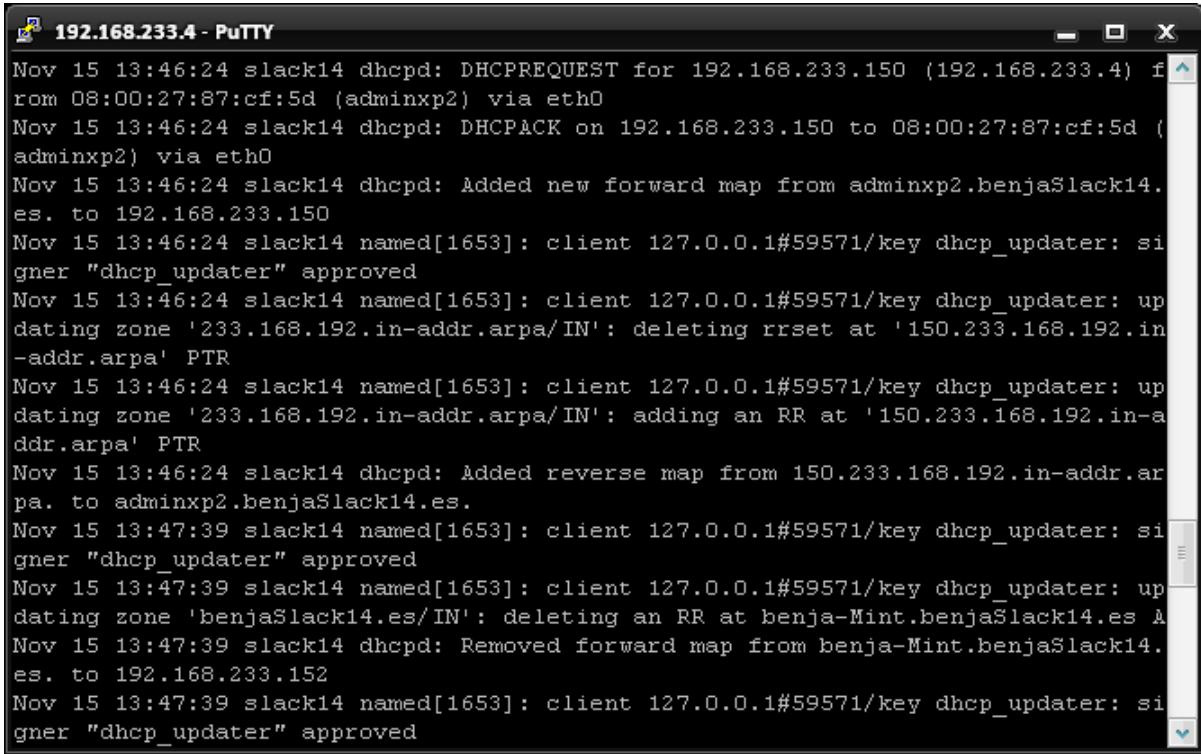
```

Reiniciar el servicio DNS y DHCP.

### **Comprobación Sincronización DHCP con DNS**

Con un cliente DHCP de cualquier sistema operativo, realizar una petición de IP.

En el servidor ejecutar “*tail -f /var/log/messages*” para ver si se añaden los nuevos equipos a la configuración de BIND:



The screenshot shows a PuTTY terminal window titled "192.168.233.4 - PuTTY". The window displays a log of system events from a Slackware system. The log includes messages from dhcpcd (DHCP client) and named (DNS server). Key entries include:

- dhcpcd: DHCPREQUEST for 192.168.233.150 (192.168.233.4) from 08:00:27:87:cf:5d (adminxp2) via eth0
- dhcpcd: DHCPACK on 192.168.233.150 to 08:00:27:87:cf:5d (adminxp2) via eth0
- dhcpcd: Added new forward map from adminxp2.benjaSlack14.es. to 192.168.233.150
- named[1653]: client 127.0.0.1#59571/key dhcp\_updater: signer "dhcp\_updater" approved
- named[1653]: client 127.0.0.1#59571/key dhcp\_updater: updating zone '233.168.192.in-addr.arpa/IN': deleting rrset at '150.233.168.192.in-addr.arpa' PTR
- named[1653]: client 127.0.0.1#59571/key dhcp\_updater: updating zone '233.168.192.in-addr.arpa/IN': adding an RR at '150.233.168.192.in-addr.arpa' PTR
- dhcpcd: Added reverse map from 150.233.168.192.in-addr.arpa. to adminxp2.benjaSlack14.es.
- named[1653]: client 127.0.0.1#59571/key dhcp\_updater: signer "dhcp\_updater" approved
- named[1653]: client 127.0.0.1#59571/key dhcp\_updater: updating zone 'benjaSlack14.es/IN': deleting an RR at benja-Mint.benjaSlack14.es A
- slack14 dhcpcd: Removed forward map from benja-Mint.benjaSlack14.es. to 192.168.233.152
- named[1653]: client 127.0.0.1#59571/key dhcp\_updater: signer "dhcp\_updater" approved

## NFS

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search nfs” e instalando los paquetes que corresponden al servidor NFS.

Editar el fichero de configuración “/etc/exports” y añadir la ruta de la carpeta compartida, la red o IP que se permite el acceso y los permisos:  
“/home/benja/shared 192.168.233.0/255.255.255.0(rw)”

Editar el fichero de denegación de equipos “/etc/hosts.deny”:

*portmap:ALL  
lockd:ALL  
mountd:ALL  
rquotad:ALL  
statd:ALL*

Editar el fichero de admisión de acceso “/etc/hosts.allow”:

*portmap: 192.168.233.0/24  
lockd: 192.168.233.0/24  
mountd: 192.168.233.0/24  
rquotad: 192.168.233.0/24  
statd: 192.168.233.0/24*

Cambiar el permiso del script de NFS: “chmod 755 /etc/rc.d/rc.nfsd”

Reiniciar el servicio NFS: “/etc/rc.d/rc.nfsd restart”

Se verifica que está funcionando mediante: “*rpcinfo -p*”

### **Cliente NFS**

Linux: tener instalado el paquete: nfs-commons

Windows: tener instalado el rol de Cliente NFS y seguir los pasos del asistente.

### **Linux**

Ejecutar: “*mount IPservidor:/ruta/recurso/compartido /ruta/local/*”

### **Sendmail**

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search mail” e instalando los paquetes que corresponden al servidor Sendmail.

#### **Añadir las entradas MX al DNS**

Abrir el fichero de zona que se haya creado en la configuración de BIND y añadir:

```
MX 10 mail.dominio.es.  
MX 20 mail2.dominio.es.  
mail A 192.168.X.X  
mail2 A 192.168.X.X
```

#### **Configuración por defecto**

Slackware debe compilar el fichero que utiliza Sendmail en base a uno de configuración más sencilla y copiar el archivo generado a la carpeta donde Sendmail hace uso de él. Cualquier modificación en el fichero de directivas de Sendmail, el demonio debe volver a ser lanzado:

```
cd /usr/share/sendmail/cf/cf  
sh Build sendmail-slackware.mc  
cp sendmail-slackware.cf /etc/mail/sendmail.cf  
cp submit.cf /etc/mail/  
chmod +x /etc/rc.d/rc.sendmail  
/etc/rc.d/rc.sendmail start
```

#### **Configuración personal**

Abrir el archivo “*/etc/mail/sendmail.mc*” y añadir:

```
LOCAL_DOMAIN(`dominio.es')  
MASQUERADE_AS(`dominio.es')  
FEATURE(`masquerade_envelope')  
FEATURE(`allmasquerade')  
EXPOSED_USER(`root')
```

Para generar el .cf se debe seguir los pasos marcados en la Configuración por defecto para generar el .cf en base al .mc modificado y reiniciar el servicio.

## **Instalación MailScanner, SpamAssassin, y ClamAV**

Acceder a <http://www.mailscanner.info/downloads.html> y descargar la versión estable de para “Solaris / BSD / Other Linux / Other Unix” y ClamAV 0.96.5 and SpamAssassin 3.3.1 easy installation package.

Descargar primero el **ClamAV** y **SpamAssassin**, extraer y ejecutar: “./install.sh”

\*\*Atención: en caso de tener la autenticación PAM junto con LDAP, se deben definir las reglas para los comandos: “*useradd, userdel, usermod, groupadd, groupdel*”

Ahora es necesario instalar:

- 1) Razor-agents-sdk y Razor2 de <http://razor.sourceforge.net/> y
- 2) DCC de <http://www.rhyolite.com/anti-spam/dcc/>

```
wget http://umn.dl.sourceforge.net/sourceforge/razor/razor-agents-sdk-2.07.tar.bz2  
wget http://umn.dl.sourceforge.net/sourceforge/razor/razor-agents-2.84.tar.bz2  
wget http://www.rhyolite.com/anti-spam/dcc/source/dcc.tar.Z
```

```
bunzip2 razor-agents-sdk-2.07.tar.bz2  
tar xvf razor-agents-sdk-2.07.tar  
cd razor-agents-sdk-2.07  
perl Makefile.PL  
make  
make test  
make install  
cd ..
```

```
bunzip2 razor-agents-2.84.tar.bz2  
tar xvf razor-agents-2.84.tar  
cd razor-agents-2.84  
perl Makefile.PL  
make  
make test  
make install  
cd ..
```

```
tar zxvf dcc.tar.Z  
cd dcc-1.3.143/  
.configure  
make install  
cd ..
```

Continuar con MailScanner:

Acceder a <http://www.mailscanner.info/downloads.html> y descargar la versión para Otros sistemas operativos.

Tener instalado el Perl con las librerías Parse de HTML y SpamAssassin.

Descomprimir el archivo descargado y situar el paquete en /opt.

Acceder a /opt/MailScanner/bin y ejecutar “checkconfig”.

## **Instalar Dovecot**

Acceder a la web oficial: <http://www.dovecot.org/download.html> y descargar el último paquete estable.

Añadir los usuarios “dovenull” y “dovecot”, con sus respectivos grupos, al sistema.

Ejecutar los comandos para instalarlo después de su descompresión:

```
./configure  
make  
sudo make install
```

### Configuración Dovecot

Copiar la configuración por defecto “/usr/share/doc”:

```
cp -r /usr/share/doc/dovecot-2.1.10/example-config/ /etc/dovecot/
```

## **Reiniciar el servicio**

Dar permisos de ejecución: “chmod 755 /etc/rc.d/rc.dovecot”

Reiniciar: “/etc/rc.d/rc.dovecot start”

Si ningún error mostrado, permanece a la escucha en el puerto 143:

## **WebMail: SquirrelMail**

Acceder a <http://squirrelmail.org/download.php> y descargar la última versión estable.

*\*\*Se da por supuesto que ya se posee instalado Apache y PHP5, y éste último configurado adecuadamente con Apache.*

Se descomprime el paquete descargado y se mueve todo su contenido al directorio raíz del servidor Web activo bajo Apache.

```
cp -r squirrelmail-webmail-1.4.22 /var/www/htdocs/squirrelmail
```

Acceder a la carpeta del squirrelmail del sitio web y ejecutar: *configure*

Seleccionar la opción ‘D’ y entonces seleccionar que se configura SquirrelMail con ‘Dovecot’. Configuración asignada, seleccionar ‘S’ para guardar cambios y ‘Q’ para salir de la configuración.

## **Probar configuración**

Acceder a <http://Servidor.com/squirrelmail/src/configtest.php> y comprobar que no existen errores con la configuración de PHP y con Dovecot:

### SquirrelMail configtest

This script will try to check some aspects of your SquirrelMail configuration and point you to errors wherever it can find them. You need to go run `conf.pl` in the `config/` directory first before you run this script.

Checking PHP configuration...

PHP version 5.4.7 OK.

Running as apache(80) / apache(80)

display\_errors:

error\_reporting: 22527

variables\_order OK: GPCS.

PHP extensions OK. Dynamic loading is disabled.

Checking paths...

Data dir OK.

Attachment dir OK.

Plugins are not enabled in config.

Themes OK.

Default language OK.

Base URL detected as: `http://192.168.233.4/squirrelmail/src` (location base autodetected)

Checking outgoing mail service....

SMTP server OK (220 slack14.benjaSlack14.es ESMTP Sendmail 8.14.5/8.14.5; Thu, 22 Nov 2012 00:33:48 +0100)

Checking IMAP service....

IMAP server ready (\* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.)

Capabilities: \* CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN

Checking internationalization (i18n) settings...

gettext - Gettext functions are available. On some systems you must have appropriate system locales compiled.

mbstring - Mbstring functions are available.

recode - Recode functions are unavailable.

iconv - Iconv functions are available.

timezone - Webmail users can change their time zone settings.

Checking database functions...

not using database functionality.

Congratulations, your SquirrelMail setup looks fine to me!

### Skin Outlook para SquirrelMail

Acceder a <http://sourceforge.net/projects/squirreloutlook/> y descargar una versión de SquirrelMail con Outlook.

**\*\*Se da por supuesto que ya se posee instalado Apache y PHP5, y éste último configurado adecuadamente con Apache.**

Se descomprime el paquete descargado y se mueve todo su contenido al directorio raíz del servidor Web activo bajo Apache.

```
cp -r squirreloutlook-1.0.3/ /var/www/htdocs/squirrelmailoutlook
```

Acceder a la carpeta del squirrelmail del sitio web y ejecutar: *configure*

Seleccionar la opción ‘D’ y entonces seleccionar que se configura SquirrelMail con ‘Dovecot’. Configuración asignada, seleccionar ‘S’ para guardar cambios y ‘Q’ para salir de la configuración.

\*\*Error de funciones vulnerable en PHP5:  
    Editar el archivo globals.php de SquirrelMail:  
    “/var/www/htdocs/outlook/functions/global.php”  
    En la línea 243: cambiar la función sqsession\_register:

```
function sqsession_register ($var, $name) {  
  
    sqsession_is_active();  
  
    if ( !check_php_version(4,1) ) {  
        global $HTTP_SESSION_VARS;  
        $HTTP_SESSION_VARS[$name] = $var;  
    } else {  
        $_SESSION["$name"] = $var;  
    }  
    session_register("$name");  
}
```

Por:

```
function sqsession_register ($var, $name) {  
    sqsession_is_active();  
    $_SESSION["$name"] = $var;  
}
```

La función siguiente: sqsession\_unregister también debe ser modificada:

```
function sqsession_unregister ($name) {  
  
    sqsession_is_active();  
  
    if ( !check_php_version(4,1) ) {  
        global $HTTP_SESSION_VARS;  
        unset($HTTP_SESSION_VARS[$name]);  
    } else {  
        unset($_SESSION[$name]);  
    }  
    session_unregister("$name");  
}
```

Por:

```
function sqsession_unregister ($name) {  
  
    sqsession_is_active();  
    unset($_SESSION[$name]);  
}
```

Acceder a <http://servidor.com/outlook/src/login.php> y acceder como un usuario registrado:

## Servidor FTP

Durante la instalación de Slackware se puede instalar o después mediante el comando “slackpkg search ftp” e instalando los paquetes que corresponden al servidor FTP.

## Configuración VSFTP

Editar el archivo “/etc/vsftpd.conf” y aplicar la siguiente configuración:

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).  
anonymous_enable=YES  
#  
# Uncomment this to allow local users to log in.  
local_enable=YES  
#  
# Uncomment this to enable any form of FTP write command.  
#write_enable=YES  
#  
# Default umask for local users is 077. You may wish to change this to 022,  
# if your users expect that (022 is used by most other ftppd's)  
local_umask=022  
#  
# Uncomment this to allow the anonymous FTP user to upload files. This only  
# has an effect if the above global write enable is activated. Also, you will  
# obviously need to create a directory writable by the FTP user.  
#anon_upload_enable=YES  
#  
# Uncomment this if you want the anonymous FTP user to be able to create  
# new directories.  
#anon_mkdir_write_enable=YES  
#  
# Activate directory messages - messages given to remote users when they  
# go into a certain directory.  
dirmessage_enable=YES  
#  
# Activate logging of uploads/downloads.  
xferlog_enable=YES  
#  
# Make sure PORT transfer connections originate from port 20 (ftp-data).
```

```
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftp_banner=Welcome to benjaSlack14.es FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
```

```

#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode (rather
# than from inetd) and listens on IPv4 sockets. To use vsftpd in standalone
# mode rather than with inetd, change the line below to 'listen=YES'
# This directive cannot be used in conjunction with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

```

Crear la lista vacía de usuarios que serán enjaulados en su home: “`touch /etc/vsftpd.chroot_list`”

Recordar que esta lista hace la acción contraria al estar habilitada la autenticación de usuarios locales, que es la de NO enjaular a aquel usuario que aparezca en la lista.

Como VSFTP no se ha configurado de manera standalone sobre inetd, hay que editar el archivo “`/etc/inetd.conf`” y quitar el comentario de:

```
# Very Secure File Transfer Protocol (FTP) server.
ftp    stream  tcp   nowait  root   /usr/sbin/tcpd  vsftpd
```

Reiniciar el servicio: “`/etc/rc.d/rc.inetd restart`”

Comprobación de acceso, ejecutar:

```
benja@slack14:~$ ftp
ftp> open
(to) ftp.benjasslack14.es
Connected to ftp.benjasslack14.es.
220 Bienvenido al FTP de Benja en benjaSlack14.es.
Name (ftp.benjasslack14.es:benja): benja
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

## Debian Server

### Licencia

GNU

### Particionamiento

S.ficheros	Size	Montado en
/dev/sda1	323M	/
/dev/sda9	7,8G	/home
/dev/sda8	368M	/tmp
/dev/sda5	7,4G	/usr
/dev/sda6	2,8G	/var
/dev/sawp	1,2G	

### Parada y arranque de servicios

Debian posee su sistema de scripts de inicio y parada de servicios alojado en “/etc/init.d”. El fichero “/etc/inittab” contiene las directivas para los servicios que inicien después de que los servicios del sistema hayan iniciado.

En “/etc/rc.d/rc.[4 | 6 | S | M]” se encuentran los scripts de inicio de los servicios para los modos gráficos, multiusuarios y monousuario

### Servidor SSH

El servidor SSH ya viene por defecto con la distribución de Debian.

### Configuración SSH

Editar el fichero “/etc/ssh/sshd\_config” y descomentar la línea “RSAAuthentication yes” y “Protocol 2”. Para permitir la versión 2 del protocolo y permitir autenticación con certificados RSA.

### Reiniciar el servicio

Para reflejar los cambios realizados en la configuración, ejecutar “/etc/init.d/sshd stop” y “/etc/init.d/sshd start”.

Realizar un restart está orientado a actualizar la configuración cuando un

Administrador ha accedido y no se quiere que se corte la conexión

### **Acceso SSH mediante clave RSA**

En el cliente SSH que se quiera conectar con el servidor debe generar el par de claves RSA:

#### **Linux**

Ejecutar “ssh-keygen -t rsa” y guardar en la carpeta por defecto, en caso que exista sobreescribir.

No introducir nada como “passphrase”.

Generada la clave pública, mediante SCP se envía la clave pública “id\_rsa.pub” al servidor SSH “scp ./ssh/id\_rsa.pub usuario@debianASORC:~” que se guardará en el \$HOME.

En el servidor SSH, acceder al lugar de la clave pública y ejecutar: “cat id\_rsa.pub >> .ssh/authorized\_keys” para que añada la clave a la lista de claves autorizadas.

Ahora en el cliente se podrá conectar con el usuario mediante SSH sin necesidad de introducir ninguna contraseña.

#### **Windows**

Descargar el programa “puttygen”, y generar una clave RSA para SSH-2. Colocar un comentario de clave descriptivo.

Copiar la clave pública e introducirla en “.ssh/authorized\_keys” del usuario que queramos conectarnos.

Introducir la clave mediante una conexión con el programa WinSCP o a través de Putty, pegando el código en la terminal.

Conectarse con el servidor SSH con Putty y con la clave RSA:

### **Servidor VNC - TightVNC**

Ejecutar: “*apt-get install tightvncserver*”

En la configuración por defecto, VNC no creará los archivos de configuración por usuario, por tanto se tiene que ejecutar para el usuario que quiera ser accedido vía VNC: “vncserver”

Se introduce una clave para acceder con el usuario actual y no se introduce una contraseña para el modo “view-only”.

VNC creará los archivos de configuración para ese usuario en su home y además se especificará en qué pantalla está disponible, por defecto la 1 (:1).

En el archivo “.vnc/xstartup” se encuentra la configuración de la visualización, resolución, colores, etc.

Cada vez que se modifique ese fichero es necesario reiniciar el servicio VNC.

### **Añadir el VNC al arranque de servicios**

Añadir el siguiente código al final del archivo “/etc/rc.local”:

```
su nombre_usuario -c "tightvncserver"
```

Cada vez que inicie la máquina se creará una sesión VNC para el usuario que se haya especificado en el archivo.

### **Acceso mediante VNCViewer**

Se puede acceder mediante un cliente en Windows, Linux o una interfaz en Java (<http://www.tightvnc.com/download-old.php>)

### **XDMCP**

Ya viene de forma nativa en las distribuciones de Debian.

### **Activar XDMCP**

Editar el archivo “*/etc/gdm3/daemon.conf*” y poner debajo de la línea donde está “[xdmcp]” el siguiente texto: “*Enable=true*”

Es necesario reiniciar GDM: “*sudo /etc/init.d/gdm3 restart*”

### **Acceder vía XDMCP**

En un cliente Linux con el servidor X instalado, ejecutar: “*X -query IP\_HOST :1*”

### **FreeNX**

Para Debian es necesario la descarga de los .DEB:

<http://www.nomachine.com/select-package.php?os=linux&id=1>

Seleccionar los paquetes acorde con la arquitectura del procesador.

Se deben descargar: el nodo, el servidor y el cliente.

Ejecutar los .DEB:

```
sudo dpkg -i nxclient_3.5.0-7_amd64.deb
sudo dpkg -i nxnode_3.5.0-9_amd64.deb
sudo dpkg -i nxserver_3.5.0-11_amd64.deb
```

### **Configuración FreeNX**

\*\*Bug en el archivo de comprobación de claves de SSH

El fichero de configuración de SSH (“*/etc/ssh/sshd\_config*”) hay una línea que marca el fichero para comprobar el acceso por clave mediante SSH (“*AuthorizedKeysFile .ssh/authorized\_keys*”). Pero en el home de NX, (“*/usr/NX/home/nx/.ssh*”) no existe ese fichero, por tanto una posible solución es renombrar el fichero “*/usr/NX/home/nx/.ssh/ authorized\_keys2*”: “*mv /usr/NX/home/nx/.ssh/ authorized\_keys2 /usr/NX/home/nx/.ssh/ authorized\_keys*”.

Cambiar los permisos de los archivos del home:

```
chown nx:root /usr/NX/home/nx/.ssh/authorized_keys
chmod 0644 /usr/NX/home/nx/.ssh/authorized_keys
chown nx:root /usr/NX/home/nx/.ssh/default.id_dsa.pub
```

```
chmod 0644 /usr/NX/home/nx/.ssh/default.id_dsa.pub
```

### Acceso con cliente NX

Descargar un cliente para Windows:

[http://www.nomachine.com/download-package.php?Prod\\_Id=3835](http://www.nomachine.com/download-package.php?Prod_Id=3835)

Seguir los pasos del asistente y finalmente la configuración de conexión con el servidor NX estará lista:

### Servidor DNS

El paquete BIND ya viene por defecto con la distribución de Debian.

### Lanzar el servicio

Como la instalación de BIND en Slackware ya crea los archivos de configuración para Localhost por defecto, queda lanzar el servicio.

Primero dar permisos de ejecución al demonio, “chmod 755 /etc/rc.d/rc.bind” y después lanzar el servicio “/etc/rc.d/rc.bind start”.

### Configuración BIND

Acceder al archivo “*named.conf.options*” y en la sección Options comprobar si existe una subsección “Forwarders”, si no añadir:

```
forward first;
forwarders {
    8.8.8.8;
    8.8.4.4;
};
```

### Creación de Zona

Acceder a “/etc/bind/zones/” copiar una zona ya creada, cambiar el nombre y editar la nueva zona:

```
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA DOMINIO.es. root.DOMINIO.es. (
    8      ; Serial
    604800   ; Refresh
    86400    ; Retry
    2419200  ; Expire
    604800 ) ; Negative Cache TTL
;
@       IN  NS  DOMINIO.es.
@     IN  A   192.168.233.7
www   IN  A   192.168.233.7
nfs   IN  A   192.168.233.7
@     IN  AAAA ::1
```

Se puede definir el prefijo “www” para acceder al servidor Web que será

configurado más tarde.

Guardar el archivo y editar el archivo “/etc/named.conf.default-zones” para añadir la nueva zona.

Comprobar que la zona ha sido correctamente creada: “*named-checkzone nombreZona /var/named/nombreZona.zone*”

Añadir la nueva zona creada al archivo “/etc/named.conf.default-zones”:

```
zone "nombreZona" IN {  
    type master;  
    file "/ruta/de/la/zona/db.nombreZona";  
    allow-update { none; };  
};
```

Comprobar que el archivo es correcto: “*named-checkconf /etc/named.conf.default-zones*”.

## Servidor DHCP

Ejecutar “*sudo apt-get install dhcp3-server*”

### Configurar servidor DHCP

Editar el fichero “/etc/dhcp/dhcpd.conf”, quitar todo el contenido y adaptar a las necesidades lo siguiente:

```
# Use this to enable / disable dynamic dns updates globally.  
#ddns-update-style none;  
  
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;  
  
# A slightly different configuration for an internal subnet.  
subnet 192.168.233.0 netmask 255.255.255.0 {  
    range 192.168.233.120 192.168.233.149;  
    option domain-name-servers 192.168.233.7, 192.168.233.4;  
    option domain-name "benjaDebian.es";  
    option routers 192.168.233.7;  
    option broadcast-address 192.168.233.255;  
    option subnet-mask 255.255.255.0;  
    default-lease-time 600;  
    max-lease-time 7200;  
}
```

Guardar y ejecutar el demonio del servidor DHCP.

En caso que no esté, hay que crear el script de inicio que debe estar en “/etc/init.d/”.

Copiar el siguiente código script, cambiando los interfaces necesarios en la variable **DHCPD\_OPTIONS**:

```
#!/bin/sh
```

```

#
#/etc/init.d/dhcpd
#      This shell script takes care of starting and stopping the ISC DHCPD service

# Put the command line options here that you want to pass to dhcpcd:
DHCPD_OPTIONS="-q eth0 eth1"

[ -x /usr/sbin/dhcpcd ] || exit 0

[ -f /etc/dhcpd.conf ] || exit 0

start() {
    # Start daemons.
    echo -n "Starting dhcpcd: /usr/sbin/dhcpcd $DHCPD_OPTIONS "
    /usr/sbin/dhcpcd $DHCPD_OPTIONS
    echo
}
stop() {
    # Stop daemons.
    echo -n "Shutting down dhcpcd: "
    killall -TERM dhcpcd
    echo
}
status() {
PIDS=$(pidof dhcpcd)
if [ "$PIDS" == "" ]; then
    echo "dhcpcd is not running!"
else
    echo "dhcpcd is running at pid(s) ${PIDS}."
fi
}
restart() {
    stop
    start
}

# See how we were called.
case "$1" in
start)
    start
    ;;
stop)
    stop
    ;;
restart)
    stop
    start
    ;;
status)
    status
    ;;
*)
    echo "Usage: $0 {start|stop|status|restart}"
    ;;
esac
exit 0

```

Dentro de “/etc/init.d” ejecutar “cat > dhcpcd” y pegar el contenido copiado anteriormente y presionar Ctrl+D para guardar el contenido.

Es necesario cambiar los permisos al archivo creado: “chmod 755 dhcpcd”  
Iniciar el servicio: “/etc/init.d/dhcpcd start”

## Comprobar el funcionamiento de DHCP

Ejecutar: “/etc/init.d/dhcpd status” y debe mostrar que el servidor DHCP está funcionando.

En caso contrario revisar el archivo “/var/log/syslog” para comprobar los errores cometidos.

### Habilitar Sincronización DHCP con DNS

Generar una clave para establecer una sincronización segura, ejecutar: “dnssec-keygen -r /dev/urandom -a HMAC-MD5 -b 128 -n USER DHCP\_UPDATER”

Para ver y copiar la clave generada, ejecutar: “cat Kdhcp\_updater.\*.private|grep Key”

Editar el fichero “/etc/bind/named.conf.default-zones” y añadir el código:

```
key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;

    # Important: Replace this key with your generated key.
    # Also note that the key should be surrounded by quotes.
    secret "CLAVE";
};
```

Y para cada zona que quiera ser actualizada, cambiar “allow-update { none; }” por “allow-update { key DHCP\_UPDATER; }”

Editar el fichero “/etc/dhcpd.conf” y cambiar la línea “#ddns-update-style none;” por (cambiando el servidor de nombres):

```
ddns-update-style interim;
ignore client-updates;
ddns-domainname "benjaDebian.es.";
ddns-rev-domainname "in-addr.arpa.;"
```

Añadir también:

```
key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;

    # Important: Replace this key with your generated key.
    # Also note that the key should be surrounded by quotes.
    secret "CLAVE";
};

zone benjaDebian.es. {
    primary 127.0.0.1;
    key DHCP_UPDATER;
}

zone 233.168.192.in-addr.arpa. {
    primary 127.0.0.1;
```

```
key DHCP_UPDATER;
}
```

Reiniciar el servicio DNS y DHCP.

### Comprobación Sincronización DHCP con DNS

Con un cliente DHCP de cualquier sistema operativo, realizar una petición de IP.

En el servidor ejecutar “*tail -f /var/log/messages*” para ver si se añaden los nuevos equipos a la configuración de BIND:

### Dynamic DNS - No-IP.org

Para instalar un servicio que controle el cambio de IP externa, hay que acceder a la web no-ip.org, registrar una cuenta y añadir el primer hostname.

Si ya se realizó con otra instalación, descargar sólo el cliente para Linux.

Al estar en Debian, hay que descomprimir y compilar el paquete. Dentro de la carpeta: “make”. Cuando termine: “make install”

Si se poseen múltiples interfaces, solicitará a qué interfaz asociar la conexión.

Se solicitará el usuario y contraseña de no-ip.

Se solicitará sobre qué cuenta se quiere estar actualizado.

Añadir el intervalo de consulta por defecto.

En la opción de ejecutar alguna cosa cuando la actualización sea completada, poner que No.

Lanzar el programa “noip2”.

Para opciones de configuración del cliente o añadir un script al inicio para que ejecute automáticamente “noip2”, consultar el archivo LEEME.PRIMERO.

### Servidor NFS

El servidor NFS no viene por defecto en el núcleo de Debian, debe ser descargado, ejecutar: “*apt-get install nfs-kernel-server*”

Editar el fichero de configuración “*/etc/exports*” y añadir la ruta de la carpeta compartida, la red o IP que se permite el acceso y los permisos:

“*/home/benja/Public 192.168.233.0/255.255.255.0(rw,no\_subtree\_check)*”

Editar el fichero de denegación de equipos “*/etc/hosts.deny*”:

```
portmap:ALL  
lockd:ALL  
mountd:ALL  
rquotad:ALL  
statd:ALL
```

Editar el fichero de admisión de acceso “*/etc/hosts.allow*”:

```
portmap: 192.168.233.0/24  
lockd: 192.168.233.0/24  
mountd: 192.168.233.0/24
```

```
rquotad: 192.168.233.0/24  
statd: 192.168.233.0/24
```

Reiniciar el servicio NFS: “*/etc/init.d/nfs-kernel-server restart*”

Se verifica que está funcionando mediante: “*rpcinfo -p*”

### **Cliente NFS**

Linux: tener instalado el paquete: nfs-commons

Windows: tener instalado el rol de Cliente NFS y seguir los pasos del asistente.

### **Linux**

Ejecutar: “*mount IPservidor:/ruta/recurso/compartido /ruta/local/*”

### **Samba**

Ejecutar “*apt-get install samba smbfs*”

Introducir el nombre del dominio o el grupo de trabajo al que corresponderá el servidor Samba.

Editar el fichero “*/etc/samba/smb.conf*” y localizar lo siguiente, para habilitar la autenticación de usuarios:

```
##### Authentication #####
```

```
# "security = user" is always a good idea. This will require a Unix account  
# in this server for every user accessing the server. See  
# /usr/share/doc/samba-doc/htmldocs/Samba3-HOWTO/ServerType.html  
# in the samba-doc package for details.  
security = user
```

Hay que añadir una contraseña de usuario para Samba:  
*smbpasswd -a <username>*

En el mismo fichero, se localiza la siguiente cabecera:

```
===== Share Definitions =====
```

Y cambiar su contenido por:

```
[homes]  
comment = Directorios Home  
browseable = yes
```

```
# By default, the home directories are exported read-only. Change the  
# next parameter to 'no' if you want to be able to write to them.  
read only = no
```

```
# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# The following parameter makes sure that only "username" can connect
# to \\server\username
# This might need tweaking when using external authentication schemes
valid users = %S
```

### Comprobación Acceso en cliente Windows

Especificar la dirección del servidor y el nombre de usuario: “\\servidor\\usuario”

## CUPS

El servidor de Impresión ya viene instalado por defecto en el sistema Debian.

### Instalación CUPS-PDF + Integración con Samba

Ejecutar: “*apt-get install cups-pdf*”

Editar el archivo de configuración de CUPS “/etc/cups/cupsd.conf” y añadir la línea:  
“Port 631”

Y añadir también la red a la que se permitirá el acceso entre las secciones de  
“<Localtion />”, “<Location /admin>” y “<Location /admin/conf>”:

```
Allow 192.168.X.X/24
Allow @LOCAL
```

Guardar el archivo y editar el fichero CUPS de PDF: “/etc/cups/cups-pdf.conf” y  
cambiar:

*Out \$HOME/PDF*  
por el lugar donde se quieran guardar los PDF generados.

Añadir a “/etc/samba/smb.conf” lo siguiente:

```
printing = cups
printcap name = cups
```

Copiar el driver PPD de CUPS-PDF dentro del directorio modelo:  
*mkdir -p `cups-config --datadir`/model/Generic*  
*cp /usr/share/ppd/cups-pdf/CUPS-PDF.ppd `cups-config --datadir`/model/Generic*

Reiniciar CUPS y Samba  
*sudo /etc/init.d/cups stop*  
*sudo /etc/init.d/samba stop*  
*sudo /etc/init.d/cups start*  
*sudo /etc/init.d/samba start*

Abrir un navegador web y acceder a <https://<ip-servidor>:631>

E ir a: Administración->Añadir Impresora.

Colocar el nombre, localización y descripción para la impresora.

Al preguntar por los credenciales se debe colocar el usuario root.

En Administración, marcar la opción de Compartir Impresoras conectadas a este sistema.

Ahora se debe añadir la impresora al directorio de Samba, editar “/etc/samba/smb.conf” con:

```
NombreDadoAlaImpresora  
comment = PDF files  
path = /localizacion/especificada/anteriormente  
browsable = yes  
read only = yes  
hide unreadable = yes  
guest ok = no
```

Se debe reiniciar Samba:

```
/etc/init.d/samba stop  
/etc/init.d/samba start
```

Comprobar integración en Samba

## VSFTP

Ejecutar: “*apt-get install vsftpd*”

Editar el archivo de configuración: “*/etc/vsftpd.conf*”

Dejar la directiva: “*anonymous\_enable=YES*” y asegurarse de que la directiva “*#write\_enable=YES*” esté comentada.

Habilitar la línea “*#local\_enable=YES*”.

Para añadir seguridad a las acciones de los usuarios es necesario habilitar la siguiente directiva: “*#chroot\_local\_user=YES*”.

Reiniciar el servicio: “*/etc/init.d/vsftpd restart*”

## VMWare Server

La instalación de VMWare Server requiere tener una cuenta en la web oficial para poder descargar los fuentes o RPM.

En caso de utilizar los RPM se necesita que Debian pueda portar ese formato a DEB, para ello es necesario el programa Alien: “*apt-get install alien dpkg-dev debhelper build-essential*”

Instalado Alien, convertir el formato:

```
alien paquete.rpm  
dpkg -i paquete.deb
```

Instalación desde los fuentes, descargar el formato TZ y descomprimirlo.  
Acceder a la carpeta descomprimida y ejecutar: “*perl vmware-install.pl*”

En la instalación seleccionar las rutas por defecto que marca el programa y seleccionar la opción que permite ejecutar el asistente de configuración de VMware server.

Aceptar los Términos de uso.

Al finalizar la instalación, se debe recomilar el núcleo de vmware que será utilizado en la virtualización, seguir los pasos que marca el asistente.

## LDAP

Ejecutar: “*apt-get install slapd ldap-utils*”

Instalado, añadir los Schemas necesarios:

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

Crear un fichero LDIF de ejemplo con lo siguiente:

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb.la

# Database settings

dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=benjaDebian,dc=es
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=benjaDebian,dc=es
olcRootPW: {SSHA}e3ZH+TckdAnUqnKARINBSM9AVlvzOcLv
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=benjaDebian,dc=es" write
by$ 
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=benjaDebian,dc=es" write by * read
```

Crear la contraseña para admin de LDAP:

```
slappasswd
New password:
Re-enter new password:
```

{SSHA}MWyKewM8KHu22/4SdiYYuyXEoAjrZEoQ

Añadir el fichero a LDAP:

"ldapadd -Y EXTERNAL -H ldapi:/// -f example.ldif"

Crear un nuevo fichero LDIF para definir la estructura del árbol LDAP:

```
dn: dc=benjaDebian,dc=es
objectClass: top
objectClass: dcObject
objectclass: organization
o: Dominio benjaDebian
dc: benjaDebian
description: LDAP Example
# Admin user.
```

```
dn: cn=admin,dc=benjaDebian,dc=es
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: {SSHA}e3ZH+TckdAnUqnKARINBSM9AVlvzOcLv
```

```
dn: ou=usuarios,dc=benjaDebian,dc=es
objectClass: organizationalUnit
ou: usuarios
```

```
dn: ou=grupos,dc=benjaDebian,dc=es
objectClass: organizationalUnit
ou: grupos
```

```
dn: uid=pepito,ou=usuarios,dc=benjaDebian,dc=es
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: pepito
sn: Perez
givenName: Pepito
cn: Pepito Perez
displayName: Pepito perez
uidNumber: 1000
gidNumber: 10000
userPassword: pass
gecos: Usuario prueba
loginShell: /bin/bash
homeDirectory: /home/john
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
```

```
shadowMin: 8  
shadowMax: 999999  
shadowLastChange: 10877  
mail: pepito@example.com  
initials: JD
```

Añadir la estructura a LDAP: “*ldapadd -x -D cn=admin,dc=benjaDebian,dc=es -W -f fexample.ldif*”

Comprobar que el usuario ha sido añadido correctamente: “*ldapsearch -xLLL -b "dc=benjaDebian,dc=es" uid=pepito sn givenName cn*”

### **Instalación Herramientas Gráficas para LDAP**

\*\*Requerimientos previos: Apache2 y PHP5 instalados y configurados.

### **PHPLdapAdmin**

Ejecutar: “*apt-get install phpldapadmin*”

En caso que el servidor Apache no se reinicie, hacerlo manualmente:  
“*/etc/init.d/apache2 restart*”

Con un navegador Web acceder a <http://servidor/phpldapadmin> para entrar al panel de acceso:

### **WINE**

Ejecutar: “*apt-get install wine*”

Después de la instalación ejecutar “*winecfg*” para cambiar la configuración inicial de Wine por la deseada.

### **Funcionamiento de WINE**

Desde la consola:

Ejecutar “*wine nombreEje.exe*”

Desde modo gráfico:

Doble click sobre el programa.exe

### **Solaris**

### **Licencia**

CDDL

### **Servidor SSH**

#### **Descarga e instalación de ssh**

El primer paso es descargar los siguientes paquetes:

- OpenSSL (Latest stable: openssl-0.9.8f)
- ZLib (Latest stable: zlib-1.2.3)

- GNU Compiler Collection (gcc Latest stable: libgcc-3.4.6)
- TCPWrapper (Opcional tcp\_wrappers-7.6)
- OpenSSH (Latest Stable: openssh-4.7p1)

Todos los paquetes se pueden descargar en la página [www.sunfreeware.com](http://www.sunfreeware.com), después se descomprimirán con “gunzip nombre.zio” y se instalan con “pkgadd –d nombre”

### **Configuración del entorno**

El primer paso es crear un directorio EMPTY con el comando :

```
#create /var/empty directory
```

```
#mkdir /var/empty
```

Se cambian los dueños a el usuario root y sys

```
# chown root:sys /var/empty
```

Se cambian los permisos, se crea el grupo y se añada al usuario root al mismo.

```
#chmod 755 /var/empty
```

```
#groupadd ssh
```

```
#useradd -g sshd -c 'sshd privsep' -d /var/empty -s /bin/false sshd
```

Se crean las contraseñas públicas y privadas

```
#ssh-keygen -t rsa1 -f /usr/local/etc/ssh_host_key -N ""
```

```
#ssh-keygen -t dsa -f /usr/local/etc/ssh_host_dsa_key -N ""
```

```
#ssh-keygen -t rsa -f /usr/local/etc/ssh_host_rsa_key -N ""
```

Se habilita SSH para el root editando el archivo del SSHD y cambiando el

```
PermitRootLogin de no a yes
```

```
/etc/ssh/sshd_config
```

```
PermitRootLogin yes
```

### **Puesta en marcha de SSH**

Para arrancar el servicio “svcadm enable ssh”

Para parar el servicio “svcadm disable ssh”

Para conectarse desde Windows se debe loguear con ssh usuario@ip

### **Servicio SCP**

Al instalar ssh se instala también SCP, para su uso habría que hacer:

```
scp [[usuario@]host-origen:]archivo-origen [[usuario@]host-destino:][archivo-destino]
```

Ejemplos de uso:

```
scp usuario@10.0.0.1:/home/usuario/imagenes/imagen.jpg
```

```
/home/usuario2/Escritorio
```

```
scp /home/usuario2/Escritorio/imagen.jpg
```

```
usuario@10.0.0.1:/home/usuario/imagenes/
```

### **Servicio SFTP**

Al instalar ssh se instala también SFTP, para arranque y parada de servicios se usan los comandos:

```
Svcadm enable sftp
```

```
Svcadm disable sftp
```

### **Servicio VNC**

El primer paso es descargar el paquete de [www.sunfree.com](http://www.sunfree.com), después, para instalarlo habrá que introducir la orden

```
# pkgadd -d vnc-4_1_2-sparc_solaris.pkg
```

El sistema hará algunas preguntas sobre si crear el directorio /usr/local y si instalar el paquete.

Para iniciar el servicio de VNC es necesario ingresar a la cuenta bajo la cual se desea que corra el entorno gráfico y ejecutar el comando vncserver (BANFIN@oracle):

```
oracle/$ vncserver -depth 16 -geometry 1270x700
You will require a password to access your desktops.
Password:
Verify:
xauth: creating new authority file /export/home/oracle/.Xauthority
New 'sp.upb.edu.co:1 (oracle)' desktop is sp.upb.edu.co:1
POSIBLE ERROR
VNC server:
bash-3.2 $ vncserver
vncserver: no se pudo encontrar "Xvnc" en su PATH.
Se necesita la aplicación de PATH, también puede recibir el siguiente error
similar a:
vncserver: no se pudo encontrar "xauth" en su PATH.
```

Xvnc está bajo el directorio /usr/X11/bin mientras xauth se encuentra bajo /usr/openwin/bin para añadirlos a la ruta, se deben agregar de la siguiente manera:

```
PATH = $PATH :/usr/X11/bin :/usr/openwin/bin
export PATH
```

## Rdesktop

Primero se debe ingresar en [www.sunfreeware.com](http://www.sunfreeware.com) y buscar la aplicación, después mostrará el paquete y sus dependencias, se debe garantizar que las librerías solicitadas se encuentren disponibles. Es necesario que "libiconv", "openssl-0.9.8l" , "libgcc-3.4.6" o "gcc-3.4.6" esté instalado.

Hay que descargar los paquetes:

```
libgcc-3.4.6-sol10-sparc-local.gz
libiconv-1.13.1-sol10-sparc-local.gz
openssl-0.9.8l-sol10-sparc-local.gz
rdesktop-1.5.0-sol10-sparc-local.gz
```

Y después descomprimirlos:

```
#gzip -d libgcc-3.4.6-sol10-sparc-local.gz
#gzip -d libiconv-1.13.1-sol10-sparc-local.gz
#gzip -d openssl-0.9.8l-sol10-sparc-local.gz
#gzip -d rdesktop-1.5.0-sol10-sparc-local.gz
```

Tras la descompresión, los archivos quedan así:

```
file libgcc-3.4.6-sol10-sparc-local package datastream
file libiconv-1.13.1-sol10-sparc-local package datastream
```

```
file openssl-0.9.8l-sol10-sparc-local package datastream  
file rdesktop-1.5.0-sol10-sparc-local package datastream
```

Una vez descomprimidos se instalan dentro de /usr/local:

```
#pkgadd -d libgcc-3.4.6-sol10-sparc-local  
#pkgadd -d libiconv-1.13.1-sol10-sparc-local  
#pkgadd -d openssl-0.9.8l-sol10-sparc-local  
#pkgadd -d rdesktop-1.5.0-sol10-sparc-local
```

Después de hacer la instalación de estos paquetes se comprueba que se encuentren instalados:

```
root@masterserver # pkginfo | grep -i libgcc  
application SMClgcc346 libgcc  
root@masterserver # pkginfo | grep -i libiconv  
application SMClconv libiconv  
root@masterserver # pkginfo | grep -i openssl  
application SMCossl openssl  
root@masterserver # pkginfo | grep -i rdesktop  
application SMCrdesk rdesktop
```

## XDMCP

Loguearse como administrador.

Abrir una terminal

Escribir gdmsetup, tras lo que aparecerá un cuadro de diálogo

Hacer click en la pestaña de XDMCP

Hacer click en la caja de Enable XDMCP

Pulsar cerrar

## FreeNX

Solo está disponible para arquitecturas SPARC

## DHCP

La configuración tiene dos pasos

Primero hay que asignar un tipo de almacenamiento y un path a las tablas DHCP  
`/usr/sbin/dhcpconfig -D -r SUNWfiles -p /var/dhcp`

Created DHCP configuration file.

Created dhcptab.

Added "Locale" macro to dhcptab.

Added server macro to dhcptab - mydhcpsrv

DHCP server started.

Después especificamos un rango de IP para el cual se ejecutarán los servicios DHCP, por ejemplo:

```
/usr/sbin/dhcpconfig -N 10.10.1.0 -t 10.10.1.1  
Added network macro to dhcptab - 10.10.1.0.  
Created network table.
```

AGREGAR (para cada uno de las ip) RANGO 192.168.233.80-90

```
pntadm -r SUNWfiles -p /var/dhcp -A 10.10.10.1 10.10.10.0
```

## SAMBA

Descargar SAMBA y darle los permisos chmod 755 a la carpeta del servidor

## CentOS

### Licencia

GPL

### Particionado

Total – 20Gb

/boot 200Mb

/4Gb

/src 7Gb

/var 7Gb

swap

### Arranque y parada de servicios

Los servicios se encuentran en /sbin/

Para arrancar un servicio hay que introducir el comando service [nombre-servicio] start

Para detener un servicio hay que introducir el comando service [nombre-servicio] stop

Para reiniciar un servicio hay que introducir el comando service [nombre-servicio] restart

### Administración remota:

**ssh, sftp, scp (Acceso por usuario y mediante clave pública/privada)**

ssh [usuario]@[ip]

ssh asorc@192.168.233.9

### VNC

Para instalar hay que descargar el paquete vnc-server

```
yum -y install vnc-server
```

Se debe crear un password para que un usuario pueda acceder , ( vncuser) que se guardará en /home/vncserver/.vnc

```
vncpasswd vncuser
```

Para editar la configuración se accede a /etc/sysconfig/vncservers y se añade:

```
VNCSEVERS="1:vncuser"  
VNCSEVERARGS[1]="-geometry 800x600"
```

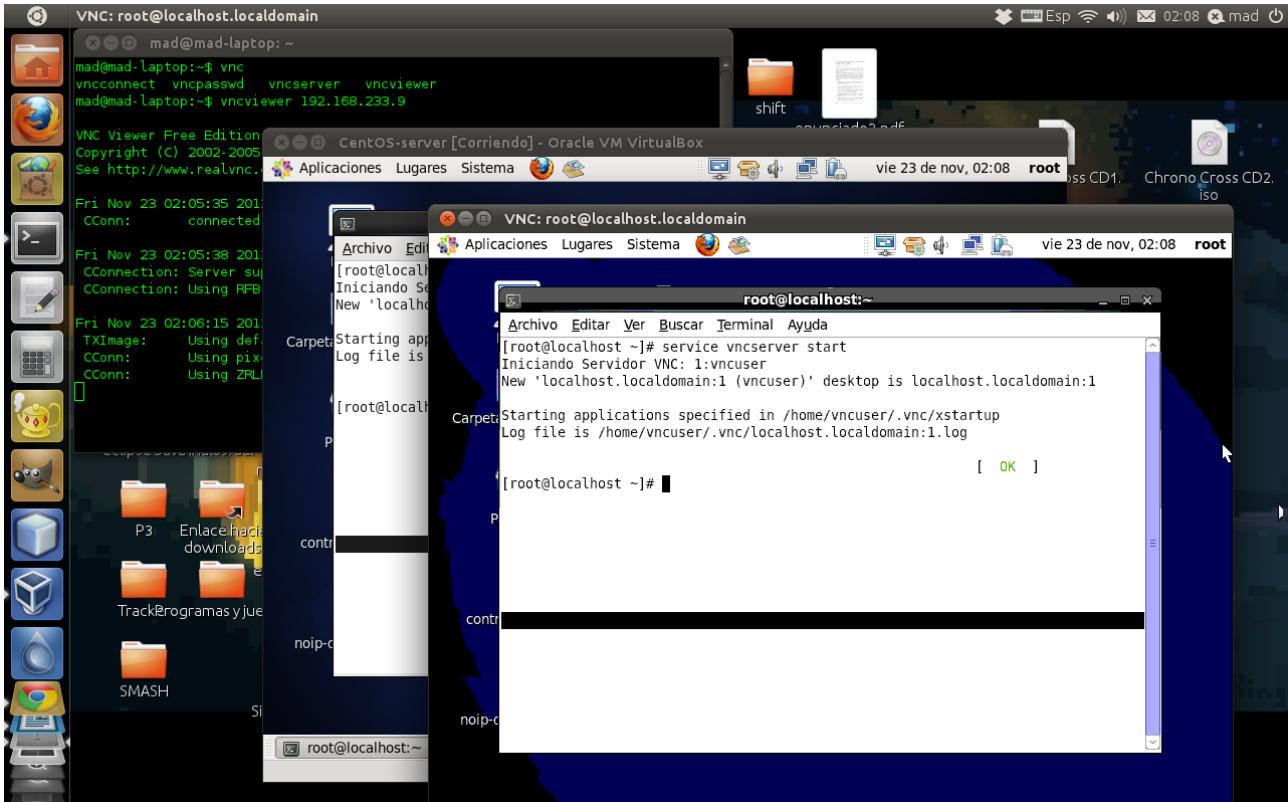
vncuser tendrá una pantalla de 800x600.

Se arranca el vncserver

service vncserver start

En el cliente debemos tener instalado vncviewer e introducir el comando  
vncviewer [ip]

vncviewer 192.168.233.9



## XDMCP

Para configurar xdmcp se accede a /etc/gdm/custom.conf y se selecciona

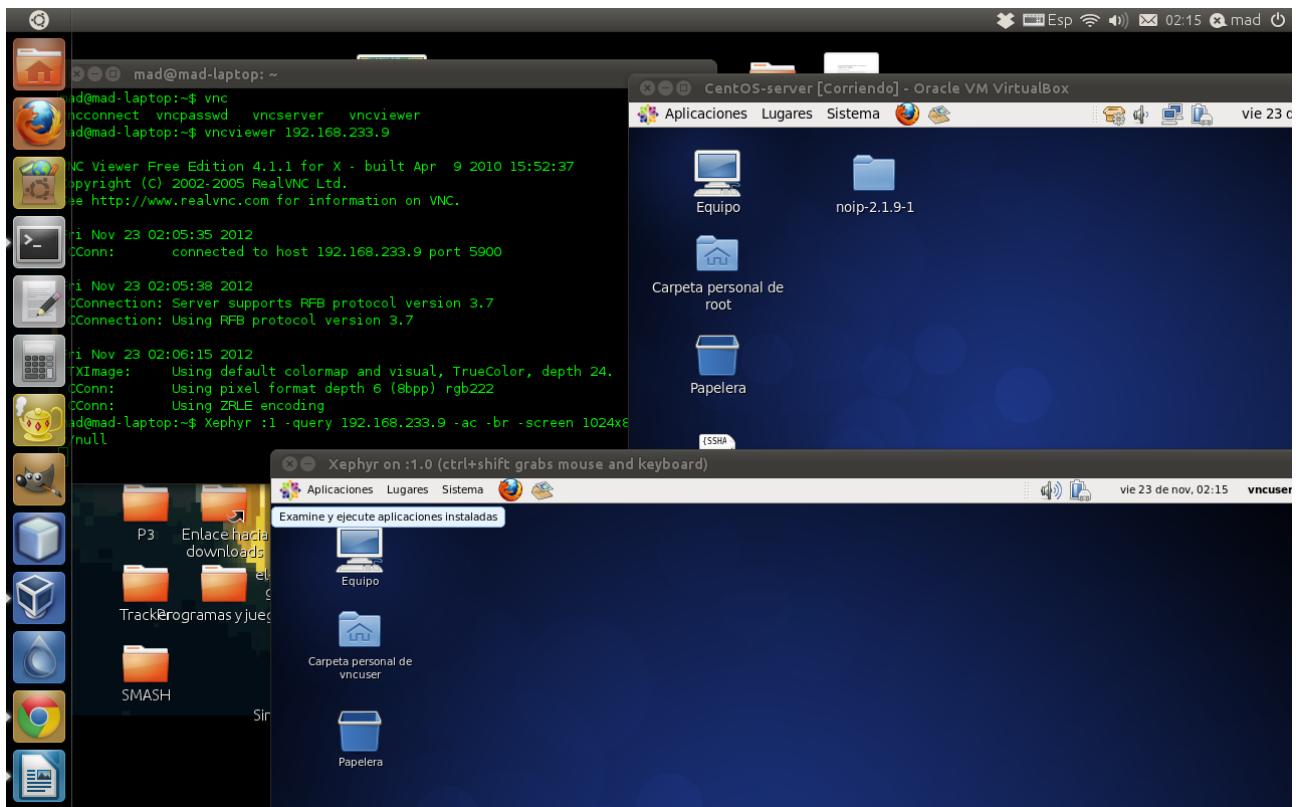
```
[xdmcp]
Enable=true
```

```
[security]
Enable=true
```

```
[greeter]
IncludeAll=true
```

Y desde el cliente se ejecuta:

```
Xephyr :1 -query 192.168.233.9 -ac -br -screen 1024x800 2>/dev/null
```



## FreeNX

Se instala el freenx:

```
yum -y install nx freenx
```

Se crea un usuario nx:

```
nxserver –adduser nxuser
nxserver –passwd nxuser
```

En /etc/nxserver/node.conf se encuentra el ficher de configuración de freenx.

Se realiza la siguiente modificación:

```
PasswordAuthentication no
AllowUsers nx
```

```
ENABLE_PASSDB_AUTHENTICATION="1"
```

Se inicia el nxserver

```
nxserver
```

Y desde el cliente se accede desde NoMachine

## Servicio DNS (estático y dinámico, como dyndns)

Para configurar el dns se instalan los paquetes bind

```
yum -y install bind bind-chroot bind-utils
```

Se configura el archivo /etc/named.conf y se definen la zone 'asorcentos.org':

The screenshot shows a desktop environment for a CentOS server running in Oracle VM VirtualBox. The main window is a text editor titled "named.conf (/etc) - gedit" containing the following configuration code:

```
options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    forward first;
    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;
    bindkeys-file "/etc/named.iscdlv.key";
};

logging {
    channel default_debug {
        file "/data/named.run";
        severity dynamic;
    };
};

controls {
    inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
    match-clients {
        127.0.0.1;
    };
    zone "asorcentos.org" {
        type master;
        file "/var/named/asorcentos.org.zone";
        allow-update { none; };
    };
}
```

The configuration includes options for directory, dump files, statistics, forwarders (8.8.8.8 and 8.8.4.4), forward policy, DNSSEC, bindkeys, logging (severity dynamic), controls (inet 127.0.0.1), and an include statement for /etc/rndc.key. The view "local" section defines a master zone for "asorcentos.org" with a file at /var/named/asorcentos.org.zone and no update access.

In the background, a file manager window is open, showing two ISO files: "Cross CD1.iso" and "Chrono Cross CD2.iso". A status bar at the bottom right of the desktop indicates "Ctrl Derecho" (Right Control).

Oracle VM VirtualBox  
CentOS-server [Corriendo] - Oracle VM VirtualBox

Ejercicio Editar Ver Buscar Herramientas Documentos Ayuda

Abrir Guardar Deshacer CORTAR COPIAR PEGAR BUSCAR REINICIAR

named.conf

```

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

controls {
    inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc-key"; };
};

include "/etc/rndc.key";

view "local" {
    match-clients {
        127.0.0.0/8;
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
    };
    recursion yes;
    include "/etc/named.rfc1912.zones";
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "asorccentos.com" {
        type master;
        file "data/asorccentos.zone";
        allow-update { none; };
    };
};

```

root@localhost:~ / named.conf (/etc) - gedit

Ancho de la tabulación: 8 Ln 22, Col 27 INS

Y en /var/named/data/asorccentos.zone se define la configuración de la zona:

Oracle VM VirtualBox  
CentOS-server [Corriendo] - Oracle VM VirtualBox

Aplicaciones Lugares Sistema vie 23 de nov, 02:54 root

asorccentos.zone (/var/named/chroot/var/named/data) - gedit

Ejercicio Editar Ver Buscar Herramientas Documentos Ayuda

Abrir Guardar Deshacer CORTAR COPIAR PEGAR BUSCAR REINICIAR

asorccentos.zone

```

$TTL 86400
@       IN      SOA     asorccentos.  alguien.gmail.com. (
                        2009091001; número de serie
                        28800 ; tiempo de refresco
                        7200 ; tiempo entre reintentos de consulta
                        604800 ; tiempo tras el cual expira la zona
                        86400 ; tiempo total de vida
)
@       IN      NS      asorccentos.com.
@       IN      TXT     "v=spf1 a mx -all"
@       IN      A       192.168.233.9
maquina1| IN      A       192.168.233.101
ftp      IN      A       192.168.233.9

```

## Servicio DHCP (asignación por MAC)

Se instala el paquete dhcp

```
yum -y install dhcp
```

En /etc/sysconfig/dhcp

DHCPDARGS=eth0

En /etc/dhcp/dhcpd.conf

```
#  
# DHCP Server Configuration file.  
# see /usr/share/doc/dhcp*/dhcpd.conf.sample  
# see 'man 5 dhcpcd.conf'  
  
ddns-update-style interim;  
ignore client-updates;  
authoritative;  
default-lease-time 900;  
max-lease-time 7200;  
option ip-forwarding off;  
option domain-name "red-local.net";  
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;  
  
shared-network redlocal {  
    subnet 192.168.233.0 netmask 255.255.255.0 {  
        option routers 192.168.233.9;  
        option subnet-mask 255.255.255.0;  
        option broadcast-address 192.168.233.255;  
        option domain-name-servers 192.168.233.9;  
        option netbios-name-servers 192.168.233.9;  
        range 192.168.233.91 192.168.233.100;  
    }  
    host pc1{  
        option host-name "pc1.red-local.net";  
        hardware ethernet 08:00:27:fb:48:bd;  
        fixed-address 192.168.233.101;  
    }  
}
```

## NFS

Se instala el paquete nfs-utils

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

En /etc/sysconfig/nfs se definen los puertos:

```
RQUOTAD_PORT=875  
LOCKD_TCPPORT=32803  
LOCKD_UDPPORT=32769  
MOUNTD_PORT=892  
STATD_PORT=662
```

En /etc/exports se añade

/carpetaacompartir ip(opciones)

service nfs start

Y desde el cliente:

mount -t nfs [ip]:/carpetaacompartir /rutadestino

### SAMBA/SMB (LDAP)

yum -y install samba samba-client samba-common

En /etc/samba/smb.conf se edita la configuración

service smb start

En el cliente se debe instalar smbclient y realizar la instrucción

smbclient //ipdemaquina/recurso -U usuario

### Servidor FTP (Serv-U, vsftpd, proftpd)

Se instala el paquete vsftpd

yum -y install vsftpd

En /etc/vsftpd/vsftpd.conf se edita la configuración.

Service vsftpd start

### Emulación de otro sistema operativo: CYGWIN, WINE, Qemu

#### Wine

yum -y install wine

## PCBSD

### Licencia

BSD

### Gestión del particionamiento

Durante el proceso de instalación se deben definir las particiones que se considere con las herramientas que se proporcionan durante la instalación.

Para este caso, se han definido tres particiones más la del Swap:

- Una partición que se sitúa en root “/”
- Una segunda que se sitúa en usr “/usr”
- Una tercera que se sitúa en var “/var”

Esta gestión permite aislar toda la paquetería, programas y contenido de las aplicaciones de la configuración del sistema, archivos temporales y archivos personales.

## **Arranque y parada de servicios**

Los servicios se arrancan mediante el comando  
nombreServicio\_enable = YES

La configuración por defecto del sistema se puede sobreescribir desde /etc/rc.conf.  
Una vez que un servicio aparece en /etc/rc.conf el servicio puede arrancarse desde  
la línea de comandos con el comando:

```
# /etc/rc.d/sshd start
```

Si un servicio no dispone de la entrada en /etc/rc.conf se puede arrancar usando la  
opción forcestart:

```
# /etc/rc.d/sshd forcestart
```

## **Problemas surgidos**

En favor de la futura release candidate la versión estable ha sido dada de lado y  
por ello la mayoría de los ports que son los archivos desde los que se instala la  
paquetería están rotos. Por todo ello no hemos podido configurar los servicios para  
este servidor.