

**UNIVERSIDAD SAN CARLOS DE GUATEMALA**

**CENTRO UNIVERSITARIO DE OCCIDENTE**

**-CUNOC-**



**MANUAL GENERAL SISTEMAS OPERATIVOS 1**

Astrid Gabriela Martinez Castillo	201731318
Fatima Odra Daniela Tezó Sum	201831039
Jhonny Ismael García Hernández	201830454

Sistemas Operativos 1.  
Ing. Francisco Rojas.

Quetzaltenango, 13 de mayo de 2021




## Introducción

El siguiente documento está centrado a la creación y control de una red utilizando herramientas como LDAP para la autenticación de los usuarios, webMail para el control de correos electrónicos y un servidor de backup, en este se mencionan los pasos a seguir para la creación de un servidor de autenticación LDAP relatando cada paso desde la creación de cuentas y la creación de usuarios en el mismo, así como también la instalación de hamachi entre otras herramientas necesarias.

## ÍNDICE

<b>Introducción</b>	<b>1</b>
<b>Marco Teórico</b>	<b>5</b>
KVM	5
(qemu-kvm) en Linux	6
Protocolo LDAP	7
WebMail	14
Hamachi	14
Bacula	17
<b>Especificaciones Técnicas</b>	<b>18</b>
KVM	18
CentOs (sin entorno gráfico)	19
Windows 10	19
<b>Instalación qemu-KVM</b>	<b>20</b>
Creación Maquina Virtual	23
Crear Cuenta Hamachi	27
Instalación Hamachi	29
<b>Configuración de Servidor LDAP</b>	<b>31</b>
Le otorgamos permisos a ldap	35
Importar esquemas básicos.	35
para hacernos este paso más cómodo se genero el script llamado	35
Configurar el registro LDAP	35
Configure syslog para habilitar el registro LDAP.	35
para esto se creo un script llamado	36
Configuración del cliente LDAP para utilizar el servidor LDAP	36
Creación de usuario nuevo	37
<b>Instalación Hamachi windows 10</b>	<b>41</b>
Instalación ldap windows 10	42
<b>Configuración de Servidor WebMail</b>	<b>46</b>
<b>Configuración de Servidor Backups</b>	<b>56</b>
Instalación de Bacula y MySQL	56



Configuración de la utilización de Mysql por parte de Bacula	57
Configuración del Server de Bacula	57
Configuración del Cliente	62
Iniciar componentes de Bacula	68
Bibliografía	69



## Marco Teórico

### KVM

#### ¿QUÉ ES KVM?


La máquina virtual basada en el kernel (KVM) es una tecnología de virtualización de open source integrada a Linux. En concreto, con KVM se puede convertir a Linux en un hipervisor que permite que una máquina de host ejecute entornos virtuales múltiples y aislados llamados máquinas virtuales (VM) o huéspedes.

#### ¿Cómo funciona KVM?

KVM convierte a Linux en un hipervisor de tipo 1 (sin sistema operativo). Todos los hipervisores necesitan algunos componentes al nivel del sistema operativo (por ejemplo, administrador de memoria, planificador de procesos, pila de entrada o salida (E/S), controladores de dispositivos, gestión de seguridad, pila de red y más) para ejecutar las máquinas virtuales. KVM cuenta con todos estos componentes porque es parte del kernel de Linux. Cada máquina virtual se implementa como un proceso regular de Linux, programada por el planificador estándar de Linux con hardware virtual dedicado como tarjeta de red, adaptador de gráficos, CPU, memoria y discos.

#### Implementar KVM

En pocas palabras, debe ejecutar una versión de Linux lanzada después de 2007 y que deba instalarse en hardware X86 que sea compatible con capacidades de virtualización. Si ya se realizó, entonces todo lo que se debe de hacer es cargar dos módulos existentes (un módulo host




del kernel y un módulo específico del procesador), un emulador y cualquier controlador que lo ayude a ejecutar sistemas adicionales. Sin embargo, al implementar KVM en una distribución Linux como la de Red Hat Enterprise Linux, se amplían las capacidades de KVM, lo que le permite intercambiar recursos entre guests, compartir bibliotecas comunes, optimizar el rendimiento del sistema y mucho más.

### (qemu-kvm) en Linux

qemu-kvm es un virtualizador de código abierto y gratuito. Proporciona emulación de hardware para el hipervisor KVM. qemu-kvm actúa como un monitor de máquina virtual junto con los módulos del kernel de KVM Linux. Emula el hardware de un sistema completo, como una PC y sus periféricos asociados. KVM es un acrónimo de máquina virtual basada en kernel. Es una solución de virtualización completa para Linux en hardware x86 que contiene extensiones de virtualización de Intel VT o AMD-V. Con KVM, se pueden ejecutar varias máquinas virtuales que ejecutan el sistema operativo Linux o Windows sin modificar. Cada máquina virtual tiene hardware virtualizado privado, es decir, una tarjeta de red, un disco, un adaptador de gráficos, etc.

Para el proyecto se utilizara para virtualizar Linux Centos, Linux , Windows.

KVM admite muchos sistemas operativos invitados. Casi todas las distribuciones de Linux. Familia BSD de sistema operativo como FreeBSD, OpenBSD, NetBSD y amigos. Solaris, Windows, Haiku, ReactOS, Plan 9, AROS Research Operating System y más.



## Protocolo LDAP

El protocolo LDAP es muy utilizado actualmente por empresas que apuestan por el software libre al utilizar distribuciones de Linux para ejercer las funciones propias de un directorio activo en el que se gestionan las credenciales y permisos de los trabajadores y estaciones de trabajo en redes LAN corporativas en conexiones cliente/servidor.

### ¿Qué es LDAP?

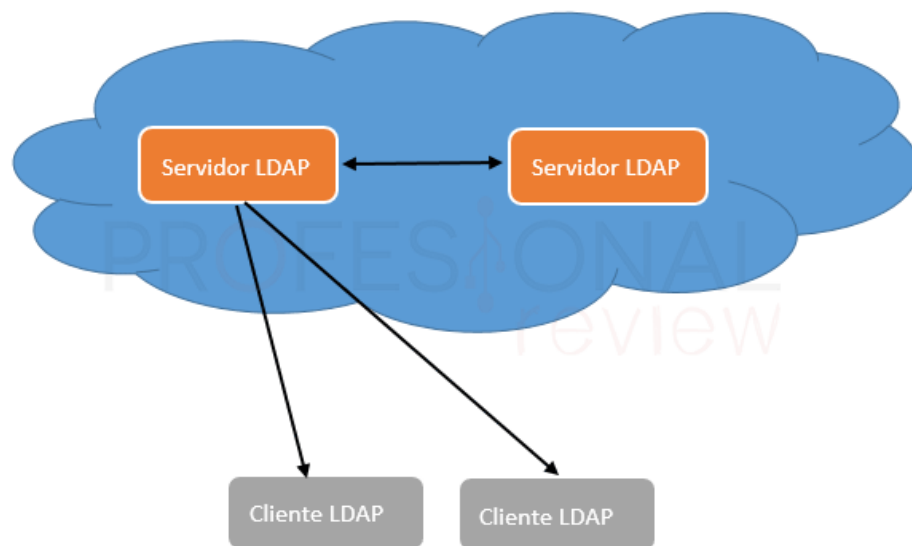
LDAP son las siglas de Protocolo Ligero de Acceso a Directorio, o en inglés (Lightweight Directory Access Protocol). Se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

**Un directorio remoto:** Es un conjunto de objetos que están organizados de forma jerárquica, tales como nombre claves direcciones, etc. Estos objetos estarán disponibles por una serie de clientes conectados mediante una red, normalmente interna o LAN, y proporcionarán las identidades y permisos para esos usuarios que los utilicen.


LDAP está basado en el protocolo X.500 para compartir directorios, y contiene esta información de forma jerarquizada y mediante categorías para proporcionarnos una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores. Es, por así decirlo, una guía telefónica, pero con más atributos y credenciales. En este caso se utiliza el término directorio para referirnos a la organización de estos objetos.

De forma general, estos directorios se utilizan básicamente para contener información virtual de usuarios, para que otros usuarios accedan y dispongan de información acerca de los contactos que están almacenados. Pero es mucho más que esto, ya que es capaz de comunicarse de forma remota con otros directorios LDAP situados en servidores que pueden estar en el otro lado del mundo para acceder a la información disponible. De esta forma se crea una base de datos de información descentralizada y completamente accesible.

### Funcionamiento de LDAP







LDAP es un protocolo basado en la conexión entre cliente y servidor. En el servidor LDAP se almacenarán los datos relativos al directorio, el cual podrá usar una amplia variedad de bases de datos para este almacenamiento, llegando a ser de grandes dimensiones.

El funcionamiento de acceso y administración es muy similar a Active Directory de Windows. Cuando el cliente LDAP se conecta con el servidor, podrá realizar dos acciones básicas, bien consultar y obtener información del directorio, o modificarla.

Si un cliente consulta la información el servidor LDAP puede conectarla directamente si tienen un directorio alojado en él, o bien redirigir la solicitud hasta otro servidor que efectivamente tenga esta información. Este podrá ser local, o remoto.


Si un cliente quiere modificar la información del directorio, el servidor comprobará si el usuario que está accediendo a este directorio tiene permisos de administrador o no. Entonces, la información y gestión de un directorio LDAP se podrá hacer de forma remota.

El puerto de conexión para el protocolo LDAP es el TCP 389, aunque por supuesto, se podrá modificar por el usuario y establecerlo en el que desee si así se lo indica al servidor.

### Cómo se almacena la información en LDAP

En un directorio LDAP podremos almacenar básicamente la misma información que en un Active Directory de Windows. El sistema está basado en la siguiente estructura:

- Entradas: llamadas objetos en Active Directory. Estas entradas son colecciones de atributos con un Nombre Distinguido (DN) Este nombre se utiliza para dar un



identificador único e irrepetible a una entrada del directorio. Una entrada puede ser el nombre de una organización y de ella colgarán unos atributos. También una persona puede ser una entrada.

- Atributos: los cuales poseen un tipo identificador y los correspondientes valores. Los tipos se utilizan para identificar los nombres de atributos, por ejemplo “mail”, “name”, “jpegPhoto”, etc. Algunos de los atributos que pertenecen a una entrada debe ser obligatorios y otros opcionales.
- LDIF: el Formato de Intercambio de Datos de LDAP es la representación en texto ASCII de las entradas LDAP. Este debe ser el formato de los archivos que se utilicen para importar información a un directorio LDAP. Cuando se escriba una línea en blanco, significará el final de una entrada.
- Árboles: Es la organización jerarquizada de entradas. Es así como podríamos organizar un directorio LDAP mediante un nombre de dominio que haría las funciones de árbol y de él colgarían los distintos departamentos o unidades organizativas de una empresa, empleados etc. Y es precisamente de esta forma como actualmente se forma los directorios, gracias al uso de un servicio DNS, podremos asociar una dirección IP con un directorio LDAP para poder acceder a él mediante el nombre de dominio

ejemplo de una entrada de un directorio LDAP generado en la conexión con el cliente:



```
dn: uid=isma,ou=People,dc=apex,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: isma
uid: isma
userPassword: {SSHA}mNMvHZgkCWSPU0LQbKkawiYvfavQimAS
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1020
gidNumber: 100
homeDirectory: /home/isma
```




en donde:

- **dn (domain name):** nombre de entrada, pero no forma parte de la propia entrada.
- **dc:** componente de dominio para identificar las partes del dominio donde se almacena el directorio LDAP.
- **cn (common name):** nombre de atributo para identificar el nombre de usuario, por ejemplo
- **sn (surname):** apellido del usuario
- **telephone number, mail...:** identificar de nombre para el atributo teléfono y correo electrónico.
- **objectClass:** distintas entradas para definir las propiedades de los atributos

Un servidor LDAP, además de almacenar un árbol, puede contener subárboles que incluyen entradas específicas del dominio principal. Además, puede almacenar referencias a otros servidores de directorio para dividir el contenido si es necesario

### Herramientas más importantes que utilizan el protocolo LDAP

En la actualidad existen diversas herramientas que utilizan este protocolo para la comunicación cliente servidor de un servicio de directorio



**OpenLDAP:** es la implementación libre del protocolo LDAP. Tiene su propia licencia y es compatible con otros servidores que utilicen el mismo protocolo. Es utilizado por distintas distribuciones Linux y BSD.

**Active Directory:** es un almacén de datos de directorio con licencia Microsoft e implementado en sus sistemas operativos server desde Windows 2000. Realmente bajo la estructura de Active Directory se encuentra un esquema LDAPv3, por lo que también es compatible con otros sistemas que implemente este protocolo en sus directorios.

**Red Hat Directory Server:** es un servidor que también se basa en LDAP similar a Active Directory, pero mediante una herramienta de código abierto. Dentro de este directorio podremos almacenar objetos como usuarios claves, grupos, políticas de permisos, etc.

**Novell Directory Services:** este es el servidor de directorio propio de Novell para gestionar el acceso a un almacén de recursos en uno o varios servidores conectados en red. Se compone de una estructura de base de datos jerárquica orientada a objetos en la que se almacenan todos los objetivos típicos de los directorios.

**Open DS:** terminamos esta lista con el directorio basado en java de SUN Microsystems, que posteriormente se liberaría para todos los usuarios. Por supuesto, está desarrollado en JAVA y necesitaremos el paquete Java Runtime Environmet para que éste funcione.

## WebMail

Un correo web es un cliente de correo electrónico, que provee una interfaz web que permite crear cuentas de e-mail que pueden ser revisadas a través de la web. Este servicio lo ofrecen muchos sitios web, en especial los portales y también los proveedores de acceso a internet (ISPs). Otras formas de acceder al correo electrónico pueden ser:


- Conectándose con un cliente de correo local a un servidor de correo remoto utilizando un protocolo ad hoc de transporte de correo, como IMAP o POP, descargar los correos y almacenarlos localmente.
- Utilizando un cliente de correo por consola (por ejemplo, Mutt).

El webmail permite listar, desplegar y borrar mediante un navegador web los correos almacenados en un servidor remoto. Los correos pueden consultarse posteriormente desde otro ordenador conectado a la misma red (por ejemplo, Internet) y que disponga de un navegador web.

Generalmente, también permite la redacción y el envío de correos, y no está limitado a la lectura de correo electrónico.

## Hamachi

LogMeIn Hamachi es una aplicación comercial que configura redes privadas virtuales capaz de establecer vínculos directos entre computadoras que están bajo firewalls de NAT sin




necesitar reconfiguración alguna (en la mayoría de los casos). En otras palabras, establece una conexión a través de Internet y simula una red de área local formada por computadoras remotas. Actualmente está disponible la versión para Microsoft Windows y la versión beta para Mac OS X y Linux.

### ¿Cómo funciona?

Hamachi es un sistema VPN de administración centralizada que consiste en un clúster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios.

El software cliente agrega una interfaz de red virtual al ordenador que es utilizada tanto para interceptar el tráfico VPN saliente como para inyectar el tráfico VPN entrante. El tráfico saliente enviado por el sistema operativo a esta interfaz es entregado al software cliente, que lo cifra y lo autentifica y luego lo envía al nodo VPN de destino a través de una conexión UDP iniciada a tal efecto. Hamachi se encarga del tunelamiento del tráfico IP, incluido el broadcast (difusión) y el multicast (multidifusión). La versión Windows reconoce y tunela, además, el tráfico IPX.

Cada cliente establece y mantiene una conexión de control con el Cluster servidor. Cuando la conexión está establecida, el cliente entra en una secuencia de identificación de usuario, seguida de un proceso de descubrimiento y sincronización de estado. El paso de autenticación de usuario autentifica al cliente contra el servidor y viceversa. El descubrimiento es utilizado para determinar la topología de la conexión a Internet del cliente, y más




concretamente para detectar la presencia de dispositivos cortafuegos y servidores NAT. El paso de sincronización extrae una vista del cliente de sus redes privadas sincronizadas con los otros miembros de esas redes.

Cuando un miembro de una red se conecta o se desconecta, el servidor da instrucciones a los otros nodos de la red para que inicien o detengan túneles con dicho miembro. Cuando se establecen túneles entre los nodos, Hamachi utiliza una técnica de NAT transversal asistido por servidor, similar al "UDP hole punching" ("perforadora de agujeros UDP"). Hasta la fecha, no se ha publicado información detallada de cómo funciona realmente. El vendedor afirma que "...atraviesa con éxito las conexiones P2P en el 95% de los casos, aproximadamente..." Este proceso no funciona en ciertas combinaciones de dispositivos NAT, que requieren que el usuario abra un puerto para la conexión. Además de esto, la versión 1.0 del software cliente es capaz de retransmitir el tráfico a través de los 'servidores de retransmisión' que mantiene el vendedor.

El bloque de direcciones 5.0.0.0 está reservado por la IANA y no está actualmente en uso en el dominio de encaminamiento de Internet, pero no está garantizado que esto continúe así en el futuro. Se espera que el fondo común de la se agotará en abril de 2090. Si este rango es asignado, los usuarios de Hamachi no podrán conectarse a ninguna dirección IP de Internet dentro de ese rango mientras estén utilizando el cliente Hamachi.

Además, utilizar un prefijo de red crea un único dominio de difusión entre todos los clientes. Esto hace posible la utilización de protocolos que dependen de la difusión IP para descubrir y anunciar servicios sobre las redes Hamachi.





Hamachi es habitualmente utilizada para jugar en red y para la administración remota. El vendedor provee servicios básicos gratis y otras características extra pagando.


## Bacula

Bacula es una colección de herramientas de respaldo capaz de cubrir las necesidades de respaldo de equipos bajo redes IP. Se basa en una arquitectura Cliente-servidor que resulta eficaz y fácil de manejar, dada la amplia gama de funciones y características que brinda; copiar y restaurar ficheros dañados o perdidos. Además, debido a su desarrollo y estructura modular, Bacula se adapta tanto al uso personal como profesional, desde un equipo hasta grandes parques de servidores.

### **Componentes:**

Los componentes de Bacula: generalmente usado en sistemas u organizaciones donde la información es ingresada desde un dispositivo o punto final de red (PC de escritorio), transporta parte de sus datos a un servidor directamente desde la dirección IP. Todo el conjunto de elementos que forman Bacula trabaja en sincronía y es totalmente compatible con bases de datos como MySQL, SQLite y PostgreSQL.

Bacula-director daemon: Es el demonio que gestiona la lógica de los procesos de backup y los demás servicios. El servidor de la base de datos debe estar accesible desde la máquina que ejecuta este demonio (o también puede estar en la misma máquina y escuchar en localhost).



En el archivo de configuración de este demonio se especifica dónde y cómo acceder al resto de demonios y recursos, la contraseña para el acceso mediante bacula-console y los trabajos o jobs.

Bacula-storage daemon:

Este demonio es el encargado de manejar los dispositivos de almacenamiento; esto exige que este demonio esté instalado en la máquina que posea la conexión física a los dispositivos de almacenamiento, tales como discos locales, grabadoras de CD o DVD, unidades de cinta, volúmenes NAS o SAN, autocargadores o librerías de cinta.

## Especificaciones Técnicas

### **KVM**

#### máquina huésped:

Debe ejecutar una versión de Linux lanzada después de 2007 y que deba instalarse en hardware X86 que sea compatible con capacidades de virtualización.

#### Límites de hardware emulado bajo KVM

- CPU: 1 a 160 CPU virtuales
- Memoria: entre 50 MB y 32 TB



### Requisitos mínimos:

- 6 GB de espacio mínimo de disco duro.
- 2 GB de memoria RAM.
- Arquitectura de procesador de 64 bits.
- Tener activada la virtualización de CPU.

### CentOs (sin entorno gráfico)

Los requisitos mínimos sin entorno gráfico son los siguientes:

- Procesador: basados en arquitectura x86 x64
- 1GB espacio en disco.
- Conectividad a internet.
- RAM de 64MB.

### Windows 10

- Procesador: Procesador a 1 GHz o más rápido o sistema en un chip (SoC)
- RAM: 1 GB para 32 bits o 2 GB para 64 bits
- Espacio en disco duro: 16 GB para un SO de 32 bits o 32 GB para un SO de 64 bits
- Tarjeta gráfica: DirectX 9 o posterior con un controlador WDDM 1.0
- Pantalla: 800x600

## Instalación qemu-KVM

### Paso 1: Verifique el soporte de virtualización en Ubuntu

Ejecute el siguiente comando para verificar si el sistema Ubuntu admite la virtualización.

```
[user@user] $ egrep -c '(vmx|svm)' /proc/cpuinfo
```

```
astridmc@AstridMC:~$ egrep -c '(vmx|svm)' /proc/cpuinfo  
4
```

Un resultado mayor que 0 0 implica que la virtualización es compatible. A partir del siguiente problema, hemos confirmado que nuestro servidor está listo para funcionar.

Para verificar si el sistema admite KVM Virtualización se debe de ejecutar el siguiente comando:

```
[user@user] $ sudo kvm-ok
```

Si la salida dice: La utilidad no está disponible en su servidor. se prosigue a instalar ejecutando el comando apt:

```
[user@user] $ sudo apt install cpu-checker
```

Ahora se ejecuta de nuevo el comando `kvm-ok` para probar su sistema.

```
[user@user] $ sudo kvm-ok
```

Si todo está bien, entonces debería ver el siguiente mensaje: Se puede usar la aceleración de KVM .

```
astridmc@AstridMC:~$ sudo kvm-ok
INFO: /dev/kvm exists
KVM acceleration can be used
astridmc@AstridMC:~$
```

## Paso 2: Instale kvm-qemu

Con la confirmación de que el sistema puede admitir la virtualización de KVM, instalaremos KVM. Virt manager, Utensilios de puente Ejecute el comando y otras dependencias:

```
[user@user] $ sudo apt install -y qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
```

Una pequeña explicación de los paquetes anteriores.

**“emu package (Quick Emulator):** Es una aplicación que le permite realizar la virtualización de hardware.

**Qemu-kvm:** El paquete es el paquete principal de KVM.

**libvirt-daemon:** Es el demonio de virtualización.

**bridge-utils:** El paquete permite crear una conexión de puente para que otros usuarios puedan acceder a una máquina virtual que no sea el sistema host.

**virt-manager:** Es una aplicación para administrar máquinas virtuales a través de una interfaz gráfica de usuario.

Antes de proseguir con la instalación se debe confirmar que el libvirtd demon esté corriendo. Para hacer esto, se ejecuta el siguiente comando.

```
[user@user] $ sudo systemctl status libvirtd
```

```
astridmc@AstridMC:~$ sudo systemctl status libvirtd
[sudo] contraseña para astridmc:
Lo sentimos, vuelva a intentarlo.
[sudo] contraseña para astridmc:
● libvirtd.service - Virtualization daemon
   Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; vendor preset:
   Active: active (running) since Mon 2021-05-10 10:19:44 CST; 2 days ago
     Docs: man:libvirtd(8)
           https://libvirt.org
   Main PID: 1263 (libvirtd)
    Tasks: 40 (limit: 32768)
   CGroup: /system.slice/libvirtd.service
           └─1263 /usr/sbin/libvirtd
             └─2702 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default
               └─2703 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default
                 └─9549 qemu-system-x86_64 -enable-kvm -name guest=centos7.0-LDAP,debu
```

Se puede habilitar el arranque al inicio haciendo lo siguiente

```
[user@user] $ sudo systemctl enable --now libvirtd
```

Se ejecute el siguiente comando para verificar que los módulos KVM estén cargados:

```
[user@user] $ lsmod | grep -l kvm
```

Se puede observar la presencia de en la salida `kvm_intel` Módulo. Este es el caso de los procesadores Intel. Obtienes el para CPU AMD `kvm_intel` Módulo en su lugar.

## Creación Máquina Virtual

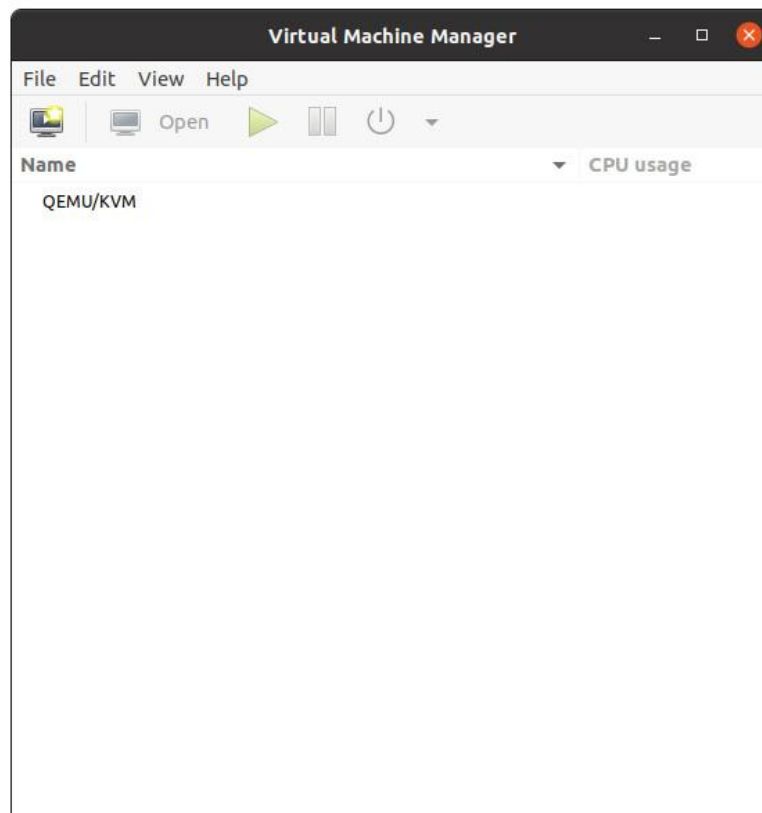
Teniendo KVM instalado correctamente, ahora crearemos una máquina virtual. Hay dos formas de hacer esto: puede crear una máquina virtual en la línea de comando o usar KVM Virt manager interfaz gráfica del usuario.

### Crear una máquina virtual usando virtual-manager

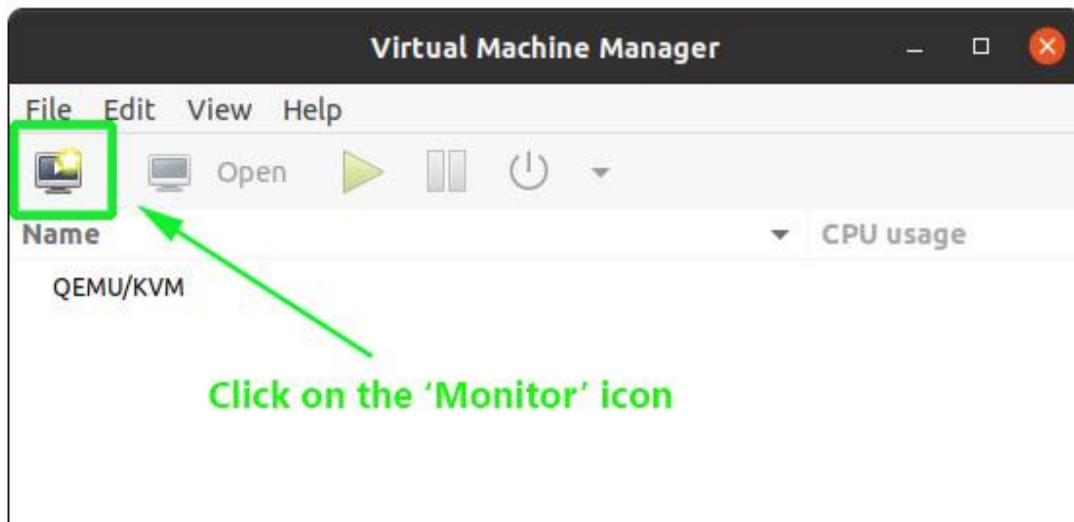
Esta utilidad permite a los usuarios crear máquinas virtuales a través de una GUI. Vaya a la terminal para iniciar y ejecutar el comando.

```
[user@user] $ virt manager
```

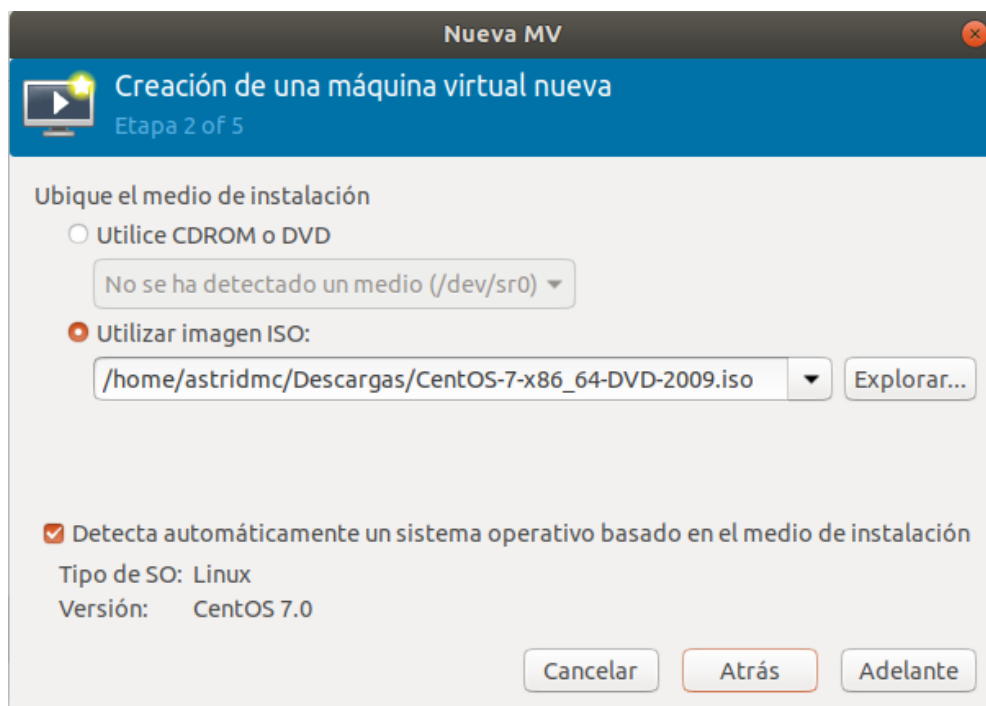
La ventana del Administrador de máquinas virtuales se abre como se muestra:



Ahora haga clic en el icono del monitor para crear una máquina virtual:

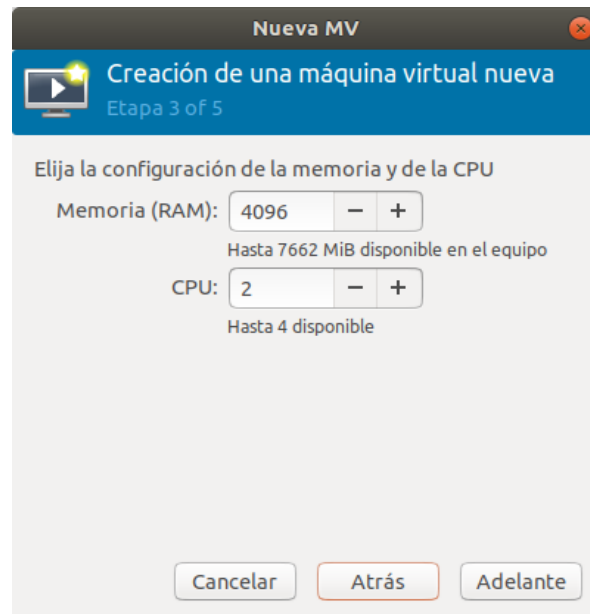


En la ventana emergente, se deberá especificar la ubicación de la imagen ISO, en este caso la de Centos 7 situada en Descargas, por lo que elegimos la primera opción: Medios de instalación local. (Imagen ISO o CD-ROM). Luego haga clic en «Adelante para continuar.





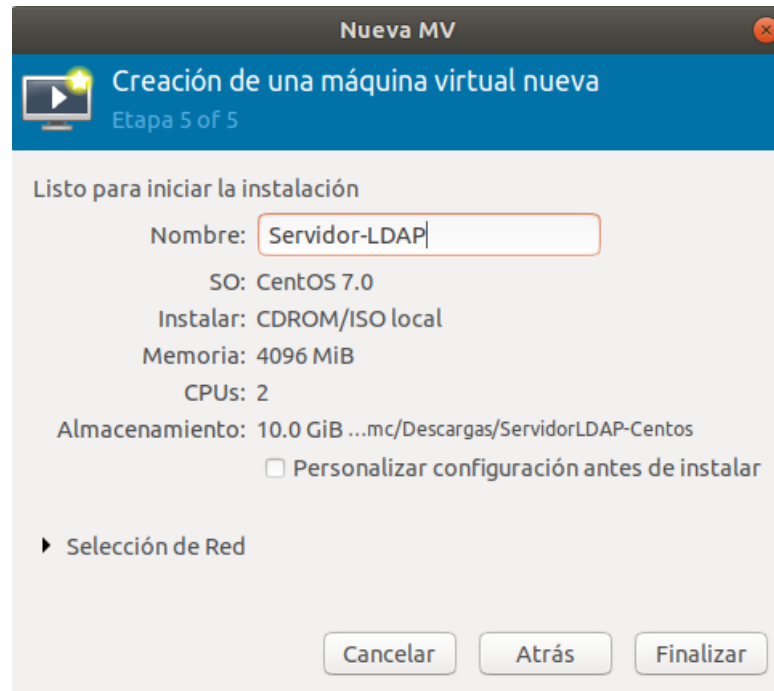
en la siguiente ventana se nos pedirá especificar el tamaño de la memoria RAM y cuantos CPU desea asignar a su máquina virtual, en este caso se le dejó 4GB de ram y 2 CPU, una vez asignado haga clic en 'Adelante'.



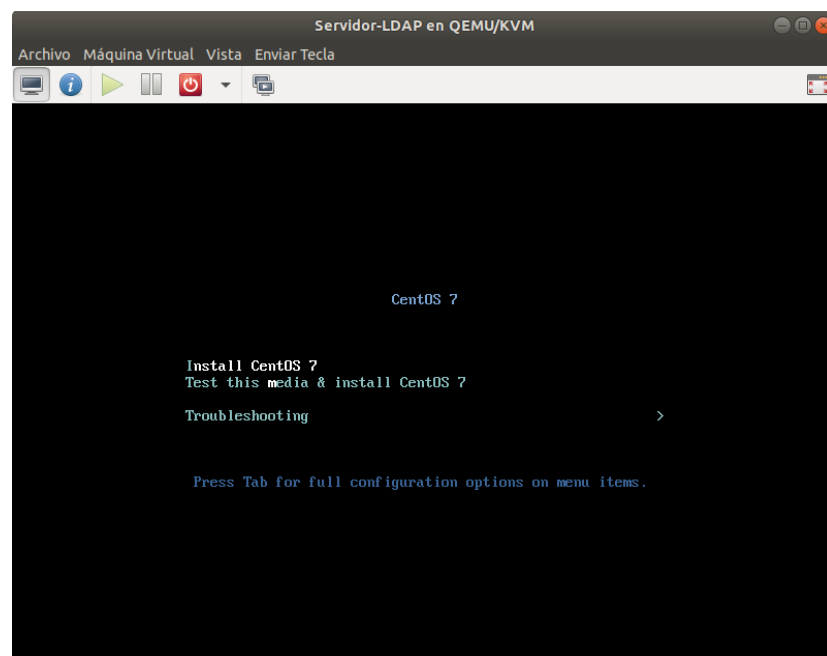
Ahora crearemos el espacio de almacenamiento, para esto nos da dos opciones, crear una imagen de disco para la máquina virtual o seleccionar o crear un almacenaje personalizado. En este caso se escogerá crear un almacenamiento personalizado y examinar almacenamiento, ingresamos el nombre que queremos que tenga y aceptar:



En el último paso, ingrese un nombre para su máquina virtual y haga clic en 'Terminado'; en este caso se esta creando la maquina virtual para el servidor LDAP es por esto que se le asigna el nombre,.



Y la máquina virtual ya estaría creada, solo faltaría la instalación de Centos 7.




## Crear Cuenta Hamachi


para crear una cuenta en hamachi nos vamos al siguiente enlace donde introduciremos nuestro correo y contraseña que deseamos ponerle a hamachi

**Registrarse** o [inicie sesión](#)

Este es su **ID de LogMeIn**, una combinación única de nombre de usuario y contraseña para los servicios de LogMeIn.

 |

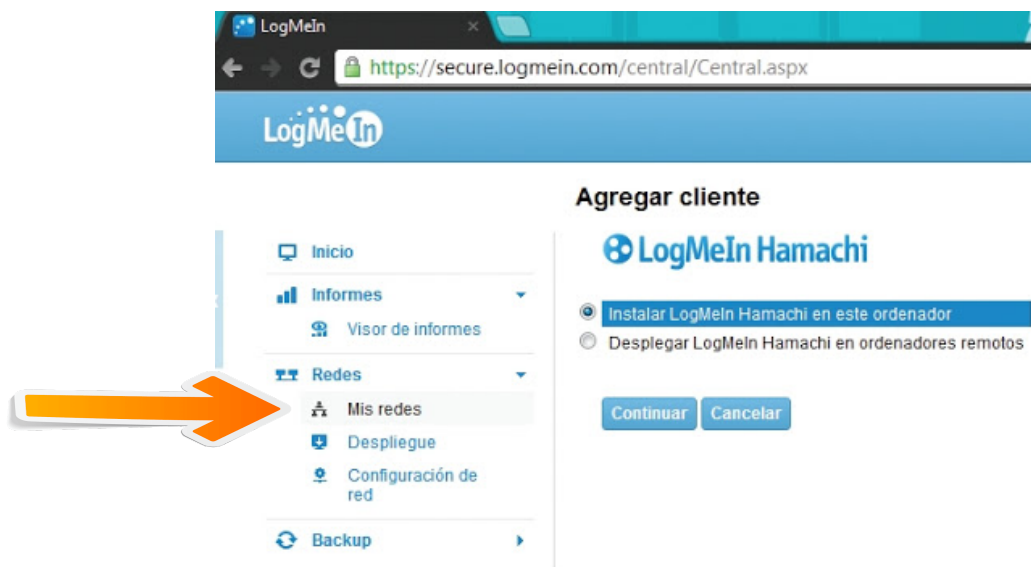
**muy débil**

 |

Acepto los [Términos](#) y la [Política de privacidad](#).  
Quiero recibir e-mails promocionales, incluidas novedades sobre productos, ofertas especiales y prácticas recomendadas, a menos que [indique lo contrario](#).

ahora validamos el correo y entramos a la pagina

<https://secure.logmein.com/central/Central.aspx>



Ahora creamos una nueva red:



y nos aparecerá la siguiente pantalla: donde debemos agregar el nombre de la red, en este caso se llamara server.miRed.com y elegimos el tipo de red en malla.

#### Agregar red (paso 1)

**Tipo y nombre de red**

Nombre de red:

Descripción de la red (opcional):

Tipo de red:

☒ Malla ☐ Hub-y-radios ☐ Puerta

**Red de malla**  
En una red de malla, cada miembro está conectado a todos los demás miembros. Es una elección típica cuando es esencial llegar a todos los miembros de la red.

Y ya tenemos una red hamachi montada:



## Instalación Hamachi

### En CentOS (Linux)

antes de instalar hamachi es necesario instalar wget con el siguiente comando:

```
yum update  
sudo yum install wget
```

Ahora instale Hamachi a través de la línea de comandos.

Descargue Hamachi desde el terminal.

```
wget http://www.vpn.net/installers/logmein-hamachi-2.1.0.165-1.x86_4.rpm
```

El paquete de instalación se descarga en el directorio actual.

Instale el paquete.

```
sudo yum install logmein-hamachi-2.1.0.165-1.x86_4.rpm
```

El cliente se instala en el ordenador local.

Importante: Antes de poder conectarse a una red debe asociar el cliente a su cuenta de LogMeIn.



para facilitar la instalación de hamachi se genero un script para correr en las maquinas

llamado **instalacion\_Hamachi.sh**

```
#!/bin/bash

# primero actualizar repositorios
yum update

# Instalar wget
echo "sudo yum install wget";
sudo yum install wget

echo "Descargando hamachi.....";
echo "sudo wget
http://www.vpn.net/installers/logmein-hamachi-2.1.0.203-1.x86_64.rpm";
sudo wget http://www.vpn.net/installers/logmein-hamachi-2.1.0.203-1.x86_64.rpm

echo "Instalando hamachi...";
echo "sudo yum install logmein-hamachi-2.1.0.203-1.x86_64.rpm";
sudo yum install logmein-hamachi-2.1.0.203-1.x86_64.rpm

echo "se debe ejecutar el comando: hamachi login"
```

## **Configuracion Hamachi**

ingrese el nombre de su cliente con el siguiente comando:

```
sudo hamachi set-nick server2
```

donde server1 es el nombre que le desea poner a su cliente.

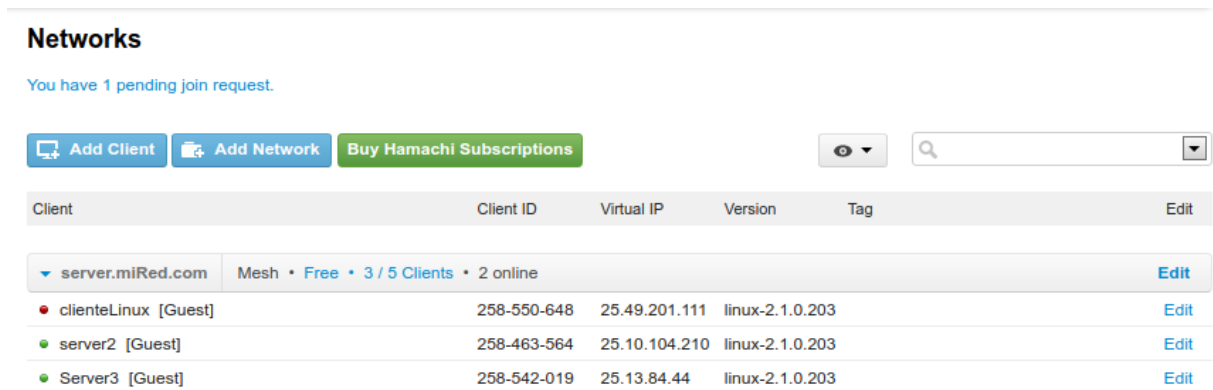
Ejecute `sudo hamachi attach [email@example.com]` con su ID de LogMeIn (dirección de e-mail) para asociar su cliente.

```
sudo hamachi attach astrid.martinez.castillo@gmail.com
```

Ejecute sudo el siguiente comando para iniciar sesión.

```
sudo hamachi login
```

y ya debería aparecer el servidor en la pagina de inicio de hamachi:



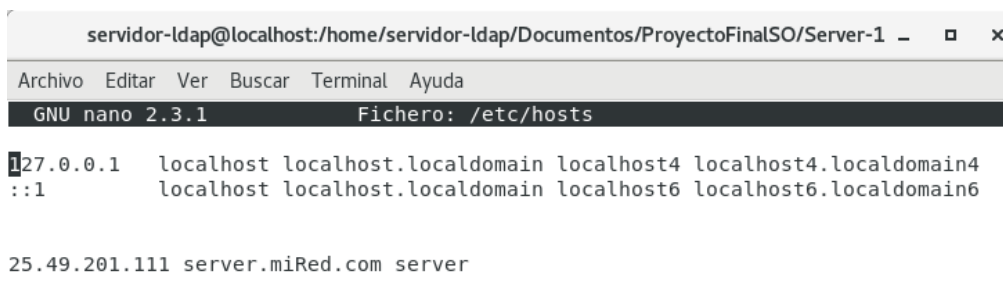
The screenshot shows the Hamachi web interface. At the top, it says "Networks" and "You have 1 pending join request." Below this are buttons for "Add Client", "Add Network", and "Buy Hamachi Subscriptions". There is also a search bar and a visibility toggle. The main part of the interface is a table listing clients connected to a network named "server.miRed.com". The table has columns for Client, Client ID, Virtual IP, Version, Tag, and Edit. There are three clients listed: "clienteLinux [Guest]", "server2 [Guest]", and "Server3 [Guest]".

Client	Client ID	Virtual IP	Version	Tag	Edit
▼ server.miRed.com Mesh • Free • 3 / 5 Clients • 2 online Edit					
● clienteLinux [Guest]	258-550-648	25.49.201.111	linux-2.1.0.203		Edit
● server2 [Guest]	258-463-564	25.10.104.210	linux-2.1.0.203		Edit
● Server3 [Guest]	258-542-019	25.13.84.44	linux-2.1.0.203		Edit

como se puede ver el server 2 ya aparece conectado y corriendo como cliente de la red

## Configuración de Servidor LDAP

escribimos la ip del servidor creado anteriormente en el archivo /etc/hosts junto con el dominio y quedaría de la siguiente manera:



The screenshot shows a terminal window with the title "servidor-ldap@localhost:/home/servidor-ldap/Documentos/ProyectoFinalSO/Server-1". The terminal is running the nano text editor on the file /etc/hosts. The content of the file is as follows:

```
GNU nano 2.3.1 Fichero: /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

25.49.201.111 server.miRed.com server
```

instalar repositorios necesarios para el servidor:

```
yum -y install openldap compat-openldap openldap-clients openldap-servers  
openldap-servers-sql openldap-devel net-tools nano
```

ahora para iniciar el demonio del servidor openldap con el siguiente comando:

```
systemctl start slapd  
sudo systemctl enable slapd  
sudo netstat -antup | grep -i 389
```

para hacernos este paso mas facil se creó un script llamado

### 1-instalacion Openldap.sh

```
#!/bin/bash  
  
echo " " >> /etc/hosts  
read -p " IP del servidor: " ipServidor;  
  
echo "  
$ipServidor server.miRed.com server" >> /etc/hosts  
  
echo "yum -y install openldap compat-openldap openldap-clients openldap-servers  
openldap-servers-sql openldap-devel net-tools nano";  
yum -y install openldap compat-openldap openldap-clients openldap-servers  
openldap-servers-sql openldap-devel net-tools nano  
  
#iniciando demonio del servidor ldap  
echo "systemctl start slapd";  
systemctl start slapd  
echo "systemctl enable slapd";  
systemctl enable slapd  
  
netstat -antup | grep -i 389
```



creamos un fichero con la contraseña cifrada que nos genera ldap llamado passwd.txt:

y agregamos el password generado al momento de ejecutar:

```
slappasswd
```

luego vamos a db.ldif en la misma carpeta y modificamos

olcRootPW: y agregamos la contraseña ejemplo

olcRootPW: {SSHA}XTGXqaGn3UCGBYhbQ7qMwa+wSOtjxIyj

le pasamos a ldap la ruta de nuestro directorio con la contraseña con la siguiente linea de comandos, así como otros archivos necesarios para configuracion:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f passwd.ldif
ldapmodify -Y EXTERNAL -H ldapi:/// -f permiss-modify.ldif
ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif
```

Para hacernos mas facil la configuracion se creo un script que realiza estos pasos llamado

2-configurar\_password\_LDDAP.sh

```
#!/bin/bash

DOCUMENTO=passwd.txt
pass=""

if [ -f $DOCUMENTO ]
then
    rm passwd.txt
    touch passwd.txt
else
    touch passwd.txt
fi
```

```
echo "slappasswd";
slappasswd >> passwd.txt
```

```
while IFS= read -r line
do
    pass=$line
done < passwd.txt
```

```
echo "olcRootPW: $pass" >> db.ldif
```

```
echo "ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif";
ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif
echo "ldapmodify -Y EXTERNAL -H ldapi:/// -f permiss-modify.ldif";
ldapmodify -Y EXTERNAL -H ldapi:/// -f permiss-modify.ldif
echo "ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif";
ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif
```

### 3. configurar\_ldap\_db.sh

```
#!/bin/bash
```

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
echo "chown ldap:ldap /var/lib/ldap/*";
chown ldap:ldap /var/lib/ldap/*
```

```
echo "ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif";
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
echo "ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif ";
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
echo "ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif";
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

```
echo "ldapadd -x -W -D "cn=admin,dc=miRed,dc=com" -f base.ldif"
ldapadd -x -W -D "cn=admin,dc=miRed,dc=com" -f base.ldif
```

Ahora copiamos el archivo de configuración de ejemplo que esta en la carpeta

/usr/share/openldap-servers/DB\_CONFIG.example hacia la carpeta /var/lib/ldap/DB\_CONFIG

```
cp /usr/share/openldap-servers/DB_CONFIG.example
/var/lib/ldap/DB_CONFIG
```

Le otorgamos permisos a ldap

```
chown ldap:ldap /var/lib/ldap/*
```

Importar esquemas básicos.

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

para hacernos este paso más cómodo se genero el script llamado

#### 4-firewall.sh

```
#!/bin/bash  
  
echo "firewall-cmd --permanent --add-service=ldap";  
echo "firewall-cmd --reload";  
  
firewall-cmd --permanent --add-service=ldap  
firewall-cmd --reload  
  
echo "local.* /var/log/ldap.log" >> /etc/rsyslog.conf
```

## Configurar el registro LDAP

Configure syslog para habilitar el registro LDAP.

```
echo "local4.* /var/log/ldap.log" >> /etc/rsyslog.conf  
systemctl restart rsyslog  
systemctl restart rsyslog
```

para esto se creo un script llamado

#### 5-ldap\_logging.sh

```
#!/bin/bash

echo "local4.* /var/log/ldap.log" >> /etc/rsyslog.conf
echo "systemctl restart rsyslog";
systemctl restart rsyslog
```

### Configuración del cliente LDAP para utilizar el servidor LDAP

Instale los paquetes de cliente LDAP necesarios en la máquina cliente.

```
yum install -y openldap-clients nss-pam-ldapd
```

ahora es necesario ingresar el siguiente comando  
donde dice ldeaserver+ ingresaremos pa ip de nuestro cliente

```
authconfig --enableldap --enableldapauth --ldapserver = 25.10.104.210  
--ldapbasedn = " dc = apex, dc = com " --enablemkhomedir --update
```

Paralograr reducir el proceso se creo el script llamado  
6-ldap\_configuracion\_cliente\_user.sh

```
#!/ bin / bash

yum install -y openldap-clients nss-pam-ldapd net-tools

read -p " Ingrese la dirección del servidor: " ip ;
authconfig --enableldap --enableldapauth --ldapserver = $ ip --ldapbasedn = " dc =  
apex, dc = com " --enablemkhomedir --update
echo " Configurado Autentifiacion ... "
systemctl reiniciar nslcd
systemctl enable nslcd --now
```

## Creación de usuario nuevo

utilizando el archivo de configuración para un usuario LDAP:

```
dn: uid=isma,ou=People,dc=apex,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: isma
uid: isma
userPassword: {SSHA}mNMvHZgkCWSPU0LQbKkawiYvfavQimAS
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1020
gidNumber: 100
homeDirectory: /home/isma
```

donde isma es un nuevo usuario y se guarda su password, se guarda un archivo con el nombre del cliente y la extensión lif.

Utilice el comando `ldapadd` con el archivo anterior para crear un nuevo usuario llamado "**isma**" en el directorio OpenLDAP.

```
ldapadd -x -W -D "cn = ldapadm, dc = miRed, dc = local" -f raj.ldif
Enter LDAP Password:
adding new entry "uid=raj,ou=People,dc=miRed,dc=local"
```

Dónde,

- -x especifican la contraseña para el nombre de usuario
- -S nombre de usuario para el que se cambia la contraseña
- -D Nombre distinguido para autenticarse en el servidor LDAP.

Nos podemos dar cuenta que es un proceso muy repetitivo y si tenemos más de un usuario se nos hara difícil la tarea de agregar uno por uno, así que se creo un script para correr cada vez que se necesite un nuevo cliente:

#### SCRIPT NUEVO CLIENTE

```
#!/bin/bash

read -p "Escriba el nombre del nuevo usuario: " usuario;
touch $usuario.ldif
echo "dn: uid=$usuario,ou=People,dc=miRed,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: $usuario
uid: $usuario" >> $usuario.ldif

MI_FICHERO=passwd.txt
pass=""

if [ -f $MI_FICHERO ]
then
    rm passwd.txt
    touch passwd.txt
else
    touch passwd.txt
fi

slappasswd >> passwd.txt

while IFS= read -r line
do
    pass=$line
```

```

done < passwd.txt

echo "userPassword: $pass
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash" >> $user.ldif

MI_FICHERO=count-user.txt
count=0

if [ -f $MI_FICHERO ]
then
    while IFS= read -r line
    do
        count=$((line + 1))
    done < count-user.txt
    echo $count | tee count-user.txt
else
    touch count-user.txt
    count=1020
    echo "1020" >> count-user.txt
fi

echo "uidNumber: $count
gidNumber: 100
homeDirectory: /home/$user" >> $usuario.ldif

read -p "Password der servidor LDAP: " paswd;
ldapadd -f $usuario.ldif -D cn=admin,dc=apex,dc=com -w $paswd

echo "se ha Agregado el usuario"

despues de correr el script Verifique las entradas LDAP.

```

```

ldapsearch -x cn = isma -b dc = miRed, dc = local

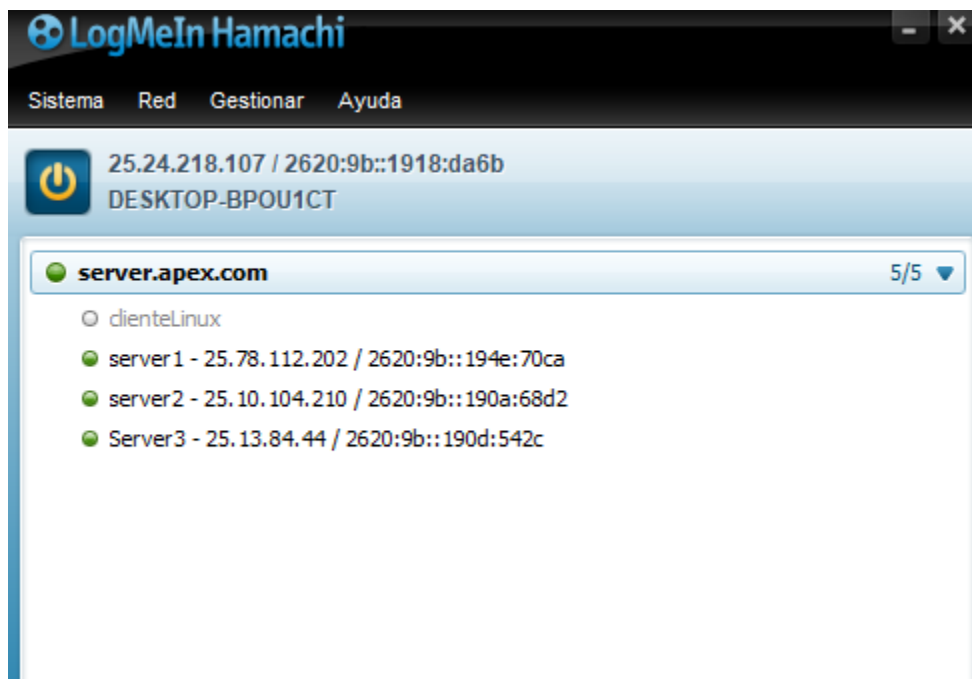
```

## Instalación Hamachi windows 10

1. Ubicarse en <https://secure.logmein.com/central/Central.aspx>
2. Click en Add Client / agregar cliente
3. Continue / continuar
4. descargar .exe de windows
5. Unirse a una red e ingresar id y contraseña (si lo requiere)







## Instalación ldap windows 10

1. Descargar version estable <http://pgina.org/download.html>
2. Dejar la configuración de la siguiente manera

En la primera pestaña seleccionamos los siguientes item

Current Plugins					
Plugin Name	Authentication	Authorization	Gateway	Notification	Description
LDAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Uses a LDAP server as a data source for authentication and/or group information.
Local Machine	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Manages local machine accounts for authenticated users, and authenticates users against the local machine.
MySQL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Uses a MySQL server as the account database.
MySQL Logger				<input type="checkbox"/>	Logs user logins to a MySQL database.

LDAP Plugin Settings

LDAP Server

LDAP Host(s) 25.78.112.202

LDAP Port 389 Timeout 10 ☐ Use SSL ☐ Validate Server Certificate

SSL Certificate File Browse...

Search DN cn=admin,dc=apex,dc=com

Search Password  ☐ Show Text

Group DN Pattern cn=%g,ou=People,dc=dom,dc=com Member Attribute memberUid

Authentication Authorization Gateway

☐ Allow Empty Passwords

User DN Pattern uid=%u,dc=example,dc=com

☒ Search for DN

Search Filter uid=%u

Search Context(s) dc=dom,dc=com

Cancel Save

Config

Authentication

Plugin

LDAP

Local Machine

↑

↓

Authorization

Plugin

LDAP

↑

↓

Gateway

Plugin

LDAP

Local Machine

↑

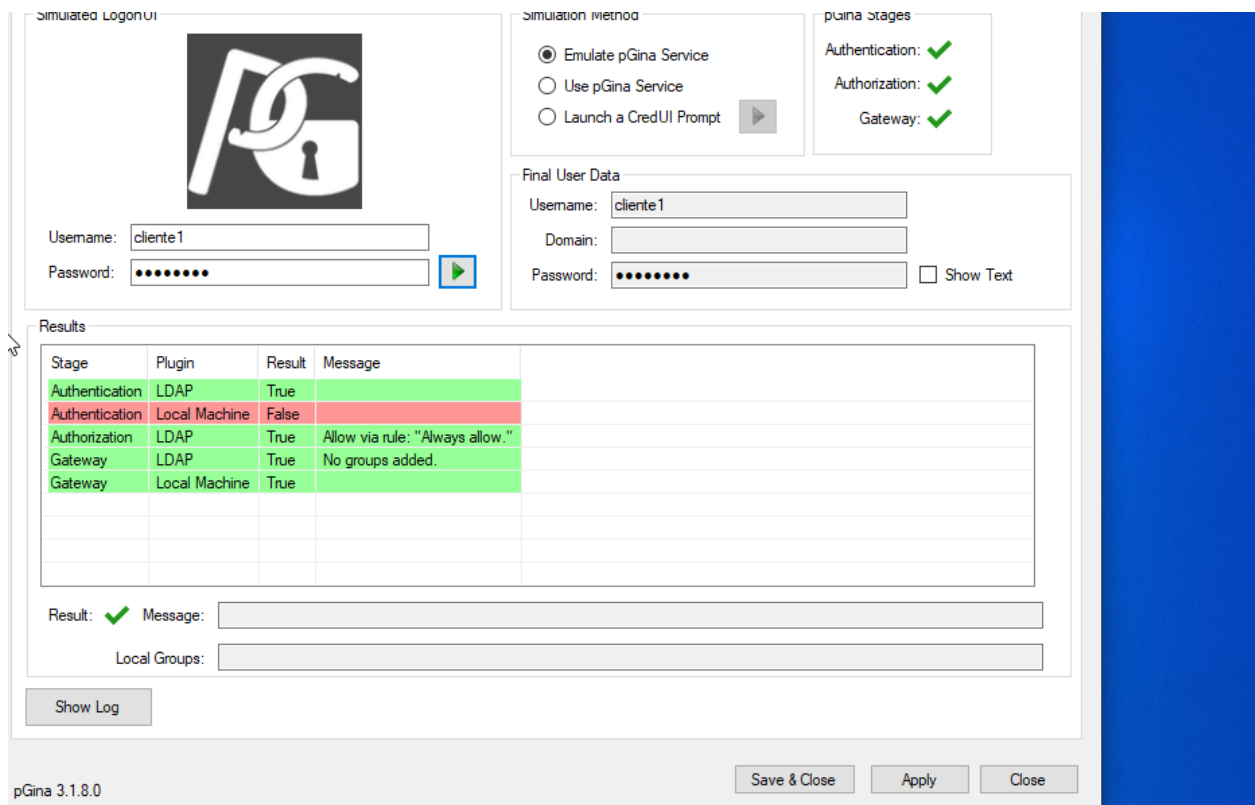
↓

Event Notification

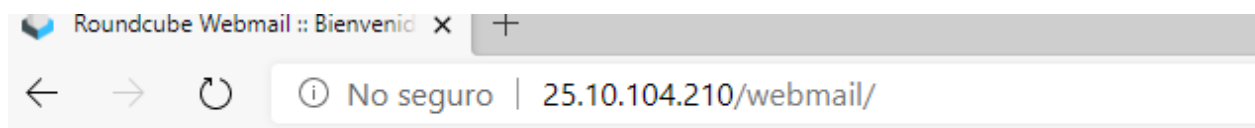
Plugin

↑

↓



La ventana de arriba es para testear si deja acceder a ldap, y la siguiente imagen es la manera de acceder a webmail con la ip del server2



## Configuración de Servidor WebMail

Un correo web es un cliente de correo electrónico, que provee una interfaz web que permite crear cuentas de e-mail que pueden ser revisadas a través de la web. Este servicio lo ofrecen muchos sitios web, en especial los portales y también los proveedores de acceso a internet (ISPs). Otras formas de acceder al correo electrónico pueden ser:


- Conectándose con un cliente de correo local a un servidor de correo remoto utilizando un protocolo *ad hoc* de transporte de correo, como IMAP o POP, descargar los correos y almacenarlos localmente.
- Utilizando un cliente de correo por consola (por ejemplo, Mutt).

### SCRIPT DE INSTALACION DE DEPENDENCIAS

```
#actualizar repositorios
yum update -y

#!/bin/bash
#instalar paquetes
yum install httpd httpd-tools mariadb-server mariadb php php-fpm php-mysqlnd
php-opcache php-gd php-xml php-mbstring php-json php-intl php-ldap

yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
yum update && yum install epel-release
yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm
yum install yum-utils
echo "Ingrese la versión de su php Ejemplo si es 7.4 o 7.4.1 ingrese 74\n"
php -v
echo "\n"
read version_php
yum-config-manager --enable remi-php$version_php
yum install php-opcache
```



```
systemctl start httpd
systemctl start mariadb
systemctl enable httpd
systemctl enable mariadb
firewall-cmd --permanent --add-service=http
firewall-cmd --reload
```

```
echo "Es necesario configurar la base de datos y configurar, para ello ejecute el
comando <mysql_secure_installation>\n"
echo "Finalizada la configuración iniciaremos sesión con <mysql -u root -p> y
ejecutaremos los siguientes comandos:\n"
```

#### **SCRIPT DE LA CREACION DE LA BASE DE DATOS**

```
create database roundcubedb;
create user roundcubeuser@localhost identified by 'roundcubepwd';
grant all on roundcubedb.* to roundcubeuser@localhost;
flush privileges;
exit;\n
```

#### **INSTALACION DE WEBMAIL Y CONFIGURACION config.inc.php**

```
#!/bin/bash
cd /var/www/html/
wget
https://github.com/roundcube/roundcubemail/releases/download/1.4.1/roundcubemail-1.4.1-complete.tar.gz
tar -xvf roundcubemail-1.4.1-complete.tar.gz
mv roundcubemail-1.4.1 webmail

cp config.inc.php /var/www/html/webmail/config/config.inic.php

chown -R apache:apache /var/www/
chmod -R 755 /var/www/html/webmail
systemctl restart httpd

echo "Se ejecutará un comando para iniciar el servidor, cada que sea necesario
iniciar el servidor deberá ejecutar el .sh IniciarServidor"
echo "Ejecutando IniciarServidor.sh"
sudo sh IniciarServidor.sh
```

```
systemctl restart httpd
systemctl restart dovecot
```

#### **ARCHIVO CONFIG.PHP**

<?php

```
/* Local configuration for Roundcube Webmail */

// -----
// SQL DATABASE
// -----
// Database connection string (DSN) for read+write operations
// Format (compatible with PEAR MDB2): db_provider://user:password@host/database
// Currently supported db_providers: mysql, pgsql, sqlite, mssql, sqlsrv, oracle
// For examples see
http://pear.php.net/manual/en/package.database.mdb2.intro-dsn.php
// Note: for SQLite use absolute path (Linux):
'sqlite:////full/path/to/sqlite.db?mode=0646'
// or (Windows): 'sqlite:///C:/full/path/to/sqlite.db'
// Note: Various drivers support various additional arguments for connection,
// for Mysql: key, cipher, cert, capath, ca, verify_server_cert,
// for Postgres: application_name, sslmode, sslcert, sslkey, sslrootcert,
// sslcrl, sslcompression, service.
// e.g. 'mysql://roundcube:@localhost/roundcubemail?verify_server_cert=false'
$config['db_dsnw'] = 'mysql://roundcubeuser:roundcubepwd@localhost/roundcubedb';

// The IMAP host chosen to perform the log-in.
// Leave blank to show a textbox at login, give a list of hosts
// to display a pulldown menu or set one host as string.
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// Supported replacement variables:
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %s - domain name after the '@' from e-mail address provided at login screen
// For example %n = mail.domain.tld, %t = domain.tld
$config['default_host'] = '25.8.167.33';

// SMTP port (default is 25; use 587 for STARTTLS or 465 for the
// deprecated SSL over SMTP (aka SMTPS))
$config['smtp_port'] = 25;

// SMTP username (if required) if you use %u as the username Roundcube
// will use the current username for login
$config['smtp_user'] = '';

// SMTP password (if required) if you use %p as the password Roundcube
// will use the current user's password for login
$config['smtp_pass'] = '';
```

```

// provide an URL where a user can get support for this Roundcube installation
// PLEASE DO NOT LINK TO THE ROUNDcube.NET WEBSITE HERE!
$config['support_url'] = '';

// this key is used to encrypt the users imap password which is stored
// in the session record (and the client cookie if remember password is enabled).
// please provide a string of exactly 24 chars.
// YOUR KEY MUST BE DIFFERENT THAN THE SAMPLE VALUE FOR SECURITY REASONS
$config['des_key'] = 'fpYV6KROV01z1G5JJnpUveCX';

// This domain will be used to form e-mail addresses of new users
// Specify an array with 'host' => 'domain' values to support multiple hosts
// Supported replacement variables:
// %h - user's IMAP hostname
// %n - http hostname ($_SERVER['SERVER_NAME'])
// %d - domain (http hostname without the first part)
// %z - IMAP domain (IMAP hostname without the first part)
// For example %n = mail.domain.tld, %t = domain.tld
$config['mail_domain'] = '%d';

// List of active plugins (in plugins/ directory)
$config['plugins'] = array('archive', 'zipdownload');

// $config['imap_auth_type'] = 'plain';
# $config['imap_auth_type'] = 'PLAIN';
$config['enable_installer'] = true;

```

#### SCRIPT DE CONFIGURACION LDAP-WEBMAIL

```

....
// LDAP, LDAP_SIMPLE and LDAP_EXOP Driver options
// -----
// LDAP server name to connect to.
// You can provide one or several hosts in an array in which case the hosts are
// tried from left to right.
// Example: array('ldap1.exemple.com', 'ldap2.exemple.com');
// Default: 'localhost'
$config['password_ldap_host'] = '25.69.102.31';

// LDAP server port to connect to
// Default: '389'
$config['password_ldap_port'] = '89';

```



```

// TLS is started after connecting
// Using TLS for password modification is recommended.
// Default: false
$config['password_ldap_starttls'] = false;

// LDAP version
// Default: '3'
$config['password_ldap_version'] = '3';

// LDAP base name (root directory)
// Example: 'dc=example,dc=com'
$config['password_ldap_basedn'] = 'dc=miRed,dc=com';

// LDAP connection method
// There are two connection methods for changing a user's LDAP password.
// 'user': use user credential (recommended, require password_confirm_current=true)
// 'admin': use admin credential (this mode require password_ldap_adminDN and
password_ldap_adminPW)
// Default: 'user'
$config['password_ldap_method'] = 'user';

// LDAP Admin DN
// Used only in admin connection mode
// Default: null
$config['password_ldap_adminDN'] = null;

// LDAP Admin Password
// Used only in admin connection mode
// Default: null
$config['password_ldap_adminPW'] = null;

// LDAP user DN mask
// The user's DN is mandatory and as we only have his login,
// we need to re-create his DN using a mask
// '%login' will be replaced by the current roundcube user's login
// '%name' will be replaced by the current roundcube user's name part
// '%domain' will be replaced by the current roundcube user's domain part
// '%dc' will be replaced by domain name hierarchal string e.g.
"dc=test,dc=domain,dc=com"
// Example: 'uid=%login,ou=people,dc=example,dc=com'
$config['password_ldap_userDN_mask'] = 'uid=%login,ou=People,dc=miRed,dc=com';

// LDAP search DN
// The DN roundcube should bind with to find out user's DN
// based on his login. Note that you should comment out the default
// password_ldap_userDN_mask setting for this to take effect.

```

```

// Use this if you cannot specify a general template for user DN with
// password_ldap_userDN_mask. You need to perform a search based on
// users login to find his DN instead. A common reason might be that
// your users are placed under different ou's like engineering or
// sales which cannot be derived from their login only.
$config['password_ldap_searchDN'] = 'cn=roundcube,ou=services,dc=miRed,dc=com';

// LDAP search password
// If password_ldap_searchDN is set, the password to use for
// binding to search for user's DN. Note that you should comment out the default
// password_ldap_userDN_mask setting for this to take effect.
// Warning: Be sure to set appropriate permissions on this file so this password
// is only accesible to roundcube and don't forget to restrict roundcube's access
// to
// your directory as much as possible using ACLs. Should this password be
// compromised
// you want to minimize the damage.
$config['password_ldap_searchPW'] = 'secret';

// LDAP search base
// If password_ldap_searchDN is set, the base to search in using the filter below.
// Note that you should comment out the default password_ldap_userDN_mask setting
// for this to take effect.
$config['password_ldap_search_base'] = 'ou=People,dc=miRed,dc=com';

// LDAP search filter
// If password_ldap_searchDN is set, the filter to use when
// searching for user's DN. Note that you should comment out the default
// password_ldap_userDN_mask setting for this to take effect.
// '%login' will be replaced by the current roundcube user's login
// '%name' will be replaced by the current roundcube user's name part
// '%domain' will be replaced by the current roundcube user's domain part
// '%dc' will be replaced by domain name hierarchal string e.g.
// "dc=test,dc=domain,dc=com"
// Example: '(uid=%login)'
// Example: '(&(objectClass=posixAccount)(uid=%login))'
$config['password_ldap_search_filter'] = '(uid=%login)';

// LDAP password hash type
// Standard LDAP encryption type which must be one of: crypt,
// ext_des, md5crypt, blowfish, md5, sha, smd5, ssha, ad, cram-md5 (dovecot style)
// or clear.
// Set to 'default' if you want to use method specified in password_algorithm
// option above.
// Multiple password Values can be generated by concatenating encodings with a +.
// E.g. 'cram-md5+crypt'

```

```

// Default: 'crypt'.
$config['password_ldap_encodage'] = 'crypt';

// LDAP password attribute
// Name of the ldap's attribute used for storing user password
// Default: 'userPassword'
$config['password_ldap_pwattr'] = 'userPassword';

// LDAP password force replace
// Force LDAP replace in cases where ACL allows only replace not read
// See
http://pear.php.net/package/Net\_LDAP2/docs/latest/Net\_LDAP2/Net\_LDAP2\_Entry.html#methodreplace
// Default: true
$config['password_ldap_force_replace'] = true;

// LDAP Password Last Change Date
// Some places use an attribute to store the date of the last password change
// The date is measured in "days since epoch" (an integer value)
// Whenever the password is changed, the attribute will be updated if set (e.g. shadowLastChange)
$config['password_ldap_lchattr'] = '';

// LDAP Samba password attribute, e.g. sambaNTPassword
// Name of the LDAP's Samba attribute used for storing user password
$config['password_ldap_samba_pwattr'] = '';

// LDAP Samba Password Last Change Date attribute, e.g. sambaPwdLastSet
// Some places use an attribute to store the date of the last password change
// The date is measured in "seconds since epoch" (an integer value)
// Whenever the password is changed, the attribute will be updated if set
$config['password_ldap_samba_lchattr'] = '';

// LDAP PPolicy Driver options
// -----

// LDAP Change password command - filename of the perl script
// Example: 'change_ldap_pass.pl'
$config['password_ldap_ppolicy_cmd'] = 'change_ldap_pass.pl';

// LDAP URI
// Example: 'ldap://ldap.example.com/ ldaps://ldap2.example.com:636/'
$config['password_ldap_ppolicy_uri'] = 'ldap://25.69.102.31/';

// LDAP base name (root directory)
// Exemple: 'dc=exemple,dc=com'

```

```

$config['password_ldap_ppolicy_basedn'] = 'dc=miRed,dc=com';

$config['password_ldap_ppolicy_searchDN'] = 'cn=someuser,dc=miRed,dc=com';

$config['password_ldap_ppolicy_searchPW'] = 'secret';

// LDAP search filter
// Example: '(uid=%login)'
// Example: '(&(objectClass=posixAccount)(uid=%login))'
$config['password_ldap_ppolicy_search_filter'] = '(uid=%login)';

// CA Certificate file if in URI is LDAPS connection
$config['password_ldap_ppolicy_cafile'] = '/etc/ssl/cacert.crt';

```

#### SCRIPT DE INICIALIZACION:


```

#!/bin/bash
sudo yum install dovecot -y
sudo systemctl enable dovecot
sudo systemctl start dovecot
setenforce 0
systemctl restart httpd
systemctl restart dovecot
sudo service dovecot restart

```

### Procedimiento:

1. Para la instalación y levantamiento de webmail primero se ejecuta el primer script que de descarga de dependencias.
2. Ubicarse en /var/www/html
3. Ejecutar el segundo script de roundcube
4. Creación del script de la base de datos si se desea se puede alterar solo que se debe modificar la conexión en el archivo config.inc.php

- 
5. Verificar que el archivo de configuración config.inc.php se copió correctamente a  
`/var/www/html/webmail/config/`
  6. Conectarse a la red hamachi y instalar LDAP client
  7. Configurar los parámetros de autenticación en el archivo  
`/var/www/html/webmail/plugins/password/config-inc.php.dist`
  8. Ejecutar el último script de inicialización
  9. Cada que se ejecute el servidor se aconseja reiniciar los servicios de apache y colocar  
`setenforce 0`
  10. El archivo config.inc.php vendría funcionando para cualquier instalación solo se debe tener cuidado con la conexión a la base de datos ya que si se desea cambiar las credenciales en este archivo se hace lo mismo
  11. EL archivo config-inc.php.dist si solo es un esquema, ya que depende del dominio que se tenga y la ip, estos dos parámetros son los más importantes los otros si puede dejarlos así.

## Instalación de ldap-cliente general :

Para instalación basta con ejecutar el siguiente script, aclarando que la ip es la virtual que brinda hamachi.

```
yum install -y openldap-clients nss-pam-ldapd net-tools
```

`read -p "Ingrese la direccion del servidor: " ip;`

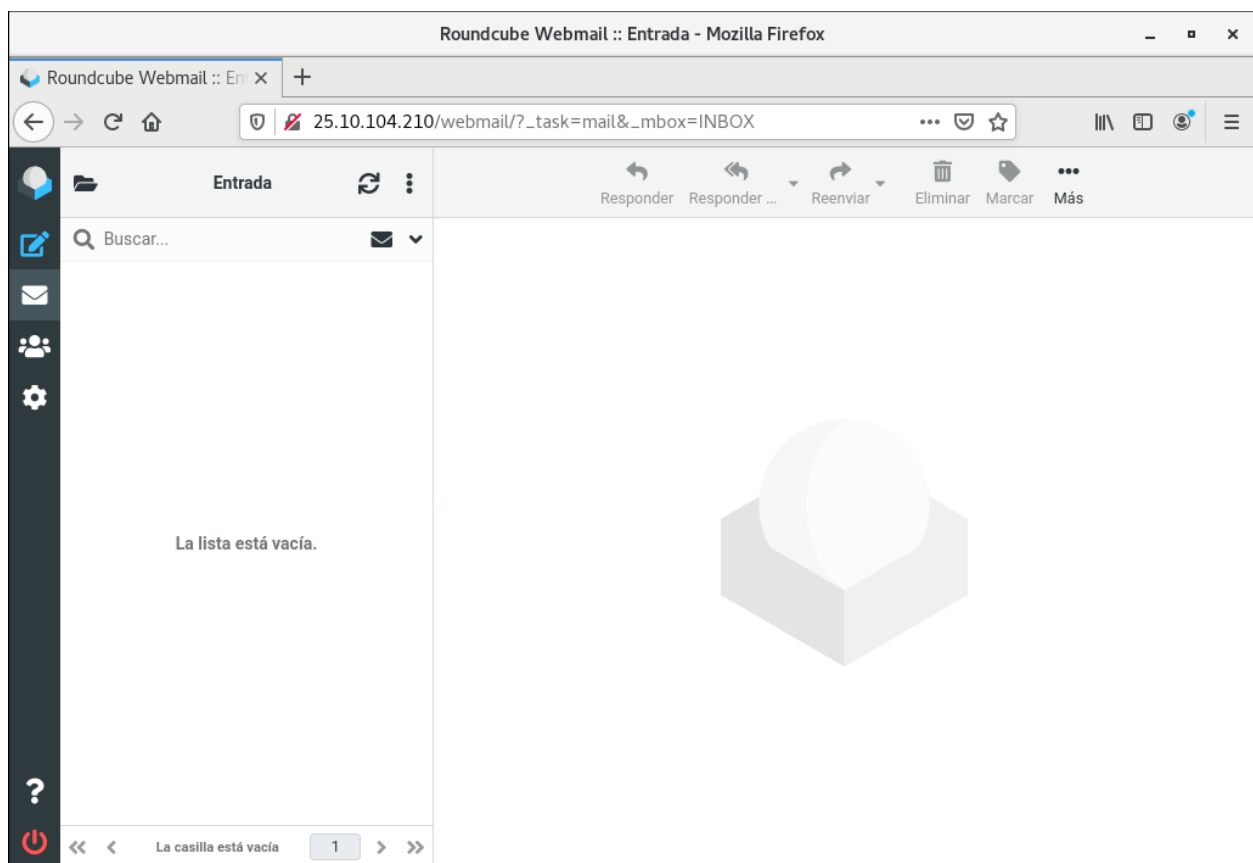
`authconfig --enableldap --enableldapauth --ldapserver=$ip --ldapbasedn="dc=apex,dc=com"`

`--enablemkhomedir --update`

`systemctl restart nsld`

`systemctl enable nsld --now`

VISTA DEL CLIENTE:



# Configuración de Servidor Backups

## Instalación de Bacula y MySQL

Para poder configurar el server de backup es necesario realizar la instalación de Bacula mediante los siguientes comandos

```
[server@serverbacula] sudo yum install -y bacula-director bacula-storage bacula-console bacula-client mariadb-server
```

Después se prosigue la inicialización de MySQL con el siguiente comando

```
[server@serverbacula] sudo systemctl start mariadb
```

Ahora que MySQL (MariaDB) esta corriendo, se crearán la base de datos de Bacula incluyendo el usuario y las tablas mediante los siguientes comandos

```
[server@serverbacula] $ /usr/libexec/bacula/grant_mysql_privileges  
[server@serverbacula] $ /usr/libexec/bacula/create_mysql_database -u root  
[server@serverbacula] $ /usr/libexec/bacula/make_mysql_tables -u bacula
```

Se corre el script de seguridad de MySQL

```
[server@serverbacula] $ sudo mysql_secure_installation
```

Después ingresamos a la consola de MySQL como usuario root

```
[server@serverbacula] $ mysql -u root -p
```

Y ahora actualizamos la contraseña y salimos de la consola.

```
MariaDB[(none)] > UPDATE mysql.user SET Password=PASSWORD('bacula_db_password') WHERE User='bacula';  
MariaDB[(none)] > FLUSH PRIVILEGES;  
MariaDB[(none)] > exit;
```

Permitimos que MariaDB inicie cuando se encienda la computadora.

```
[server@serverbacula] $ sudo systemctl enable mariadb
```

## Configuración de la utilización de Mysql por parte de Bacula

De forma predeterminada, Bacula está configurado para usar la biblioteca PostgreSQL. Debido a que estamos usando MySQL, necesitamos configurarlo para usar la biblioteca MySQL en su lugar.

Se ejecuta este comando:

```
[server@serverbacula] $ sudo alternatives --config libbaccats.so
```

Se mostrará el siguiente mensaje

```
There are 3 programs which provide 'libbaccats.so'.

  Selection    Command
-----
    1          /usr/lib64/libbaccats-mysql.so
    2          /usr/lib64/libbaccats-sqlite3.so
*+ 3          /usr/lib64/libbaccats-postgresql.so

Enter to keep the current selection[+], or type selection number: 1
```

y se deberá ingresar 1.

## Configuración del Server de Bacula

Bacula tiene varios componentes que deben configurarse de forma independiente para que funcionen correctamente. Todos los archivos de configuración se pueden encontrar en el `/etc/bacula` directorio.

Se empezará por el director de Bacula.



Abra el archivo de configuración de Bacula Director en el editor de texto de su preferencia. Se utilizará vi:

```
[server@serverbacula] $ sudo vi /etc/bacula/bacula-dir.conf
```

### Configuración del recurso del director

En el archivo bacula-dir.conf buscamos el recurso Director y configuramos para que escuche en 127.0.0.1 (localhost), agregando la `DirAddress` de la siguiente manera.

```
Director {                                # define myself
    Name = bacula-dir
    DIRport = 9101                        # where we listen for UA connections
    QueryFile = "/etc/bacula/query.sql"
    WorkingDirectory = "/var/spool/bacula"
    PidDirectory = "/var/run"
    Maximum Concurrent Jobs = 1
    Password = "@@DIR_PASSWORD@@"        # Console password
    Messages = Daemon
    DirAddress = 127.0.0.1
}
```

### Configuración de los trabajos locales

Un trabajo de Bacula se utiliza para realizar acciones de copia de seguridad y restauración. Los recursos del trabajo definen los detalles de lo que hará un trabajo en particular, incluido el nombre del cliente, el conjunto de archivos para respaldar o restaurar, entre otras cosas.

```
Job {
    Name = "BackupLocalFiles"
    JobDefs = "DefaultJob"
}
```

```
Job {
  Name = "RestoreLocalFiles"
  Type = Restore
  Client=BackupServer-fd
  FileSet="Full Set"
  Storage = File
  Pool = Default
  Messages = Standard
  Where = /bacula/restore
}
```

### Configurar el conjunto de archivos

Un conjunto de archivos de Bacula define un conjunto de archivos o directorios para incluir o excluir archivos de una selección de respaldo y son utilizados por trabajos.

```
FileSet {
  Name = "Full Set"
  Include {
    Options {
      signature = MD5
      compression = GZIP
    } File = /
  }
  Exclude {
    File = /var/lib/bacula
    File = /proc
    File = /tmp
    File = /.journal
    File = /.fsck
    File = /bacula }
}
```

## Configurar la conexión del demonio de almacenamiento

En el archivo de configuración de Bacula Director, el recurso de almacenamiento define el demonio de almacenamiento al que debe conectarse el director.

```
Storage {
  Name = File
# Do not use "localhost" here
  Address = backup_server_private_FQDN      # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "@@SD_PASSWORD@@"
  Device = FileStorage
  Media Type = File }
```

## Configurar conexión de catálogo

En el archivo de configuración de Bacula Director, el recurso Catálogo define dónde la Base de datos que el Director debe usar y conectarse.

```
# Generic catalog service
Catalog {
  Name = MyCatalog
# Uncomment the following line if you want the dbi driver
# dbdriver = "dbi:postgresql"; dbaddress = 127.0.0.1; dbport =
  dbname = "bacula"; dbuser = "bacula"; dbpassword = "bacula_db_password"
}
```

## Configurar Pool

Un recurso Pool define el conjunto de almacenamiento utilizado por Bacula para escribir copias de seguridad.

```
# File Pool definition
Pool {
    Name = File
    Pool Type = Backup
    Label Format = Local-
    Recycle = yes                # Bacula can automatically recycle Volumes
    AutoPrune = yes              # Prune expired volumes
    Volume Retention = 365 days  # one year
    Maximum Volume Bytes = 50G   # Limit Volume size to something reasonable
    Maximum Volumes = 100        # Limit number of Volumes in Pool
}
```

### Comprobación de la configuración del director

```
[server@serverbacula] sudo bacula-dir -tc /etc/bacula/bacula-dir.conf
```

Si no hay mensajes de error, el archivo bacula-dir.conf no tiene errores de sintaxis.

### Configurar recurso de almacenamiento

Se busca el recurso de almacenamiento. Esto define dónde el proceso SD escuchará las conexiones. Se agrega el SDAddress parámetro y se asigna al FQDN privado (o dirección IP privada) de su servidor de respaldo:

```
Storage {                                # definition of myself
    Name = BackupServer-sd
    SDPort = 9103                        # Director's port
    WorkingDirectory = "/var/lib/bacula"
    Pid Directory = "/var/run/bacula"
    Maximum Concurrent Jobs = 20
    SDAddress = backup_server_private_FQDN
}
```

## Configurar dispositivo de almacenamiento

Se busca el recurso del dispositivo llamado "FileStorage" y se actualiza el valor de Archive Device para que coincida con su directorio de copias de seguridad:

```
Device {
    Name = FileStorage
    Media Type = File
    Archive Device = /bacula/backup
    LabelMedia = yes;                # lets Bacula label unlabeled media
    Random Access = Yes;
    AutomaticMount = yes;            # when device opened, read it
    RemovableMedia = no;
    AlwaysOpen = no;
}
```

## Verificar la configuración del daemon de almacenamiento

Verifiquemos que no haya errores de sintaxis en su archivo de configuración de Storage

Daemon:

```
[server@serverbacula] sudo bacula-sd -tc /etc/bacula/bacula-sd.conf
```

Si no hay mensajes de error, el archivo bacula-sd.conf no tiene errores de sintaxis.

## Configuración del Cliente

### Organizar la configuración del server bacula

Se organizará la información en archivos separados para agregar nuevas configuraciones como trabajos, conjuntos de archivos y grupos.

Se empezará con la creación de un directorio

```
[server@serverbacula] sudo mkdir /etc/bacula/conf.d
```

Se agregara la siguiente línea al final del archivo bacula-dir.conf

```
[server@serverbacula] sudo vi /etc/bacula/bacula-dir.conf
@|"find /etc/bacula/conf.d -name '*.conf' -type f -exec echo @{} \;"
```

### Agregar grupo de archivos remotos

Se agrega un Pool adicional a la configuración de Bacula Director, que se usará para configurar los trabajos de respaldo remoto. Se abre el archivo

```
[server@serverbacula] sudo vi /etc/bacula/conf.d/pools.conf
```

Se coloca lo siguiente

```
Pool {
  Name = RemoteFile
  Pool Type = Backup
  Label Format = Remote-
  Recycle = yes                # Bacula can automatically recycle Volumes
  AutoPrune = yes              # Prune expired volumes
  Volume Retention = 365 days  # one year
  Maximum Volume Bytes = 50G   # Limit Volume size to something reasonable
  Maximum Volumes = 100        # Limit number of Volumes in Pool
}
```

Se verifica que no haya ningún error

```
[server@serverbacula] sudo bacula-dir -tc /etc/bacula/bacula-dir.conf
```

### Instalacion y configuracion del cliente Bacula

Se instala el cliente Bacula con el siguiente comando

```
[server@serverbacula] sudo yum install bacula-client
```

En el archivo bacula-fd.conf se agrega lo siguiente

```
Director {
    Name = BackupServer-dir
    Password = "password"
}
###
FileDaemon {                                # this is me
    Name = ClientHost-fd
    FDAddress = client_private_ip
    FDport = 9102                            # where we listen for the director
    WorkingDirectory = /var/spool/bacula
    Pid Directory = /var/run
    Maximum Concurrent Jobs = 20
}
###
Messages {
    Name = Standard
    director = BackupServer-dir = all, !skipped, !restored
}
```

```
[server@serverbacula] sudo bacula-fd -tc /etc/bacula/bacula-fd.conf
```

Si el comando no devuelve ningún resultado el archivo de configuración tiene una sintaxis válida. Reinicie el demonio de archivos para usar la nueva configuración:

```
[server@serverbacula] sudo systemctl restart bacula-fd
```

Luego se ejecuta el siguiente comando para iniciar Bacula File Daemon automáticamente al arrancar:

```
[server@serverbacula] sudo systemctl enable bacula-fd
```

Se configura un directorio en el que Bacula Server pueda restaurar archivos.

Posteriormente se crea la estructura de archivos y bloqueando los permisos y la propiedad por seguridad con los siguientes comandos:

```
[server@serverbacula] sudo mkdir -p /bacula/restore  
[server@serverbacula] sudo chown -R bacula:bacula /bacula  
[server@serverbacula] sudo chmod -R 700 /bacula
```

Ahora se procede a configurar el Backup Server para poder conectarnos al Bacula Client.

#### Agregando conjunto de archivos (servidor)

En el servidor bacula, abrimos un archivo llamado filesets.conf, en el directorio de configuración de Bacula Director que creamos anteriormente:

```
[server@serverbacula] sudo vi /etc/bacula/conf.d/filesets.conf
```

Se crea un recurso FileSet para cada conjunto particular de archivos que vamos a utilizar en los trabajos de respaldo. Ejemplo, un FileSet que solo incluye los directorios home y etc:

```
FileSet {  
  Name = "Home and Etc"  
  Include {  
    Options {  
      signature = MD5  
      compression = GZIP  
    }  
    File = /home  
    File = /etc  
  }  
}
```



```
Exclude {  
    File = /home/bacula/not_important  
}  
}
```

Podemos crear varios FileSets de ser necesarios. Saliendo y guardando cuando se haya terminado.

Ahora podemos crear un trabajo de respaldo usando nuestro nuevo FileSet.

### Agregando cliente y trabajo de respaldo al servidor Bacula

Abrimos el conf.d/clients.conf archivo:

```
[server@serverbacula] sudo vi /etc/bacula/conf.d/clients.conf
```

### Agregando recurso de cliente

Utilizando la información para conectarse al Host del Cliente. Esto incluye el nombre, la dirección y la contraseña del demonio de archivos del cliente.

Se ingresa esta definición de recurso de cliente en el archivo:

```
Client {  
    Name = ClientHost-fd  
    Address = client_private_FQDN  
    FDPort = 9102  
    Catalog = MyCatalog  
    Password = "password"          # password for Remote FileDaemon  
    File Retention = 30 days        # 30 days  
    Job Retention = 6 months        # six months  
    AutoPrune = yes                 # Prune expired Jobs/Files  
}
```

### Creando un trabajo de respaldo:

Se pega este trabajo de respaldo en el archivo, sustituyendo el nombre de host del Cliente por el texto resaltado:

```
Job {  
  Name = "BackupClientHost"  
  JobDefs = "DefaultJob"  
  Client = ClientHost-fd  
  Pool = RemoteFile  
  FileSet="Home and Etc"  
}
```

Al finalizar solo guardamos los cambios realizados.

### Verificar la configuración del director

Se verifica que no haya errores de sintaxis en el archivo de configuración de Director:

```
[server@serverbacula] sudo bacula-dir /etc/bacula/bacula-dir.conf
```

Si vuelve al indicador de shell, no hay errores de sintaxis en los archivos de configuración de Bacula Director.

### Configuraciones Especiales

Para que el backup y el restore funcionen correctamente es necesario utilizar los siguientes comandos para liberal el firewall

```
[server@serverbacula] firewall-cmd --zone=public --add-port=9102/tcp --permanent  
[server@serverbacula] firewall-cmd --zone=public --add-port=9103/tcp --permanent  
[server@serverbacula] firewall-cmd --reload
```

## Reiniciando Bacula Director

Para poner en vigencia los cambios de configuración que se realizaron, se debe de

```
[server@serverbacula] sudo systemctl restart bacula-dir
```

## Iniciar componentes de Bacula

Inicie Bacula Director, Storage Daemon y File Daemon local con estos comandos:

```
[server@serverbacula] sudo systemctl start bacula-dir  
[server@serverbacula] sudo systemctl start bacula-sd  
[server@serverbacula] sudo systemctl start bacula-fd
```

Si todos comenzaron correctamente, ejecute estos comandos para que se inicien automáticamente al arrancar:

```
[server@serverbacula] sudo systemctl enable bacula-dir  
[server@serverbacula] sudo systemctl enable bacula-sd  
[server@serverbacula] sudo systemctl enable bacula-fd
```



## Bibliografía

Anicas, M. (2020a, noviembre 1). *How To Back Up a CentOS 7 Server with Bacula*.

DigitalOcean.

<https://www.digitalocean.com/community/tutorials/how-to-back-up-a-centos-7-server-with-bacula>

Anicas, M. (2020b, diciembre 23). *How To Install Bacula Server on CentOS 7*.

DigitalOcean.

<https://www.digitalocean.com/community/tutorials/how-to-install-bacula-server-on-centos-7>


Atmaca, G. (s. f.). *Re: [Bacula-users] problem ..is waiting on Storage «FileI»*. . .

Bacula-Users.

<https://www.mail-archive.com/bacula-users@lists.sourceforge.net/msg66076.html>

B., G. (2020, 27 noviembre). *Cómo cambiar permisos y propietarios en Linux través de la línea de comandos*. Tutoriales Hostinger.

<https://www.hostinger.es/tutoriales/cambiar-permisos-y-propietarios-linux-linea-de-comandos/>

  
*Bacula - Users - waiting for client to connect to storage file.* (s. f.). Bacula Users.

<http://bacula.10910.n7.nabble.com/waiting-for-client-to-connect-to-storage-file-t82426.html>

Castillo, J. A. (2019, 5 enero). *LDAP: Qué es y para qué se utiliza este protocolo.*

Profesional Review. <https://www.profesionalreview.com/2019/01/05/ldap/>

*CentOS 7 : OpenLDAP : Server World.* (s. f.). Server World.

[https://www.server-world.info/en/note?os=CentOS\\_7&p=openldap](https://www.server-world.info/en/note?os=CentOS_7&p=openldap)

colaboradores de Wikipedia. (2020, 22 septiembre). *Webmail.* Wikipedia, la enciclopedia

libre. <https://es.wikipedia.org/wiki/Webmail>

Community, B. (2015, 4 marzo). *The best free enterprise open source backup software*

*for Linux.* Bacula. <https://www.bacula.org/>

*¿Qué es KVM?* (s. f.). Red Hat.

<https://www.redhat.com/es/topics/virtualization/what-is-KVM>

R. (2018, 3 abril). *Step by Step OpenLDAP Server Configuration on CentOS 7 / RHEL 7.*

ITzGeek.

<https://www.itzgeek.com/how-tos/linux/centos-how-tos/step-step-openldap-server-configuration-centos-7-rhel-7.html/2?fbclid=IwAR13ReTEx-djp0i362NCMF4jl4deL-UzWyLP0a3OEDcTl10zlgHkKWDYV70>



R. (2020, 10 noviembre). *Cómo instalar KVM en Ubuntu 20.04*. Geeks en Cuarentena.

<https://geeksencuarentena.com/linux/como-instalar-kvm-en-ubuntu-20-04/>

*Webmail mit Roundcube unter CentOS 7.x [Linux - Wissensdatenbank]*. (s. f.).

Wissensdatenbank.

[https://dokuwiki.nausch.org/doku.php/centos:mail\\_c7:roundcube\\_1](https://dokuwiki.nausch.org/doku.php/centos:mail_c7:roundcube_1)