# Implementación de Servicios de Infraestructura de TI bajo el sistema Operativo GNU/Linux Zentyal

Juan Camilo Medina Morales, David Espitia Beltrán, Arturo Enrique Castro Díaz, Albert Hernández Severino, Franklin Campo
*Escuela de Ciencias Básicas y Tecnología, Universidad Nacional Abierta y a Distancia UNAD*
*Medellín, Colombia*
jmedinamo@unadvirtual.edu.co
despitiabe@unadvirtual.edu.co
aecastrod@unadvirtual.edu.co
ashernandez@unadvirtual.edu.co
facampom@unadvirtual.edu.co

***Resumen*** **-** Se pretende ilustrar los pasos a seguir para implementar un servidor Zentyal basado en Linux Server, sobre el cual se van a configurar servicios de TI tales como DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server y Print Server y VPN.

***Palabras clave*** *– Zentyal, DHCP, Firewall, Dominio, VPN, Server, Proxy.*

## I. INTRODUCCIÓN

Toda solución tecnológica debe ir acompañada de una debida documentación que permita apropiarse de los conceptos implementados y generar nuevos conocimientos a partir de los adquiridos. Es por esto que este tutorial se enfoca en cómo instalar y configurar un servidor Linux (Zentyal) para dar soporte tecnológico a una empresa que requiera de configuraciones de TI.

## II. INSTALACIÓN Y CONFIGURACIÓN DE ZENTYAL

Para dar inicio con esta proceso de instalación, lo primero que se debe hacer es descargar la iso de zentyal desde el link http://www.zentyal.com/es/zentyal-server/ y seguir los siguientes pasos:

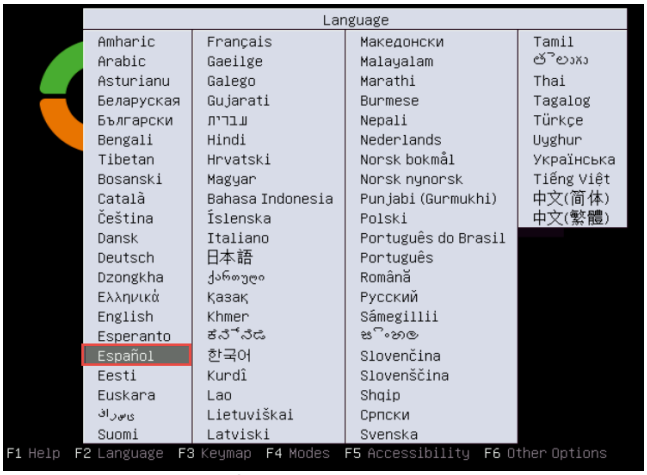


Fig. 1 Selección de idioma del sistema operativo


Fig. 2 Selección del modo de instalación

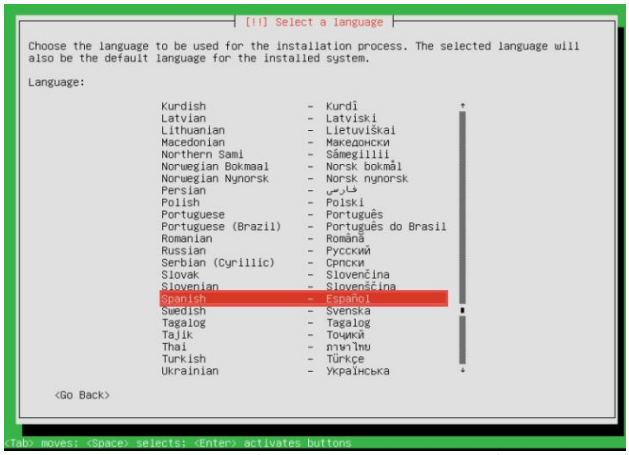


Fig. 3 Selección del idioma de la instalación


Fig. 4 Selección de la ubicación


Fig. 5 Configuración de teclado


Fig. 6 Nombre del servidor

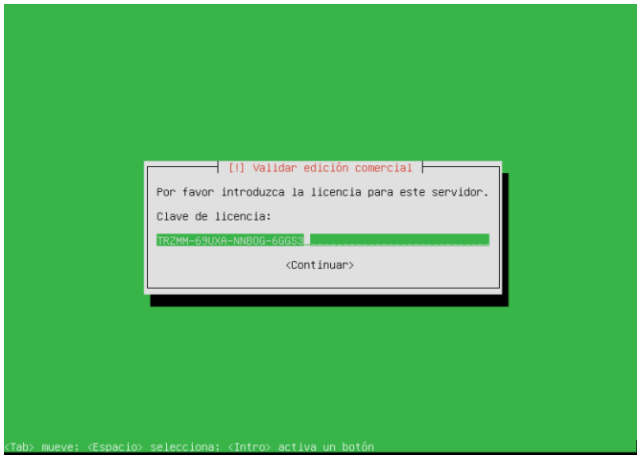


Fig. 7 Licencia del servidor


Fig. 8 Nombre de usuario

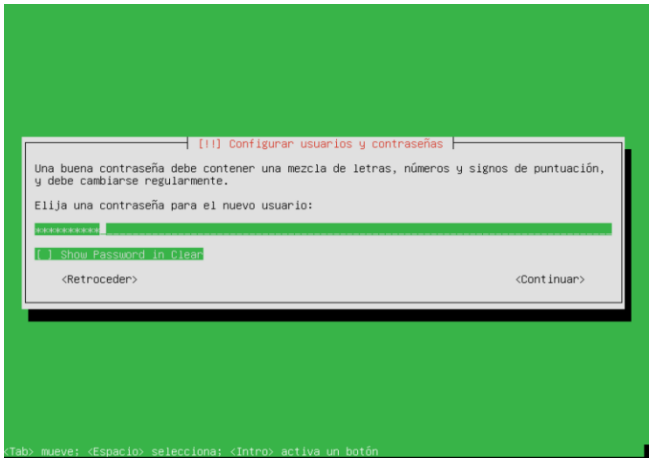


Fig. 9 Contraseña del usuario

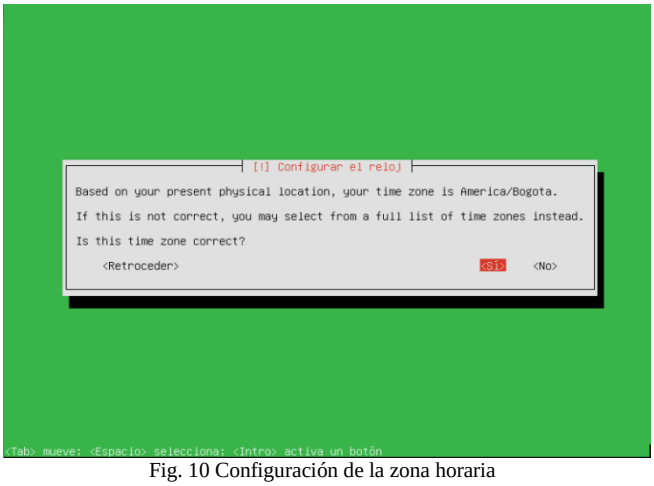


Fig. 10 Configuración de la zona horaria

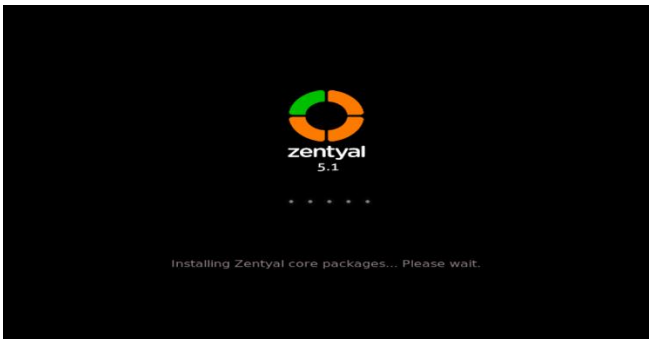


Fig. 11 Inicio de Zentyal

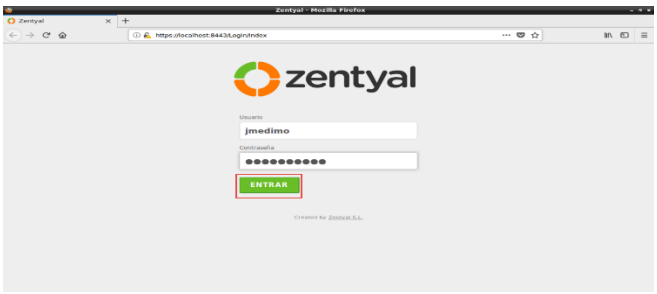


Fig. 12 Ingreso a la administración modo gráfico


Fig. 13 Pantalla de bienvenida para dar inicio a la configuración inicial

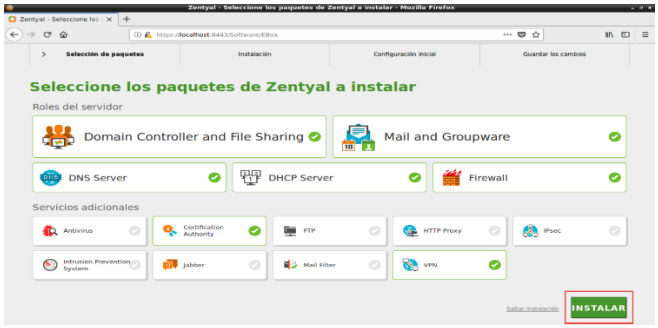


Fig. 14 Selección de paquetes y servicios a instalar

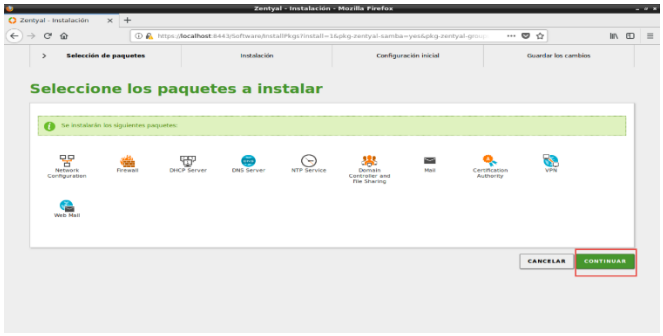


Fig. 15 Resumen de los paquetes a instalar

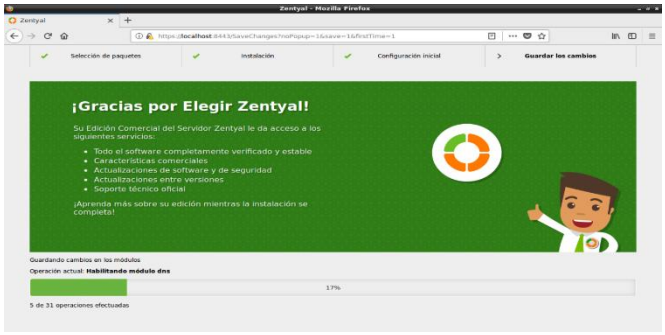


Fig. 16 Progreso de la instalación

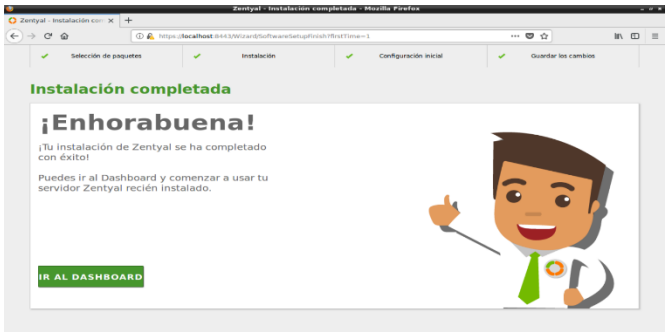


Fig. 17 Fin de la instalación y configuración de paquetes

## III. TEMÁTICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO

Zentyal no es más que un Ubuntu con multitud de paquetes adaptados en conjunto, Zentyal emplea una GUI web para su gestión y administración.

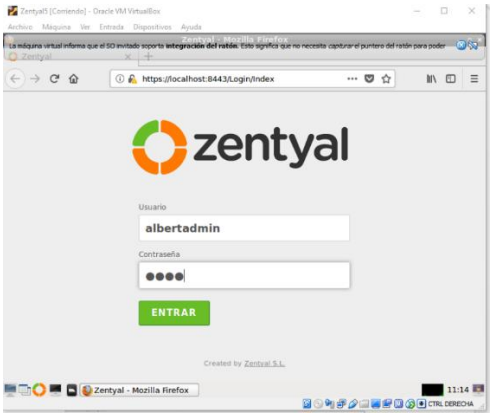


Fig. 18

Después de ingresar con el usuario y la clave antes suministrados para su instalación, veremos un asistente que nos agilizara el proceso de configuración.

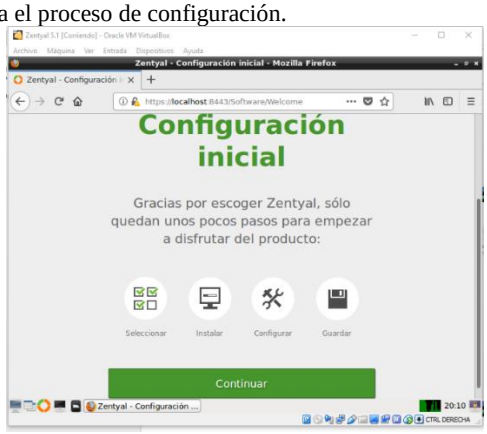


Fig. 19

Instalación del paquete controlador de domino, este paquete a su vez instala otras dependencias como el servidor NTP, DNS, fundamentales para su operación.

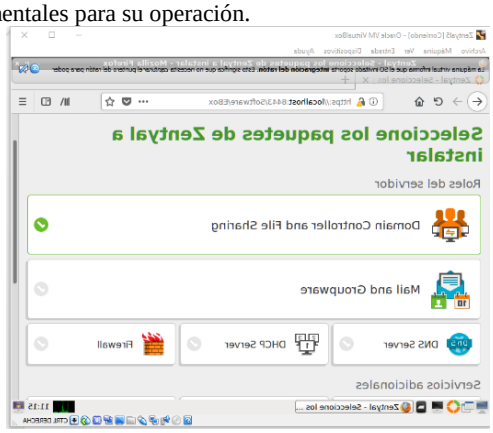

Fig. 20

Después de seleccionarlos se instalarán los paquetes.

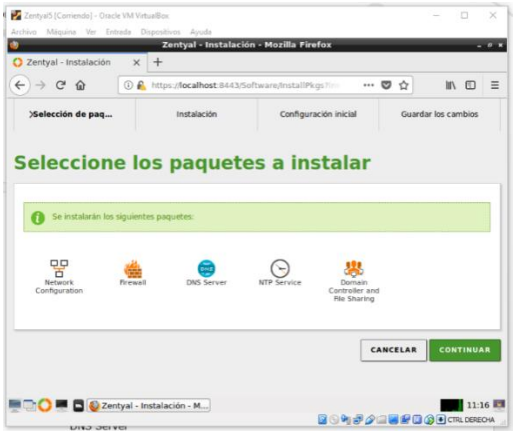


Fig. 21

El controlador de dominio instalara otras dependencias como el networkconfigurator, firewall, DNS server y el servidor NTP.

El proceso de instalacion es demorado y requiere de una conexión a intenet para descargar los paquetes requeridos.


Fig. 22

Configuración de la red.


Fig. 23

Ahora desde la maquina Ubuntu nos conectamos a la máquina de Zentyal utilizando el protocolo Http, webadmin:

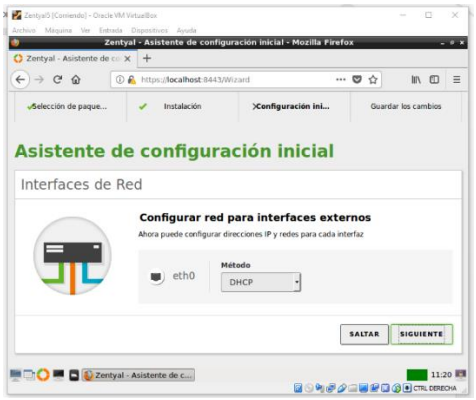


Fig. 24

Configuración del dominio local.


Fig. 25

Este dominio se cambia por *dcunad.local* ya que se generó conflicto, en usar el nombre de la maquina igual al del dominio.

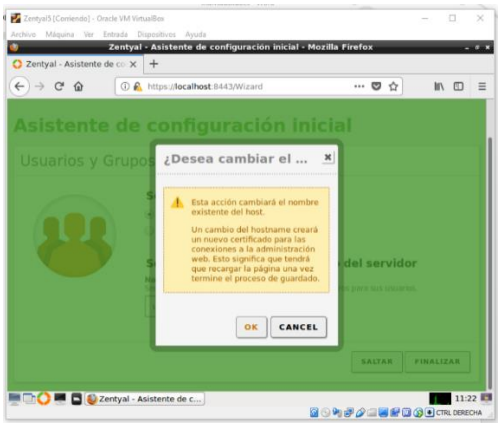


Fig. 26

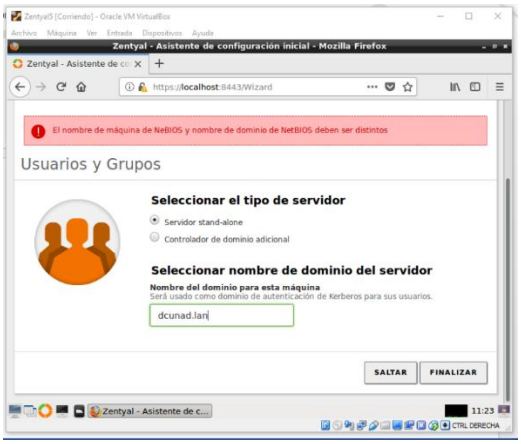


Fig. 27

En el apartado de sistema y general.

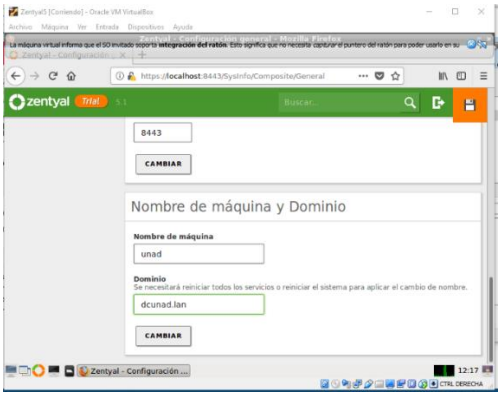


Fig. 28

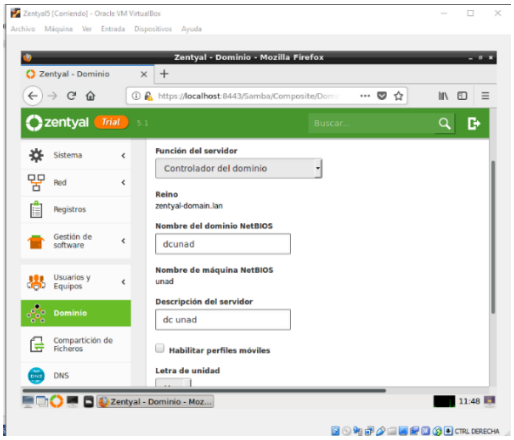


Fig. 29

Se selecciona una contraseña al usuario administrador del dominio.

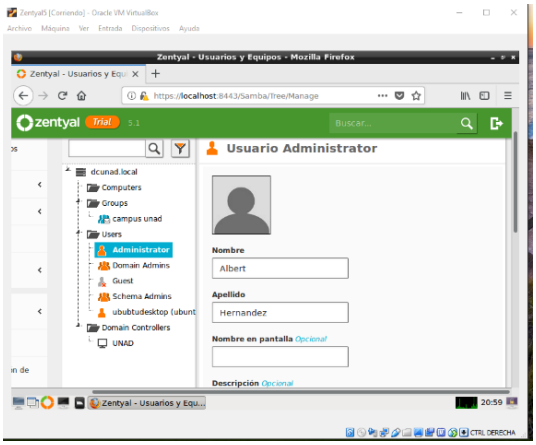


Fig. 30

Ahora procedemos a crear un usuario el Ubuntu desktop y otro para Windows XP, que se unirán después al dominio. Este usuario estará almacenado en el controlador de dominio.

Primero crearemos un grupo de usuarios.

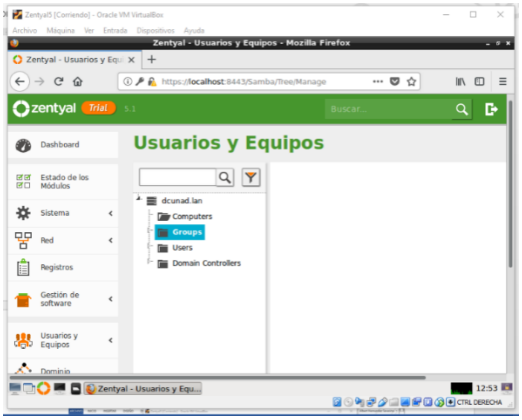


Fig. 31

Le daremos un nombre para esta práctica.

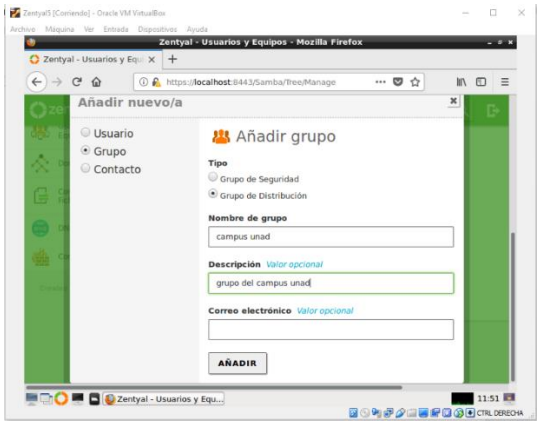


Fig. 32

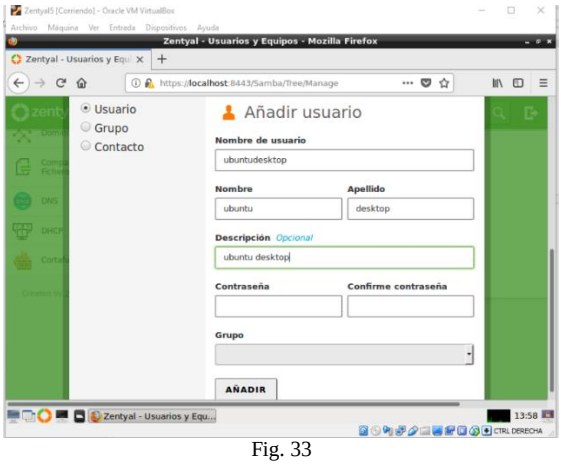


Fig. 33

Paso siguiente se agrega al grupo.

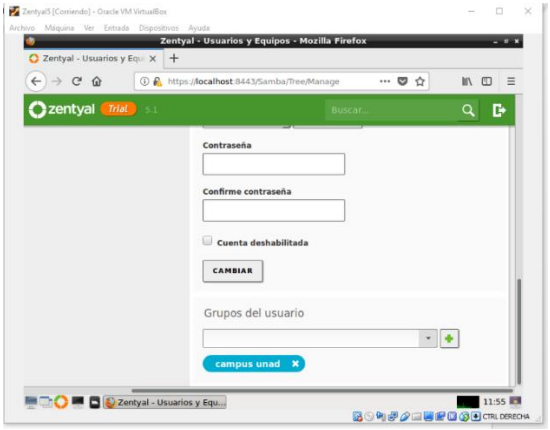


Fig. 34

Habilitando el servicio DCHP.

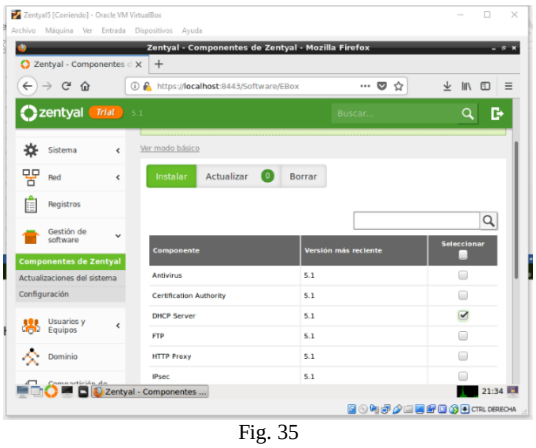


Fig. 35

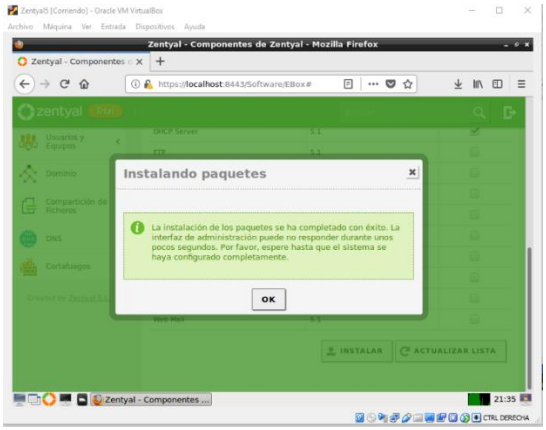


Fig. 36

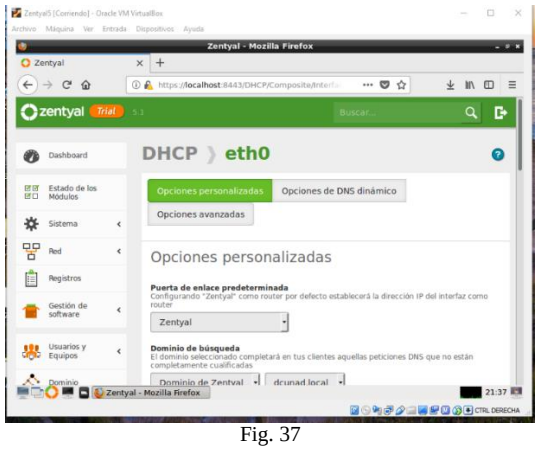


Fig. 37

Indicaremos cual será el dominio de búsqueda cuando el DHCP a signe direcciones de red a los clientes.

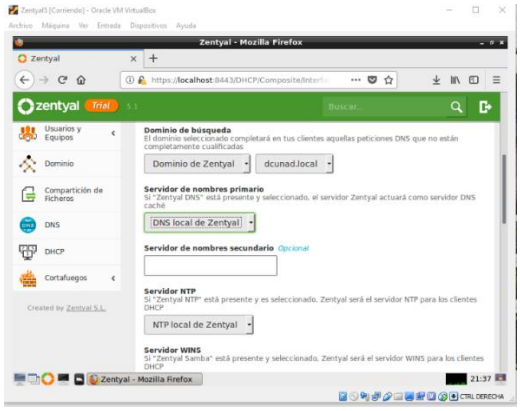


Fig. 38

Ahora se deben asignar los rangos de direcciones IP.

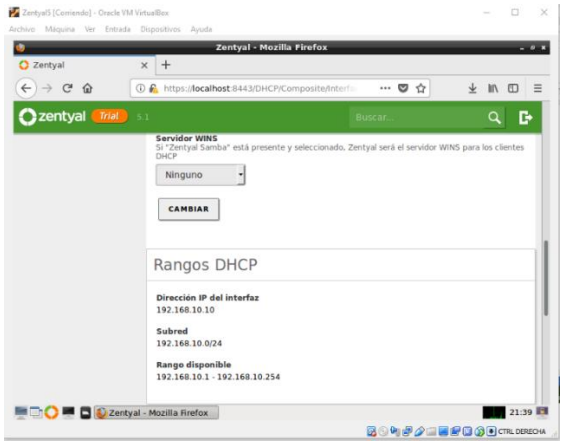


Fig. 39

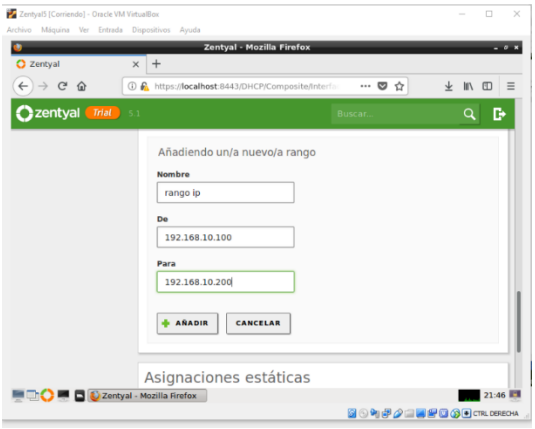


Fig. 40

Como se observa en la imagen aparase nuestro dnsdcunad.local y la IP 192.168.10.10 del servidor como puerta de enlace. Está correcto.

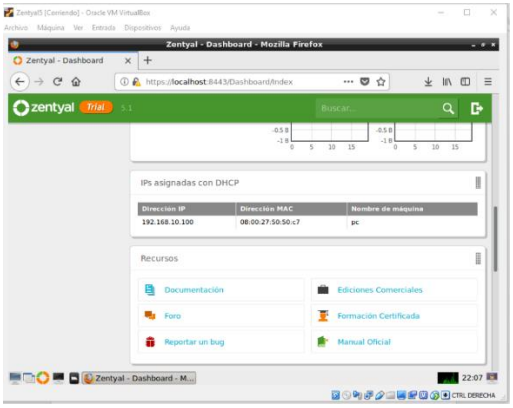


Fig. 41

***Unión Maquina Windows al domino DCUNAD.LOCAL***

Ahora uniremos esta máquina al dominio de Zentyal,

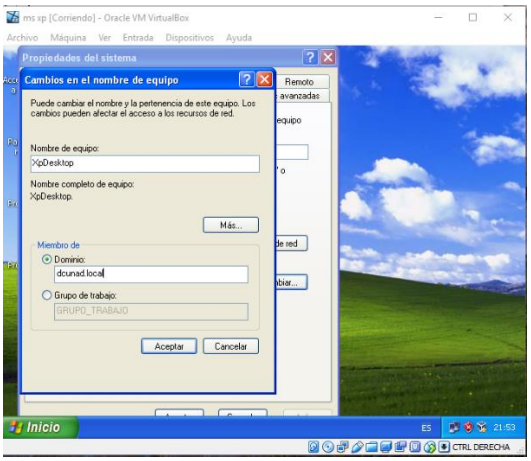


Fig. 42

En Windows es muy sencillo, iremos a propiedades del equipo y escogemos dominio en grupo de trabajo.

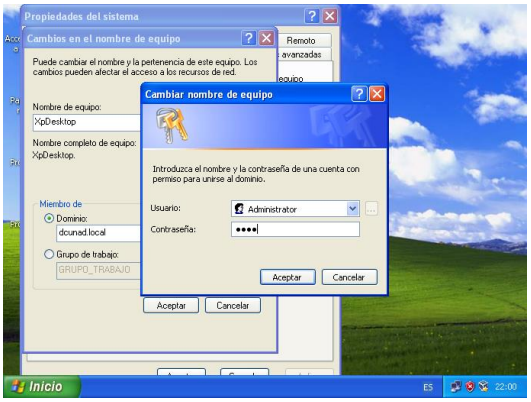


Fig. 43

Ahora probamos la conectividad por medio del DHCP, primero con Windows XP que ya lo tengo listo en mi equipo virtual.

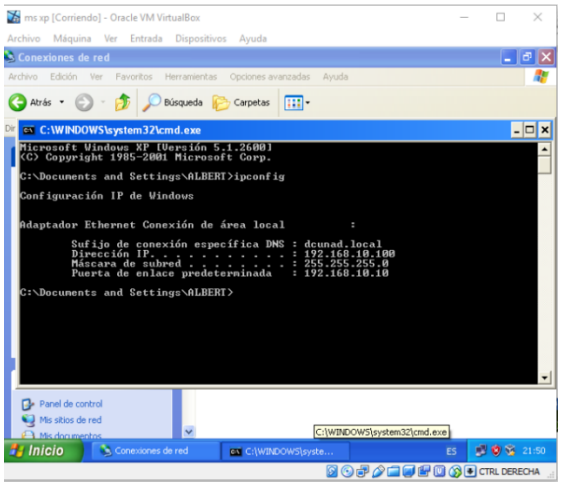


Fig. 44

Debemos indicar el dominio y las credenciales.

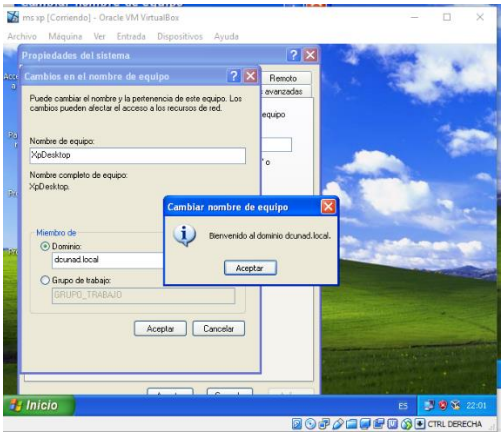


Fig. 45

Reiniciamos la máquina, y en el login ya podemos poner el usuario que creamos en Zentyal.

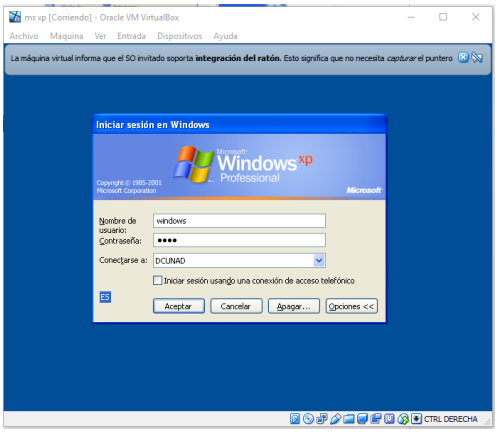


Fig. 46

En este momento ya atenemos una mauina en el dominio, y un usuario logueado y autenticado tambien por el DC.

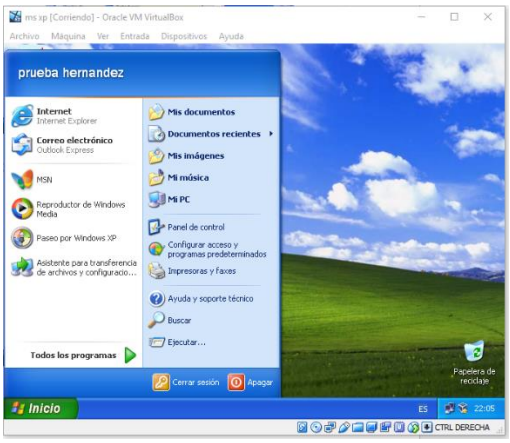


Fig. 47

Validamos el acceso en Zentyal.


Fig. 48

Como se observa tenemos el equipo pc en la carpeta de *computers*.

***Unión Maquina Ubuntu Desktop al domino DCUNAD.LOCAL***

Usaremos pbis-open, para gestionar la conexión y autenticación con el DC.

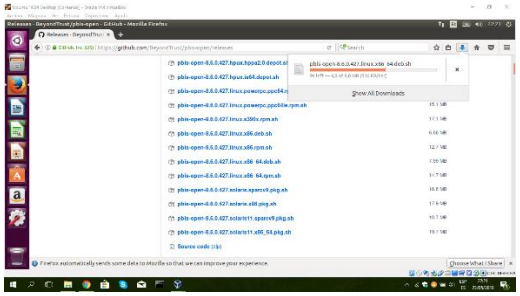

Fig. 49

En nuestra máquina virtual iremos al Github de pbis-open y descargaremos el paquete adecuado para nuestra máquina, en este caso un Ubuntu de 64 bit.

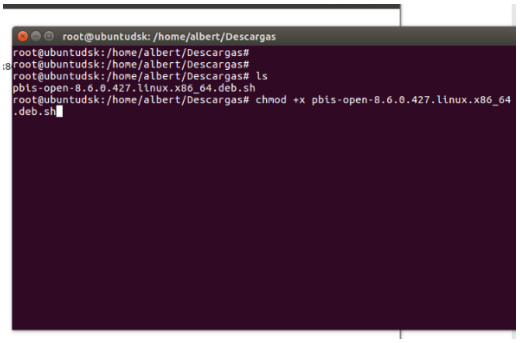


Fig. 50

Una vez descargado, procedemos a darle permisos de ejecución con el comando *chmod +x.*

Procedemos a instalar el paquete.

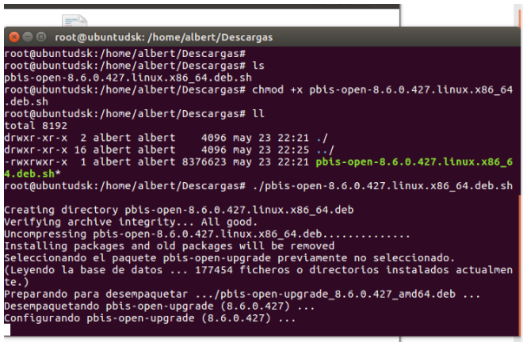


Fig. 51

Después de instalar el paquete, debemos cambiar la configuración de la tarjeta de red, para que la practica sea funcional, se debe poner el adaptador como interno, de esta manera el equipo cliente se podrá conectar con el servidor DC.

Para unir el Ubuntu desktop, pasamos el comando *domainjoin-cli join*. Con el uniremos la maquina al DC.

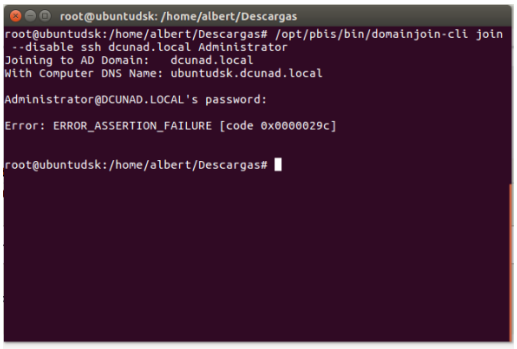


Fig. 52

Con el parámetro *greete-show-manual-login* en true ya se pueden hacer los inicios de sesión remotos.

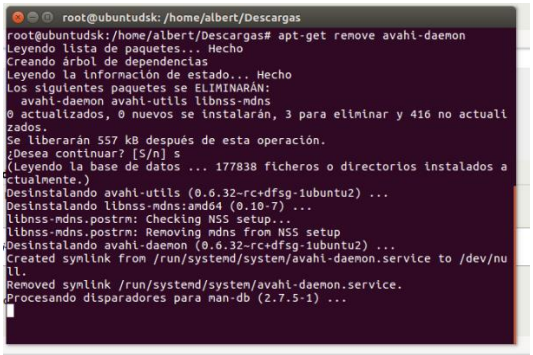


Fig. 57

Debemos eliminar el paquete *avahi-deamon* y con ello ya podemos unir la máquina.

También debemos hacer un cambien en el archivo nsswitch.conf, el cual permitirá el inicio de la sesión usando un alias de correo.

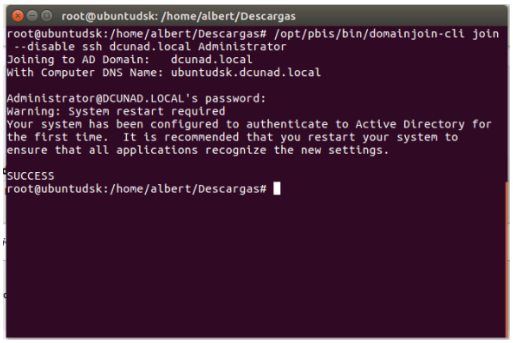


Fig. 53

Ahora reiniciamos la máquina.

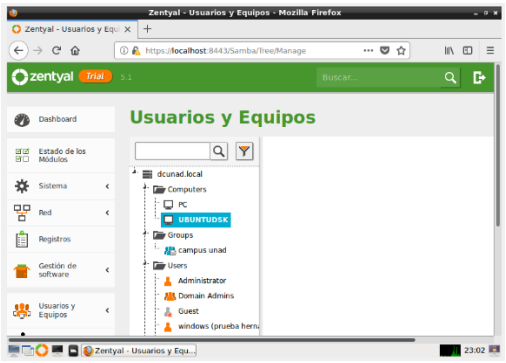


Fig. 54

Validamos y ya tenemos la maquina en el DC.

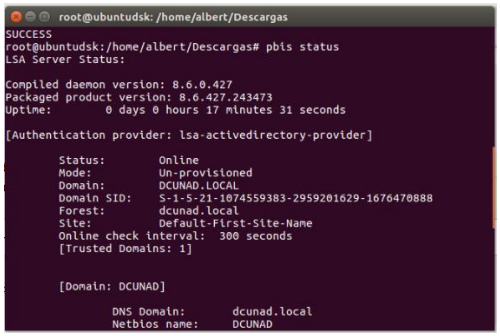


Fig. 55

Si ejecutamos *pbis status* también veremos que la máquina está en el DC.

Ahora para que podamos iniciar sesión en el dominio, debemos configurar un archivo de lightdm. El cual habilitara el login para usuarios remotos.

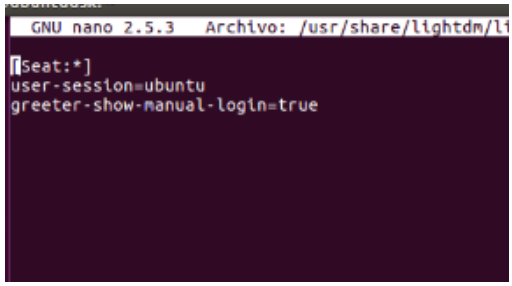


Fig. 56

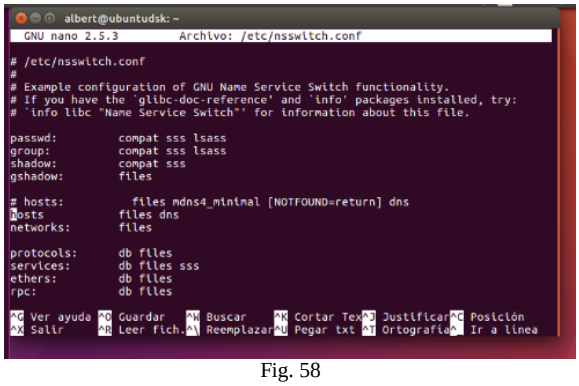


Fig. 58

También debemos copiar las plantillas de configuración. Para que el sistema use bash.

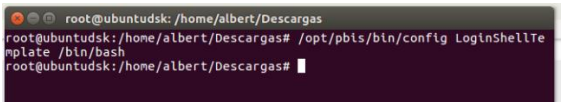


Fig. 59

## IV. TEMÁTICA 2: CONFIGURACION PROXY

Para esta sección se implementa y configura de manera detallada el control del acceso de una estación GNU/Linux Ubuntu Desktop a los servicios de conectividad a Internet desde Zentyal a través de un proxy que filtra la salida por medio del puerto 3128.

Se elige el tipo de configuración necesario para la actividad.

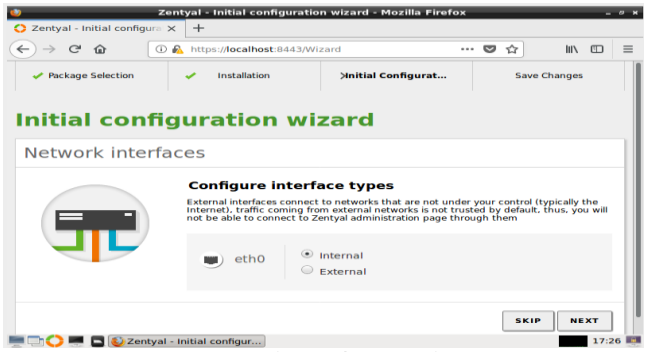


Fig. 60 Configuración de Interfaces

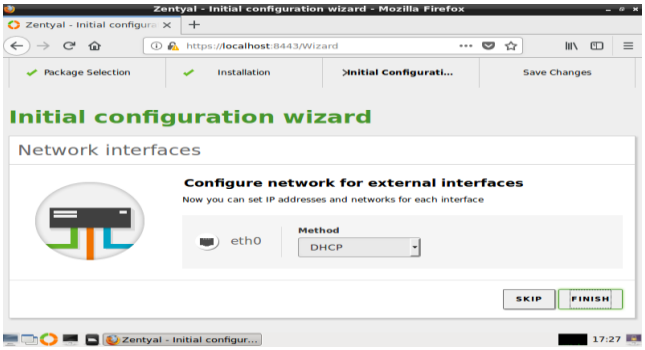


Fig. 61 Configuración de Redes

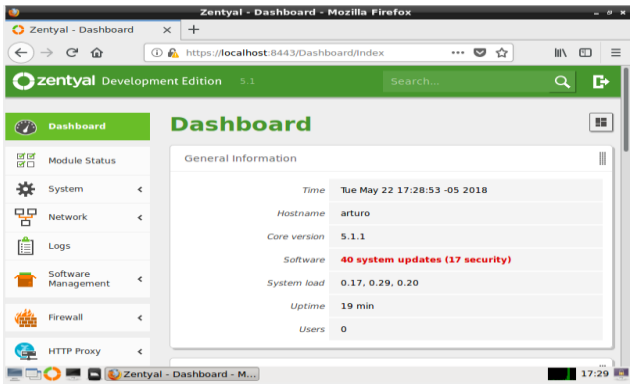


Fig. 62 Ingreso a Dashboard

En este momento ya podemos iniciar sesión con el usuario creado en Zentyal.

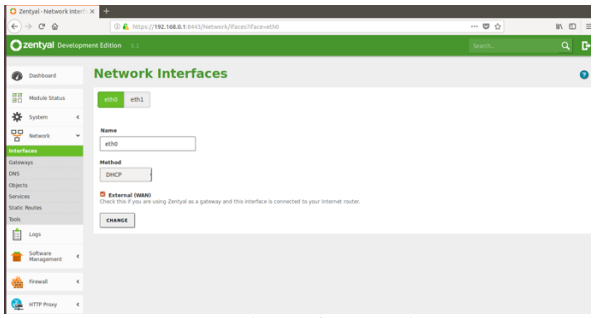


Fig. 63 Configuración de Interfaces

Dentro de la configuración de Zentyal hay dos configuraciones de red. Una de las redes es la red WAN la cual es de internet y la otra interfaz es de la red LAN, donde está conectada la máquina de Ubuntu. La IP de la red LAN es la siguiente 192.168.0.1. Y la red WAN está configurada por DHCP.

A continuación, se muestra la configuración de la red LAN.

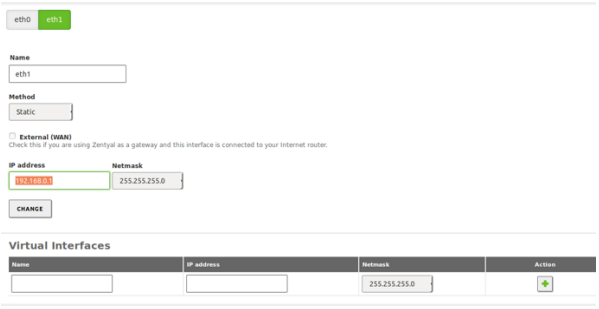


Fig. 64 Configuración de Red WAN

Para realizar los requerimientos de temática entramos a HTTP Proxy opción General Settings

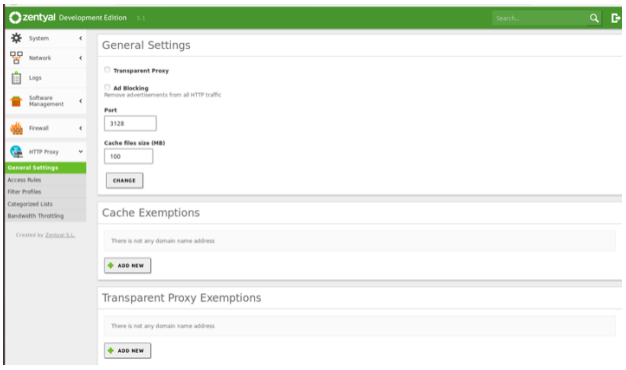


Fig. 65 Configuracion de HTTP Proxy

Se debe habilitar el proxy en el Zentyal y se entre a Module Status y se le da clic al checkbox de HTTP Proxy y guardamos los cambios.

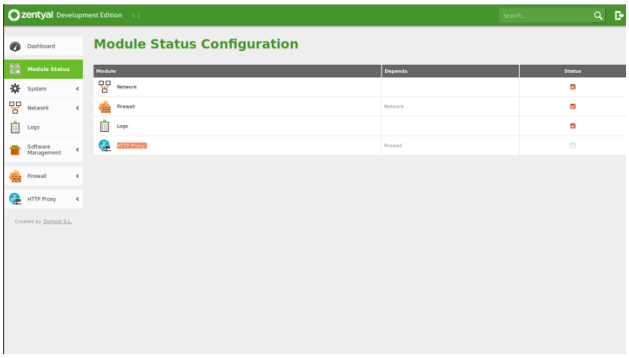


Fig. 66 Habilitar de HTTP Proxy

Nos vamos a Firefox de la máquina de Ubuntu para realizar la configuración del Proxy.

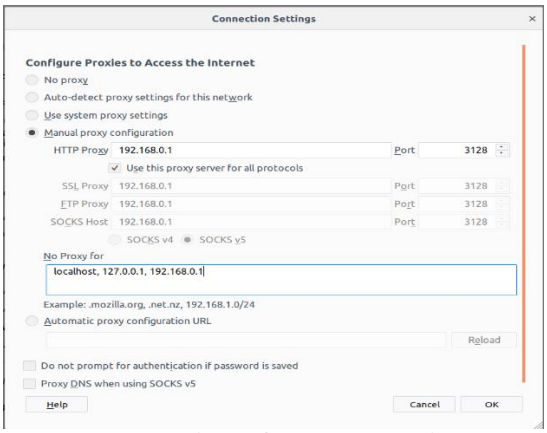


Fig. 67 Configuración de Proxy en Firefox

Se prueba en el Ubuntu de escritorio que ingrese una página por ejemplo Google.

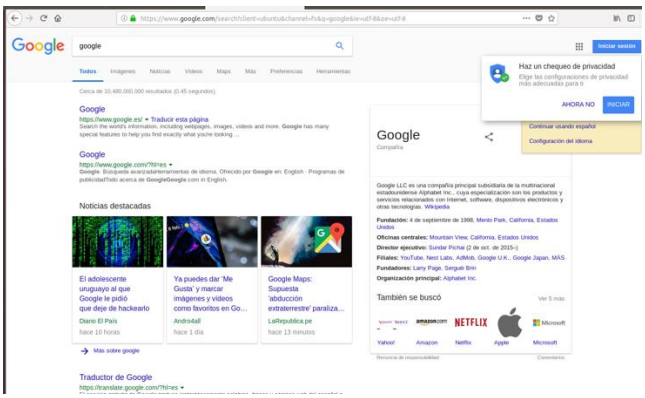


Fig. 68 Prueba de Proxy por puerto 3128

Si queremos bloquear por ejemplo la página de google.com. Nos vamos a HTTP Proxy opción FilterProfiles

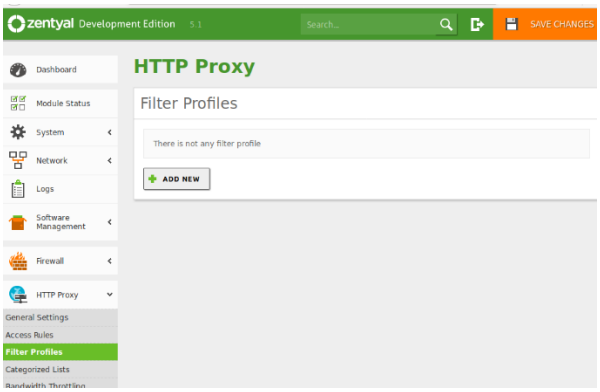


Fig. 69 Filtros de HTTP Proxy

Ahora estando aquí le damos en Add New y creamos nuestro filter.


Fig. 70 Adicionar Filtros de HTTP Proxy

Le realizamos clic al botón de configuración y nos aparece esta ventana.

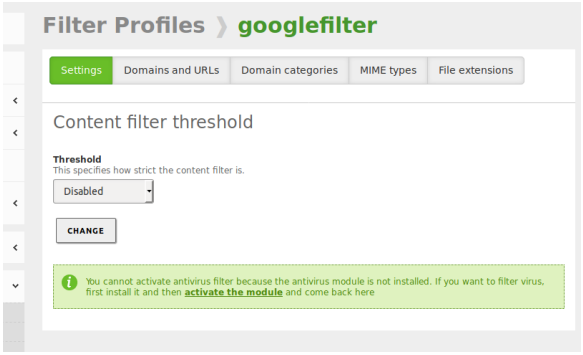


Fig. 71 Configurar Filtro creado

Le damos clic a “Domains and URLs”.

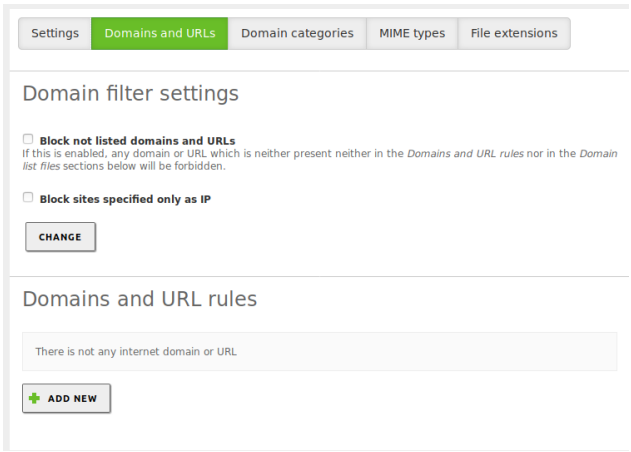


Fig. 72 Creando Dominios y Reglas

Le damos AddNew

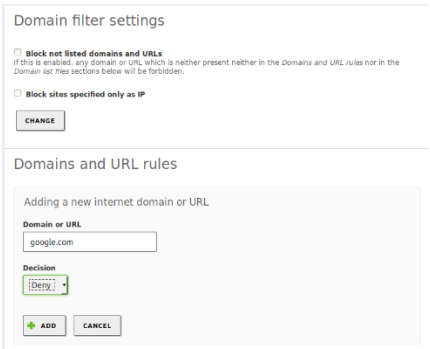


Fig. 73 Configurar Filtro creado con Deny

Probamos y efectivamente esta denegado el acceso

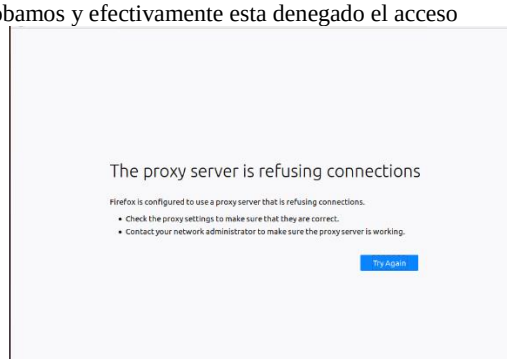


Fig. 74 Prueba de bloqueo HTTP Proxy

## V. TEMÁTICA 3: CORTAFUEGOS

Para este trabajo, la configuración de cortafuegos debe bloquear el acceso de los equipos de la red LAN a páginas de entretenimiento y redes sociales, por tanto, se seleccionarán las más representativas como Spotify, Youtube, Twitter y los servicios de Facebook incluyendo Instagram.

Por tanto, accedemos al menú Cortafuegos, en la opción Filtrado de Paquetes, luego accedemos a la opción Reglas de filtrado para redes internas.


Fig. 75 Acceso a las opciones de cortafuegos.

Después añadimos las direcciones IP de los sitios que se les va a denegar el acceso, se rechazarán paquetes desde los sitios Twitter, Youtube, Spotify y las redes sociales de la empresa Facebook, (Facebook e Instagram).

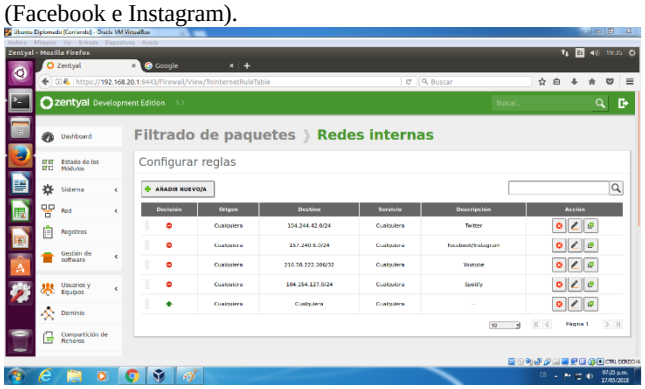


Fig. 76 Modificación de reglas de filtrado para redes internas.

Al guardar los cambios en el servidor se accede desde un equipo conectado a la red interna (en este caso Ubuntu Desktop) para abrir el navegador e intentar acceder a los sitios bloqueados donde se quedará en el proceso de carga sin acceder a la página solicitada.

Fig. 77 Verificación de las restricciones en Ubuntu Desktop.

## VII. TEMÁTICA 4: VPN

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

### *Configuración VPN*

Para configurar adecuadamente una VPN desde el servidor Zentyal debemos contar con dos aspectos muy importantes, un certificado de autoridad (CA) y un servidor VPN.

El CA lo generamos desde el módulo *Autoridad de Certificación*, en el cual le debemos asignar un nombre para su creación.


Fig. 78

En el caso del servidor VPN, lo creamos en el módulo VPN ingresando al sub-menu*Servidores*, allí se solicita que se le asigne de igual forma un nombre.

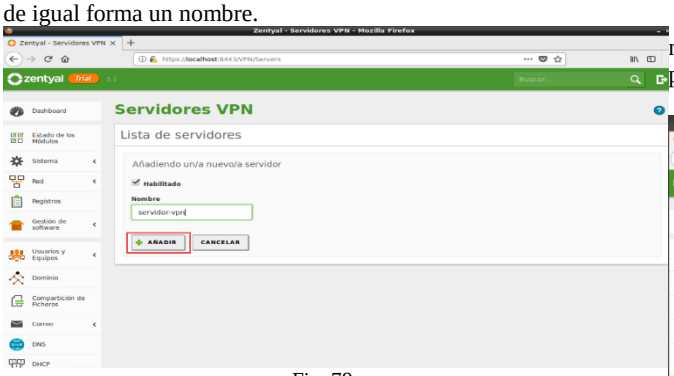


Fig. 79

Se debe tener presente que en la configuración de la VPN se debe parametrizar el certificado del servidor previamente creado y activar la interfaz TUN.


Fig. 80

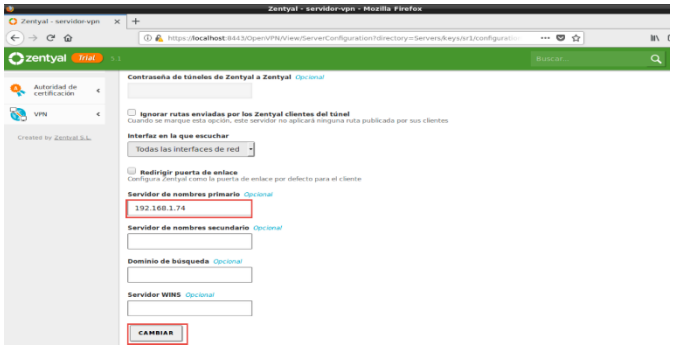


Fig. 81

Ya con esta configuración guardada se debe generar un nuevo CA para el cliente de VPN.


Fig. 82

Con el nuevo certificado podemos dirigirnos a Servidores en el módulo de VPN, donde podemos ingresar a la opción que nos permite descargar el paquete de la configuración del cliente.

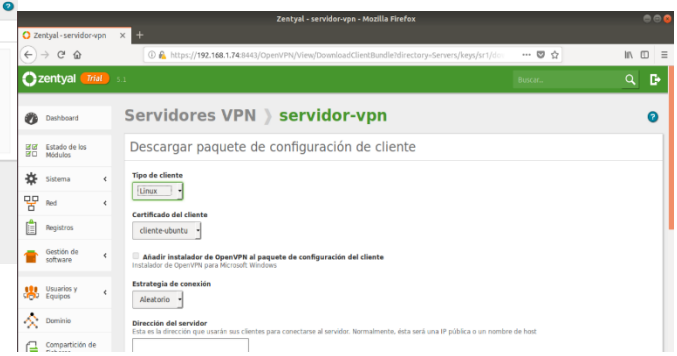


Fig. 83

Debemos seleccionar el tipo de cliente en el que vamos a realizar la conexión y el certificado asociado para el cliente.

De igual forma se debe parametrizar la IP del servidor para proceder con la descarga.

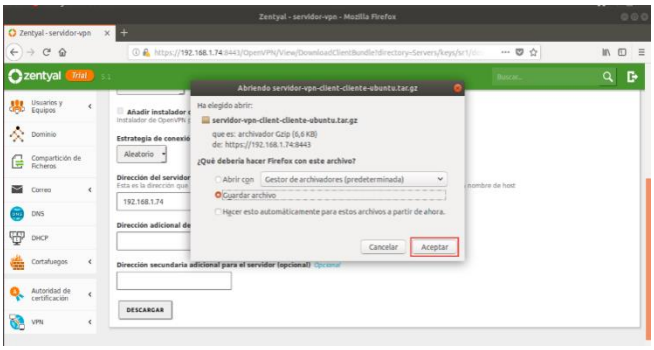

Fig. 84

Para realizar la prueba de conexión es necesario que el archivo de configuración VPN que descargamos sea transferido al cliente. Se debe descomprimir.

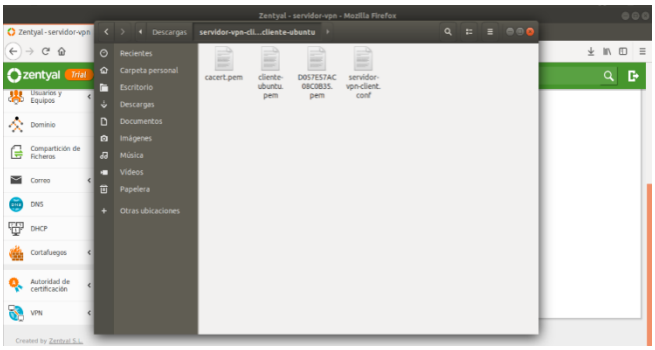

Fig. 85

Ya con los archivos debidamente descomprimidos, vamos a los ajustes de Ubuntu (máquina cliente) y en el apartado de red añadimos una red VPN. Basta con seleccionar la opción *Importar desde un archivo* y seleccionar el archivo *.conf* que descomprimimos.

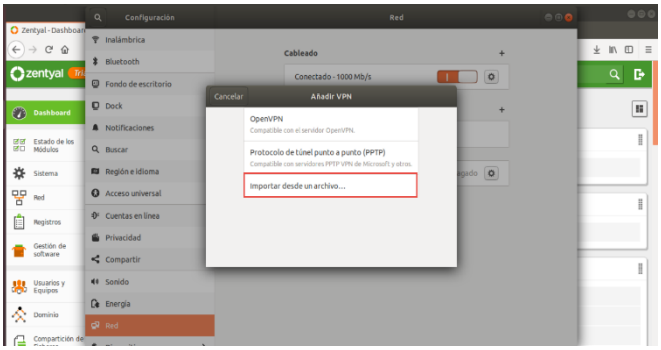

Fig. 86

Automáticamente reconocerá la configuración de la conexión VPN.

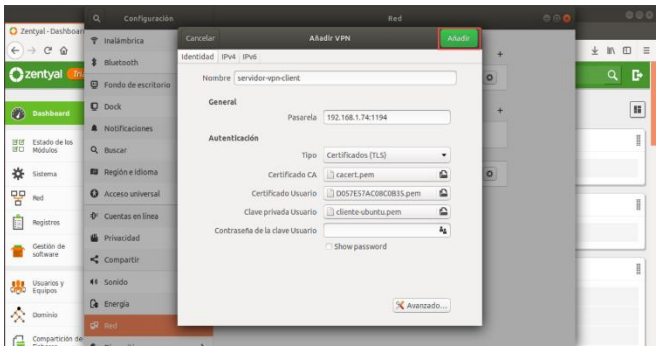

Fig. 87

Cuando tengamos la conexión establecida será visible a través de la consola de administración de Zentyal, donde nos mostrarán los clientes conectados a la VPN con su respectiva IP.

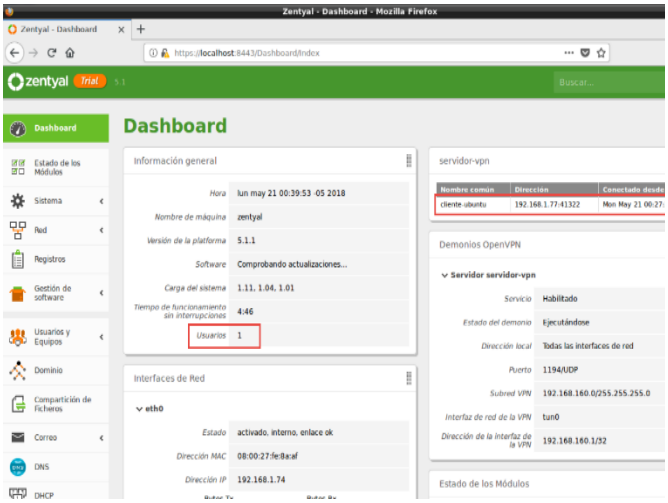

Fig. 88

## VIII. TEMÁTICA 4: FILE SERVER Y PRINT SERVER

**Producto esperado:**

Implementación y configuración detallada del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través del controlador de dominio LDAP a los servicios de carpetas compartidas e impresoras.

**Print Server y Carpetas Compartidas**

Inicialmente creamos un directorio llamado compartido en nuestro */home/franklincampo*.

Posteriormente creamos el archivo *diplomado_unad_2018_franklincampo.txt*.

Validamos que nuestra máquina virtual tenga conexión a la red con el comando *ifconfig* para ver la dirección IP y hacemos un *ping* para www.google.com.

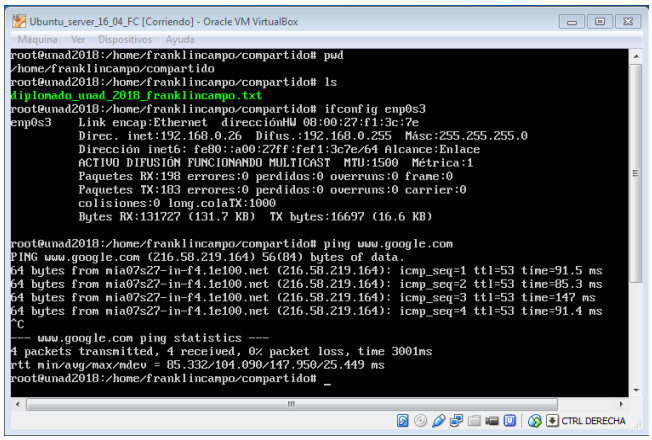


Fig. 89 Crear directorio

Posteriormente instalamos el servicio SAMBA con el comando *apt-get install samba-common-bin*.

Una vez instalado revisamos su estado con el comando */etc/init.d/smbd status*.

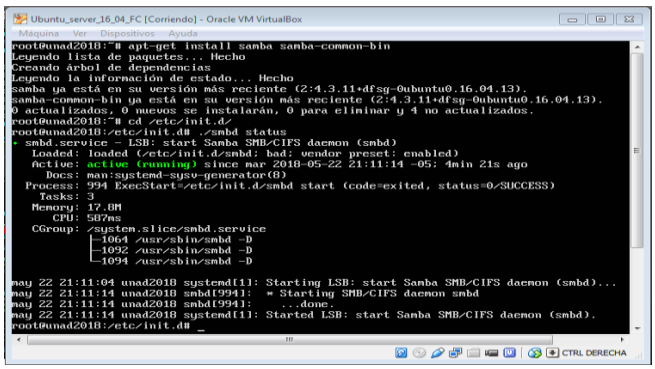


Fig. 90 Instalación Servidor SAMBA

Creamos un usuario samba llamado franklin *useradd –s /bin/nologin franklin*.

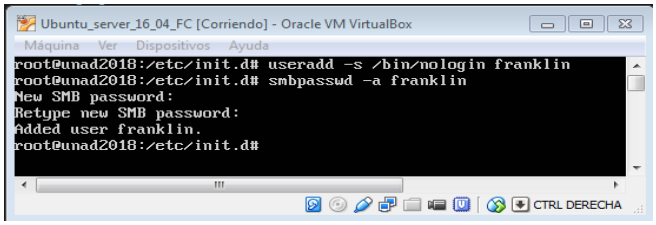


Fig. 91 Agregar usuario SAMBA

Configuramos los repositorios para la Instalación Webmin, agregamos la siguiente URL:

*deb http://download.webmin.com/download/repository sarge contrib* al repositorio */etc/apt/sources.list*.

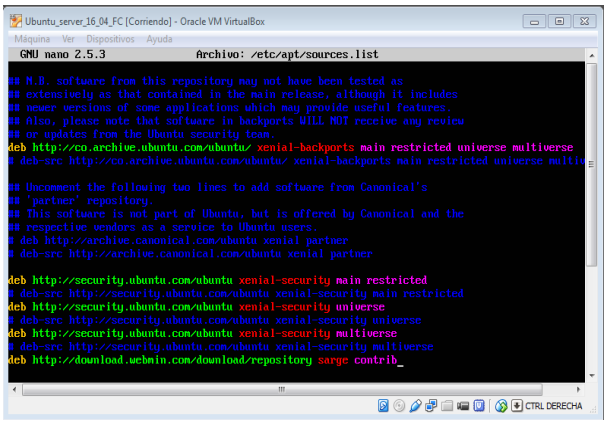


Fig. 92 Configuración repositorio Webmin

Posteriormente descargamos la llave para que permita realizar la descarga con el comando *wget http://www.webmin.com/jcameron-key.asc*.

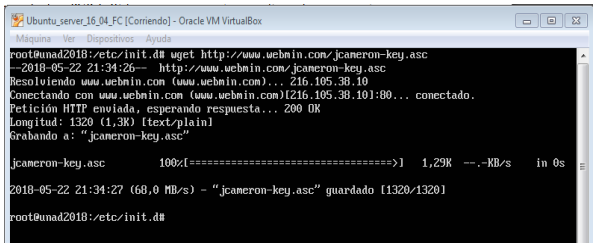


Fig. 93 Agregar llave al repositorio Webmin

Agregamos la llave con el comando *apt-key add jcameron-key.asc*.

Realizamos la actualización de repositorios antes de la instalación con el comando *apt-get update.*

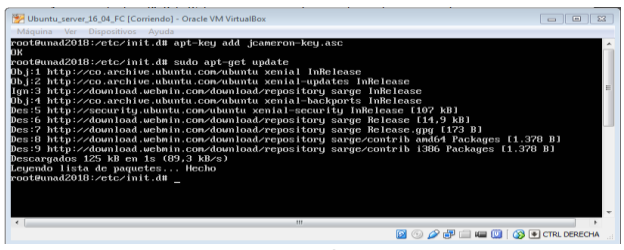


Fig. 94 Actualización del servidor

Realizamos la instalación de webmin con el comando *apt-get install webmin*.

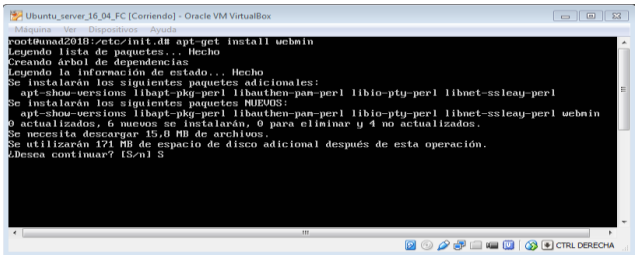

Fig. 95 Instalación Webmin

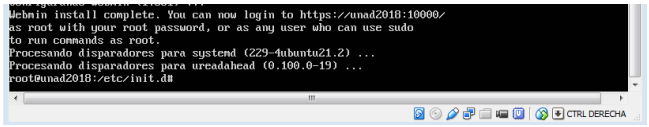

Fig. 96 Instalación Webmin finalizada

Accedemos al servidor webmin https://192.168.0.26:10000 fijamos user root y contraseña.

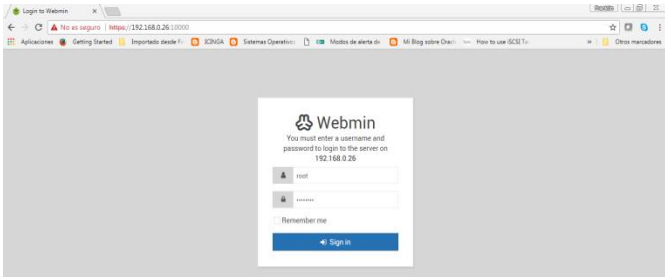

Fig. 97 Acceso web a Webmin

Aquí podemos evidenciar que hemos accedido satisfactoriamente.

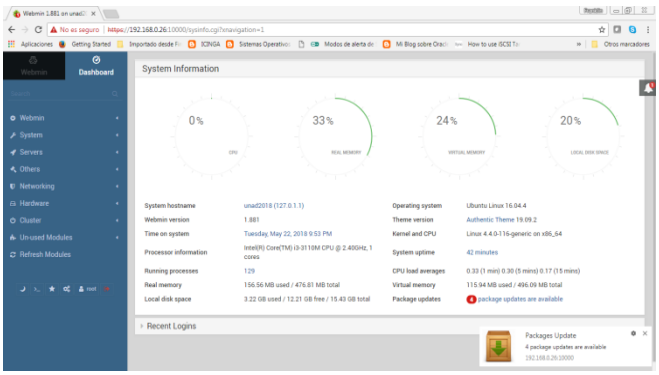

Fig. 98 Estado del servidor Webmin

Revisamos en el modulo de SAMBA los recursos compartidos

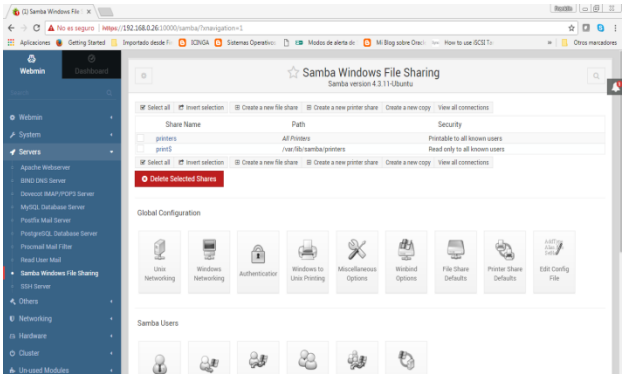

Fig. 99 Revisión modulo SAMBA

Ahora miremos las características del usuario SAMBA el cual creamos anteriormente.

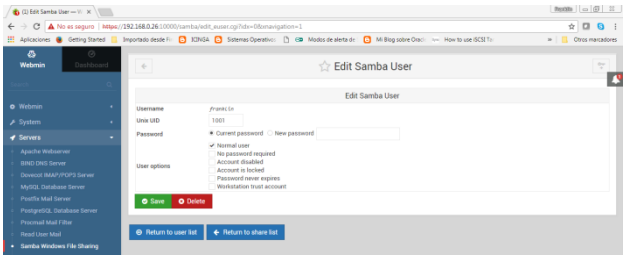

Fig. 100 Características usuario SAMBA

Ahora instalamos una impresora virtual para la prueba de impresión con clientes Linux Ubuntu y Windows con el comando *apt-get install cups-pdf.*

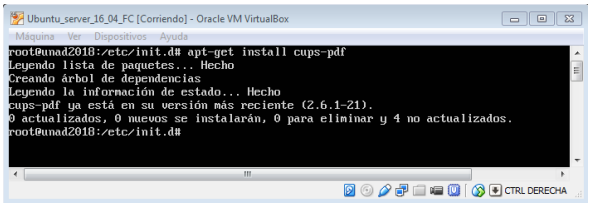

Fig. 101 Instalación impresora virtual cups

En seguida podemos apreciar a través del servidor Webmin en el módulo Hardware que ya quedó instalada la impresora virtual.

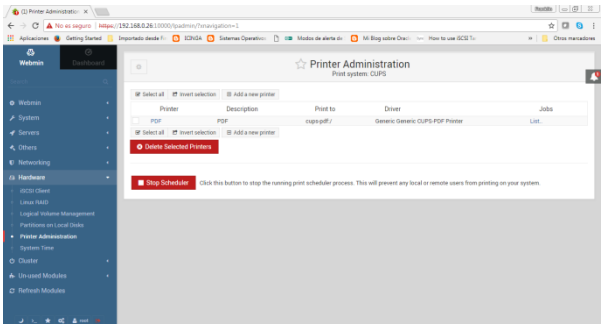

Fig. 102 Revisión servicio de impresión cups con webmin

Agregamos una impresora virtual nueva llamada Printerunad y en la descripción es Impresora Unad, Además seleccionamos el controlador HP Color LaserJet PCL6CUPS.

En el Local Device colocamos *Null device* porque es virtual y no física.

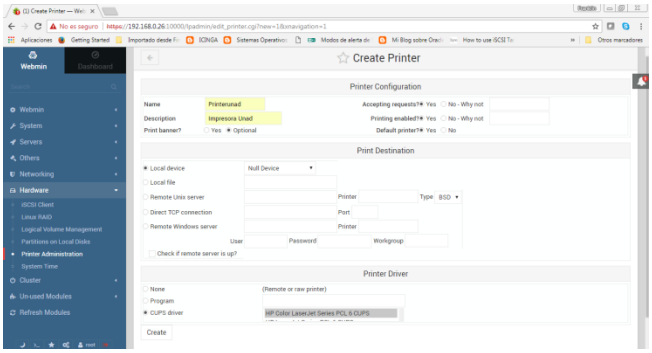


Fig. 103 Agregar impresora virtual Printerunad

Como podemos ver a través de Webmin en el módulo Hardware que ya quedó instalada la impresora virtual llamada Printerunad.

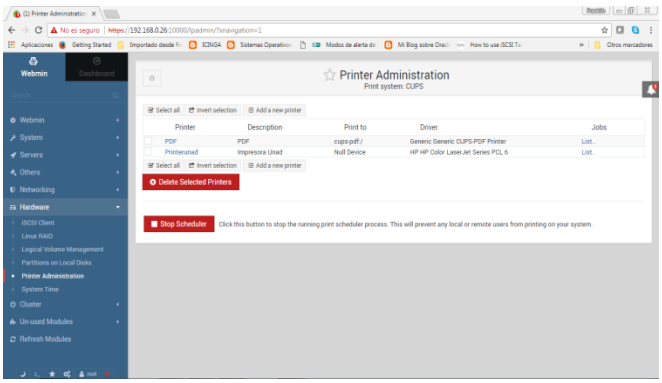


Fig. 104 Modulo Hardware Webmin

Posteriormente vamos a una maquina Windows e intentamos conectarnos a la impresora Printerunad.

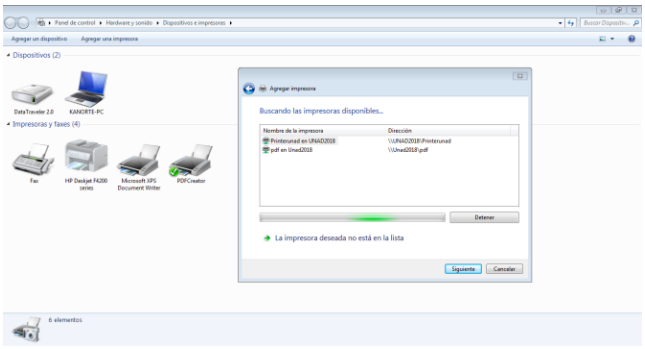

Fig. 105 Conexión de impresora desde Windows

Seleccionamos el controlador HP LaserJet PCL6CUPS.

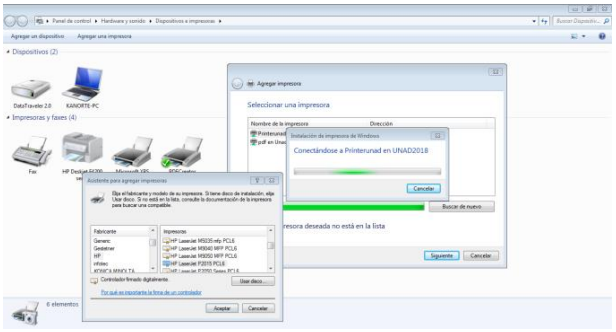

Fig. 106 Conexión de impresora desde Windows

Vemos como el asistente de impresión nos informa que la impresora se ha agregado correctamente

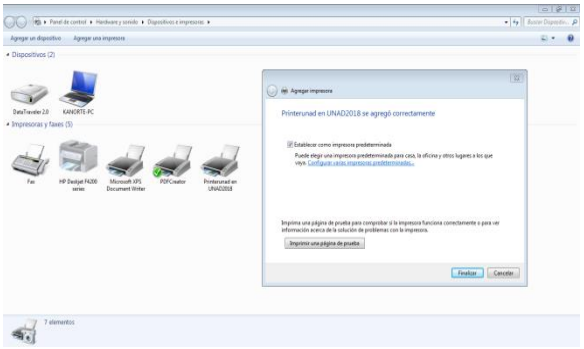

Fig. 107 Conexión de impresora desde Windows

Dejamos la impresora PrinterUnad como impresora predeterminada.

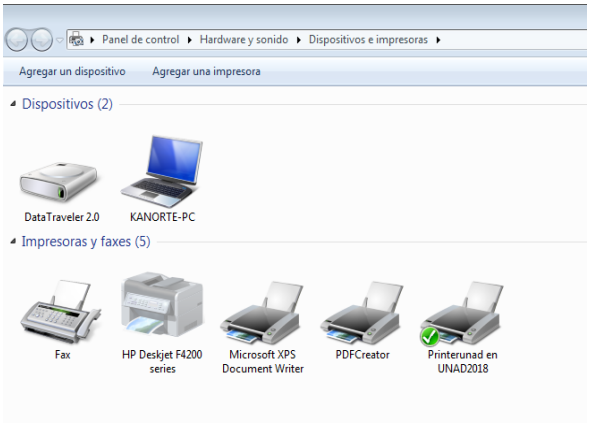


Fig. 108 Conexión de impresora desde Windows

A continuación realizamos el mismo proceso pero en una estación cliente Linux Ubuntu. Iniciamos el asistente de instalación de impresoras.

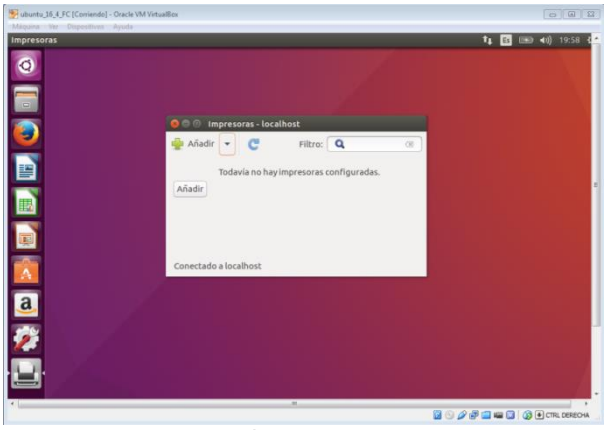


Fig. 109 Conexión de impresora desde Ubuntu

Seleccionamos instalar una impresora de red y el asistente encuentra la impresora utilizando la dirección IP como argumento.

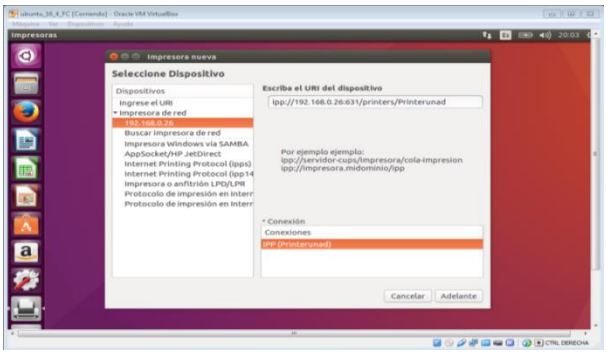


Fig. 110 Conexión de impresora desde Ubuntu

Realizamos la descripción de la impresora.

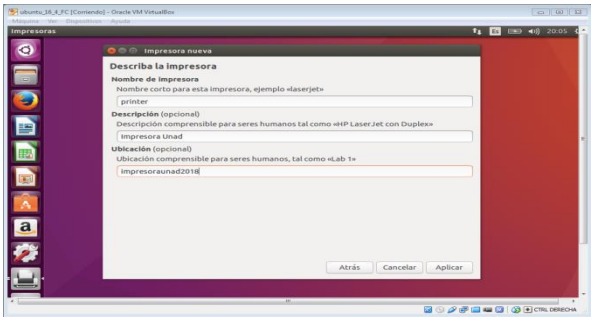


Fig. 111 Conexión de impresora desde Ubuntu

Finalizamos la instalación de la impresora enviando una página de prueba.

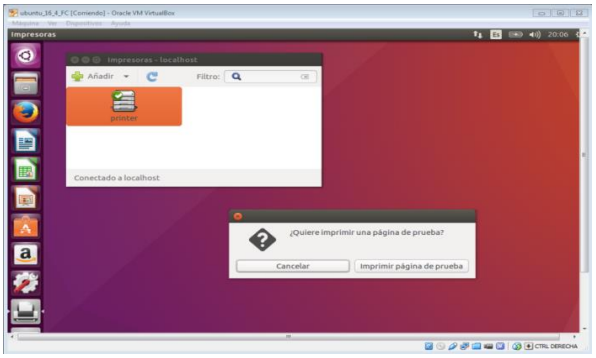


Fig. 112 Conexión de impresora desde Ubuntu

El asistente de Impresión nos informa que la página de prueba ha sido enviada.

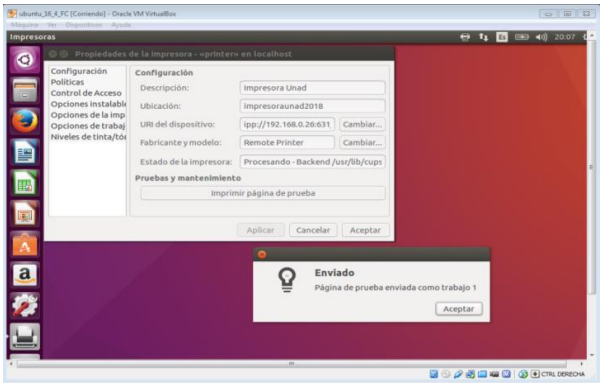


Fig. 113 Conexión de impresora desde Ubuntu

Para poder administrar las impresiones del servidor de impresión Unad utilizamos la interfaz de administración web que trae la impresora virtual *cups* incorporado.

La editamos con el *comando nano –w /etc/cups/cupsd.conf* y modificamos los parámetros: "*Listen localhost:631*" por "*Listen *:631*". Con este cambio podemos acceder a la consola de administración desde cualquier dirección IP.

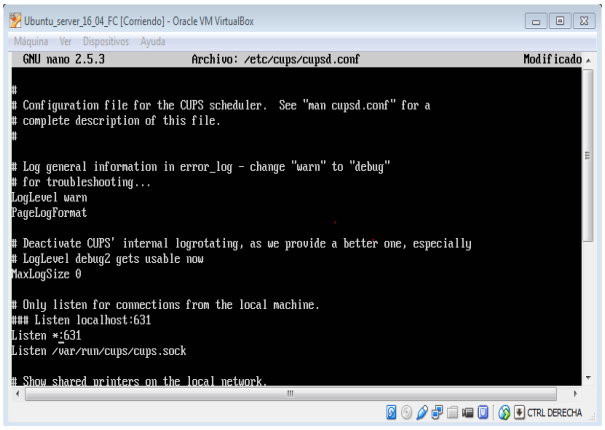


Fig. 114 Configuración para la administración impresión

Además del puerto debemos agregar las siguientes líneas en el archivo */etc/cups/cupsd.conf*:

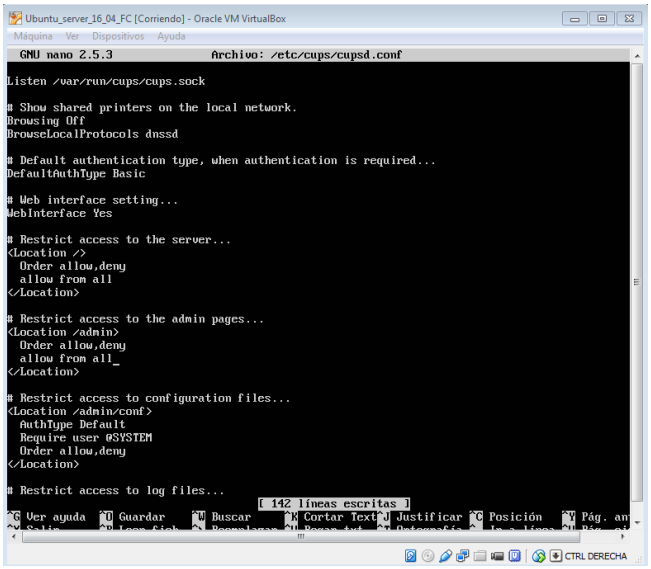


Fig. 115 Configuración para la administración impresión

Reiniciamos el servidor de impresión virtual cups comando */etc/init.d/cups restart* y posteriormente validamos su estado con el comando */etc/init.d/cups status*.

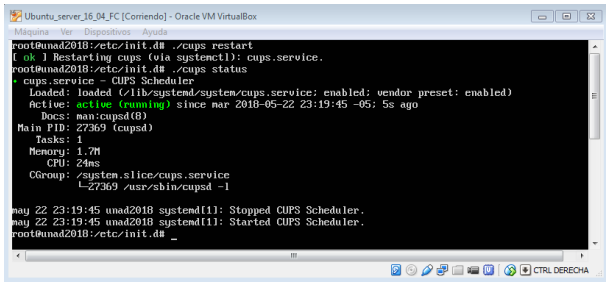


Fig. 116 Reinicio del servicio de impresión

Ahora bien procedemos a administrar el servidor de impresión con el administrador web de cups, es así como podemos ver como existen dos impresiones en cola para el servidor Printerunad, las cuales corresponden a la enviada desde un equipo Windows y otra enviada desde un equipo Linux Ubuntu.


Fig. 117 Administración impresión cups

Ahora bien procedemos a validar las carpetas compartidas desde nuestro servidor PrintServer en donde podemos evidenciar que existe un directorio compartido unad2018 en nuestro servidor.

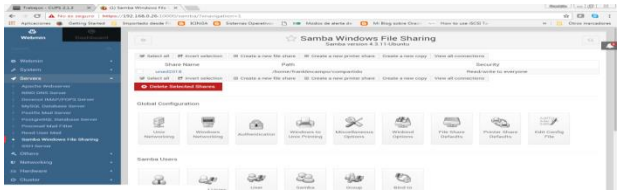


Fig. 118 Carpetas compartidas

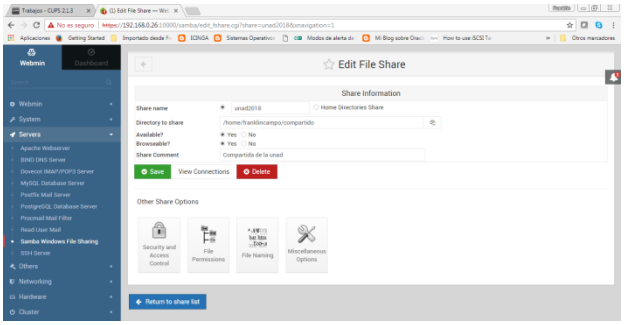


Fig. 119 Carpetas compartidas

Conectamos la estación de computo Linux Ubuntu Desktop al directorio compartido del Linux Ubuntu server con el usuario y password samba el cual creamos anteriormente.

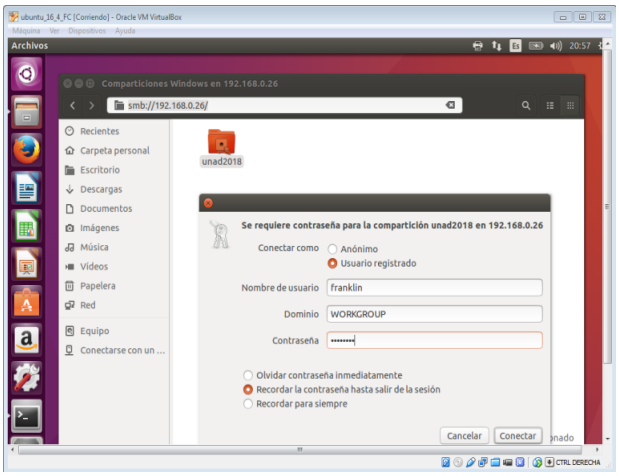


Fig. 120 Conexión Ubuntu carpetas compartidas

A continuación podemos acceder a la información contenida en el directorio compartido.

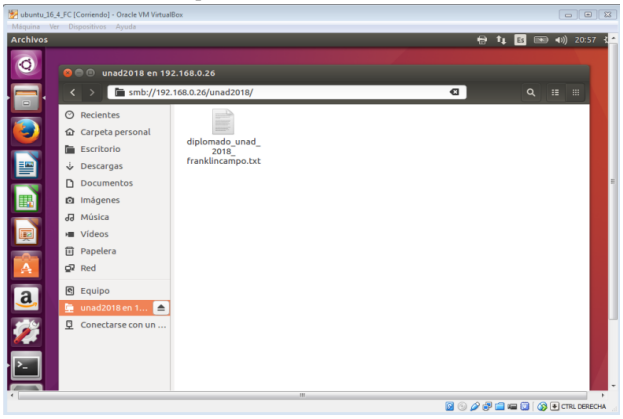


Fig. 121 Ubuntu Carpetas compartidas

## IX. TEMÁTICA 5: ADMINISTRACIÓN SERVIDOR LDAP

Instalamos el servidor LDAP con el comando *apt-get install slapd ldap-utils*.

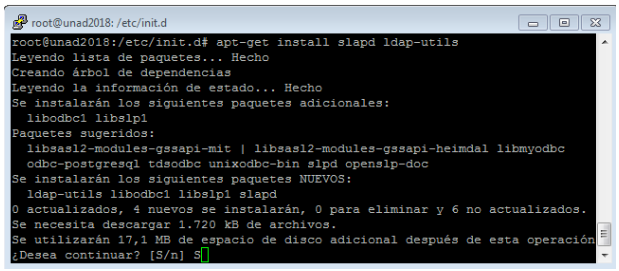


Fig. 122 Instalación LDAP

Fijamos y confirmamos el password para el usuario administrador del LDAP.

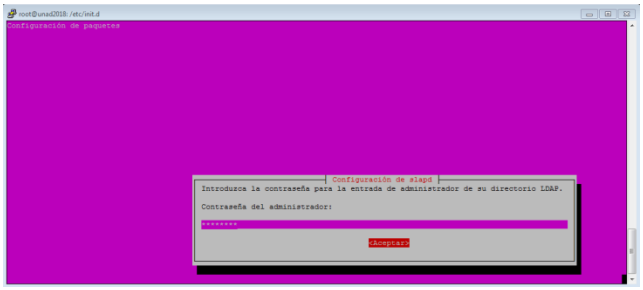


Fig. 123 Instalación LDAP Password

Revisamos el Archivo /etc/hosts con el fin de validar el nombre del equipo y la dirección IP 192.168.0.26 y el nombre del ordenador es unad2018.

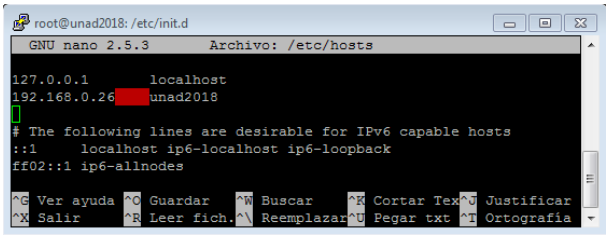


Fig. 124 Instalación LDAP hosts

Intalamos la librería NSS para LDAP la cual ofrece una interfaz para acceder y configurar distintas bases de datos utilizadas para almacenar cuentas de usuario entre otras, /etc/passwd, /etc/group, /etc/hosts, LDAP, etc.

Para hacer esto ejecutamos el comando *apt-get install libnss-ldap*.

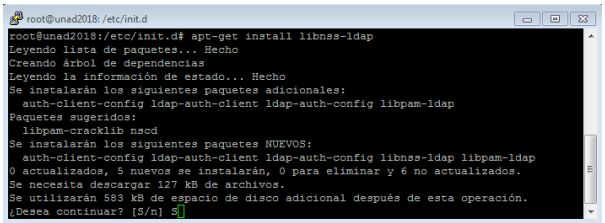


Fig. 125 Instalación LDAP

Asignamos la dirección URL del servidor LDAP ldapi:///192.168.0.26.

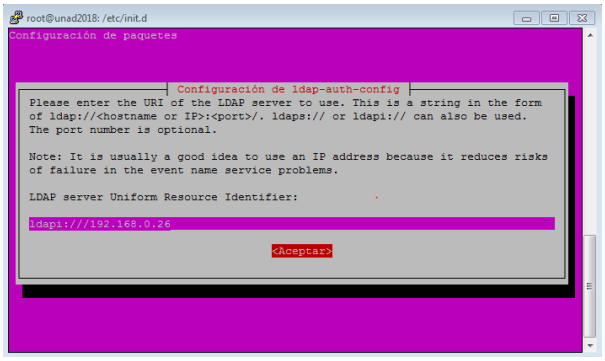


Fig. 126 Instalación LDAP URL

Escribimos el nombre global único Distinguished Name – DN *dc=unadpoppayan,dc=net*.

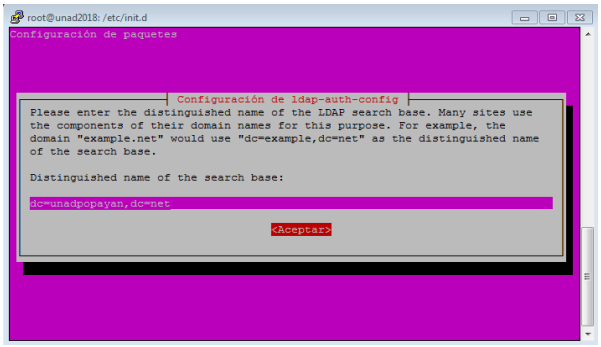


Fig. 127 Instalación LDAP

Seleccionamos la Versión 3 del LDAP.


Fig. 128 Instalación Versión LDAP

Indicamos que las contraseñas se guarden en un archivo independiente que sólo podrá ser leído por el root únicamente.

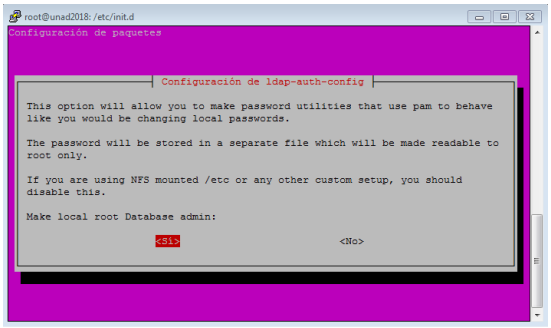


Fig. 129 Instalación LDAP

El sistema nos pregunta si queremos que sea necesario identificarse para realizar consultas en la base de datos de LDAP. Seleccionamos la opción No.

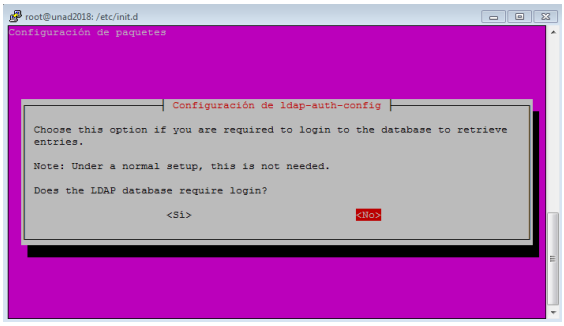


Fig. 130 Instalación LDAP

Escribimos un nombre global único Distinguished Name – DN *cn=manager,dc=unadpopayan,dc=net*

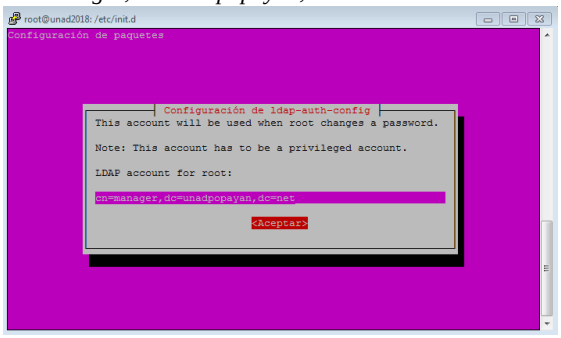


Fig. 131 Instalación LDAP

Digitamos la contraseña del LDAP fijada anteriormente.

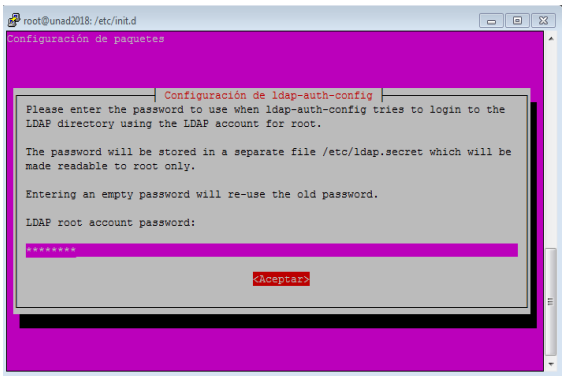


Fig. 132 Instalación LDAP

Instalación terminada del LDAP.

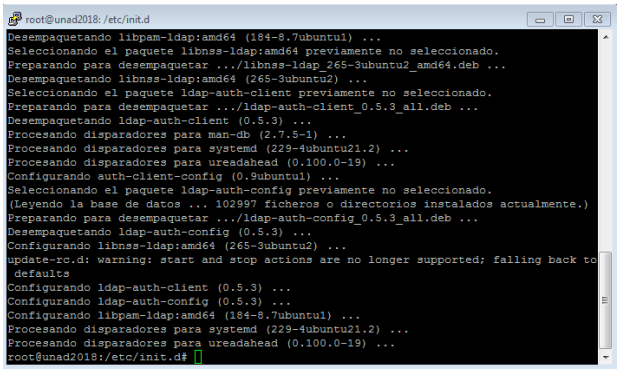


Fig. 133 Instalación LDAP Terminada

Si se requiere cambiar algún parámetro solo debemos reconfigurar el LDAP con el comando *dpkg-reconfigure ldap-auth-config*.

Ahora configuramos la autenticación para los clientes utilizando *auth-client-config*, un script que nos ayuda a modificar los archivos de configuración de PAM y NSS.

Ejecutamos el siguiente comando *auth-client-config -t nss -p lac_ldap*.

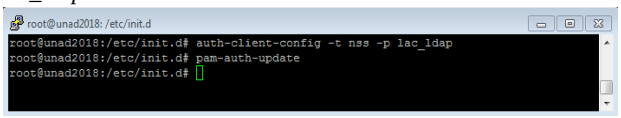


Fig. 134 Autenticación LDAP

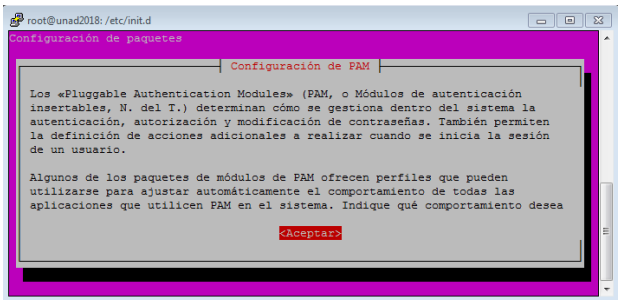


Fig. 135 Autenticación LDAP

Seleccionamos los cuatro tipos de autenticación.

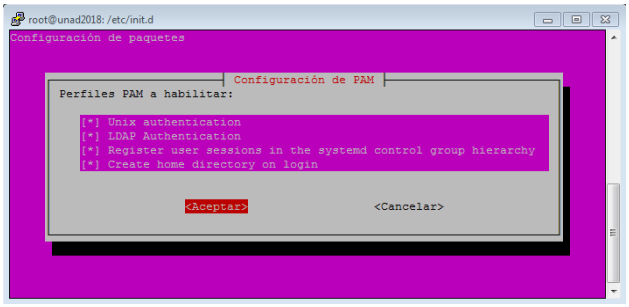


Fig. 136 Autenticación LDAP

Para ver la configuración del LDAP podemos consultar el archivo.

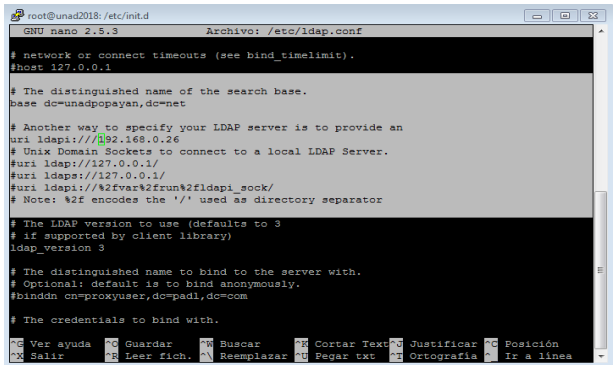


Fig. 137 Configuración LDAP

Posteriormente Configuramos el demonio SLAPD (Standalone LDAP Daemon) es un programa multiplataforma, que se ejecuta en segundo plano, atendiendo las solicitudes de autenticación LDAP que se reciban en el servidor. Para esta configuración ejecutamos el siguiente comando: *dpkg-reconfigure slapd*.

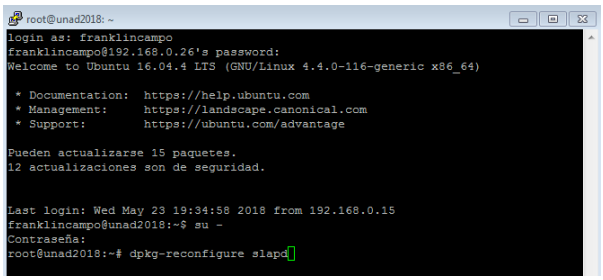


Fig. 138 Configuración SLAPD

Nos pregunta si queremos omitir la configuración del servidor damos la opción No.

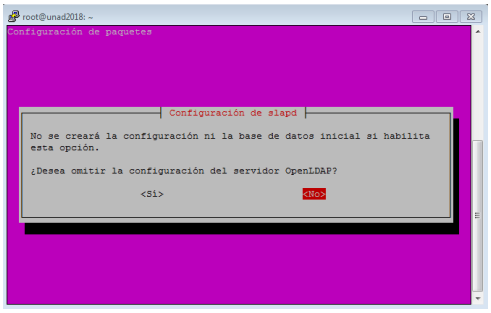


Fig. 139 Configuración LDAP

Introducimos el nombre de dominio DNS.

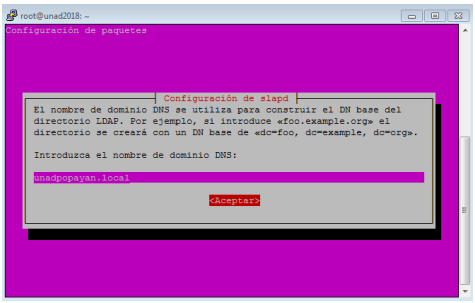


Fig. 140 Nombre del dominio DNS

Introducimos el nombre de la Organización.

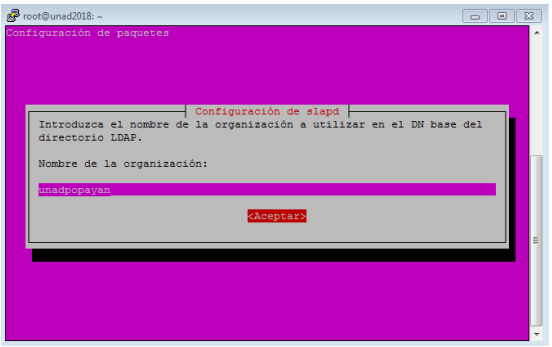


Fig. 141 nombre de la Organización

Introducimos y confirmamos la contraseña de Administración LDAP.

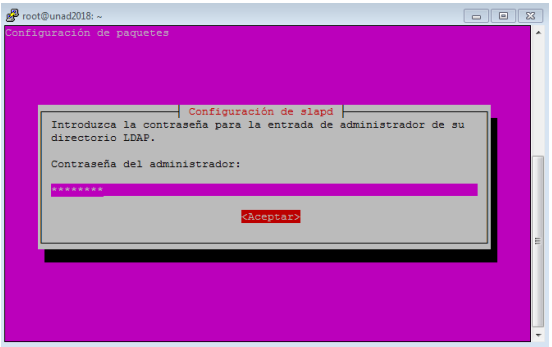


Fig. 142 Contraseña de Administración

Seleccionamos el motor de Base de Datos MariaDB.

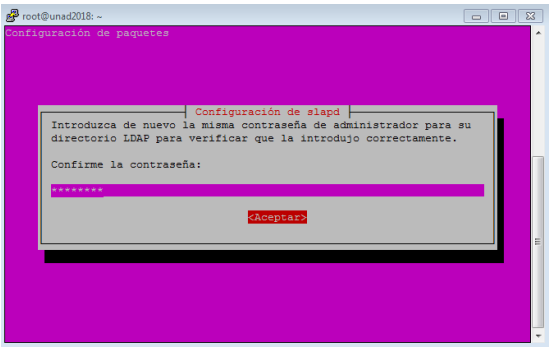


Fig. 143 Selección base de datos MariaDB

Nos pregunta si deseamos borrar la base de datos SLAPD damos la opción No.

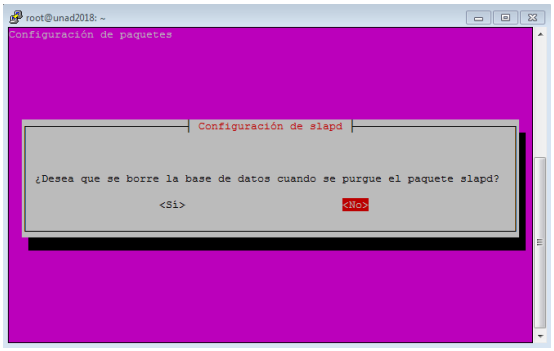


Fig. 144 Instalación SLAPD

Nos pregunta si deseamos mover la base de datos antigua le damos la opción Sí.

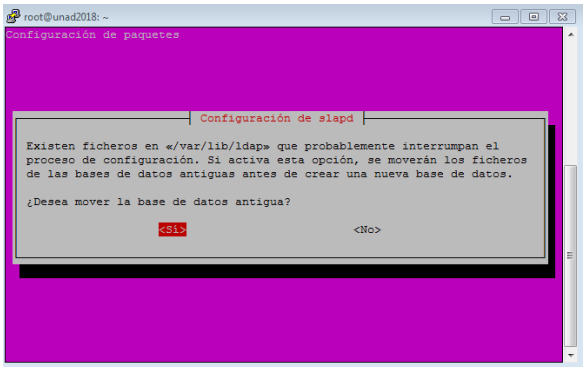


Fig. 145 Instalación SLAPD

Además nos pregunta si deseamos permitir el protocolo LDAP versión 2 el cual debe ser compatible con la versión 3 le damos la opción No.

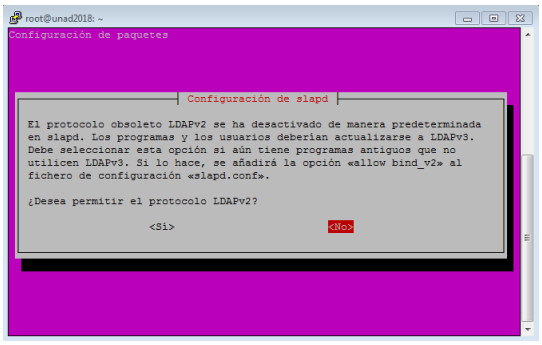


Fig. 146 Instalación SLAPD

Ahora accedemos a la Administración Webmin del Linux Ubuntu server LDAP.

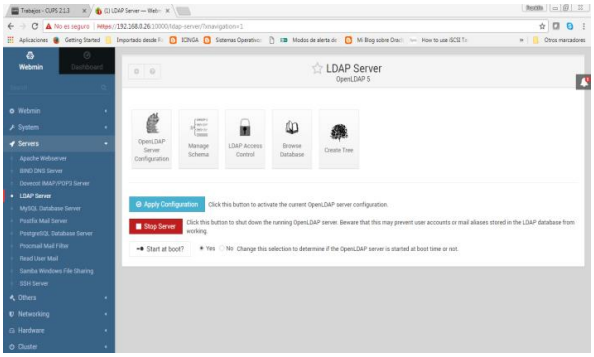


Fig. 147 Administración LDAP Webmin

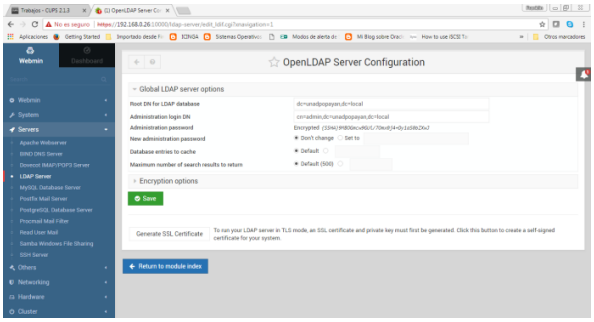


Fig. 148 Administración LDAP Webmin

Ahora procedemos a Configurar el Cliente que se conectará a nuestro LDAP En el equipo cliente Linux Ubuntu Desktop.

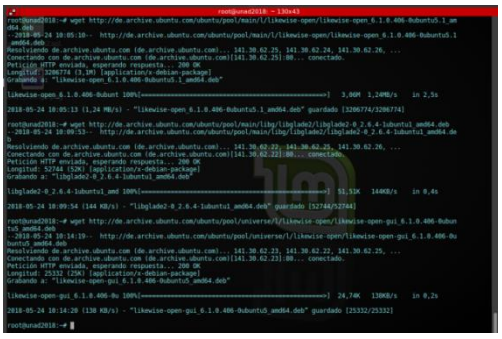

Fig. 149 Cliente Ubuntu LDAP

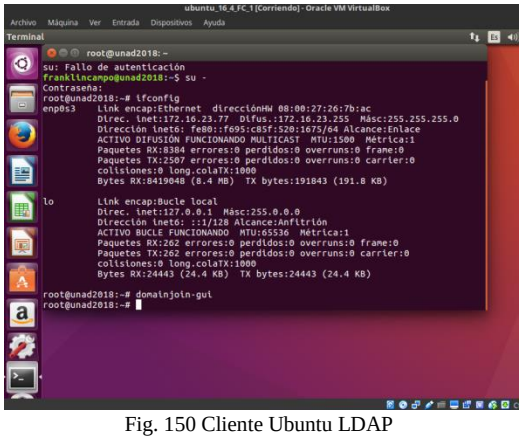


Fig. 150 Cliente Ubuntu LDAP

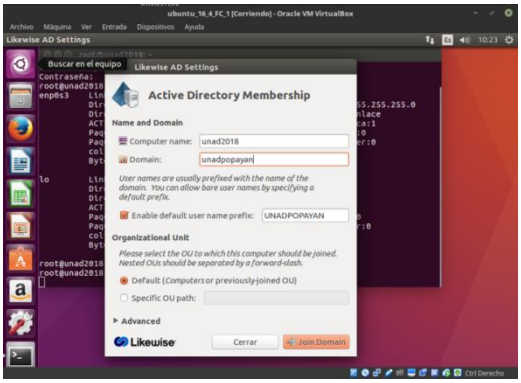

Fig. 151 Cliente Ubuntu LDAP

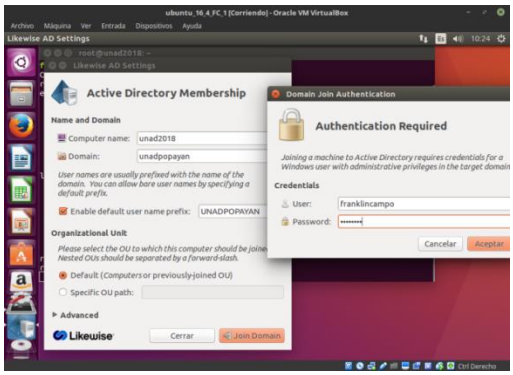

Fig.152 Cliente Ubuntu LDAP

## CONCLUSIONES

Con esta investigación se finaliza el ciclo del desarrollo del diplomado en Linux, en el cual se pusieron en práctica muchas tecnologías desarrolladas en la comunidad del software libre, algo que nos demuestra que el software libre está a la par del software de pago.

Con estas actividades se adquirieron las habilidades y destrezas necesarias para gestionar y administrar un entorno ti con Linux. Encontramos muchas herramientas que permiten interactuar con las redes de Windows NT, sin problema alguno y configuraciones de servidores usando Zentyal.

## RECONOCIMIENTOS

Muchas gracias a los ingenieros YERMAN AUGUSTO HERNANDEZ y a DANIEL ANDRES GUZMAN, por darnos la oportunidad de aprender muchas cosas en este curso y ponerse en la tarea de enseñarnos para ser mejores profesionales.

## REFERENCIAS

[1] Zentyalorg. (2018). Zentyalorg. Recuperado el 19 de Mayo, 2018, Obtenido de https://doc.zentyal.org/2.2/es/appendix-b.html

[2] Wordpresscom. (2016). 4sysadmins. Recuperado el 19 de Mayo, 2018, Obtenido de https://nebul4ck.wordpress.com/2016/07/10/configurar-cliente-openvpn-linux/.

[3] Zentyal Community. (2017). Instalación de Zentyal. [Wiki]. Tomado de: https://wiki.zentyal.org/wiki/Es/5.1/Instalacion

[4] D. del Barrio. (2012). Firewall Zentyal. El Taller del Bit. Tomado de: http://eltallerdelbit.com/firewall-zentyal

[5] El manual del Administrador de Debian. (s.f.). Firewall o el filtrado de paquetes. Tomado de: https://debian-handbook.info/browse/es-ES/stable/sect.firewall-packet-filtering.html