

**INFORME FINAL DE HABILIDADES PRÁCTICAS DIPLOMADO DE  
PROFUNDIACION EN LINUX.**

**JOHAN ANDRÉS BOLAÑOS PUENTES.**

**INFORME DE HABILIDADES PRÁCTICAS DIPLOMADO DE  
PROFUNDIZACIÓN CISCO EN LINUX**

**DAVID ALBERTO CASTAÑO ALDANA  
TUTOR DIPLOMADO DE PROFUNDIZACIÓN LINUX**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD  
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS.  
BOGOTA DC.  
2019**

# Contenido

Introducción.....	4
1. Desarrollo De Escenarios .....	5
1.1 Escenario 1.....	5
1.2 Escenario 2.....	13
1.3 Escenario 3.....	17
1.4 Escenario 4.....	21
Conclusiones. ....	25
Referencias Bibliograficas. ....	26

## **Resumen.**

GNU / LINUX es un sistema de licencia libre, siendo una de sus características, permitir a los usuarios acceder a sus funcionalidades sin que eso implique una transacción comercial. Al ser de código abierto, Linux puede ser modificado por los mismos usuarios, para ser mejorado y especializado y de esta manera atender las necesidades en los diferentes entornos y ramas de la ingeniería. Este sistema operativo tiene herramientas de multiprocesamiento y multitarea, que permiten ofrecer ductilidad y versatilidad en funciones de seguridad, haciendo que se pueda aplicar a cualquier dispositivo informático. En el desarrollo del diplomado se enfoca su manejo sobre distintas distribuciones tanto de servidores como de equipos de escritorio que ofrecen diferentes funcionalidades, servicios como: manejo de información, transferencia de datos, servicios web, seguridad informática, firewall, proxy, entre otros. Otra de las ventajas de estos sistemas de código abierto, es que su desarrollo es acompañado de documentación robusta que permite a sus usuarios entender su funcionamiento. En el desarrollo de las actividades propuestas se identificarán los servicios utilizados, las ventajas y potencial que se puede tener, al saber administrar los diferentes servicios sobre las distribuciones de Linux.

## **Introducción.**

En la actualidad los sistemas informáticos con sistema operativos Linux han evolucionado contando con altos estándares de seguridad, complejidad y especificaciones técnicas que permiten efectuar diferentes funcionalidades, es por lo tanto que a través de diferentes ejercicios planteados se pretende complementar los conocimientos, garantizando así la adquisición de destrezas. Todo esto se lleva a cabo con el material indicado por la universidad, logrando así que tome una importancia para el estudiante conocer estos procedimientos, conceptos y terminología empleada.

# 1. Desarrollo De Escenarios

## 1.1 Escenario 1.

Implementación y configuración detallada bajo Zentyal Server del acceso de una estación de trabajo GNU/Linux Ubuntu Desktop a través de un usuario y contraseña, así como también el registro de dicha estación en los servicios de Infraestructura IT de Zentyal.

Iniciar sesión con las credenciales establecidas.



Figura 1. Inicio de sesión

Ingresar la licencia de activación.



Figura 2. Clave de activación Trial

Apertura configuración inicial



Figura 3. Pantalla de configuración inicial

Selección de los módulos que queremos instalar



Figura 4. Módulos Zentyal

Iniciar la instalación de los módulos



Figura 5. Instalación módulos

Elección de la opción de ip static.



Figura 6. Configuración de IP

Ingresar el nombre al dominio



Figura 7. Configuración de dominio

Habilitación de los servicios

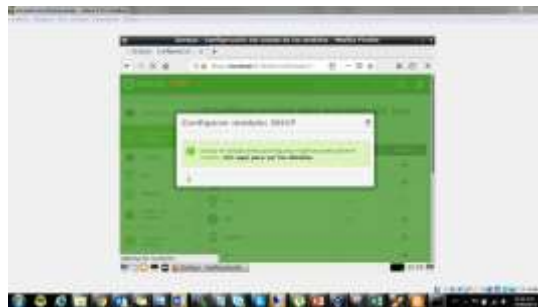


Figura 8. Habilitación de módulos

Es necesario realizar algunos cambios en la configuración de las tarjetas de red en Virtual-Box.

El primer cambio es dejar el adaptador 1 como NAT



Figura 9. Configuración tarjeta de red

El segundo cambio es dejar el adaptador 2 como red interna



Figura 10. Configuración tarjeta de red

Después de efectuar la configuración de los adaptadores se procede a configurar el servicio DHCP en el servidor.

Para ello se debe dejar el adaptador eth0 por DHCP



Figura 11. Configuración eth0

El adaptador eth1 se le va a asignar una IP fija



Figura 12. Configuración eth1



Asignación de rangos en el módulo DHCP.



Figura 13. Asignación de rangos DHCP

Realizando estos cambios, se observa el equipo asignado por DHCP



Figura 14. Evidencia equipo Ubuntu DHCP

Una vez realizada la configuración del DHCP y de realizar todas las validaciones se procede a validar que nuestro dominio este correctamente configurado.



Figura 15. Validación dominio

Validación desde una maquina con Ubuntu que responda nuestro servidor con Zentyal

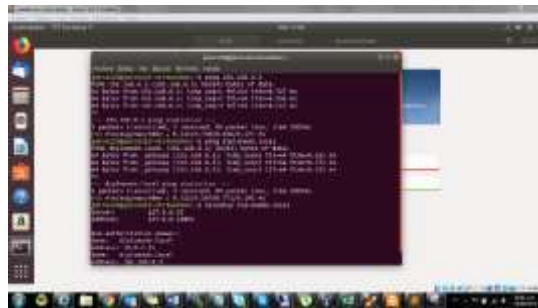


Figura 16. Ping al servidor Zentyal desde Ubuntu desktop

Validación de las configuraciones del DNS



Figura 17. Validación DNS

Después de esto se procede con la creación del usuario AD

Ingreso a pestaña Usuarios y equipos – añadir usuario



Figura 18. Creación usuario AD

Se debe llenar los datos que aparecen allí y dar clic en Añadir, después de esto el usuario quedara creado, importante: se debe añadir al grupo de administradores.



Figura 19. Validación de usuario creado

*Nota: Se deben guardar todos los cambios realizados*

Una vez creado el usuario en el Directorio Activo, se procede a unir la maquina con Ubuntu al dominio. Para esto se necesita instalar PBIS el cual nos permitira agregar la maquina al Zentyal.

Se realiza la descarga del agente



Figura 20. PBIS descargado

Se procede a instalar, para ello se debe dar permisos con el comando: `$ sudo chmod a+x pbis-open-8.2....` después si ejecutamos el comando `$ sudo ./pbis-open-8.2.1.2979.linux.x86_64.deb.sh`

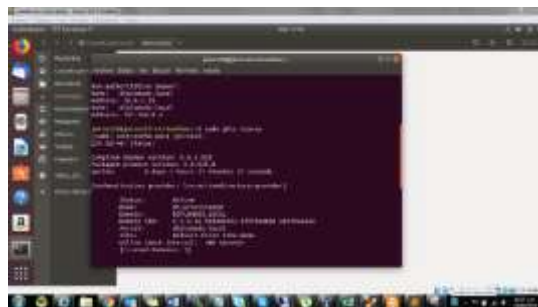


Figura 21. Instalación de PBIS en Ubuntu

Se procede a unir el Ubuntu al dominio con el comando `sudo /opt/pbis/bin/domainjoin-cli join diplomado.local Administrator@movich.local`

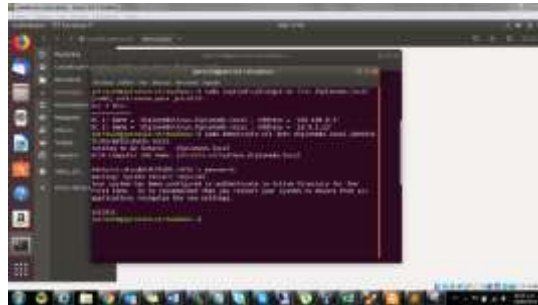


Figura 22. Evidencia equipo añadido al dominio

*Nota: Se puede evidenciar que esta añadido al dominio, ahora debemos reiniciar la máquina para que se apliquen los cambios.*

Para finalizar validamos el inicio de sesión en la maquina con Ubuntu

Ingresar con el usuario creado



Figura 23. Validación de usuario creado

- Ingreso los datos de inicio.



Figura 24. Ingreso de usuario de dominio en Ubuntu

Validación del acceso exitoso.



Figura 25. Validación de acceso exitoso

## 1.2 Escenario 2.

Implementación y configuración detallada bajo Zentyal Server del 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.

Portal de gestión Zentyal



Figura 26. Ingreso portal Zentyal.

A través de este entorno web se puede hacer la instalación del Proxy HTTP.



Figura 27. Instalación proxy HTTP.

Luego de la instalación se procede al dashboard para hacer la configuración del proxy http y se selecciona la opción "General Settings"



Figura 28. Instalación proxy HTTP.

El sistema indica que el modulo http proxy esta desactivado y nos la opción de hacer la activación



Figura 29. Verificación proxy HTTP.

Una vez el proxy es habilitado se continúa con la configuración de las reglas para el acceso a contenidos en internet, tales como:

- En el campo periodo de tiempo se especifica en qué momento se aplicara la regla
- En el campo decisión seleccionamos se aplicará a los miembros de un Objeto de Zentyal o a cualquier tipo de tráfico que atraviese el proxy.
- En el campo decisión, existen 3 opciones de selección, permitir todo, denegar todo y aplicar filtros, seleccionamos esta.
- Seleccionamos el perfil de "Filter profiles " le damos un nombre al filtro que vamos configurar

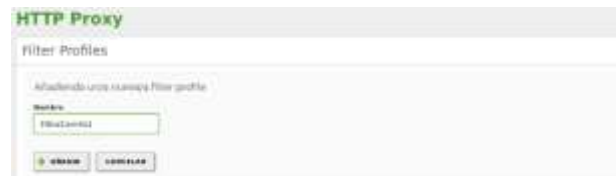


Figura 30. Perfiles de filtrado.

Seleccionar una opción de configuración, así mismo el sistema nos avisara que el módulo de antivirus debe ser activado para poder usarlo.



Figura 31. Configuración de Perfiles de filtrado.

Configuración de las páginas a establecer, junto con la decisión de permitir o denegar el acceso.



Figura 32. Configuración de dominio.



Figura 33. Configuración de dominio.



Figura 34. Configuración de dominio.

Verificación de la configuración realizada.



Figura 35. Verificación de la configuración de dominios.

Aplicación del filtro a las reglas de acceso.



Figura 36. Aplicación filtro.

Pruebas sobre navegador en desktop y configuración sobre el navegador Mozilla del desktop el proxy configurado con la dirección ip y el puerto 3128.



Figura 36. Aplicación filtro.



Pruebas sobre las páginas web configuradas.



Figura 37. Verificación de webs configuradas.

### 1.3 Escenario 3.

Implementación y configuración detallada bajo Zentyal Server para la restricción de la apertura de sitios o portales Web de entretenimiento y redes sociales, evidenciando las reglas y políticas creadas. La validación del Funcionamiento del cortafuego aplicando las restricciones solicitadas, se hará desde una estación de trabajo GNU/Linux Ubuntu Desktop.

Configuración inicial Zentyal.



Figura 38. Configuración inicial Zentyal.

Panel de Configuración Zentyal.



Figura 39. Panel de Configuración Zentyal.

Selección de paquetes a instalar.



Figura 40. Paquetes a instalar.

Selección interfaz red.



Figura 41. Selección interfaz de red.

Finalización de la instalación y configuración de componentes.



Figura 42. Finalización proceso de instalación.

Agregar los objetos con las IP de los sitios a bloquear.



Figura 43. Agregación de objetos IP.

A cada objeto se le agregan Miembros, en los cuales se especifican la IP y la máscara de subred.



Figura 44. Agregación Miembros dentro de objetos IP.

Selección Cortafuegos y filtrado de paquetes.



Figura 45. Sección de firewall.

Selección reglas de filtrado para redes internas.



Figura 46. Sección de firewall.

Creación de las reglas de filtrado.

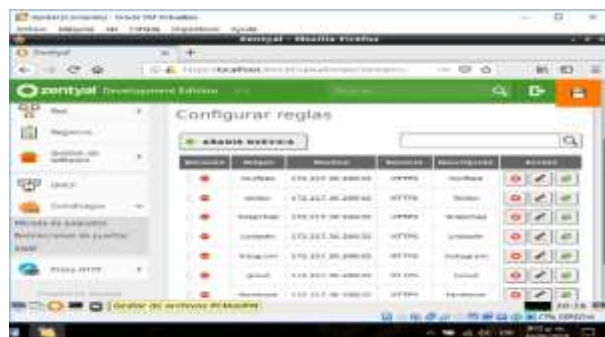


Figura 47. Reglas de filtrado.

**Nota:** En las reglas creadas se estipula que se deniega el servicio por HTTPS a las ips de los sitios seleccionados, posterior a esto re direcciona a la ip de Google.com (172.217.30.206)

Verificación desde maquina con sistema operativo Ubuntu.



Figura 48. Reglas de filtrado.

Verificación desde maquina con sistema operativo Ubuntu.



Figura 49. Verificación filtrado.

## 1.4 Escenario 4.

Implementación y configuración detallada bajo Zentyal Server 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

File Server y Print Server

Ingresar a la opción de compartición de ficheros y damos clic en Añadir Nuevo



Figura 50. Añadir Nuevo fichero

Ingresar los datos para crear el archivo que queremos compartir y damos clic en añadir.



Figura 51. Ingreso de datos

Una vez creado se accede a control de acceso



Figura 52. Configuración control de acceso



Figura 53. Control de acceso creado

Damos clic sobre añadir nuevo y después seleccionamos el usuario y los permisos que deseamos dar.

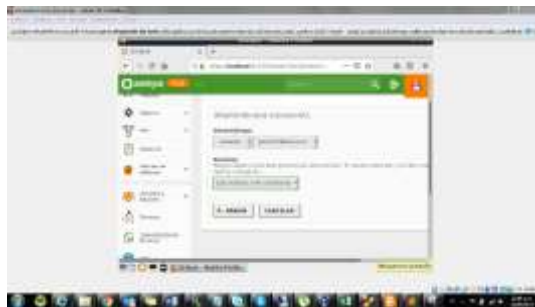


Figura 54. Asignación de permisos

Guardar configuración.



Figura 55. Guarda cambios

Validación del acceso a la carpeta creado desde el equipo Ubuntu

Se ingresan los datos `smb://192.168.0.3/` y se procede a conectar



Figura 56. Evidencia acceso carpeta compartida



## **Conclusiones.**

- Mediante el desarrollo de esta actividad se me permitió el correcto análisis e identificación del contenido del curso y sus temáticas, de acuerdo a las indicaciones dadas.
- Se logra la correcta realización de los requerimientos planteados, enfocados en interpretar, identificar, aplicar y aprender en forma clara el Afinamiento de contenidos sobre GNU/Linux y el alistamiento del server para aplicar lo aprendido en el diplomado.
- Al analizar la temática planteada se puede obtener un análisis que ha permitido generar un espacio crítico y de aplicación en este tipo de procesos.
- Mediante el desarrollo de esta actividad se me permitió la correcta implementación de las terminologías necesarias en este entorno.

## Referencias Bibliograficas.

- Módulo del curso de Diplomado De Profundización En Linux (Opción De Trabajo De Grado). UNAD. Bogotá. D.C. Consultado De: <https://campus01.unad.edu.co/ecbti46/course/view.php?id=115>
- Lopez Sanches, M.J & Belle, S., & Auli, F. (2008). Sistema operativo GNU/Linux básico, ES: Universitat Oberta de Catalunya, Recuperado de <http://hdl.handle.net/10609/189>
- Antonio, P. (2009). Administración de Sistemas GNU/LINUX, Fundación Código Libre Dominicano. Recuperado de <http://www.mclibre.org/descargar/docs/manual-fclid/perpinan-gnu-linux-administracion-200307.pdf>
- Josep, J. E., & Remo, S. B. (2007). Administración avanzada de GNU/Linux. Universitat Oberta de Catalunya – UOC. Recuperado de <http://hdl.handle.net/10609/226>
- Garcia, J. & Perramont, X. (2007), Aspectos avanzados de seguridad en redes. Universitat Oberta de Catalunya – UOC. Recuperado de <http://hdl.handle.net/10609/204>