

Debatir, Generar, Determinar e Implementar Soluciones GNU/Linux.

Jhonatan Gonzalez Velez
e-mail: jhogove@hotmail.com
Ricardo Augusto Castañeda Gutiérrez
e-mail: ricardocasta@misena.edu.co
Rainer David Buevas
e-mail: rdbuevas@live.com
Deisy Liliana Cataño
e-mail: dailu469@hotmail.com
Dairon Jeffrey Jaimes
e-mail: daijemen@gmail.com

Resumen: El presente trabajo aprovecha los conocimientos previos a través del diplomado y nuevos conocimientos adquiridos por medio de investigaciones propias, que permitieron el desarrollo de las distintas temáticas planteadas sobre una plataforma GNU/Linux Zentyal Server 5.0, con lo cual se obtuvo un mayor conocimiento en el área y la solución de una problemática planteada como Ingenieros en Sistemas.

Palabras Clave: GNU/Linux, Open Source, Servicios de Red, Zentyal Server.

1 Introducción

El Sistema Operativo de Ubuntu es un sistema operativo basado en GNU/Linux, distribuido como software libre, el cual incluye su propio entorno de escritorio denominado Unity, orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario. Está compuesto de múltiple software normalmente distribuido bajo una licencia libre o de código abierto.

Zentyal Server, es una solución basada en Ubuntu LTS que incorpora todos los servicios de red requeridos en un entorno comercial pequeño y mediano. Tiene como software integrado; Samba, Postfix, Dovecot, Fetchmail, Sieve, SOGo, SOGo ActiveSync, Amavis, ClamAV, SpamAssassin, Iproute2, Netfilter, Squid, BIND, ISC DHCP Software, ntpd, OpenSSL, OpenVPN e ejabbered.

El presente trabajo que corresponde a la evaluación final se enfoca en el afinamiento de contenidos sobre GNU/Linux, aprovechando conocimientos previos a través del diplomado y nuevos conocimientos por medio de investigaciones propias, que permitieron el desarrollo de las distintas temáticas de DHCP Server, DNS Server, Controlador de Dominio, Proxy no transparente, Cortafuegos, File Server, Print Server y VPN, sobre una plataforma GNU/Linux Zentyal Server 5.0.

2 Temática 1: DHCP Server, DNS Server y Controlador de Dominio

Para el cumplimiento de esta temática, y continuación de la implementación de los servicios de DHCP, DNS y controlador de dominio, inicialmente se realizó la instalación

La distribución Zentyal Server, haciendo uso de la herramienta VirtualBox, teniendo como sistema anfitrión Ubuntu desktop, adicional a la instalación del servidor, se montó 3 máquinas adicionales con sistemas operativos, Ubuntu desktops, Ubuntu Server y Windows 7, esto con el fin de validar el correcto funcionamiento del servidor en una red interna.

La instalación del servidor no fue complicada gracias a que en la página oficial de Zentyal al igual que en otros portales se encuentra, mucha información acerca de esta distribución la cual detalla el paso a paso en el montaje del sistema operativo y resolución de problemas que puedan presentarse.



Figura 1. Interfaz de acceso al dashboard de Zentyal server, primera imagen al iniciar el servidor luego de la instalación.

Entre los pasos más importantes en el desarrollo de la actividad podemos ilustrar los siguientes:

Configuración inicial del servidor: como primer paso después de la instalación del servidor, se realizó la configuración básica, en donde podemos seleccionar los paquetes que queremos instalar, realizar configuración de zona horaria, configuración de las tarjetas de red entre otros parámetros

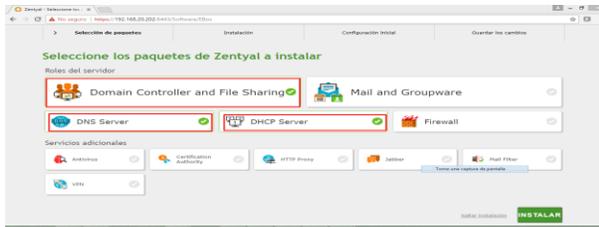


Figura 2. Instalacion de paquetes en el servidor zentyal.

Luego de la configuración de Zentyal continuamos con la instalación y configuración del servicio de DHCP, para lo cual esta distribución provee un completo asistente de configuración el cual permite la creación de rangos DHCP, asignación de IP reservados y todas las utilidades y características avanzadas de un servidor DHCP, el correcto funcionamiento de este servicio se pudo validar en la red interna creada para tal fin, donde se realizó pruebas de asignación de IP de forma automática y validación de ping entre las maquinas clientes y el servidor.

```
rainer-buelvas@localhost:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.338 ms
^C
--- 192.168.10.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.338/0.517/0.696/0.179 ms
rainer-buelvas@localhost:~$
```

Figura 3. Validación de conectividad entre la maquina cliente con S.O Ubuntu y el servidor Zentyal.

Otro de los servicios instalado fue el DNS, el cual resulta de gran importancia en una red local, para poder hacer uso de otros servicios como páginas web, ftp, SSH utilizando el nombre de las maquinas o alias que se designe para cada servidor, dejando que el servidor DNS se encargue de traducir a sus respectivas direcciones IP, una de las utilidades o herramientas que encontré en el paquete DNS server de Zentyal es la opción de DNS dinámico, que es de gran ayuda para que se cuente con el registros de todas las maquinas que estan en la red inmediatamente se les asigne configuración de tarjeta por DHCP.

```
rainer-buelvas@ubuntu:~$ ping zentyal
PING zentyal.zentyal5.local (192.168.10.1) 56(84) bytes of data:
64 bytes from zentyal.zentyal5.local (192.168.10.1): icmp_seq=1 ttl=64 time=0.760 ms
64 bytes from zentyal.zentyal5.local (192.168.10.1): icmp_seq=2 ttl=64 time=0.885 ms
^C
--- zentyal.zentyal5.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 0.760/0.822/0.885/0.068 ms
rainer-buelvas@ubuntu:~$
```

Figura 4. Validación del funcionamiento del servidor DNS por medio de la utilidad ping al nombre del servidor desde una maquina cliente.

Continuando con la actividad se realizó instalación y configuración del controlador de dominio, siendo este uno de los servicios más complejos de los trataron en

esta temática, básicamente mi tarea con este servicio consistió en agregar maquinas clientes y luego validar que los usuarios se pudieran autenticar utilizando las credenciales establecidas previamente en el módulo de usuarios del controlador de dominio.

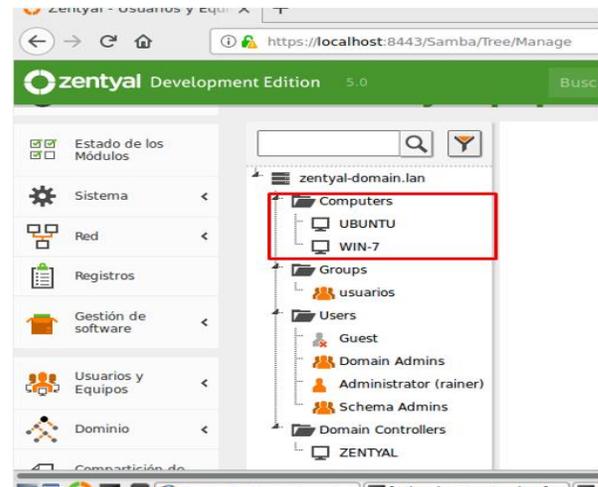


Figura 5. Listado de maquinas clientes inscritas en el dominio zentyal-domain.lan

3 Temática 2: Proxy No Transparente

Se descargó de la página oficial el archivo .iso y en VirtualBox se crea una máquina virtual personalizada, en esta a diferencia de otras se configura 2 tarjetas de red, una para acceso externo y otra interno.

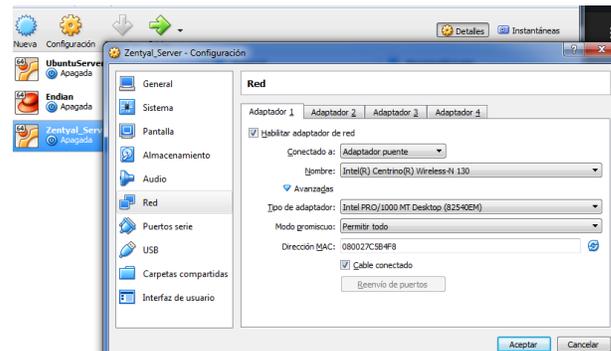


Figura 6. Configuración de las tarjetas de red en la maquina virtual.

Posterior en almacenamiento se configura para que inicie desde el archivo .iso Seguimos las diferentes opciones que se nos permite y según necesitemos, entre ellas idioma, país, configuración del teclado, el sistema detecta las tarjetas de red que configuramos e inicia a configurar la primera para acceder a la red externa y descargar los diferentes complementos y actualizaciones necesarias, también se configura el nombre al equipo y creamos nuestro usuario administrador.

A esta instalación el sistema se reinicia y al volver a cargar automáticamente se habrá una página web donde podemos realizar las diferentes configuraciones, esta nos pide usuario y contraseña que son las que inicialmente creamos.



Figura 7. Sistema Zentyal ya instalado y solicitando usuario para empezar a configurar los complementos.

Luego de ingresar y para configurar lo que requerimos vamos a instalar los diferentes complementos o módulos necesarios

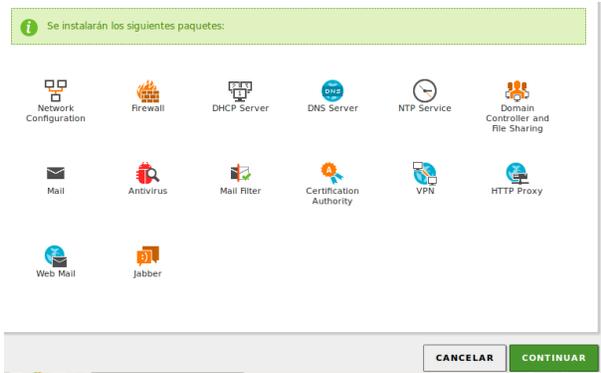


Figura 8. Módulos seleccionados para instalar.

Posterior a la instalación de estos complementos procedemos a configurar las tarjetas de red.

Interfaces de Red



Figura 9. Configurando la red.

También configuramos nuestro dominio para posterior entrelazar los diferentes equipos y sistemas operativos que queremos actúen los servicios y proxy que configuremos en nuestro servidor Zentyal.



Figura 10. Nombre del dominio que se configuro.

Al terminar de configurar podemos realizar actualizaciones en el sistema, estas las podemos trabajar desde nuestra consola de comandos ejecutando los comandos: **Sudo apt-get update** y **Sudo apt-get upgrade**

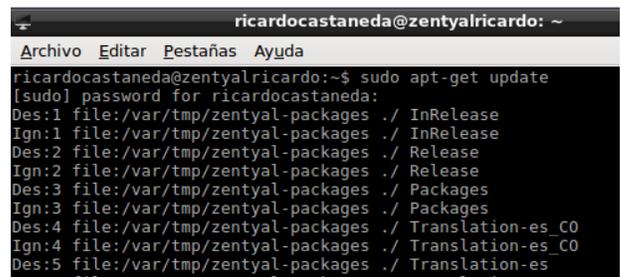


Figura 11. Ejecución de comandos para actualizar sistema

Para configurar nuestro Proxy Transparente debemos inicialmente instalar y configurar otros módulos como DHCP.



Figura 12. Se confirma módulo instalado y se inicia configuración.

Empezamos configurando nuestra red interna, asignamos un nombre y un rango de direcciones, aceptamos y guardamos los diferentes cambios que realizamos.



Figura 13. Nombre y asignación de IP límites al rango.

Procedemos a configurar nuestros cortafuegos para tener acceso al servicio DHCP siguiendo los diferentes pasos.



Figura 14. Configuración del paquete que permite el acceso al servicio DHCP.

Siempre a cada configuración realizada damos guardar, confirmamos que queden los cambios regresando a la página principal. Ahora para configurar el Proxy vamos al servicio y seleccionamos Transparent Proxy, si requerimos

podemos cambiar los puertos, aquí podemos dejar el requerido en la temática, guardamos los cambios. Posterior procedemos a crear un perfil añadiendo una configuración, el nivel de restricción, en la parte de Dominios y URLs podemos especificar los accesos o contenidos a bloquear.



Figura 15. Habilitando el Proxy y cambiando el puerto.

Damos en cambiar y colocamos la URL o contenidos, aceptamos y guardamos los cambios.

Domains and URL rules



Figura 16. Ejemplo donde se bloquea el acceso a una página.

Posterior configuramos el proxy en las maquinas dentro del dominio y confirmamos acceso a la red, pero sin poder ingresar a las páginas que configuremos o bloqueemos, esto buscando seguridad a la información o encaminar el objetivo del uso de los equipos.

4 Temática 3: Cortafuegos

I. Resumen.

A continuación, se presentará en el presente artículo la instalación y puesta en funcionamiento del servidor Zentyal, el cual es un servidor de red unificada de código abierto, para la presente temática # 3 puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (Gateway), gestionando las amenazas de seguridad.

En el presente trabajo, inicialmente veremos cómo gestionar la instalación del servidor Zentyal y cómo este puede realizar una restricción de contenidos y paginas para la apertura de sitios no deseados mediante reglas y políticas generadas.

II. Objetivos

- Realizar la instalación del servidor Zentyal.
- Realizar la restricción de sitios por medio de Zentyal.
- Realizar la validación del correcto funcionamiento de las reglas y políticas

III. Informe de contenidos

Inicialmente veremos cómo realizar la instalación del servidor Zentyal. La forma ideal de instalar Zentyal en una máquina nueva desde cero es utilizar el instalador de CD personalizado. Este CD contiene Zentyal y todas sus dependencias. La versión 5.0 está basada en Ubuntu Server 16.04 64bit.

IV. Procedimiento

Después de que Zentyal finalice toda su instalación Y después de haber reiniciado el servicio finalmente nos aparecerá el panel principal:

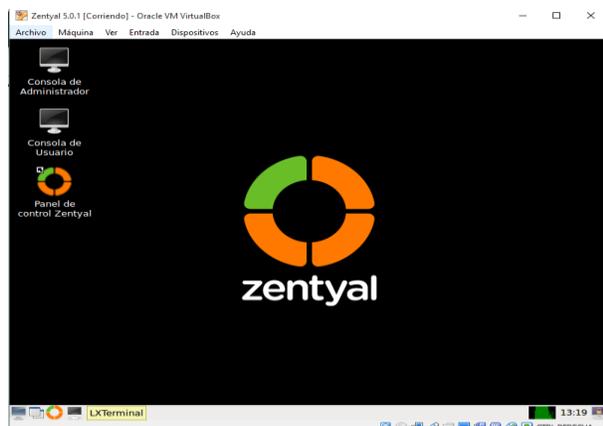


Figura 17. Escritorio Zentyal Server.

Iniciamos el servicio con nuestro usuario y contraseña creada desde el home del servidor.

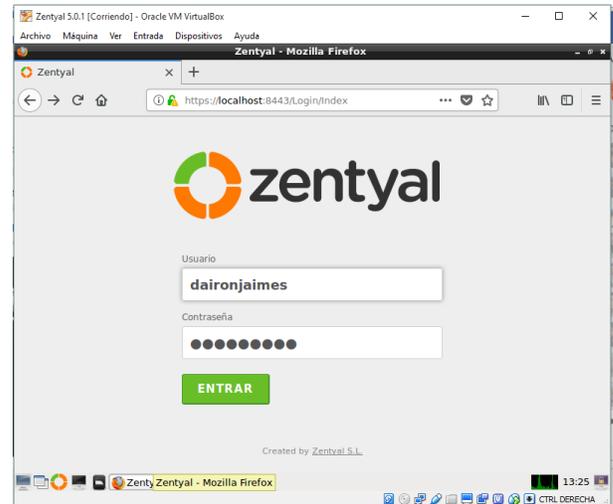


Figura 18. Login Zentyal Server.

Ahora seleccionamos los servicios requeridos para nuestros servicios:

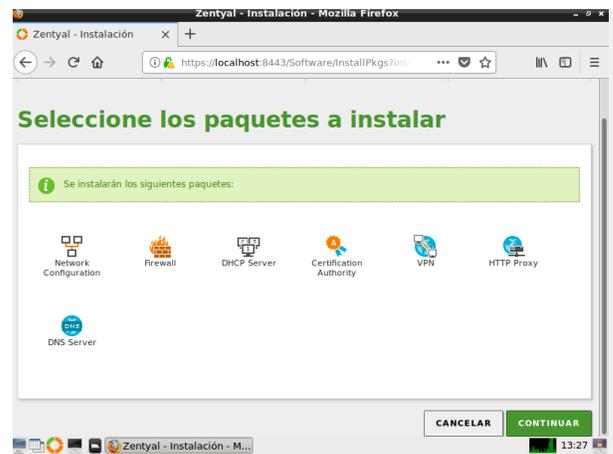


Figura 19. Instalación Zentyal Server.

La mejor opción es crear un objeto con las direcciones de los dominios de Facebook y bloquear el acceso al servicio https de esos dominios desde cualquier equipo de mi red corporativa. A pesar de que, me tomo bastante tiempo encontrar los dominios principales de Facebook.

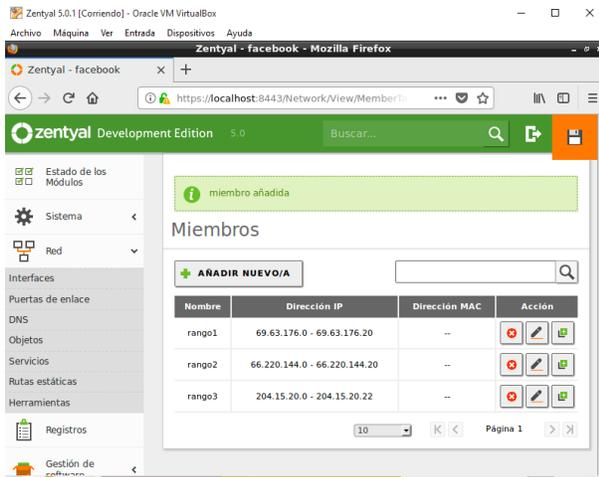


Figura 20. Miembros.

Ahora realizamos las siguientes acciones:

- Crear (si no está ya creado) un servicio https con los puertos 443
- Crear una regla en el firewall que combine los dos elementos anteriores

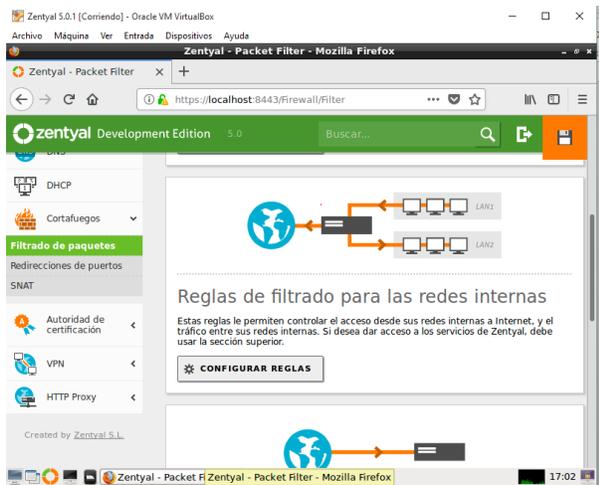


Figura 21. Reglas de filtrado.

Ahora configuramos el objeto "Facebook" en la regla:

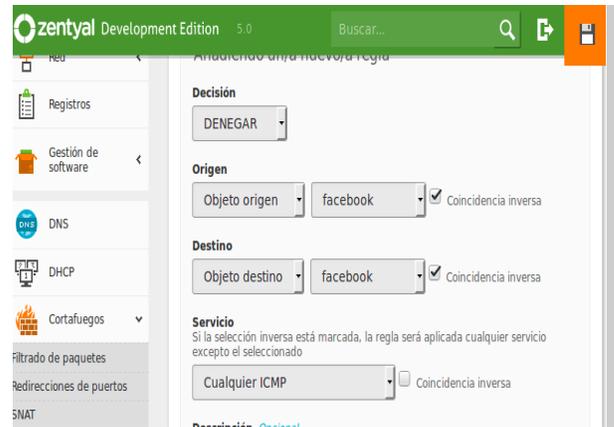


Figura 22. Objeto Facebook.

Ahora guardamos los cambios:

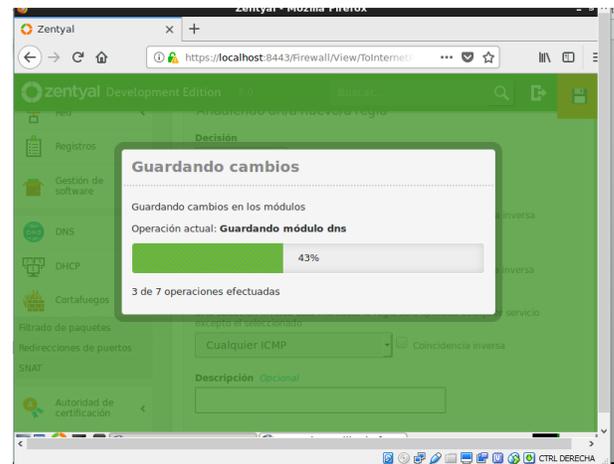


Figura 23. Guardado de cambios.

Posteriormente se deniegan acceso por protocolos en tráfico a la página de Facebook:

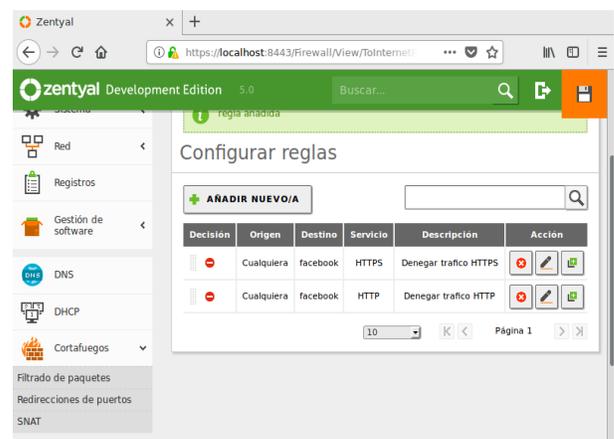


Figura 24. Denegación acceso.

5 Temática 4: File Server y Print Server

En esta temática se busca 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.

Para el desarrollo de esta temática es necesario instalar en Zentyal los siguientes módulos: Controlador de Dominio y Compartición de ficheros y DNS.

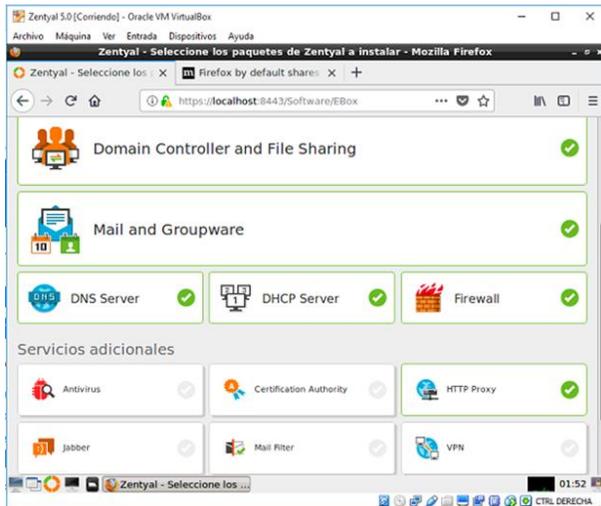


Figura 25. Instalación de módulos.

Antes de iniciar la configuración del File Server es necesario verificar la conectividad entre nuestro servidor Zentyal y la máquina cliente de Ubuntu. Desde Ubuntu hacemos un ping a la dirección 102.168.10.1.

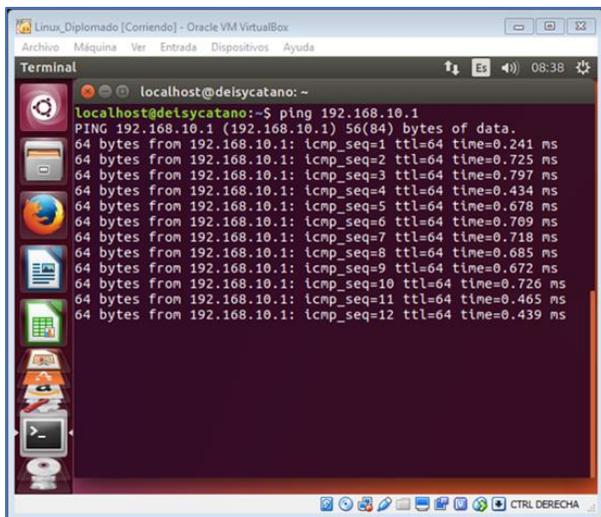


Figura 26. Conectividad.

Luego Configuramos el controlador de En Linux se utiliza el protocolo LDAP que funciona como Active Directory.

En la configuración del Dominio, es importante habilitar la opción de perfiles móviles, para que un usuario se pueda conectar en la red en cualquier equipo.



Figura 27. Configuración de dominio.

Agregamos el equipo cliente – Ubuntu al dominio.

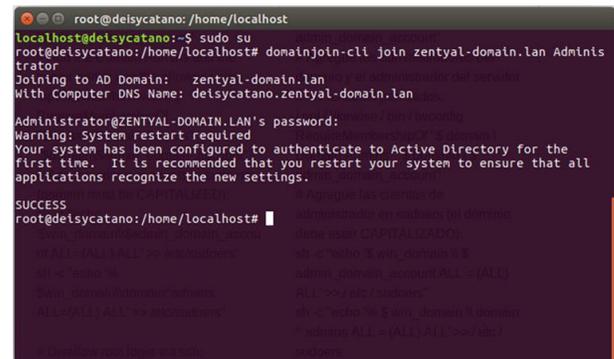


Figura 28. Cliente al dominio.

Esperamos que nos aparezca al mensaje SUCCESS y reiniciamos la máquina para que tome los cambios. Verificamos en Zentyal que ya el equipo este asociado al Dominio.

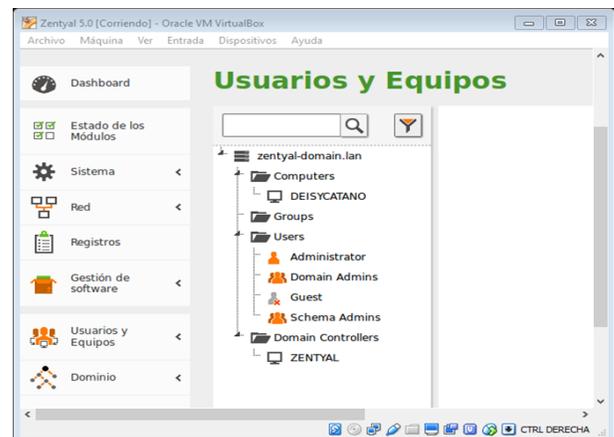


Figura 29. Verificación del dominio.

File Server. Seleccionamos el módulo **Compartición de Ficheros.**

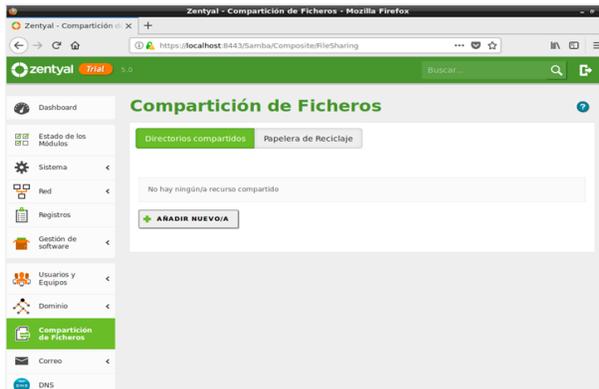


Figura 30. Compartición de archivos.

En Directorios compartidos añadimos uno nuevo y lo habilitamos, indicamos el nombre del recurso compartido y la ruta. Añadir. Luego Guardamos Cambios.

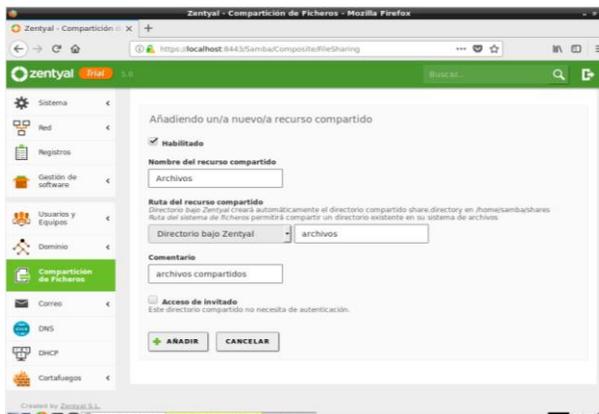


Figura 31. Adición de nuevo recurso.

Luego vamos a Control de Acceso y añadimos uno nuevo. Seleccionamos usuarios y seleccionamos el usuario en este caso dcatanoa y el tipo de permiso (lectura y escritura) y guardamos los cambios.

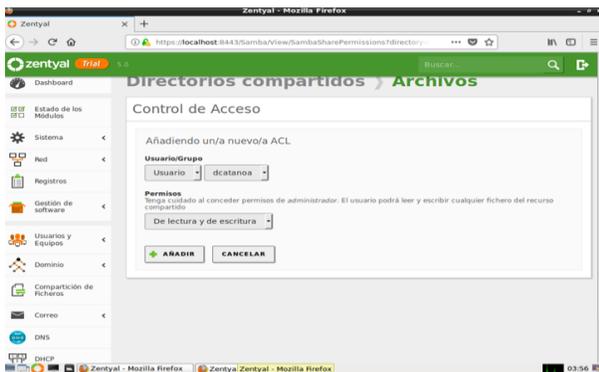


Figura 32. Control de acceso.

En el equipo Cliente – Ubuntu, vamos a la siguiente ubicación `smb://192.168.10.1/Archivos`.

Donde nos solicitan credenciales para la compartición de archivos en 192.168.10.1, digitamos el usuario al que le dimos permisos de lectura y escritura sobre el recurso compartido y el dominio de Zentyal-domain, digitamos la contraseña del usuario. Clic en conectar.

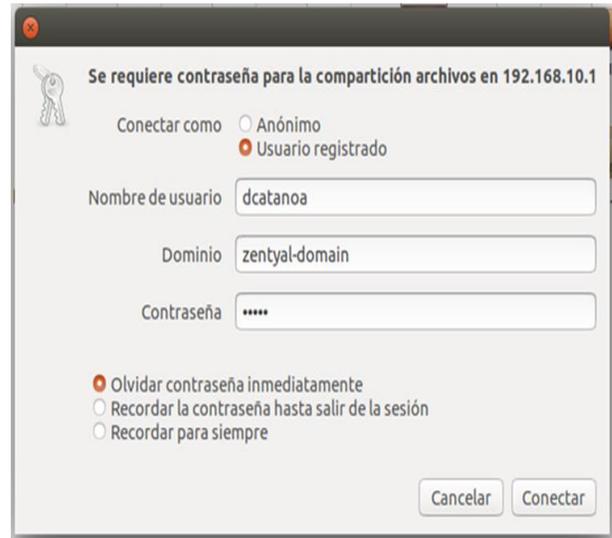


Figura 33. Credenciales.

Verificamos que ya podemos acceder a nuestro recurso compartido desde el servidor.

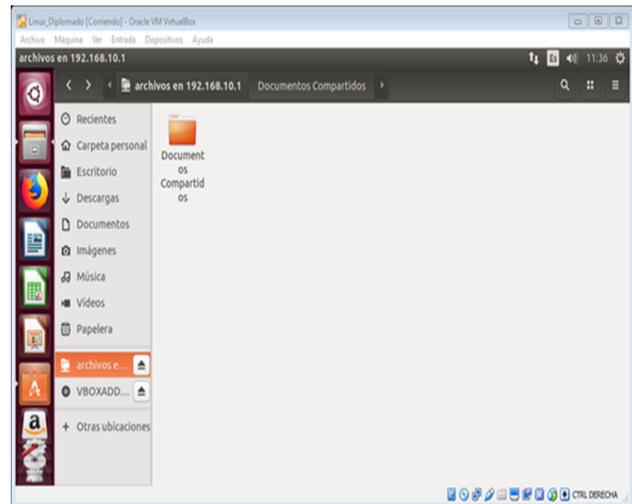


Figura 34. Acceso a recurso compartido.

Es importante tener en cuenta que en la Versión de Zentyal 5.0 ya no viene el módulo para configurar el Print Server.

6 Temática 5: VPN

El objetivo que se desarrollara en esta temática es conectar el sistema anfitrión Windows, con la VPN Zentyal creada, la cual otorgue un acceso a una estación de trabajo en la red virtual LAN que en este caso será un Ubuntu Desktop.

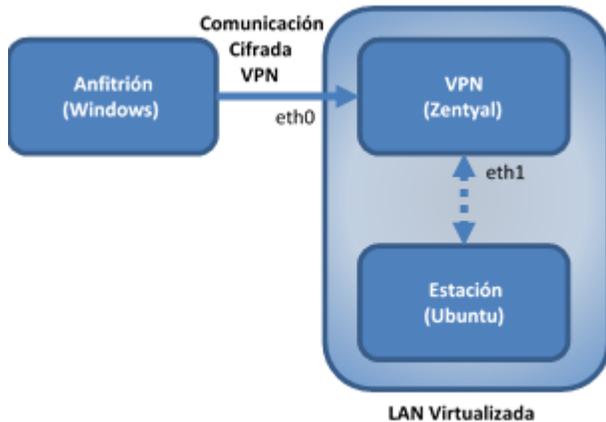


Figura 35. Esquema VPN.

La configuración que se realizará en los Sistemas Operativos es la siguiente:

- GNU/Linux Zentyal Server 5.0 (Virtual)
 - Adaptador 1 (VirtualBox): Adaptador puente (Wifi)
 - IP eth0: 192.168.0.11/24
 - Puerta de enlace eth0: 192.168.0.11
 - Adaptador 2 (VirtualBox): Red interna
 - IP eth1: 192.168.100.1/24
- GNU/Linux Ubuntu Desktop 16.04 LTS (Virtual)
 - Adaptador 1 (VirtualBox): Red interna
 - IP: 192.168.100.2/24
- Microsoft Windows 10 (Anfitrión)
 - IP: 192.168.0.10/24
 - Puerta de enlace: 192.168.0.1

Para comenzar a configurar la VPN, es necesario crear una Autoridad de Certificación y certificados individuales para el servidor VPN y los clientes remotos, sin embargo, es importante tener en cuenta que Zentyal expedirá el certificado del servidor VPN automáticamente cuando se crea un nuevo servidor VPN, actuando Zentyal como una Autoridad de Certificación.

Para esto, en el Tablero de Zentyal se procede a la pestaña Autoridad de certificación – General, y se crea

la Autoridad de Certificación con la siguiente información para luego presionar Crear:

Nombre de la Organización: AutoridadUnad
 Código de país: CO
 Ciudad: Bogotá
 Estado: Cundinamarca
 Días para expirar: 365

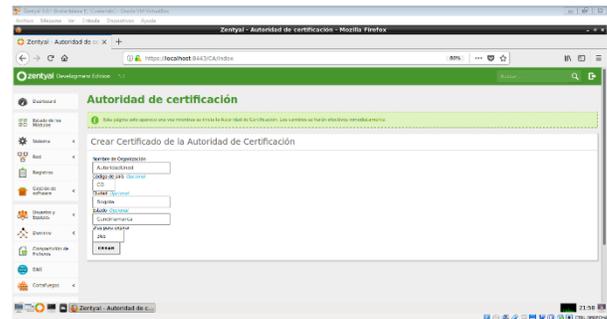


Figura 36. Autoridad de Certificación.

Creada la Autoridad de Certificación, se crea el certificado individual del cliente con la siguiente información para luego presionar Expedir.

Se debe tener en cuenta que el servidor VPN creará automáticamente el certificado individual del servidor.

Nombre común: Jhonatan
 Días para expirar: 365

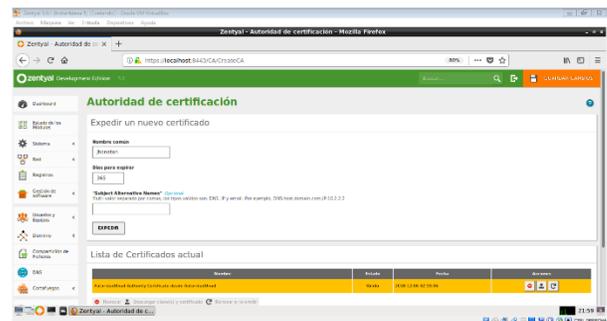


Figura 37. Nuevo Certificado.

D Se presiona Guardar Cambios - Guardar - Ok.

Ahora que ya se tienen los certificados listos, se debe configurar el servidor VPN presionando Añadir Nuevo en la pestaña VPN - Servidores.

Luego se escribe el nombre del Servidor VPN que en este caso será VPN-Jhonatan y se presiona Añadir.

Ya creado el servidor VPN se da clic en el botón de Configuración.

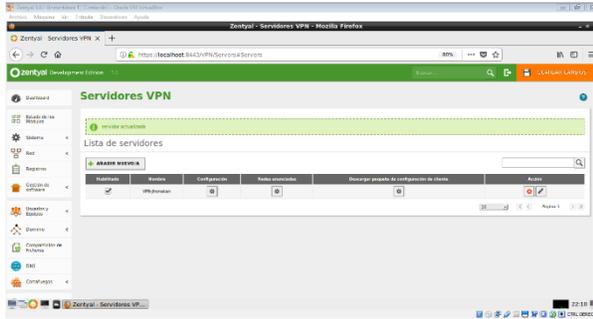


Figura 38. Servidores VPN.

Estando en la configuración de la VPN, se realizan cambios según requerimientos, en el cual para este caso se deja todo por defecto ya que no es necesario realizar modificaciones.

Se presiona Guardar Cambios - Guardar - Ok.

Se regresa a la pestaña VPN - Servidores, donde se da clic en el botón Descargar paquete de configuración de cliente, con el cual, realizando la siguiente configuración se da clic en Descargar.

Tipo de cliente: Windows (Anfitrión)
 Certificado de cliente: Jhonatan
 Dirección del servidor: 192.168.0.11 (IP eth0 de Zentyal)

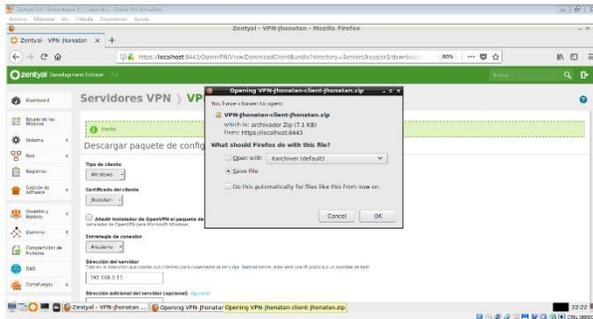


Figura 39. Descarga de Certificados.

Se puede comprobar que el servidor VPN está en ejecución en la pestaña Dashboard.

Una vez configurado el servidor VPN en Zentyal con sus certificados, se procede a verificar la configuración de la terminal de Ubuntu como una estación en la LAN virtual comunicada con la interfaz eth1 de Zentyal.

Para esto, el Adaptador 1 de Ubuntu en la Red de Virtual Box debe estar como Red interna, y configurada la red internamente con la IP 192.168.100.2/24 (eth1 de Zentyal tiene la IP 192.168.100.1/24).

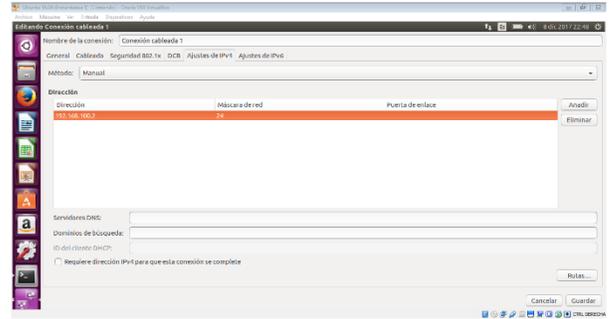


Figura 40. Configuración de Red de Ubuntu.

Se puede comprobar la comunicación de la red LAN virtual entre Zentyal y Ubuntu haciendo comandos ping entre sí.

Ahora que ya se tienen configurados el servidor VPN en Zentyal y la estación Ubuntu en una red LAN virtual, se procede a la configuración del sistema anfitrión de Windows para que este pueda conectarse a la VPN y establecer una comunicación con la estación Ubuntu de la red LAN virtual.

Para esto, se copia en el sistema anfitrión Windows el archivo comprimido que se descargó anteriormente en Zentyal y se descarga e instala el software relacionado a continuación desde las páginas oficiales en el mismo sistema anfitrión Windows.

- OpenVPN (<https://openvpn.net/index.php/open-source/downloads.html>). Herramienta de conectividad basada en el software libre SSL (Secure Sockets Layer) y VPN Virtual Private Network (red virtual privada) que ofrece una conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente.
- Putty (<http://www.putty.org/>). Cliente SSH, Telnet, rlogin, y TCP raw con licencia libre. Disponible originalmente para Windows, ahora también para plataformas Unix, y se desarrolla para Mac OS clásico OS X.
- Xming (<http://www.straightrunning.com/XmingNotes/>). Implementación portátil del sistema de ventanas X para sistemas operativos Microsoft Windows XP, 2003, Vista y 7.

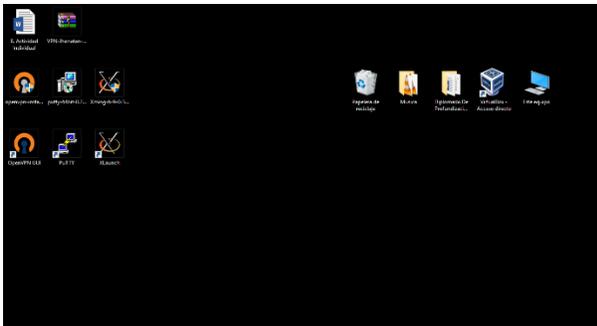


Figura 41. Sistema Anfitrión con Software Instalado.

Luego de realizar las instalaciones, se abre OpenVPN en el sistema anfitrión, y se descomprimen y pegan los certificados descargados en Zentyal en la ruta "C:\Users\usuario\OpenVPN\config" o "C:\Program Files\OpenVPN\config".

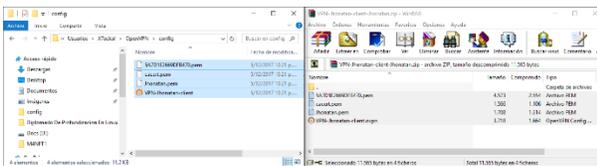


Figura 42. Copiado de Certificados a Putty en Windows.

Luego se da clic derecho en el icono de OpenVPN – Conectar en el área de notificación en la barra de tareas. Lo cual establece una comunicación entre el anfitrión y el sistema Zentyal por VPN. Esto se puede comprobar con el comando en Windows ping -t 192.168.100.2

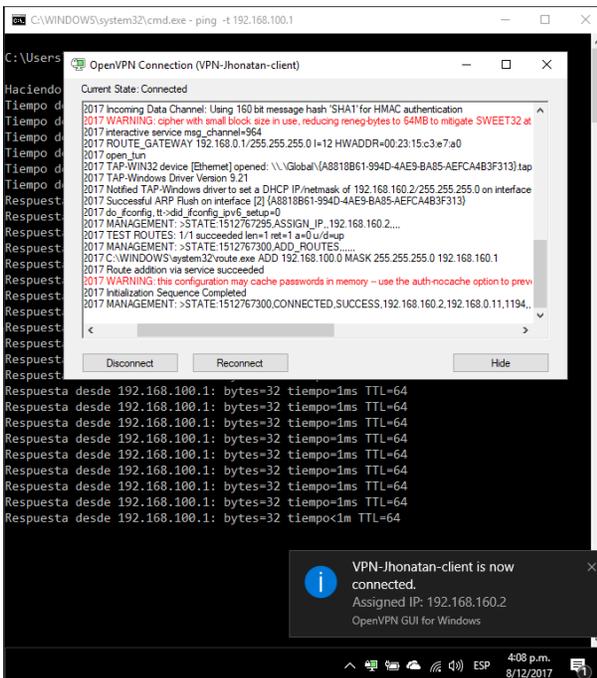


Figura 43. Conexión VPN Windows-Zentyal.

Comprobada la conexión entre las partes, se procede a realizar una conexión por SSH desde el sistema anfitrión Windows a la estación de Ubuntu. (Previa instalación del software OpenSSH-Server en Ubuntu con el comando sudo apt install openssh-server).

Se abre Putty en el sistema anfitrión Windows y en la pestaña Connection - SSH - X11, se activa la casilla Enable X11 forwarding.

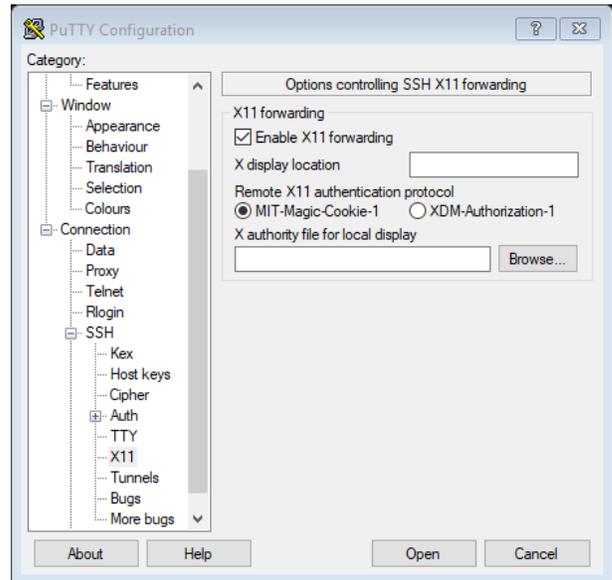


Figura 44. Putty - Enable X11 forwarding.

Ahora en el mismo Putty se procede a la pestaña Session y en Host Name (or IP Address), se coloca la IP de la estación de Ubuntu (192.168.100.2), y se presiona Open.

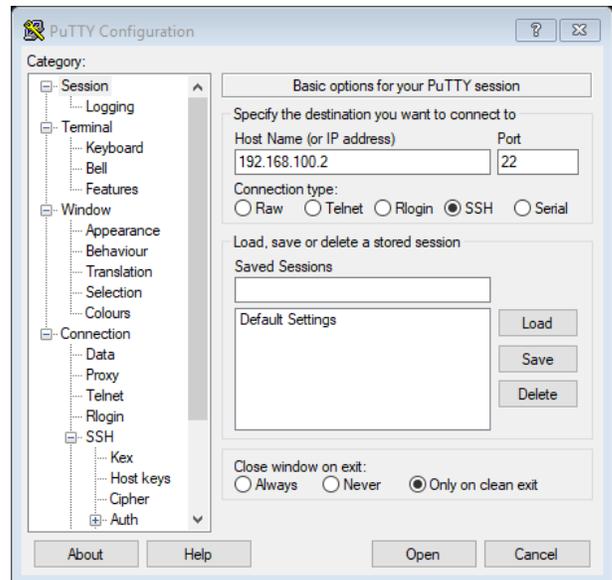


Figura 45. Putty – Conexión SSH Windows-Ubuntu.

Se confirma el mensaje que surge en la conexión, y luego se escribe el usuario y la contraseña del Ubuntu en la terminal que aparece.

Ya habiendo ingresado al sistema Ubuntu por SSH desde el sistema anfitrión Windows, se abre el gestor de archivos Nautilus con el comando Nautilus desde Putty.

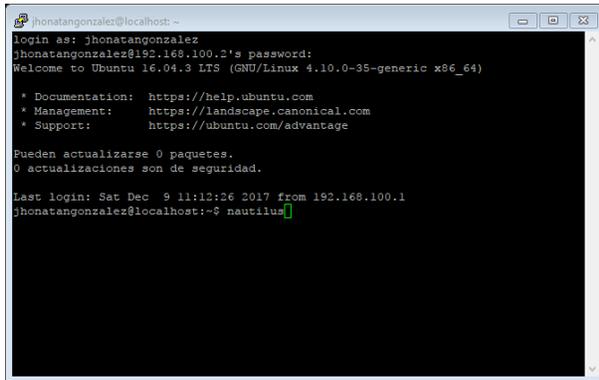


Figura 46. Conexión SSH Windows-Ubuntu.

Con el gestor de archivos abierto, se crea una carpeta en el escritorio del equipo remoto de Ubuntu.



Figura 47. Creación de Carpeta por SSH con Nautilus.

Finalmente, se abre Ubuntu, evidenciando que la carpeta creada remotamente desde SSH en el escritorio se encuentra allí, dando cumplimiento al punto de la temática de evidenciar el ingreso a algún contenido o aplicación de la estación de trabajo.

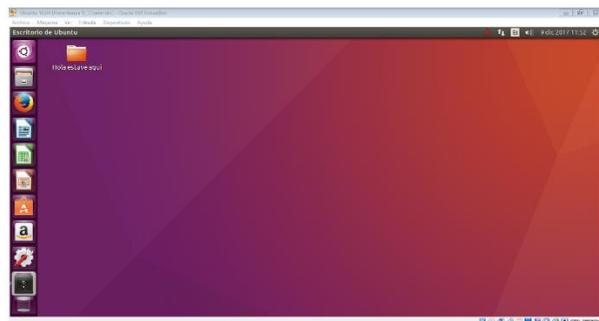


Figura 48. Carpeta Creada en escritorio de Ubuntu.

7 Conclusiones

- Zentyal Server es un sistema basado en Ubuntu de ediciones LTS, el cual incorpora servicios de red requeridos en un entorno comercial pequeño y mediano.
- Una Red Privada Virtual o VPN, es una tecnología de red de computadoras que permite una extensión segura de la LAN sobre una red pública o no controlada como el Internet.
- OpenVPN es una VPN SSL con todas las funciones que implementa la extensión de red segura OSI de capa 2 o 3 utilizando el protocolo estándar SSL/TLS.
- Una autoridad certificadora hace referencia a una entidad de confianza que se encarga de expedir y revocar certificados digitales que sirve para legitimar o desvirtuar ante terceros la confiabilidad de la información.
- Los certificados en OpenVPN permiten identificar en internet de forma fiable y segura a servidores y clientes, permitiendo establecer conexiones seguras vía VPN.
- PuTTY es un cliente de SSH y telnet de código abierto, para conectarse originalmente desde plataformas Windows.
- Xming es el servidor del sistema de ventanas X, líder para sistemas operativos Microsoft Windows.

8 Referencias

- El [1] Wikipedia. (2017). Zentia [En línea]. Disponible en: <https://es.wikipedia.org/wiki/Zentia>
- [2] Zentia. (2017). Linux Small Business [En línea]. Disponible en: <http://www.zentia.org/>
- [3] Zentia. (2017). Zentia Server 5 [En línea]. Disponible en: <http://www.zentia.org/server/>
- [4] Periañez, F. (2016). Tutorial de VirtualBox. Modo: Adaptador puente [En línea]. Disponible en: http://fpg.x10host.com/VirtualBox/modo_adaptador_puente.html
- [5] Periañez, F. (2016). Tutorial de VirtualBox. Modo: Red interna [En línea]. Disponible en: http://fpg.x10host.com/VirtualBox/modo_red_interna.html
- [6] Zentia Community. (2017). Es/5.0/Instalación [En línea]. Disponible en: <https://wiki.zentia.org/wiki/Es/5.0/Instalacion>
- [7] Wikipedia. (2017). Red Privada virtual [En línea]. Disponible en: https://es.wikipedia.org/wiki/Red_privada_virtual
- [8] Zentia Community. (2017). Es/5.0/Servicio de redes privadas virtuales (VPN) con OpenVPN [En línea]. Disponible en: [https://wiki.zentia.org/wiki/Es/5.0/Servicio_de_redes_privadas_virtuales_\(VPN\)_con_OpenVPN](https://wiki.zentia.org/wiki/Es/5.0/Servicio_de_redes_privadas_virtuales_(VPN)_con_OpenVPN)

- [9] Rodríguez, G. (2015). Sesión SSH con interfaz gráfica [En línea]. Disponible en: <https://www.driverlandia.com/sesion-ssh-con-interfaz-grafica/>
- [10] Wikipedia. (2017). OpenVPN [En línea]. Disponible en: <https://es.wikipedia.org/wiki/OpenVPN>
- [11] Wikipedia. (2017). PuTTY [En línea]. Disponible en: <https://es.wikipedia.org/wiki/PuTTY>
- [12] Wikipedia. (2017). Xming [En línea]. Disponible en: <https://es.wikipedia.org/wiki/Xming>