

Tabla de contenido

Capitulo 1. Linux y Ofimática	8
1.1 Introducción	8
1.2 Rocky Linux.....	9
1.2.1 Ventajas.....	9
1.3 Arquitectura	10
1.4 Requisitos de Sistema	10
1.5 Estructura de directorios.....	10
1.6 Particiones recomendadas para instalar Rocky Linux	11
1.7 Procedimiento de Instalación Rocky Linux 9.....	13
1.7.1 Planeación.....	13
1.7.2 Obtención de los medios.....	13
1.7.3 Instalación	13
1.7.3.1 Preparar Máquina Virtual.....	14
1.8 Comandos básicos en linux	26
1.8.1 Comando cat	26
1.8.2 Comando more.....	27
1.8.3 Comando ls.....	27
1.8.4 Comando cd	28
1.8.5 Comando mkdir.....	28
1.8.6 Comando rm.....	28
1.8.7 Comando cp	28
1.8.8 Comando mv	29
1.8.9 Comando clear	29
1.8.10 Comando grep.....	29
1.8.11 Comando history	29
1.8.12 Comando tail	29
1.8.13 Comando su.....	30
1.8.13.1 Cambiar de usuario a super usuario.....	30
1.9 Información básica para gestión de dispositivos de red.....	31
1.9.1 Nombres de dispositivos de red.....	31

Temas Especiales

1.9.2	NetworkManager	32
1.9.3	Asignación de nombre de anfitrión.....	34
1.9.4	Otras herramientas útiles del intérprete de comando	35
1.10	Deshabilitar lista de usuario en el login	36
1.11	Habilitar el DVD como repositorio de instalación.....	37
1.12	Habilitar el acceso a internet vía proxy web	38
1.13	LibreOffice	41
1.13.1	Componetes de LibreOffice.....	41
1.13.1.1	Writer	41
1.13.1.2	Calc	41
1.13.1.3	Impress	42
1.13.1.4	Draw	42
1.13.1.5	Base	42
1.13.1.6	Math	42
1.13.2	Ventajas de LibreOffice	42
1.13.3	Requisitos mínimos de LibreOffice.....	43
1.13.3.1	En Microsoft Windows	43
1.13.3.2	En Apple macOS (Mac OS X).....	43
1.13.3.3	En GNU/Linux	44
Capítulo 2.	Acceso Remoto.....	45
2.1	Definición	45
2.2	SSH.....	45
2.2.1	Habilitar SSH con OpenSSH en Rocky Linux	46
2.2.1.1	Algunos parámetros configuración del servicio ssh.....	47
2.2.1.2	Como conectarse a un servidor que tiene habilitado el servicio ssh	47
2.2.1.3	Copia de archivos con scp	49
2.2.2	Bitacoras del servicio SSH.....	50
2.3	Escritorio remoto	50
2.3.1	Protocolo de comunicaciones	51
2.3.2	VNC.....	51
2.3.2.1	Instalar VNC Server en Rocky Linux.....	51
2.3.2.2	Conexión al escritorio remoto desde Linux.....	54
2.3.2.3	Conexión al escritorio remoto desde Windows	54

Temas Especiales

2.3.3 RDP y xRDP	56
2.3.3.1 Instalar xrdp	56
2.3.3.2 Conexión a escritorio remoto habilitado con xrdp desde cliente Windows	57
2.4 Servidor ftp.....	59
2.4.1 Habilitación de servidor ftp con vsftpd	59
2.4.2 Archivos de configuración de vsftpd	60
2.4.3 Conexión al servidor ftp	61
Capítulo 3. DNS y DHCP	63
3.1 DNS.....	63
3.1.1 Definición de DNS.....	63
3.1.2 NIC (Network Information Center).....	64
3.1.3 Dominio	64
3.1.4 FQDN	65
3.1.5 Datos necesarios para registrar un dominio	66
3.1.6 Procedimiento de registro.....	66
3.1.7 Componentes DNS	67
3.1.7.1 Clientes DNS	67
3.1.7.2 Servidores DNS	67
3.1.7.2.1 ¿Cuántos servidores DNS debe haber para resolver un dominio?	68
3.1.7.2.2 Tipos de resoluciones DNS.....	69
3.1.7.3 Tipos de búsqueda DNS.....	69
3.1.7.4 Zonas de Autoridad	70
3.1.7.4.1 Tipos de registros en las zonas de autoridad.....	70
3.1.8 Herramientas para probar un servidor DNS.....	71
3.1.8.1 Uso del comando host.....	72
3.1.8.2 Uso del comando dig	72
3.1.8.3 Uso del comando nslookup	73
3.1.9 BIND.....	74
3.1.10 Instalación y Configuración de servidor DNS maestro con BIND	74
3.1.10.1 Procedimiento para instalar BIND.....	74
3.1.10.2 Configuración de servidor DNS primario con BIND	74
3.1.10.2.1 Configuración de servidor DNS sin uso de vistas.....	75
3.1.10.2.2 Configuración de servidor DNS con uso de vistas	83

Temas Especiales

3.2 DHCP.....	89
3.2.1 Definición de DHCP	89
3.2.2 ¿Por qué usar DHCP?.....	90
3.2.3 Ventajas de DHCP.....	91
3.2.4 DHCP por Internet Software Consortium, Inc	91
3.2.5 Anatomía del protocolo	91
3.2.6 Instalación de servidor DHCP	92
3.2.7 Configuración de servidor DHCP	92
3.2.7.1 Asignación de direcciones IP estáticas	94
3.2.7.2 Limitar el acceso por dirección MAC.....	95
Capítulo 4. Servidores Web y Servidores de Base de Datos.....	98
4.1 Servidor Web.....	98
4.1.1 Introducción	98
4.1.2 ¿Qué es un servidor web?.....	98
4.1.3 Características generales de los Servidores Web.....	98
4.1.3.1 Servicio de archivos estáticos.....	99
4.1.3.2 Seguridad y autenticación	99
4.1.3.3 Contenido dinámico	99
4.1.3.4 Servidores virtuales.....	99
4.1.3.5 Servidores Intermedios	99
4.1.3.6 Protocolos Adicionales	100
4.1.4 Servidor Web Apache.....	100
4.1.4.1 Ventajas.....	100
4.1.4.2 Configuración	100
4.1.4.3 Licencia	101
4.1.4.4 Instalación de Apache en Rocky Linux	101
4.1.4.5 SELinux y apache	101
4.1.4.6 Inicio rápido de uso de Apache	103
4.1.4.7 Host Virtuales	103
4.1.4.8 Restricción de acceso basada en ip y/o host.....	106
4.1.4.9 Restricción de acceso basada en usuario	107
4.1.4.10 Configuración de apache con soporte SSL/TLS	108
4.1.4.10.1 Acerta de HTTPS.....	108

Temas Especiales

4.1.4.10.2	Acerca de SSL y TLS	109
4.1.4.10.3	Certificados digitales.....	109
4.1.4.10.4	Acerca de RSA	110
4.1.4.10.5	Certificados X.509	111
4.1.4.10.6	Acerca de OpenSSL	111
4.1.4.10.7	Acerca de las autoridades de certificadoras.....	111
4.1.4.10.8	Validación de un certificado digital	111
4.1.4.10.9	Habilitar apache para soporte SSL/TLS	112
4.1.4.11	Host virtual para redirección de URL's	114
4.1.4.12	Habilitar otros puertos en apache.....	115
4.2	Servidor de Base de Datos	115
4.2.1	Introducción	115
4.2.2	MySQL	116
4.2.3	MariaDB.....	116
4.2.3.1	¿En qué casos sería recomendable usar MariaDB?	116
4.2.3.2	¿Cuánto cuesta MariaDB?	117
4.2.3.3	¿Por qué debería usar MariaDB en lugar de MySQL?	117
4.2.4	Instalación de MariaDB en Rocky Linux	117
4.2.5	Creación y eliminación de base de datos en MariaDB	118
4.2.6	Cambios de configuración	119
4.2.6.1	Ejemplo 1:.....	119
4.2.6.2	Ejemplo 2:.....	119
4.2.6.3	Ejemplo 3.....	120
4.2.7	Respaldo y restauración de bases de datos	122
Capítulo 5.	Servidor de Correos Electrónicos	124
5.1	Definición	124
5.2	Términos y Protocolos Utilizados.....	124
5.2.1	Agente de Usuario de Correo - MUA.....	124
5.2.2	Agente de transferencia de correo – MTA.....	124
5.2.3	Agente de entrega de correo – MDA	124
5.2.4	Protocolo SMTP	125
5.2.5	Protocolo POP3	125
5.2.6	Protocolo IMAP	125

Temas Especiales

5.2.7	Multipurpose Internet Mail Extensions – MIME	125
5.2.8	Direcciones de correo electrónico	125
5.2.9	Proveedores de correo electrónico	125
5.2.10	Postfix	126
5.2.11	Dovecot	126
5.2.12	Buzón de correo	126
5.2.13	Tipos de buzones de correo	126
5.2.14	SASL	127
5.3	Formato Básico de un mensaje de Correo Electrónico	127
5.4	Funcionamiento	127
5.5	Software para habilitar servidor de correo en Rocky Linux	128
5.6	Pasos para configurar el servidor de correo	129
5.6.1	Creación de la firma y certificado digital para el servidor de correo	129
5.6.2	Habilitación de puertos en el firewall para servicios de correo	129
5.6.3	Configuración de Postfix	129
5.6.4	Configuración de Dovecot	130
5.6.5	Configuración de cliente de correo de escritorio	132
5.6.6	Configuración de cliente de correo Web	137
Capítulo 6.	Samba	144
6.1	Protocolo SMB	144
6.2	Funcionamiento de SMB	145
6.3	Samba	145
6.4	Características de samba	145
6.5	Que ofrece samba	145
6.6	Funcionamiento de samba	146
6.7	Uso de Samba	146
6.8	Inconvenientes de SMB y Samba	147
6.9	Paquetes a instalar en Rocky Linux	147
6.10	Permisos en firewall de Rocky Linux	147
6.11	Iniciar el servicio y añadirlo al arranque del sistema	147
6.12	Cuentas de usuario en samba	148
6.12.1	Creación de un usuario de samba	148
6.12.2	Eliminar un usuario de samba	148

Temas Especiales

6.12.3	Modificación de password de usuario samba.....	148
6.13	Grupos de usuarios en samba	149
6.14	Contexto y permiso de los directorios a compartir con Samba	150
6.15	Compartir carpetas en samba	150
6.15.1	Ejemplo de compartir una carpeta al público con acceso total	151
6.15.2	Ejemplo de compartir una carpeta restringida a usuarios validos.....	153
6.16	Ocultando archivos que inician con punto.....	154
6.17	Compartir el directorio de inicio de un usuario	154
6.18	Compartir impresoras en samba.....	155
6.19	Conectarse a un recurso compartido desde Rocky Linux	155
6.19.1	Cliente Linux samba usando mount	155
6.19.2	Cliente Linux samba usando smbclient	156
6.19.3	Cliente Linux para samba usando Nautilus	156
6.20	Conectarse a un recurso compartido desde Windows	157
6.20.1	Cliente Windows Samba usando explorador de Windows	157
6.20.2	Cliente Windows Samba usando consola de comandos	159
	Bibliografía	161

Capítulo 1. Linux y Ofimática

1.1 Introducción

GNU es un sistema operativo de tipo Unix desarrollado por y para el Proyecto GNU, y auspiciado por la Free Software Foundation con su propio núcleo llamado GNU Hurd. Está formado en su totalidad por software libre, mayoritariamente bajo términos de copyleft. GNU significa GNU No es Unix (**GNU is Not Unix**). Este proyecto fue iniciado por Richard Stallman y anunciado el 27 de septiembre de 1983, con el objetivo de crear un sistema operativo completamente libre.

Por otro lado, GNU/Linux®, es también, un sistema operativo libre tipo Unix; multiplataforma, multiusuario y multitarea. Este sistema operativo, es la combinación de varios proyectos, entre los cuales destacan GNU (ya mencionado en el párrafo anterior) y el núcleo Linux (creado en 1991 por Linus Torvalds); es poderoso y sumamente versátil con licencia libre y que implemente el estándar POSIX (acrónimo de Portable Operating System Interface, que se traduce como Interfaz de Sistema Operativo Portable). La gran diferencia entre el sistema operativo GNU y el Sistema Operativo formado por la combinación GNU/Linux, está en que GNU/Linux tiene partes del software privativo (es decir que no se cuenta con las fuentes de esas partes).

Al ser GNU/Linux Software Libre, el usuario tiene la libertad de redistribuir y modificar el sistema operativo de acuerdo a necesidades específicas, siempre que se incluya el código fuente, tal como lo indica la Licencia Pública General GNU. Esto también incluye el derecho a poder instalar el núcleo de GNU/Linux® en cualquier número de ordenadores o equipos de cómputo que el usuario desee. Pero, cuando hablamos de software libre, no hablamos de software gratuito, si no que hacemos relación a la libertad y no al precio, puesto que la licencia GPL (Licencia Pública General) bajo la cual se distribuye GNU/Linux, está diseñada para asegurar que el usuario tenga siempre la libertad de distribuir copias del software (y cobrar por el servicio si así lo desea). La licencia GPL tiene como objetivo garantizar al usuario la libertad de compartir y cambiar el software libre, es decir, asegurarse de que el software siempre permanezca libre para todos los usuarios.

GNU/Linux® es también la mejor alternativa de siglo XXI para los usuarios que no solo desean libertad, sino que también desean un sistema operativo estable, robusto y confiable. Es un sistema operativo idóneo para utilizar en Redes, como es el caso de servidores, estaciones de trabajo y también para computadoras personales.

Las características de GNU/Linux® le permiten desempeñar múltiples tareas en forma simultánea de forma segura y confiable. Los distintos servicios se pueden detener, iniciar o reiniciar independientemente sin afectar al resto del sistema, permitiendo operar las 24 horas del día los 365 días del año.

Tal ha sido el impacto alcanzado por GNU/Linux® en los últimos años, que muchas de las empresas de Software más importantes del mundo, entre las cuales están IBM, Oracle y Sun Microsystems, han encontrado en GNU/Linux una plataforma con un muy amplio mercado y se han volcado al desarrollo de versiones para Linux de sus más importantes aplicaciones. Grandes corporaciones, como Compaq, Dell, Hewlett Packard, IBM y muchos más, llevan varios años distribuyendo equipos con GNU/Linux® como sistema operativo.

Gracias a sus características, la constante evolución de los ambientes gráficos para X Window®(X Windows System, es un sistema de gestor de ventanas, común en sistemas operativos del tipo UNIX), que cada vez son de más fácil uso, como es el caso de GNOME y KDE; también gracias al trabajo de cientos de programadores y usuarios fieles alrededor del mundo, Linux ha dejado de ser un sistema operativo poco atractivo y complicado de utilizar para convertirse en una alternativa real para quienes buscan un sistema operativo confiable y poderoso, ya sea para una servidor, estación de trabajo o la computadora personal de un usuario intrépido.

1.2 Rocky Linux

Rocky Linux es una distribución de Linux, desarrollada por Rocky Enterprise Software Foundation, apta para HPC (Computación de Alto Rendimiento), especialmente adecuada para servidores y aplicaciones de escritorio. El sistema operativo es de código abierto y compatible a nivel binario con el sistema operativo comercial conocido como Red Hat Enterprise Linux (RHEL). Rocky Linux se considera el sucesor no oficial de CentOS, un fork de RHEL. El sistema operativo es adecuado para una variedad de usos diferentes y es una solución estable y fácil de usar tanto para empresas como para particulares, lanzada completamente para ser compatible con código binario usando el código de fuente del sistema operativo de Red Hat Enterprise Linux (RHEL). El objetivo del proyecto es proporcionar un soporte comunitario, y un sistema operativo de producción a nivel empresa. Cada versión es mantenida por un periodo de 10 años por medio de actualizaciones de seguridad. La ultima versión es la versión 9 la cual será mantenida hasta el año 2032

1.2.1 Ventajas

- **Equipo:** el equipo que está detrás de Rocky Linux garantiza la aceptación necesaria y era el motivo de optimismo antes del lanzamiento. Como confundador de CentOS, Gregory Kurtzer sabe exactamente lo que aprecian y valoran los usuarios de la popular distribución y ahora también puede tener en cuenta este conocimiento con el sucesor. Por ello, Rocky Linux tiene el potencial de convertirse en un digno sucesor desde el principio.
- **Estabilidad:** La estabilidad está primer plano con Rocky Linux, como en su momento fue una de las ventajas de CentOS. En lugar de muchas actualizaciones nuevas, la atención se centra en un sistema que funciona sin problemas y sin sorpresas desagradables.
- **Compatibilidad:** Rocky Linux es compatible en términos binarios con Red Hat Enterprise Linux y, por tanto, es una alternativa que merece la pena. La migración de CentOS, AlmaLinux y otras distribuciones también es muy fácil con la herramienta migrate2rocky. Además, las imágenes de contenedores y las ofertas basadas en la nube no son un problema para Rocky Linux.
- **Código abierto:** Rocky Linux continúa el camino que CentOS allanó en su día no solo en términos de compatibilidad binaria. También se continúa con la idea del código abierto, del que al final se beneficiarán todos los usuarios. Si la nueva variante de Linux consigue unir a una comunidad igualmente amplia y comprometida, nada se interpondrá en el camino de una documentación sin fisuras, una gestión de la seguridad premeditada y, por supuesto, actualizaciones y correcciones periódicas en beneficio de los usuarios reales. El predecesor ya se acercaba a las necesidades de sus usuarios; ahora esperan que el sucesor pueda seguir en la línea.

1.3 Arquitectura

Ya está disponible en la versión 9.4, y en esta versión ya soporta las mismas arquitecturas que Red Hat Enterprise Linux:

- AMD e Intel 64 bits
- ARM 64 Bits (aarch64)
- IBM Power System - PowerPC (ppc64le)
- IBM Z 64 Bits (s390x)

1.4 Requisitos de Sistema

Hardware recomendado para operar Rocky Linux:

- Memoria RAM: 2 GB (mínimo).
- Espacio en Disco Duro: 10 GB (mínimo) - 20 GB (recomendado).
- CPU: 10 GHz Simple o Múltiple
- Instalación: USB Stick o DVD

1.5 Estructura de directorios

Todos los archivos y directorios aparecen debajo del directorio raíz «/», aún si están almacenados en dispositivos físicamente diferentes.

Entre los directorios que se pueden encontrar en un computador donde se ha instalado Rocky Linux tenemos:

Directorio	Descripción
/bin	Mandatos binarios esenciales (como son cp, mv, ls, rm, mkdir, etc.)
/boot	Archivos utilizados durante el inicio del sistema (núcleo y discos RAM)
/dev	Dispositivos esenciales.
/etc	Archivos de configuración utilizados en todo el sistema y que son específicos del anfitrión.
/home (opcional)	Directorios de inicio de los usuarios locales.
/lib y /lib64	Bibliotecas compartidas esenciales para los binarios de /bin/, /sbin/ y el núcleo del sistema. /lib64/ corresponde al directorio utilizado por sistemas de 64-bit.
/mnt	Sistemas de archivos montados temporalmente.
/media	Puntos de montaje para dispositivos de medios, como son las unidades lectoras de discos compactos.
/opt	Paquetes de aplicaciones de terceros.
/proc	Sistema de archivos virtual que documenta sucesos y estados del núcleo. Contiene, principalmente, archivos de texto.
/root (opcional)	Directorio de inicio del usuario root (super-usuario).
/sbin	Binarios (Ejecutables) de administración de sistema.
/tmp	Archivos temporales
/srv	Datos específicos de sitio, servidos por el sistema.

Temas Especiales

/usr	Jerarquía secundaria para datos compartidos de solo lectura (Unix system resources). Este directorio debe poder ser compartido para múltiples anfitriones, y, debe evitarse que contenga datos específicos del anfitrión que los comparte cuando se hace a través de NFS.
/usr/bin	Comandos binarios.
/usr/include	Archivos de inclusión estándar (cabeceras de desarrollo).
/usr/lib y /usr/lib64	Bibliotecas compartidas. /usr/lib64/ corresponde al directorio utilizado por sistemas de 64-bit.
/usr/share	Datos compartidos, independientes de la arquitectura del sistema. Consiste en imágenes, archivos de texto, archivos de audio, etc.
/usr/local	Jerarquía terciaria para datos compartidos de solo-lectura, específicos del anfitrión.
/var	Archivos variables, como son bitácoras, bases de datos, directorio raíz de servidores HTTP y FTP, colas de correo, archivos temporales, etc.
/var/lib	Información de estado variable. Algunos servidores como MySQL y PostgreSQL, almacenan sus bases de datos en directorios subordinados de éste.
/var/lock	Archivos de bloqueo de los servicios en ejecución.
/var/log	Archivos y directorios, utilizados para almacenar las bitácoras de eventos del sistema.
/var/mail (opcional)	Buzones de correo de usuarios.

1.6 Particiones recomendadas para instalar Rocky Linux

Para uso general o práctica del uso de las bondades del sistema operativo Rocky Linux, se recomienda utilizar un diseño de tres particiones (predeterminado del instalador de Rocky Linux):

Partición	Descripción
/boot	Requiere de 1024 MiB.
/	Si se utiliza el diseño de tres particiones, asignar el resto del espacio disponible en la unidad de almacenamiento. Si se van asignar particiones para los directorios mencionados adelante, se requieren de 3072 MiB a 5120 MiB.
/swap	Si se tiene menos de 2 GiB de RAM, se debe asignar el doble del tamaño del RAM físico ; si se tiene más de 1 GiB RAM, se debe asignar una cantidad igual al tamaño del RAM físico, más 2 GiB. Ésta será siempre la última partición del espacio disponible para almacenamiento y jamás se le asigna punto de montaje.

Los siguientes directorios jamás deberán estar fuera de la partición que corresponda a /, es decir, jamás se deben asignar como particiones separadas:

- /etc
- /bin
- /dev
- /lib y /lib64

Temas Especiales

- /media
- /mnt
- /proc
- /root
- /sbin
- /sys

En Rocky Linux 9 el directorio /usr se puede separar como partición independiente gracias a que el proceso de arranque se encarga de montarla cuando es necesario. Sin embargo, es preferible que /usr forma parte de la misma partición que corresponda a /, pues el proceso de arranque —que es gestionado por SystemD— utiliza subdirectorios de éste durante el inicio del sistema.

En sistemas que utilizan SystemD hay además los siguientes cambios:

- Directorios ocultos de /dev —como /dev/.udev, /dev/.mdadm, /dev/.systemd o /dev/.mount—
- ahora van dentro de /run.
- /dev/shm corresponde ahora a /run/shm.
- /var/lock corresponde ahora a /run/lock.
- /tmp corresponde ahora a /run/tmp.

Otras particiones que se recomienda asignar, de acuerdo al uso que se le vaya a dar al servidor, son:

Partición	Descripción
/usr	Requiere al menos 3072 MiB en instalaciones básicas. Debe considerarse el equipamiento lógico se planea instalar a futuro. Para uso general se recomiendan al menos de 5120 MiB, y, de ser posible, considere un tamaño óptimo de hasta 20480 MiB.
/tmp	Requiere al menos 350 MiB y puede asignarse hasta 5 GiB o más, dependiendo de la carga de trabajo y del tipo de aplicaciones. Si, por ejemplo, el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GiB, asumiendo que es de una sola cara y de densidad simple.
/var	Requiere al menos 3072 MiB en estaciones de trabajo sin servicios . En servidores regularmente se le asigna al menos la mitad del espacio disponible para almacenamiento .
/home	En estaciones de trabajo, a esta partición se asigna al menos la mitad del espacio disponible para almacenamiento.
/usr/local	Requiere al menos 3072 MiB en instalaciones básicas. Debe considerarse el equipamiento lógico que se planea compilar desde código fuente, e instalar, a futuro. Al igual que /usr, para uso general se recomiendan al menos de 5120 MiB, y, de ser posible, considere un tamaño óptimo de hasta 20480 MiB.
/opt	Requiere al menos 3072 MiB en instalaciones básicas. Debe considerarse el equipamiento lógico de terceros que se planea instalar a futuro. Al igual que /usr, para uso general se recomiendan al menos de 5120 MiB, y, de ser posible, considere un tamaño óptimo de hasta 20480 MiB.
/var/lib	Si se asigna como partición independiente de /var, lo cual permitiría optimizar el registro por diario utilizando el modo journal para un mejor desempeño, requiere

	al menos 3072 MiB en instalaciones básicas. Deben considerarse las bases de datos o directorios de LDAP, que se planeen hospedar a futuro.
/var/www	Si se asigna como partición independiente de /var, lo cual permitiría optimizar el registro por diario utilizando el modo writeback para un mejor desempeño, requiere al menos 3072 MiB en instalaciones básicas. Deben considerarse los anfitriones virtuales, aplicaciones y contenido para ser servido a través del protocolo HTTP, que se planeen hospedar a futuro.

1.7 Procedimiento de Instalación Rocky Linux 9

1.7.1 Planeación.

Antes de comenzar, determine primero los siguientes puntos:

- Finalidad productiva. ¿Va ser un servidor, estación de trabajo o escritorio? ¿Qué uso va tener el equipo? ¿Qué servicios va a requerir? Idealmente lo que se establezca en este punto debe prevalecer sin modificaciones a lo largo de su ciclo productivo.
- Ciclo de producción. ¿Cuánto tiempo considera que estará en operación el equipo? ¿Seis meses, un año, dos años, cinco años?
- Capacidad del equipo. ¿A cuántos usuarios simultáneos se brindará servicio? ¿Tiene el equipo la cantidad suficiente de RAM y poder de procesamiento suficiente?
- Particiones del disco duro. Determine cómo administrará el espacio disponible de almacenamiento. Para más detalles al respecto, consulte el documento titulado «Estándar de Jerarquía de Sistema de Archivos.»
- Limitaciones. Tenga claro que Rocky Linux —al igual que sucede con Red Hat Enterprise Linux — es un sistema operativo diseñado y enfocado específicamente para ser utilizado como sistema operativo en servidores, desarrollo de programas y estaciones de trabajo. Salvo que posteriormente se añada algún almacén dnf como EPEL, Remi, AL Server o RPMFusion, este sistema operativo carecerá de soporte para medios de audio y video en formatos privativos — como ocurre son el soporte para MP3, DivX, H.264, MPEG, etc.— y que sólo incluye Software Libre que se encuentre exento de problemas de patentes.

1.7.2 Obtención de los medios.

Descargue la imagen ISO del DVD de Rocky Linux 9 para arquitectura x86_64 desde algunos de los sitios espejo que encontrará en el siguiente URL

Tome en cuenta que para la arquitectura x86_64 podrá encontrar enlaces para descargar desde Torrent o directamente el archivo ISO del DVD instalador; descargue el archivo que le sea útil, no es necesario descargar todos, dependiendo de si desea realizar una instalación mínima (descague Minimal), una instalación con los elementos más comunes de Uso de Rocky Linux (descague DVD) o descague Boot si desea instalar Rocky Linux desde otra fuente como http y otro.

1.7.3 Instalación

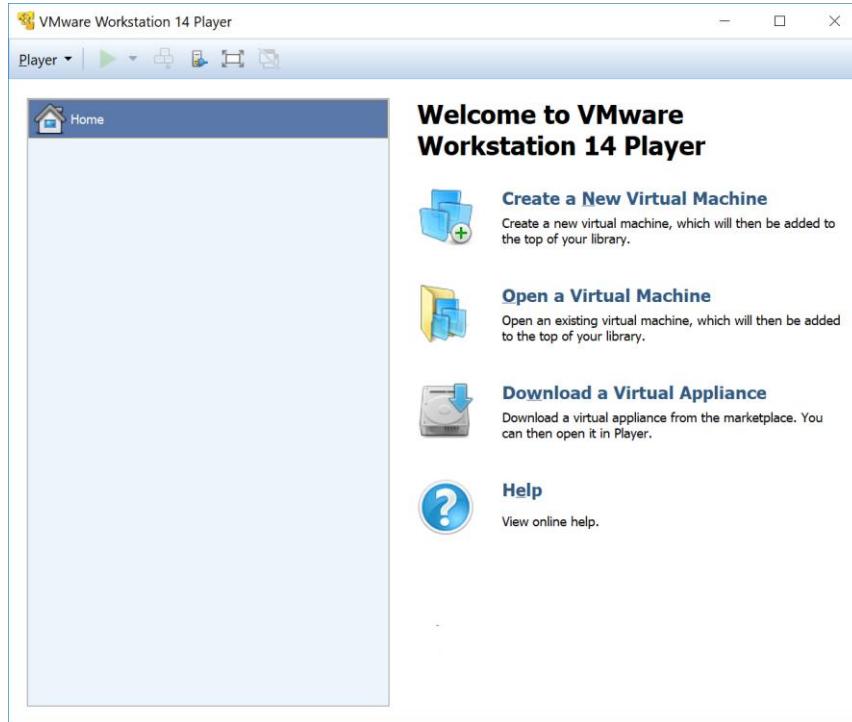
NOTA IMPORTANTE:

Antes de empezar con el tipo de instalación que realizaremos para la asignatura, debemos tener presente que este sistema operativo, como cualquier otro se puede instalar directamente hasta en su computador personal en lugar de su sistema operativo actual (que podría ser alguna versión de Microsoft Windows o tal vez alguna otra distribución Linux) lo cual haría que su sistema actual deje de existir. La otra opción si no desea perder su sistema operativo actual es utilizar una máquina virtual, para lo cual puede hacer uso de software como VMWare o VirtualBox, software que le permitirá definir una máquina virtual (no física) que según los parámetros de memoria, procesador y disco duro que usted defina para esta máquina, restará estos recursos asignados de su máquina real cuando la máquina virtual este en uso.

En la asignatura haremos uso de VMWare Workstation Pro para definir una máquina virtual con los recursos necesarios para hacer nuestras prácticas.

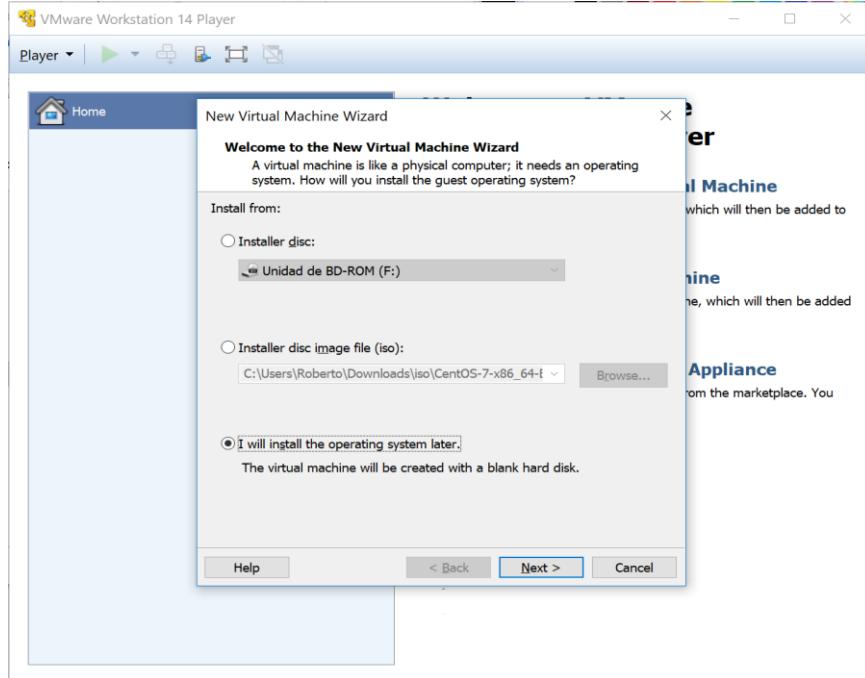
1.7.3.1 Preparar Máquina Virtual

- i. Por comodidad, usaremos VMPlayer que viene con el instalador de VMWare Workstation Pro:

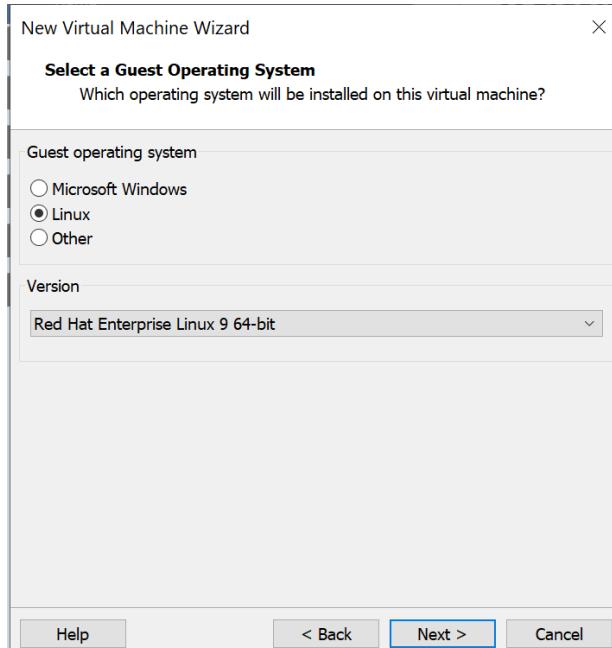


- ii. Hacemos clic en la opción “**Create a New Virtual Machine**” para crear nuestra máquina virtual. En la ventana que se lanzará, nos aseguramos de seleccionar la opción “**I will install the operating system later**” y hacemos clic en el botón Next:

Temas Especiales

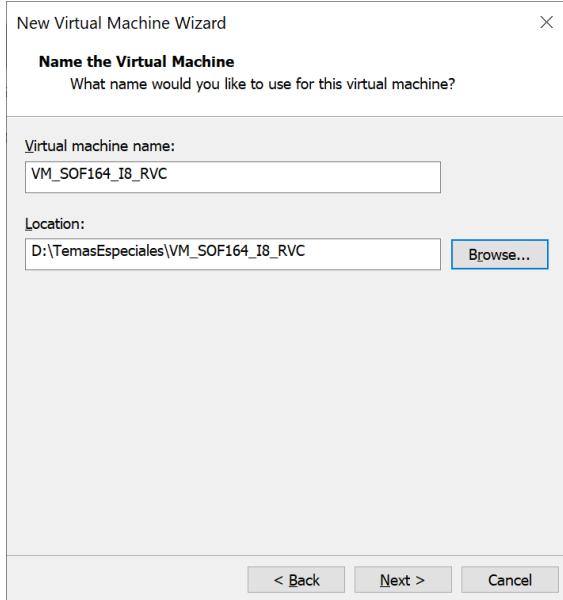


- iii. En la siguiente ventana nos aseguramos de escoger la opción Linux y en la Versión escogemos **Red Hat Enterprise Linux 9 64-bit** y hacemos clic en el botón Next

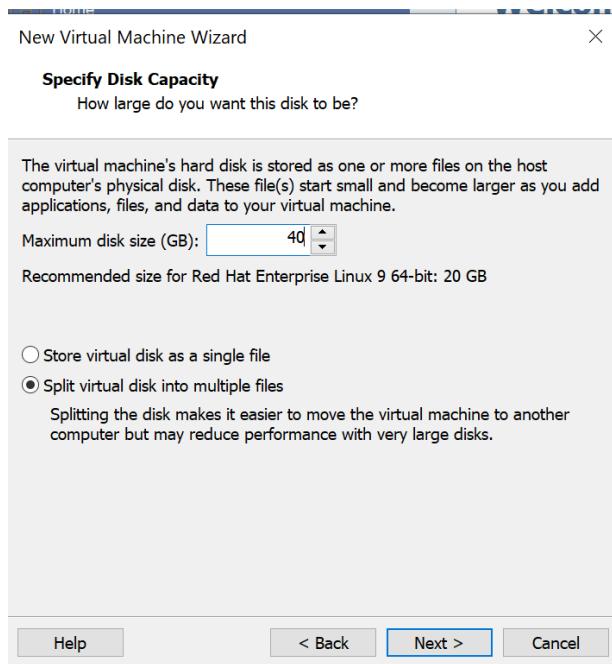


- iv. En la siguiente ventana damos el nombre a nuestra máquina virtual (sugerencia VM_SOF164_GRUPO_INICIALES, Ej: VM_SOF164_I8_RVC). Luego, escogemos donde se guardará dicha máquina virtual. Si estamos trabajando en los equipos del laboratorio, para no perder nuestra máquina virtual guardaremos nuestra máquina virtual en la unidad D, caso contrario elija la ruta que mejor le parezca y hacemos clic en el botón Next:

Temas Especiales

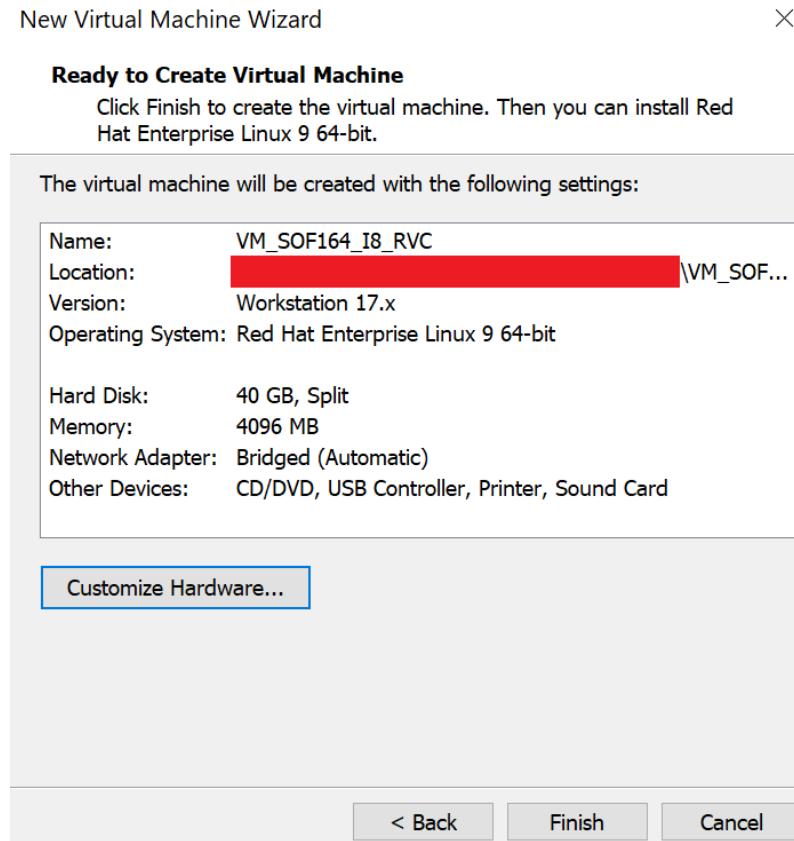


- v. En la siguiente ventana, dimensionamos el disco duro en un tamaño adecuando para tener problemas de espacio durante el desarrollo de la asignatura, nos aseguramos de seleccionar la opción “**Split virtual disk into multiple files**” y hacemos clic en el botón Next



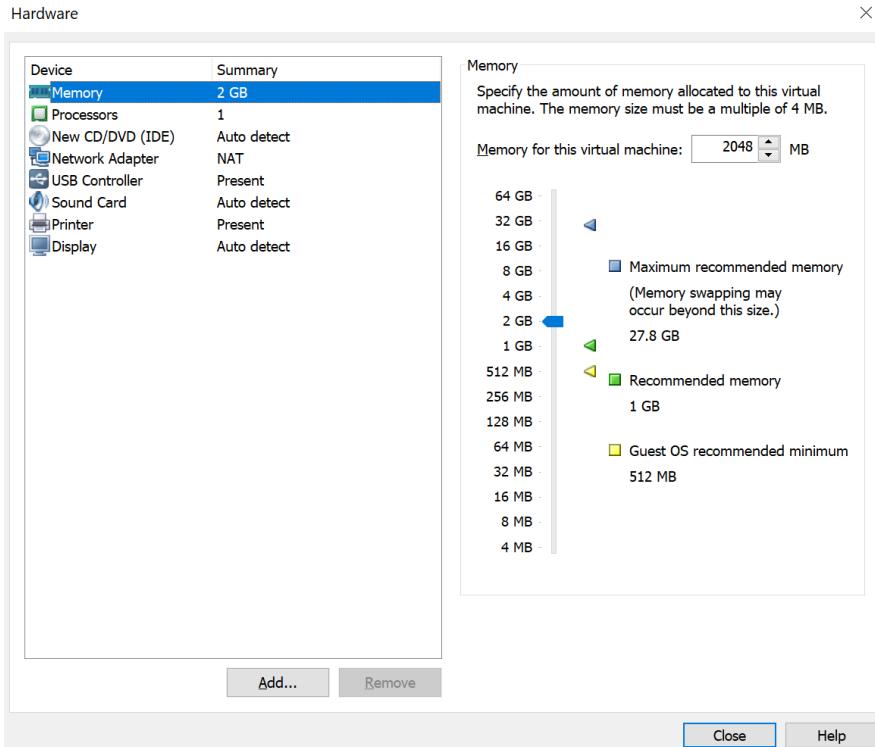
- vi. En la siguiente ventana hacemos clic en el botón **Customize Hardware**

Temas Especiales

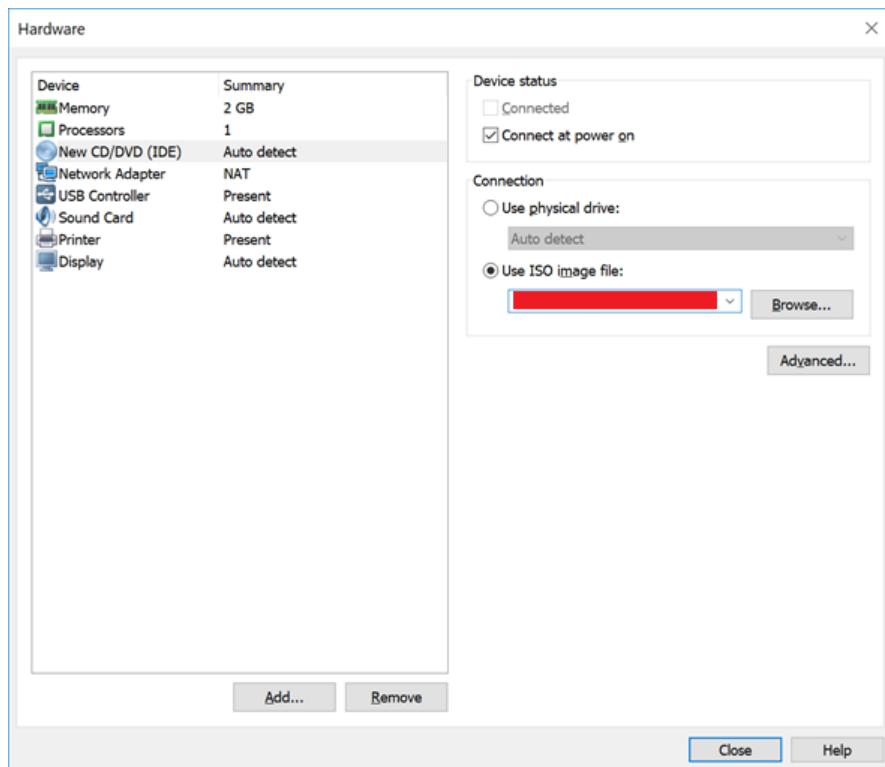


- vii. El primer parámetro que cambiaremos a la máquina virtual será la memoria, debemos disponer de al menos 2048 MB. Si en está trabajando en su equipo personal, asegúrese que su computador tiene al menos 4 GB de memoria RAM para poder asignar los 2048 MB que necesitamos para nuestra virtual, caso contrario, su computador trabajará muy lentamente cuando su virtual esté funcionando.

Temas Especiales

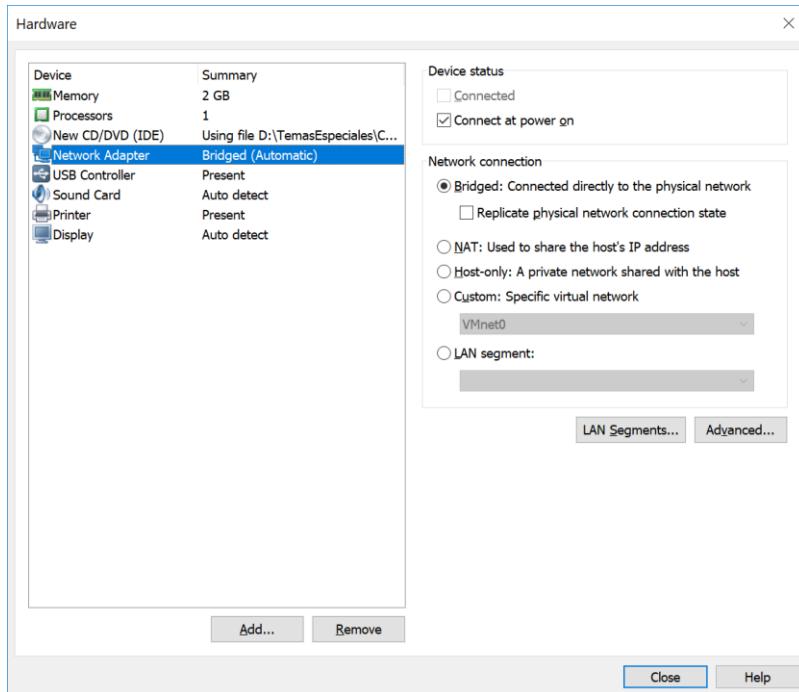


- viii. Luego seleccionamos la opción **New CD/DVD (IDE)**, nos aseguramos de seleccionar la opción **Use ISO image file**, y haciendo uso del botón **Browse** buscamos el archivo iso del instalador de Rocky Linux 9.x

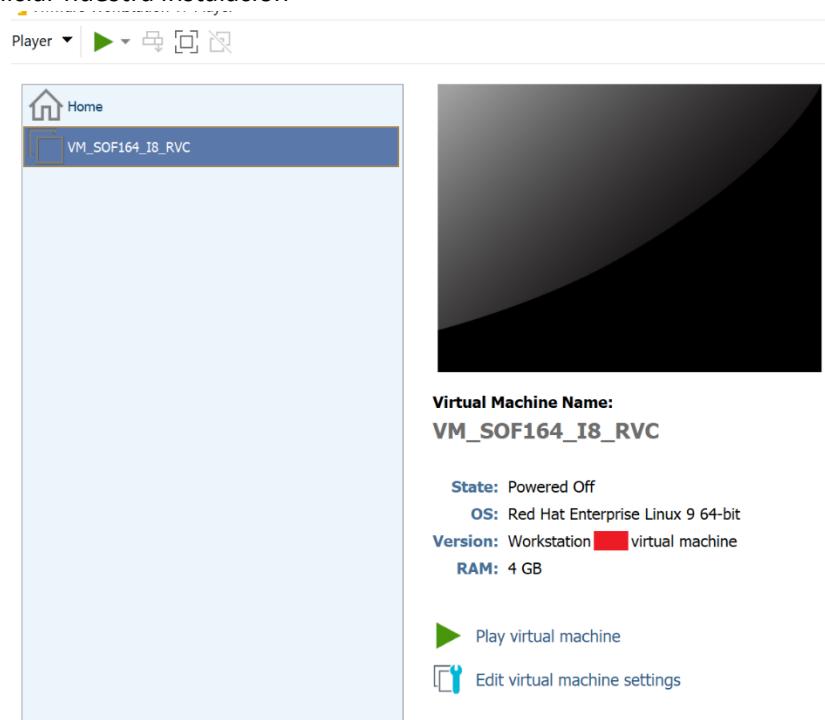


Temas Especiales

- ix. Luego cambio la opción **Network Adapter** y nos aseguramos de que tengamos seleccionada la opción Bridge. Luego de eso presionamos el botón **Close** y en la siguiente ventana hacemos clic en el botón **Finish**



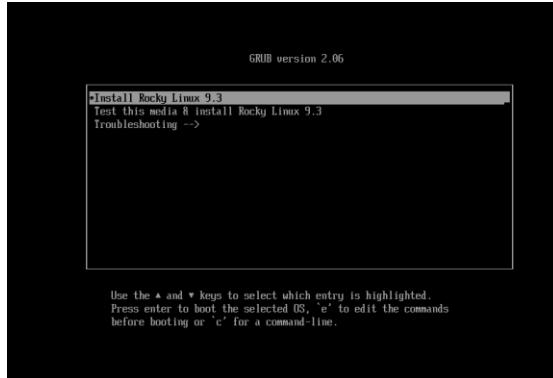
- x. Una vez creada nuestra máquina virtual, hacemos clic en la opción **Play virtual machine** para iniciar nuestra instalación



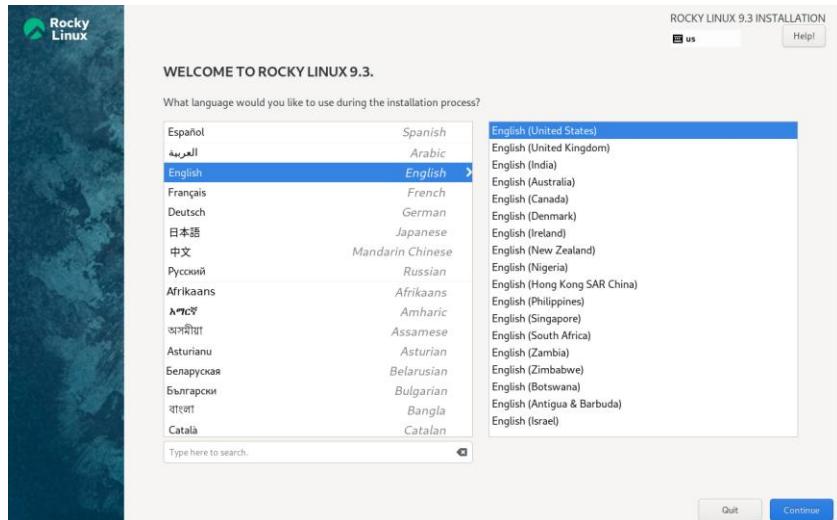
Temas Especiales

NOTA: Si está trabajando en una maquina real, asegúrese de grabar el iso en un DVD o BD, dependiendo del tamaño de la imagen que haya decidido descargarse. Luego debe iniciar su computador con el DVD o BD que grabo para proceder a instalar.

- xi. Cuando el instalador de Rocky Linux 9 nos visualice las opciones hacemos un clic sobre la maquina virtual y con las teclas de movimiento del cursor, nos aseguramos de seleccionar **Install Rocky Linux 9.x**, luego presionamos la tecla enter y esperamos a que el instalador inicie.

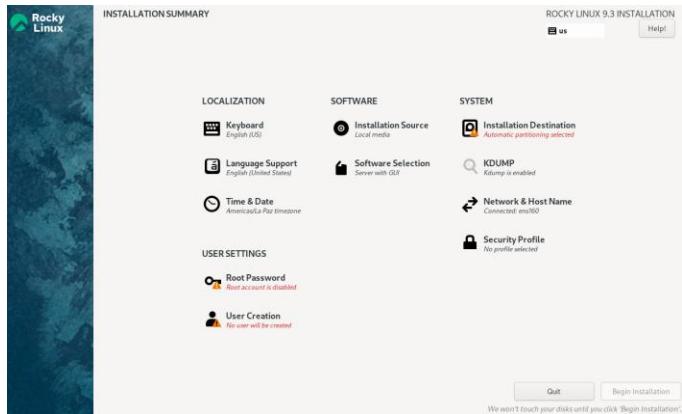


- xii. En la primera pantalla que nos muestre el instalador podremos escoger el idioma que queremos utilizar para la instalación y el sistema. Dejaremos el idioma tal como está en la imagen en inglés y solo hacemos clic en el botón **Continue**

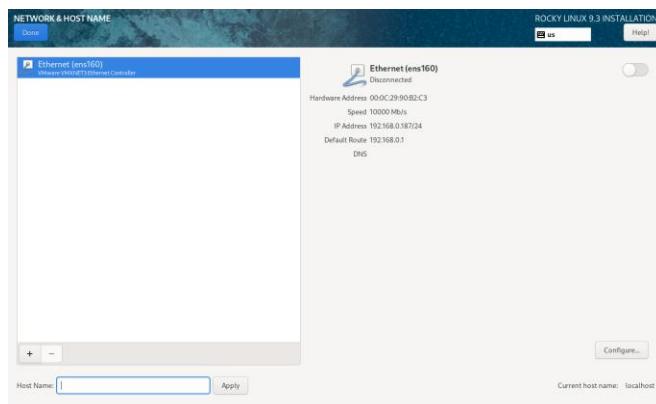


- xiii. En la siguiente pantalla tenemos varias opciones para configurar y si no vemos todas, podemos usar el mouse para movernos y ver todas las opciones en la pantalla, a través de la barra de desplazamiento que se muestra cuando ponemos el cursor del mouse en el lado derecho de la pantalla dentro de la máquina virtual.

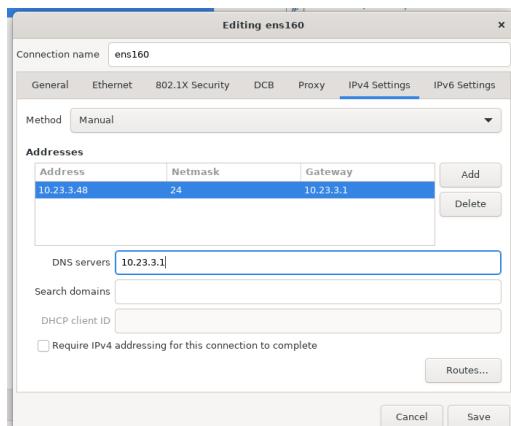
Temas Especiales



- xiv. Podemos hacer clic en cualquiera de las opciones y modificar a conveniencia en cualquier orden. Empezaremos con la red y nombre del servidor. Para esto hacemos clic en la opción **NETWORK & HOSTNAME**.

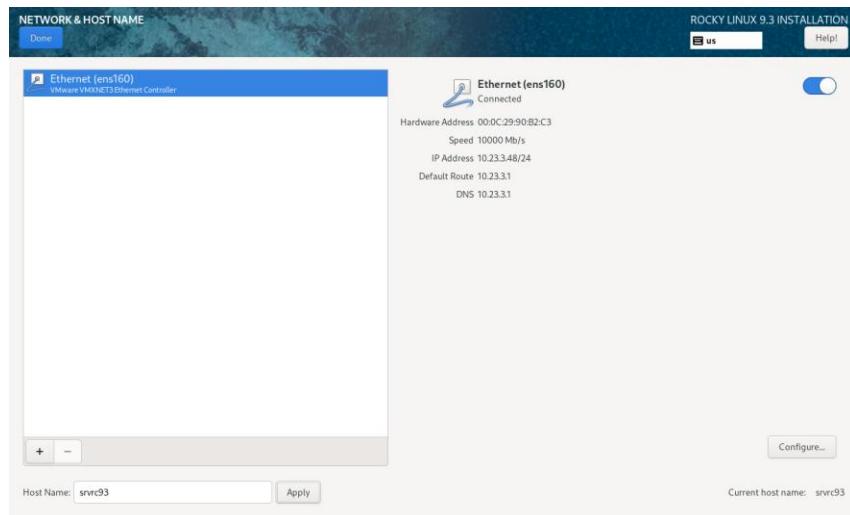


- xv. En esta pantalla hacemos clic en el botón **Configure** para poder asignar la configuración de IP de red desde la instalación. (Podremos cambiar esto luego de instalar). En la pantalla que se nos visualizará, elegimos **IPv4 Setting** (**NOTA: No use esta IP de la imagen en su configuración en los laboratorios, solo es un ejemplo, solicite que se le asigne una IP en clases.**). En esta pestaña escogemos **Manual** en el método de configuración y dentro de las casillas respectivas llenamos con la información que se les brinde en clases. Luego hacer clic en el botón **Save** (**Previo mejor si va a la pestaña IPv6 Setting y en Method elige Disabled**)

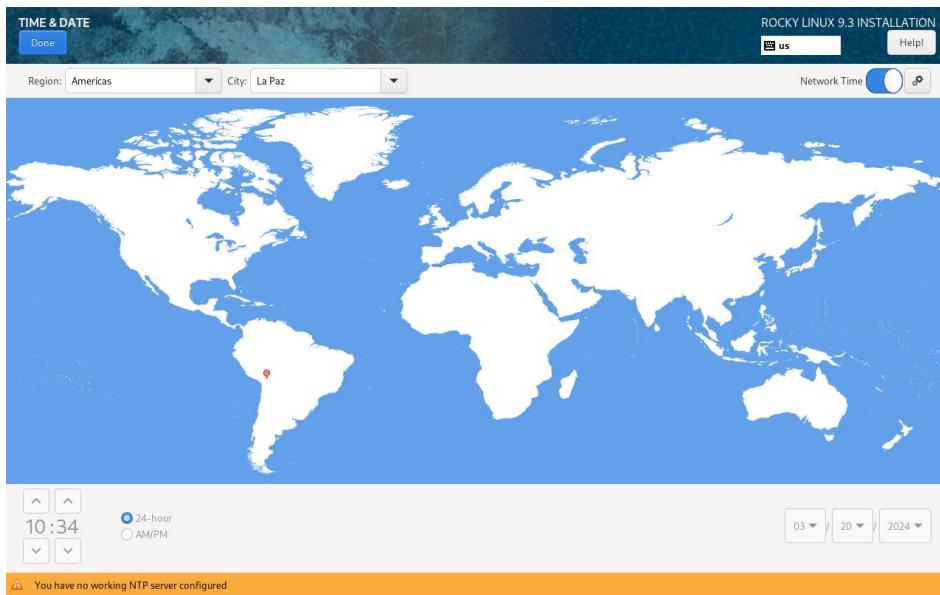


Temas Especiales

- xvi. Esto nos hará retornar a la pantalla anterior en la cual pondremos el nombre que queremos que tenga nuestro servidor y si ya lo sabemos el dominio y luego nos aseguramos que la tarjeta de red está habilitada (Para esto asegurese que el botón al lado del texto ethernet este habilitado, es decir en azul no en gris) En el cuadro de texto Host name, notaremos que por defecto viene vacío; esto lo cambiamos por el nombre que tendrá nuestro servidor (si no lo cambiamos el instalador utilizará localhost), pero debemos definir al menos el nombre que tendrá temporalmente (En la figura se está usando como ejemplo el nombre **srvc93** – Esto ya le debemos haber definido antes de instalar nuestro servidor, no ese este nombre solo es un ejemplo). Si cambia el nombre hace clic en el botón **Apply** y luego hacemos clic en el botón **Done**. Al hacer esto, volveremos a la pantalla del inciso **xiii**.

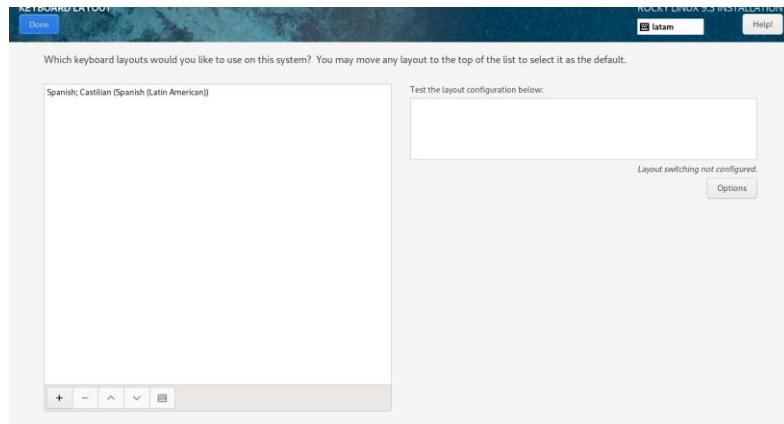


- xvii. Cuando volvamos a ver la pantalla del inciso **xiii** haremos clic en la opción **Time & Date** y en la pantalla que se nos presenta nos aseguraremos de ubicarnos en el mapa con la ayuda del mouse en La Paz. Luego hacemos clic en el botón **Done**. Al hacer esto, volveremos a la pantalla del inciso **xiii**.

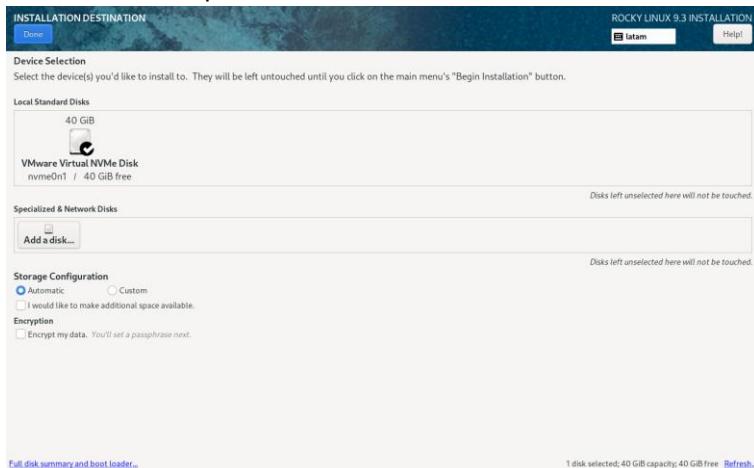


Temas Especiales

- xviii. Cuando volvamos a ver la pantalla del inciso **xiii** haremos clic en la opción **KEYBOARD** si queremos cambiar la distribución de teclado, dependiendo del teclado que usted tenga, el cual podría ser español de España o español latino. Como ejemplo utilizaremos esta pantalla para cambiar el teclado a **Spanish, Castilian (Spanish Latin America)** utilizando el botón + para agregar el nuevo teclado y el botón – para eliminar el teclado que no queremos usar. Luego hacemos clic en el botón **Done**. Al hacer esto, volveremos a la pantalla del inciso **xiii**. Ud debe cambiar por el idioma correcto de su teclado

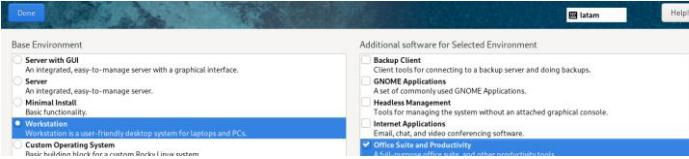
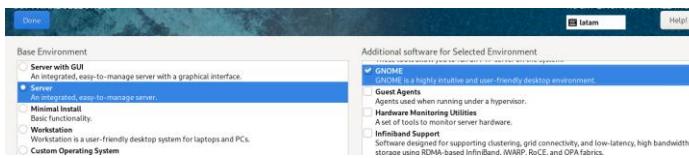
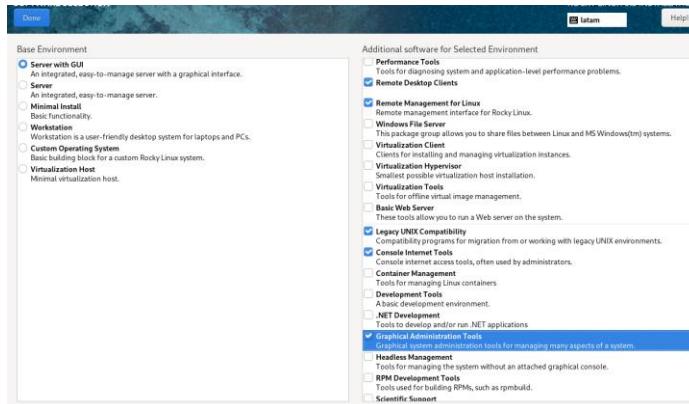


- xix. Cuando volvamos a ver la pantalla del inciso **xiii** haremos clic en la opción **INSTALLATION DESTINATION** y nos aseguramos elegir **Automatic**. Luego hacemos clic en el botón **Done**. Al hacer esto, volveremos a la pantalla del inciso **xiii**.

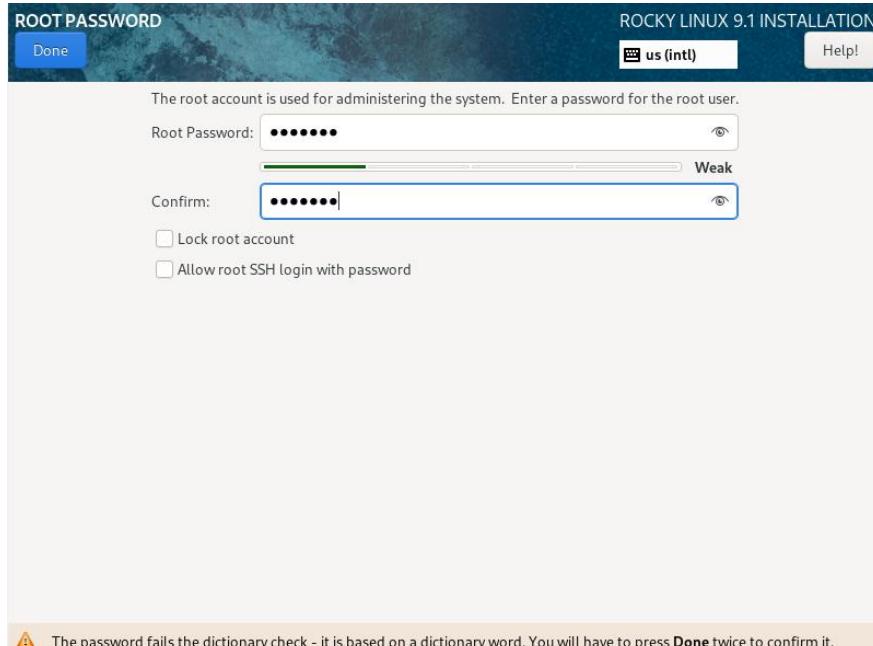


- xx. Cuando volvamos a ver la pantalla del inciso **xiii** haremos clic en la opción **SOFTWARE SELECTION**. En esta pantalla nos aseguramos de seleccionar lo que se muestra en la imagen para **Server with GUI, Server y Workstation**. Luego hacemos clic en el botón **Done**. Al hacer esto, volveremos a la pantalla del inciso **xiii**.

Temas Especiales



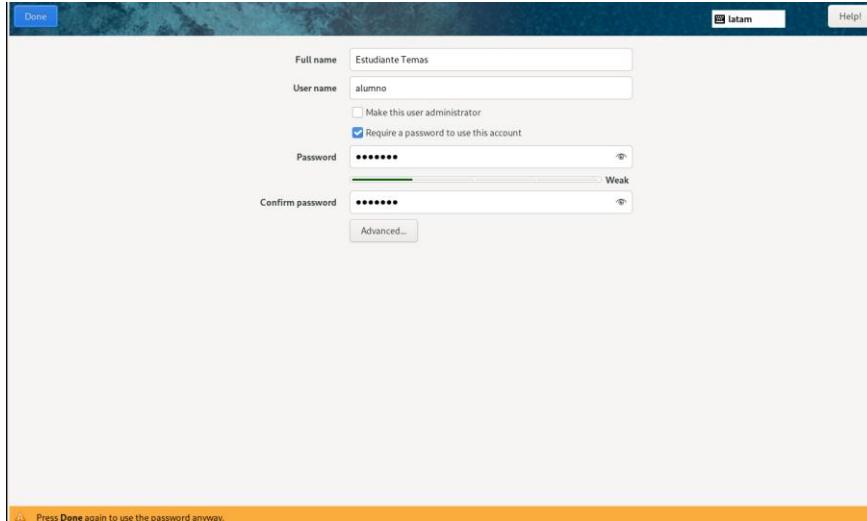
- xxi. Hacemos clic en Root Password al volver una vez más a la pantalla del inciso **xiii**, nos habilitará la pantalla para definir el password del usuario root, lo definimos. Deberemos hacer dos veces clic en el botón **Done**, si es que colocamos una contraseña muy fácil para que el instalador acepte la contraseña (Es nos lo avisa en el mensaje abajo en la ventana).



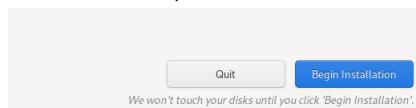
- xxii. Al volver a la ventana mostrada en la ventana que vimos en el punto **xiii**, hacemos clic en **User Creation**, para crear un usuario estándar que será el que normalmente usaremos para

Temas Especiales

ingresar como un usuario normal. Es importante recordar el nombre de cuenta (User name) y el password que ingresamos



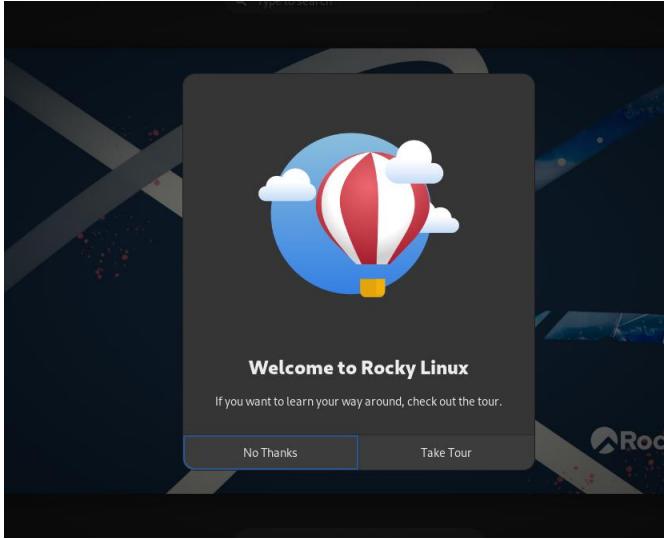
- xxiii. Al volver a la ventana mostrada en la ventana que vimos en el punto **xiii**, notaremos que la opción **Begin Installation**, ya está activada, hacemos clic en ese botón.



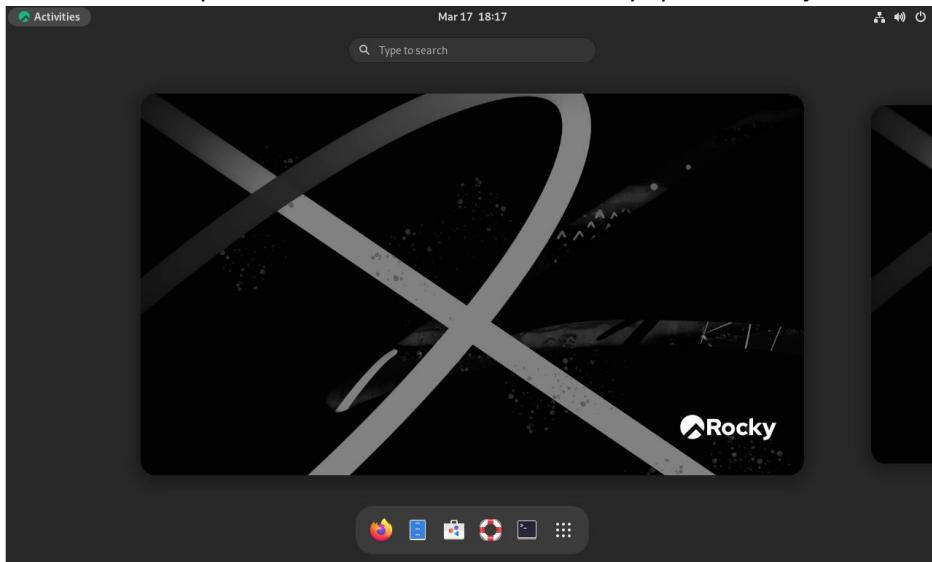
- xxiv. Luego solo esperamos que la instalación finalice. Una vez se nos muestre el botón **Reboot System**, la instalación a finalizado y hacemos clic en dicho botón para reiniciar el servidor.



- xxv. Una vez reinicie el servidor e iniciemos sesión con nuestro usuario creado, veremos la siguiente pantalla



- xxvi. Haremos clic en el botón No Thanks y ya podremos empezar a trabajar.
xxvii. Ahora si veremos cómo se nos muestra el escritorio de Rocky Linux cada vez que iniciamos sesión en modo gráfico. Podremos hacer clic en el centro para ver el escritorio, ya que la pantalla que se nos muestra es la que se ve cada vez que hacemos clic en el menú principal que está en la parte superior izquierda donde se nos muestra el texto Activities. Los iconos de la parte inferior nos permitirán abrir un navegador, un manejador de archivos, una consola o ir a ver más aplicaciones entre otras cosas. Ahora ya puede trabajar en su servidor.



1.8 Comandos básicos en linux

1.8.1 Comando cat

Es una maravillosa utilidad que nos permite visualizar el contenido de uno o más archivos de texto sin la necesidad de un editor. Para utilizarlo solo debemos usar el comando, seguido del (de los) nombre(s) de archivo(s) que deseamos visualizar. Ejemplos:

- Para ver el archivo prueba.txt cuando ya estoy en el directorio del archivo:

`cat prueba.txt`

- Para ver el archivo prueba.txt cuando no estoy en el directorio del archivo y el directorio donde esta el archivo es /home/estudiante:
`cat /home/estudiante/prueba.txt`
- Para ver los archivos hosts y sysctl.conf que estan en el directorio /etc, deberemos ejecutar:
`cat /etc/hosts /etc/sysctl.conf`

1.8.2 Comando more

Permite visualizar un archivo de texto, pero visualizarlo por páginas cuando el archivo es demasiado largo para verse en una sola pantalla. Para seguir viendo más abajo del archivo que se visualiza con el comando more, podemos usar la tecla ENTER o la BARRA ESPACIADORA. Si ya no se quiere seguir viendo el archivo y no se quiere llegar hasta el final, solo deberemos presionar la tecla **q**

Ejemplos:

- Para ver el archivo prueba.txt cuando ya estoy en el directorio del archivo:
`more prueba.txt`
- Para ver el archivo prueba.txt cuando no estoy en el directorio del archivo y el directorio donde esta el archivo es /home/estudiante:
`more /home/estudiante/prueba.txt`
- Para ver los archivos hosts y sysctl.conf que estan en el directorio /etc, deberemos ejecutar:
`more /etc/hosts /etc/sysctl.conf`

1.8.3 Comando ls

Permite listar el contenido de un directorio o carpeta (En windows usamos el comando DIR en su lugar). Su sintaxis es:

`ls /ruta/del/directorio/a/listar`

Ejemplos:

- Listar los archivos y directorios del directorio actual:
`ls`
- Listar los archivos y directorios del directorio actual (otra forma):
`ls .`
- Listar los archivos y directorios del directorio /home/estudiante:
`ls /home/estudiante`
- Listar los archivos y directorios del directorio /etc/sysconfig mostrando los usuarios y grupos propietarios, permisos y fechas de los archivos: `ls -l /etc/sysconfig`
- Idem anterior, pero que también queremos que se muestren los archivos y directorios ocultos: `ls -la /etc/sysconfig`

Podemos ver la ayuda de este comando para ver con más detalle las opciones que tiene este comando, ejecutando: `man ls`

NOTA: Este comando, al igual que el comando cat y otros permite usar comodines y expresiones para especificar que archivos y/o directorios se quieren listar.

1.8.4 Comando cd

Este comando permite cambiarse a directorios que se encuentra en una ruta diferente al directorio actual en que te encuentres. Ejemplos:

- Para cambiarse al directorio raiz: `cd /`
- Para cambiarse al directorio que está un nivel arriba del directorio actual: `cd ..`
- Para cambiarse al directorio /etc/sysconfig: `cd /etc/sysconfig`
- Para cambiarse al anterior directorio donde estabas antes de cambiarte al directorio actual: `cd -`

No olvidar que tambien podemos usar este comando con rutas relativas

1.8.5 Comando mkdir

Este comando permite crear uno o más directorios. Ejemplos:

- Deseas crear el directorio fotos dentro del directorio actual donde ya te encuentras: `mkdir fotos`
- Desear crear el directorio cartas dentro del directorio /home/estudiante/Documents, cuando aun no estas dentro del directorio /home/estudiante/Documents y no deseas cambiarte a este directorio: `mkdir /home/estudiante/Documents/cartas`
- Deseas crear el directorio informes, dentro del directorio /home/estudiante/Documents/trabajo, pero aun no existe el directorio trabajo, solo existe hasta el directorio /home/estudiante/Documents, para poder crear el directorio trabajo e informes de un saque usas el comando mkdir con el parametro -p, es decir ejecutaremos lo siguiente: `mkdir -p /home/estudiante/Documents/trabajo/informes`

1.8.6 Comando rm

Este comando permite borrar archivos y/o directorios. Ejemplos:

- Borrar el archivo carta.txt que esta en el directorio actual: `rm cartas.txt`
- Borrar el directorio docs que se encuentra dentro del directorio /home/estudiante: `rm -r /home/estudiante/docs`
- Borrar los archivos que terminan en txt que están dentro del directorio /home/estudiante/Documents: `rm /home/estudiante/Documents/*.txt`

1.8.7 Comando cp

Permite copiar archivo o directorio origen a un archivo o directorio destino. Ejemplos:

- Copiar el archivo prueba.txt ubicado en /home a un directorio de respaldo que esta ubicado dentro de /home/estudiante:
`cp /home/prueba.txt /home/estudiante/respaldo`
- Copiar el contenido de un directorio (archivos y sub-directorios) a otro directorio, por ejemplo el contenido del directorio /home/ejercicios al directorio /home/estudiante/respaldo, deberemos ejecutar el comando cp con el parámetro -r :
`cp -r /home/ejercicios /home/estudiante/respaldo`

1.8.8 Comando mv

Permite mover archivo(s) o directorio(s) a otro archivo o directorio, es decir, que tambien sirve para renombrar archivo(s) o directorio(s). Ejemplos:

- Mover el archivo carta.txt del directorio actual al directorio /home/estudiante/Documents:
`mv carta.txt /home/estudiante/Documents`
- Mover el archivo carta.txt del directorio actual al directorio /home/estudiante/Documents, pero con el nombre carta.doc:
`mv carta.txt /home/estudiante/Documents/carta.doc`
- Renombrar el archivo carta.txt que está en el directorio actual para que ahora tenga el nombre permiso.txt: `mv carta.txt permiso.txt`

1.8.9 Comando clear

Este comando permite limpiar la pantalla. Ejemplo: `clear`

1.8.10 Comando grep

Este comando permite buscar información contenida en uno o más archivos, ya sea especificando el valor exacto del texto a buscar o a traves de una expresión regular. Ejemplo, queremos buscar el texto computador dentro del archivo informe.txt: `grep "computador" informe.txt`

1.8.11 Comando history

Permite listar la historia de comando ejecutados con el usuario actual, pero solo hasta un determinada cantidad de comandos ejecutados. Ejemplos:

- Listar la historia de comandos ejecutados por el usuario actual: `history`
- Listar la historia de comandos ejecutados por el usuario actual, pero en lugar que se muestre toda la historia de golpe, hacer que se muestre por páginas: `history | more`
- De la historia de comandos ejecutados por el usuario actual, mostrar solo los comandos que tengan el texto cp: `history | grep "cp"`

NOTA: En cualquiera de estos ejemplos notaremos que cada comando mostrado es acompañado por un número a la izquierda. Si queremos ejecutar nuevamente el comando, tal cual lo ejecutamos en alguna de esas lineas de historia de comandos, para ejecutar sin volver a escribir el comando tal cual se ejecuto en esa ocación, usaremos el signo de admiración (el carácter !) acompañado del número de la historia del comando a volver a ejecutar (supongamos el comando con el número 301): `!301`

1.8.12 Comando tail

Es un comando que permite mostrar las ultimas lineas de uno o más archivos de texto. Por defecto nos muestra las ultimas 10 lineas, pero se puede indicar cuantas lineas quiero ver del final de un archivo. Ejemplos:

- Ver las ultimas 10 lineas del archivo cartas.txt que esta en el directorio actual:

- ```
tail cartas.txt
```
- Ver las últimas 35 líneas del archivo cartas.txt que está en el directorio actual:  
`tail -35 cartas.txt`
  - Ver las últimas 6 líneas del archivo cartas.txt que está en el directorio actual:  
`tail -6 cartas.txt`

Este comando tambien nos permite hacer seguimiento a un archivo o varios archivos usando chmel parámetro -f. En lugar de mostrar las últimas líneas y terminar, tail mostrará las últimas líneas y seguirá leyendo del archivo; conforme se le añadan nuevas líneas, tail las imprimirá. Esta función es particularmente útil para archivos de registro o bitacoras.

Para cerrar tail cuando esté haciendo seguimiento, basta interrumpirlo con Ctrl+C.

Ejemplo, hacer seguimiento del archivo messages que esta dentro del directorio /var/log de su servidor: `tail -f /var/log/messages`

### 1.8.13 Comando su

Permite cambiar de usuario. Ejemplos:

- Cambiar del usuario actual al usuario juan, sin cargar las variables de ambiente del usuario juan: `su juan`
- Cambiar del usuario actual al usuario juan, cargando las variables de ambiente del usuario juan: `su - juan`

#### 1.8.13.1 Cambiar de usuario a super usuario

Primero ingresemos al sistema como un usuario normal (estudiante). Luego, abra una consola y ejecute el comando `su` sin argumentos e ingrese la clave de acceso de root cuando se le solicite:

```
su
```

Este comando le solicitará la contraseña del root. Debe ingresarla

Ejecute lo siguiente para ver las variables de entorno:

```
echo $USER; echo $LOGNAME; echo $SHELL; echo $PATH; echo $HOME
```

Lo anterior debe devolver la siguiente salida:

```
estudiante
estudiante
/bin/bash
/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:/home/estudiante/.local/bin:/home/estudiante/bin
/root
```

Observe que, aunque se tienen privilegios de root, se carece de las variables de entorno de éste, por lo cual algunos ejecutables sólo se podrán utilizar si se especifica la ruta exacta de éstos (ejemplos: /sbin/service, /sbin/chkconfig, /sbin/fsck y /sbin/fdisk).

Ejecute exit.

**exit**

En una consola ejecuta el comando **su**, esta vez con la opción **-l** (que es lo mismo que «**su -**» o bien «**su --login**» o «**su - root**») e ingrese la clave de acceso de root cuando se le solicite:

**su -l**

Ejecute lo siguiente para consultar las variables de entorno:

```
echo $USER; echo $LOGNAME; echo $SHELL; echo $PATH; echo $HOME
```

Lo anterior debe devolver la siguiente salida:

```
root
root
/bin/bash
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
/root
```

Observe que además de los privilegios de root, se tienen también de las variables de entorno de éste, pues en realidad se ha realizado un ingreso (login) como root.

Ejecute **exit** para regresar como usuario regular (estudiante).

**exit**

## 1.9 Información básica para gestión de dispositivos de red

### 1.9.1 Nombres de dispositivos de red

Tradicionalmente, las interfaces de red en Linux se enumeran como **eth[0123...]**, pero estos nombres no se corresponden necesariamente con las etiquetas reales en la tarjeta madre. Las plataformas de servidor modernas con múltiples adaptadores de red pueden encontrar nombres no deterministas y contraintuitivos de estas interfaces. Esto afecta tanto a los adaptadores de red incrustados en la placa base (Lan-on-Motherboard, o LOM) como a los adaptadores complementarios (de puerto único y multipuerto).

Rocky Linux 9 admite varios esquemas de nombres diferentes. De manera predeterminada se asignan nombres fijos basados en firmware, topología e información de ubicación. Esto tiene la ventaja de que los nombres son totalmente automáticos, totalmente predecibles, que permanecen fijos incluso si se agrega o quita el hardware (no se lleva a cabo una nueva enumeración), y que el hardware dañado se puede reemplazar sin problemas. La desventaja es que a veces son más difíciles de leer que los nombres **eth0** o **wlan0** tradicionalmente utilizados. Por ejemplo: **enp5s0**.

Rocky Linux 9 sigue la siguiente política de esquemas de nombres para dar nombre a los dispositivos de red:

- Esquema 1: Da los nombres que incorporan el firmware o el BIOS y proporciona los números de índice para los dispositivos incorporados (ejemplo: **eno1**), se aplican si esa información del firmware o BIOS es aplicable y está disponible, sino recaen en el esquema 2.

## Temas Especiales

---

- Esquema 2: Da los nombres que incorporan Firmware o BIOS y proporciona los números de índice de ranura PCI Express HotPlug (ejemplo:ens1) se aplican si esa información del firmware o BIOS es aplicable y está disponible, sino que recae en el esquema 3.
- Esquema 3: Da los nombres que incorporan la ubicación física del conector del hardware (ejemplo: enp2s0) se aplican si corresponde, de lo contrario caen directamente al esquema 5 en todos los demás casos.
- Esquema 4: Da los nombres que incorporan la dirección MAC de la interfaz (ejemplo: enx78e7d1ea46da), no se usan por defecto, pero están disponibles si el usuario lo elige.
- Esquema 5: El esquema de nomenclatura de kernel tradicional impredecible, se utiliza si todos los otros métodos fallan (ejemplo: eth0).

En resumen, si utiliza Rocky Linux 9 o Red Hat™ Enterprise Linux 9 los dispositivos de red integrados a la tarjeta madre utilizan el esquema eno[1,2,3,4...]; los dispositivos PCI Express HotPlug ens[1,2,3,4,...]; los dispositivos PCI utilizan el esquema enp[ranura PCI]p[puerto ethernet] y —en el caso de dispositivos virtuales— eno[ranura PCI]p[puerto ethernet]\_[interfaz virtual] o enp[ranuraPCI]p[puerto ethernet]\_[interfaz virtual]. Ejemplos:

- eno1 corresponde al primer dispositivo de red integrado en la tarjeta madre.
- eno2 corresponde al segundo dispositivo de red integrado en la tarjeta madre.
- eno3 corresponde al tercer dispositivo de red integrado en la tarjeta madre.
- enp1p1 corresponde al dispositivo de red en la primera ranura PCI, primer puerto ethernet.
- enp2p1 corresponde al dispositivo de red en la segunda ranura PCI, primer puerto ethernet.
- enp3p1 corresponde al dispositivo de red en la tercera ranura PCI, primer puerto ethernet.
- enp3p2 corresponde al dispositivo de red en la tercera ranura PCI, segundo puerto ethernet.
- enp3p2\_1 corresponde al dispositivo de red en la tercera ranura PCI, segundo puerto ethernet, primer dispositivo virtual.

Pueden determinarse los dispositivos de red presentes en el sistema revisando el contenido del directorio /sys/class/net/:

```
ls /sys/class/net/
```

Puede consultarse la asignación de nombres de dispositivos de red presentes en el sistema, a través del archivo /etc/udev/rules.d/70-persistent-net.rules..

```
vi /etc/udev/rules.d/70-persistent-net.rules
```

En Rocky 9 si queremos desactivar esta nueva nomenclatura deberá buscar información como cambiar esto en los argumentos para el núcleo de Linux (**net.ifnames** y **biosdevname**) los cuales verá se modifican a través del grub.

### 1.9.2 NetworkManager

NetworkManager es una implementación que permite a los usuarios regulares controlar y añadir dispositivos de red. Resulta perfecto para facilitar la administración de interfaces inalámbricas, conexiones de VPN, conexiones PPPoE y cualquier conexión de red desde el escritorio. En un servidor es absurdo permitir esto ya que por lo general la administración del mismo se hace de manera remota a través de una consola de texto a través de SSH. La única ventaja que

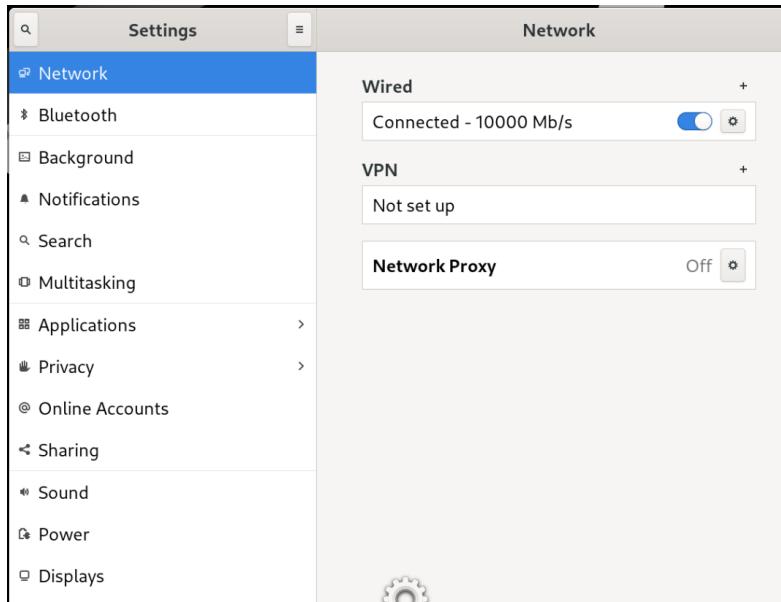
## Temas Especiales

---

tiene frente al servicio network es que detecta, activa y desactiva automáticamente los dispositivos ethernet cuando se conecta y desconecta el cable correspondiente.

En Rocky Linux 9 y Red Hat™ Enterprise Linux 9, NetworkManager viene activo e instalado de modo predeterminado en cualquier tipo de instalación.

Como estaremos trabajando con el modo gráfico usted puede ir a la interface del NetworkManager haciendo clic con el botón secundario sobre el escritorio y luego clic en **Settings** y finalmente hacemos clic en Network, lo cual nos llevará a ver una ventana como la mostrada en la figura siguiente (A la cual también puede llegar haciendo clic en el icono de red de su barra horizontal superior del lado derecho)



Una vez realizada estas acciones podrá ver las interfaces de red que usted tiene trabajando en su servidor y podrá activarlas (si no lo están), desactivarlas o configurarlas a conveniencia.

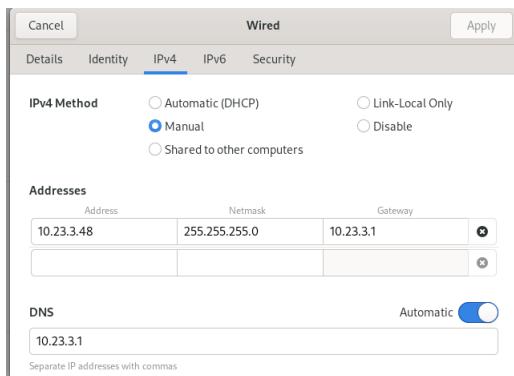
Si elegimos el botón que muestra el icono de un engranaje podremos configurar la interfaz de red seleccionada y se nos lanzara la siguiente ventana:



## Temas Especiales

---

Para cambiar la configuración de red de la tarjeta de red seleccionada de nuestro servidor elegiremos la pestaña marcada IPv4 (o IPv6 si vamos a trabajar con IP versión 6). Esto nos siguiente ventana de configuración IP versión 4:



En esta ventana deberemos seleccionar configuración **Manual**, para luego ingresar la IP, mascara, puerta de enlace y el servidor DNS que usará nuestro servidor (use la configuración que se le asigne). Una vez ingresada la configuración hacemos clic en el botón **Apply**. Al volver a la ventana anterior desactivamos la interface y la volvemos a activar (tal como se explicó hace dos párrafos) para que la configuración sea activada.

**NOTA: Si ya hicimos la configuración al momento de instalar no necesitará tocar esta parte, solo en caso que requiera cambiarlo**

### 1.9.3 Asignación de nombre de anfitrión

Cuando hablamos de nombre de anfitrión nos referimos al nombre que quiere que tenga su servidor. Puede ser que usted al momento de instalar su servidor no se haya fijado que hay una sección donde se pide ese dato y que si usted no lo cambia su servidor es instalado con el nombre `localhost.localdomain`.

El nombre del anfitrión, nombre de servidor o hostname (como usted prefiera llamarlo) debe ser un FQDN (acrónimo de Fully Qualified Domain Name o Nombre de Dominio Plenamente Calificado) resuelto por un servidor de nombres de domino (DNS). El nombre del anfitrión, tiene el formato **nombre.dominio**. Por ejemplo podría ser: [srvr9.sof164.net](http://srvr9.sof164.net) . En el texto hemos subrayado el dominio para que usted note la diferencia en el ejemplo.

El nombre de su servidor se puede cambiar cuando usted lo vea necesario. Para poder realizar esto, tenemos las siguientes opciones:

Como primera opción, si utiliza Fedora™, Rocky Linux 9 y Red Hat™ Enterprise Linux 9 puede configurar el nombre de su servidor editando el archivo `/etc/hostname`:

**`vi /etc/hostname`**

En este archivo solo ponga el nombre que desea para su servidor reemplazando el valor que ya existe en dicho archivo, al finalizar no debe presionar la tecla ENTER, solo grabar el archivo y salir del mismo. Para que el cambio tenga efecto, reinicie el servidor o simplemente reinicie el servicio de `systemd-hostnamed` ejecutando con el usuario root el siguiente comando:

```
systemctl restart systemd-hostnamed
```

La segunda opción para cambiar el nombre de su servidor, es ejecutar lo siguiente utilizando herramientas de SystemD:

```
hostnamectl set-hostname nombre.dominio
systemctl restart systemd-hostnamed
```

**NOTA:** Para poder ejecutar estos comandos debe estar logueado en una consola con el usuario root.

Si usted luego quiere verificar el cambio, ejecute el siguiente comando como root:

```
hostnamectl status
```

El resultado de ejecutar este comando podría ser:

```
Static hostname: nombre_nuevo_del_servidor
Icon name: computer-vm
Chassis: vm
Machine ID: 6b79493a1c72445dafe62e023f7127c4
Boot ID: 948cd346e04144919aa8c915cd8b0135
Virtualization: vmware
Operating System: Rocky Linux 9.4 (Blue Onyx)
CPE OS Name: cpe:/o:rocky:rocky:9::baseos
Kernel: Linux 5.14.0-362.8.1.el9_3.x86_64
Architecture: x86-64
Hardware Vendor: VMware, Inc.
Hardware Model: VMware Virtual Platform
```

### 1.9.4 Otras herramientas útiles del intérprete de comando

Si usted desea saber si tiene conexión de red a un servidor que tiene habilitado responder al comando ping, en una consola de su servidor, ejecute ping hacia la dirección de la red del servidor al que desea saber que tiene conexión.

```
ping -c3 192.168.70.1
```

La opción -c3 indica que sólo se harán 3 pings hacia la dirección IP de destino.

Para ver la información de todos los dispositivos de red del sistema, se ejecuta lo siguiente:

```
ip addr show
```

En el pasado lo anterior se hacía utilizando ifconfig.

Para ver la información de un dispositivo de red específico, ens33 en el siguiente ejemplo, se ejecuta lo siguiente:

```
ip addr show ens33
```

En el pasado lo anterior se hacía ejecutando ifconfig ens33.

## Temas Especiales

---

Para ver la información de estado de todos los dispositivos de red del sistema, se ejecuta lo siguiente:

```
ip link show
```

Para ver la información de estado de un dispositivo de red en particular, eth0 en el siguiente ejemplo, se ejecuta lo siguiente:

```
ip link show ens33
```

Para detener un dispositivo de red, ens33 en el ejemplo, se ejecuta lo siguiente:

```
ip link set ens33 down
```

En el pasado lo anterior se hacía ejecutando ifdown ens33.

Para iniciar un dispositivo de red, ens33 en el ejemplo, se ejecuta lo siguiente:

```
ip link set ens33 up
```

En el pasado lo anterior se hacía ejecutando ifup ens33.

Ejecute lo siguiente para ver las rutas estáticas:

```
ip route list
```

En el pasado lo anterior se hacía ejecutando route.

Para hacer una consulta hacia los servidores DNS definidos para el sistema y comprobar si hay resolución de nombres, podemos ejecutar cualquiera de los siguientes tres comandos:

```
host www.uagrm.edu.bo
dig www.uagrm.edu.bo
nslookup www.uagrm.edu.bo
```

## 1.10 Deshabilitar lista de usuario en el login

Si deseamos que el sistema no nos visualice la lista de usuarios regulares con los que nos podemos loguear al sistema, podemos realizar los siguientes pasos para desactivar esta opción.

- i. Cambiarse al **root**
- ii. Cambiarse al directorio **/etc/dconf/db/gdm.d/**
- iii. Crear o editar el archivo **00-login-screen**, colocando solo el siguiente contenido

```
[org/gnome/login-screen]
No mostrar la lista de usuarios
disable-user-list=true
```

- Ejecutar el comando: **dconf update**. Luego ya puede cerrar sesión o reiniciar su servidor para probar el cambio

## 1.11 Habilitar el DVD como repositorio de instalación

El gestor de paquetes de Rocky 9 (conocido antes como yum, pero ahora reemplazado por dnf), por defecto cada vez que le pedimos instalar algún paquete, realiza la instalación desde los repositorios de línea, para lo cual necesitamos que nuestro servidor tenga acceso a internet, pero si deseamos que utilice el DVD de instalación como repositorio (sobre todo si tenemos la distribución todo en uno) podemos realizar el siguiente procedimiento, pero antes deberemos tener el DVD disponible en nuestro lector de DVD real (si es una maquina real) o virtual (si es una máquina virtual):

- i. Cambiarse al **root**
- ii. Cambiarse al directorio **/etc/yum.repos.d**
- iii. Crear un archivo de configuración de repositorio, por ejemplo **dvd.repo**
- iv. Agregar el siguiente texto (puede tomar como base cualquiera de los archivos repo existentes y modificar a lo que sigue):

```
[baseosDVD]
name=Rocky Linux $releasever - BaseOSDVD
baseurl=file:///media/dvdrom/BaseOS
gpgcheck=1
enabled=1
countme=1
metadata_expire=-1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-Rocky-9

[appstreamDVD]
name=Rocky Linux $releasever - AppStreamDVD
baseurl=file:///media/dvdrom/AppStream
gpgcheck=1
enabled=1
countme=1
metadata_expire=-1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-Rocky-9
```

- v. Hay que editar el archivo **dvd.repo** para que en la sección baseurl solo tenga la ruta del directorio donde va montar el DVD de Rocky. Por ejemplo, supongamos que donde usted montará su DVD será en el directorio /media/dvdrom, entonces el archivo se verá como en la tabla anterior.
- vi. Si no existe la carpeta /media/dvdrom, debemos crearla, como siempre con el usuario root, ejecutando el comando: **mkdir /media/dvdrom**
- vii. Ahora debemos hacer que el dvd este montado en esta carpeta. Para lograr eso hacemos lo siguiente:
  - a. Primero, si es una maquina real ponemos el dvd, pero si es una maquina virtual, solo debemos conectar el dvd en la maquina virtual
  - b. Luego, en una consola de comandos del servidor linux, con el usuario root, debemos ejecutar el comando “**df -h**” para ver donde está montado actualmente el dvd. Al ejecutar el comando podríamos ver las siguientes líneas, donde prestaremos atención a la línea /run/media porque es ahí donde está montado actualmente el dvd y podremos saber cómo reconoce el sistema a su DVD:

| Filesystem          | Size | Used | Avail | Use% | Mounted on |
|---------------------|------|------|-------|------|------------|
| devtmpfs            | 4.0M | 0    | 4.0M  | 0%   | /dev       |
| tmpfs               | 1.8G | 0    | 1.8G  | 0%   | /dev/shm   |
| tmpfs               | 726M | 10M  | 716M  | 2%   | /run       |
| /dev/mapper/rl-root | 36G  | 7.8G | 28G   | 23%  | /          |

|                |       |      |      |      |                                            |
|----------------|-------|------|------|------|--------------------------------------------|
| /dev/nvme0n1p1 | 1014M | 286M | 729M | 29%  | /boot                                      |
| tmpfs          | 363M  | 112K | 363M | 1%   | /run/user/1002                             |
| tmpfs          | 363M  | 108K | 363M | 1%   | /run/user/1000                             |
| /dev/sr0       | 8.4G  | 8.4G | 0    | 100% | /run/media/estudiante/Rocky-9-4-x86_64-dvd |

- c. En esta guía hemos resaltado en rojo una de las líneas, la de **/run/media/estudiante/Rocky-9-4-x86\_64-dvd**. Entonces de esta línea sacamos dos cosas:
- **/dev/sr0** (El nombre del dispositivo DVD en su sistema)
  - **/run/media/estudiante/Rocky-9-4-x86\_64-dvd** (El directorio donde el sistema monto el DVD)
- d. Procedemos a desmontar el DVD ejecutando:  
`umount /run/media/estudiante/Rocky-9-4-x86_64-dvd`
- e. Ahora procedemos a montar el DVD en la carpeta que **configuramos** en el archivo de repositorio que era /media/dvdrom:  
`mount /dev/sr0 /media/dvdrom/`

Ahora ya podra usar el dvd como repositorio, pero debe asegurarse que el dvd este montado donde lo configure en su archive dvd.repo y para cada instalación que haga al usar comando dnf indicando que no use los otros repositorios y solo use los dos repositorios que habilita con el dvd es decir, en este caso (baseosDVD y appstreamDVD), es decir así:

```
dnf --disablerepo=* --enablerepo=baseosDVD,appstreamDVD -y install tigervnc-server
```

En este ejemplo instalamos el paquete tigervnc-server desde el dvd.

### NOTA IMPORTANTE:

Para no tener el dvd como repositorio permanente, colocar el parametron Enabled con el valor 0 y no con el valor 1, asi cuando quiera Volver a usar los repositorios de linea, simplemente tendra que Volver a usar el comando dnf sin agregar los parámetros --disablerepo o --enablerepo, o simplemente borre el archivo que habilita el dvd como repositorio (en este ejemplo el archivo se llamo dvd.repo)

Ej, el mismo comando para instalar el paquete tigervnc-server pero de los repositorios solo habilitados y disponibles (no olvide deshabilitar o borrar el repositorio del dvd si lo realizó)

```
dnf -y install tigervnc-server
```

## 1.12 Habilitar el acceso a internet vía proxy web

Un **proxy**, o **servidor proxy**, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio le permite ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, proxy web, etc.

## Temas Especiales

---

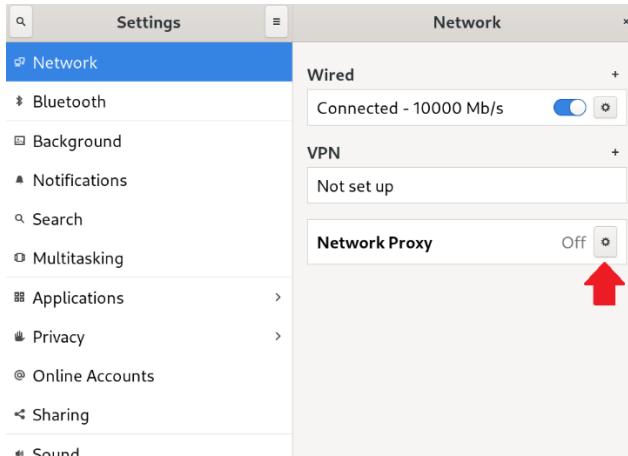
Un **proxy web**, se trata de un proxy para una aplicación específica: el acceso a la web con los protocolos HTTP y HTTPS, y accesoriamente FTP. Aparte de la utilidad general de un proxy, puede proporcionar una caché compartida para las páginas web y contenidos descargados, actuando entonces como servidor proxy-caché. Esta caché es compartida por múltiples usuarios con la consiguiente mejora en los tiempos de acceso para consultas coincidentes y liberando de carga a los enlaces de acceso a Internet.

### NOTA IMPORTANTE:

Si su servidor accede a internet sin necesidad de un servidor proxy o con proxy transparente, **NO NECESITA CONFIGURAR LA OPCIÓN PROXY y NO NECESITA HACER LO QUE SE INDICA EN ESTE PUNTO.**

Si tiene la necesidad de que su servidor Rocky Linux 9 acceda a internet vía proxy web no transparente, tiene 2 opciones para caso de usar un proxy web no transparente: la que permite habilitar internet solo para el usuario con el que se realiza la configuración o la opción que permite habilitar para todo el sistema y todos los usuarios. Para el caso de usar proxy web transparente tiene la tercera opción que es la que habilita el acceso a internet para todo su sistema.

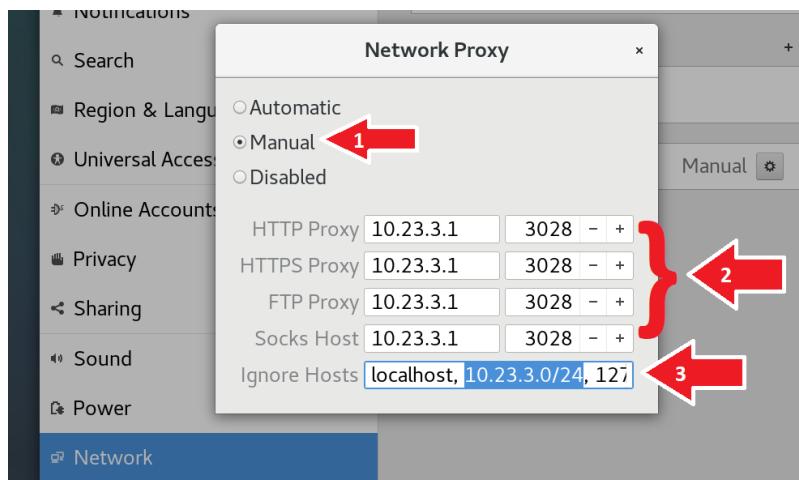
**OPCIÓN 1 PARA CONFIGURAR ACCESO A INTERNET VIA PROXY NO TRANSPARENTE** (Solo para ese usuario cuando el proxy web no es proxy transparente), hágalo utilizando NetworkManager (Ya explicamos más arriba como llegar al NetworkManager), en la ventana que se muestra hacemos clic en el ícono para seleccionar que queremos configurar en la opción de proxy, en el orden marcado en las figuras a continuación:



Luego de hacer clic en el ícono marcado con la flecha y veremos la siguiente ventana, donde para nuestro caso procederemos así:

- 1) Elegimos como método Manual,
- 2) ingresamos la ip y el puerto del servidor donde está habilitado el servicio proxy (supongamos que el proxy está en la IP 10.23.3.1 y que el puerto es el 3128)

- 3) En la casilla **ignore host**, agregamos el host, IP o red para quien no deseamos tener conexión de red vía proxy (en este caso colocaremos, además de lo que ya viene, aumentaremos toda nuestra red del laboratorio y si hace falta algún dominio local que tengamos; en este caso para nuestra red aumentaremos **10.23.3.0/24** con lo que especificamos que con esta red nuestro servidor no necesita usar proxy). Observe en la figura hemos agregado una red. Usar como separador



#### **OPCIÓN 2 PARA CONFIGURAR ACCESO A INTERNET VIA PROXY WEB NO TRANSPARENTE:**

Este procedimiento solo servirá para el usuario con el que realiza el cambio, no establece el proxy para todo el sistema, pero, si necesitamos establecer el proxy para todo el sistema, y no solo para un usuario, entonces no es necesario hacer el paso anterior. En todo caso, deberemos editar el archivo **environment** que está dentro del directorio **/etc** y colocar dentro de este archivo la configuración del proxy para el sistema del siguiente modo:

```
all_proxy="http://10.23.3.1:3128/"
http_proxy="http://10.23.3.1:3128/"
https_proxy="http://10.23.3.1:3128/"
ftp_proxy="http://10.23.3.1:3128/"
no_proxy="localhost,127.0.0.0/8,10.23.3.0/24,::1,sof164.net,*.sof164.net,
.sof164.net"
```

En este ejemplo le hemos marcado con rojo, lo que agregamos en la casilla ignore host en la interfaz gráfica, pero hemos marcado con azul lo que no pusimos en el ejemplo de la interfaz gráfica, para indicar que con cualquier computador que forme parte del dominio **sof164.net** no necesitaremos usar proxy para establecer conexión por red.

Por otro lado, si deseamos instalar algun paquete con el comando **dnf**, también tendremos que editar el archivo **dnf.conf** que está dentro del directorio **/etc/dnf** (mejor si sacamos primero una copia de seguridad) y luego agregar la siguiente línea:

```
proxy=http://10.23.3.1:3128/
```

**NOTA IMPORTANTE:** No haga nada de todo esto si no está usando proxy web no transparente para acceder a internet.

**OPCION 3 CUANDO ESTÁ USANDO PROXY WEB TRANSPARENTE**, asegúrese de colocar como Gateway (puerta de enlace por defecto) y como DNS por defecto la IP de su servidor proxy. Consulte en clases que ip usar como Gateway y DNS

**NOTA IMPORTANTE: SI NO USA NINGUN TIPO DE PROXY WEB NO TRANSPARENTE NO HAGA NINGUNA DE LAS 3 OPCIONES ANTES MENCIONADAS.**

## 1.13 LibreOffice

LibreOffice es un paquete de software de oficina (suite ofimática, es decir, es una recopilación de aplicaciones informáticas utilizadas en oficinas, para realizar diferentes funciones sobre archivos y documentos, como crear, modificar, organizar, escanear, imprimir, entre otros), libre y de código abierto desarrollado por The Document Foundation. Se creó como bifurcación de OpenOffice en 2010. El entorno está programado en los lenguajes informáticos Java, C++ y Python.

El formato de archivo propio de LibreOffice es OpenDocument, un formato estándar y abierto que está siendo adoptado por gobiernos de todo el mundo como formato de archivo obligatorio para la publicación y aceptación de documentos.

Está diseñada para ser compatible con los principales paquetes ofimáticos, incluyendo Microsoft Office, aunque algunas características de diseño y atributos de formato son manejados de forma diferente o no son compatibles. LibreOffice está disponible en más de 120 idiomas (incluyendo español, catalán, vasco y gallego) y para diferentes sistemas operativos, incluyendo Microsoft Windows, Mac OS X 10.4 Tiger o superior y GNU/Linux (incluyendo un visor de LibreOffice para Android), así como en forma de una suite de oficina en línea. Es la suite ofimática por defecto en las distribuciones Linux más populares.

### 1.13.1 Componetes de LibreOffice

LibreOffice incluye las siguientes aplicaciones:

#### 1.13.1.1 Writer

LibreOffice Writer es el componente procesador de texto de LibreOffice. Writer es una herramienta con múltiples funciones para crear cartas, libros, informes, boletines, folletos y otros documentos. Puede insertar en documentos Writer gráficos y objetos desde otros componentes. También puede exportar archivos a HTML, XHTML, XML, al Formato de Documentos Portables de Adobe (PDF) y a varios formatos de archivos de Microsoft Word. Además, se conecta con su cliente de correo electrónico.

#### 1.13.1.2 Calc

LibreOffice Calc es el componente hoja de cálculo de LibreOffice. Calc tiene todas las características de análisis avanzado, gráficos y funciones para la toma de decisiones que se pueden esperar de una hoja de cálculo de alto desempeño. Incluye más de 300 funciones para operaciones financieras, estadísticas y matemáticas, entre otras. El Gestor de Escenario provee análisis hipotético. Calc genera diagramas en 2D y en 3D, que pueden integrarse dentro de otros documentos de LibreOffice. Puede también abrir y trabajar con documentos de Microsoft Excel y guardarlos en formato Excel. Calc puede exportar hojas de cálculo a PDF y a HTML.

### 1.13.1.3 Impress

LibreOffice Impress es el componente para elaboración de presentaciones de LibreOffice. Impress proporciona todas las herramientas de presentación multimedia comunes, tales como efectos especiales, animación y herramientas de dibujo. Está integrado con las funciones gráficas avanzadas de los componentes de Draw y Math de LibreOffice. Las diapositivas pueden ser mejoradas con los efectos especiales de texto Fontwork, así como clips de sonido y video. Impress es compatible con archivos de formato Microsoft PowerPoint e incluso puede abrir y guardar su trabajo en numerosos formatos gráficos, incluyendo Macromedia Flash (SWF).

### 1.13.1.4 Draw

LibreOffice Draw es el componente de edición de graficos vectoriales de LibreOffice. Draw es una herramienta para creación de gráficos vectoriales que puede producir de todo, desde diagramas simples o diagramas de flujo a dibujos artísticos en 3D. Su característica de Conector inteligente le permite definir sus propios puntos de conexión. Puede utilizar Draw con el propósito de crear dibujos para utilizarlos en otros componentes de LibreOffice y puede crear sus propias imágenes prediseñadas y agregarlas a la galería. Draw puede importar gráficos de los formatos más comunes y guardarlos en más de 20 formatos, incluyendo PNG, HTML, PDF y Flash).

### 1.13.1.5 Base

LibreOffice Base es el componente de gestión de base de datos de LibreOffice. Base proporciona herramientas para el trabajo diario con bases de datos dentro de una interfaz sencilla. Puede crear y editar formularios, reportes, consultas, tablas, vistas y relaciones, de manera que la gestión de una base de datos es bastante parecida a otras aplicaciones de características similares. Base proporciona varias características nuevas, tales como la habilidad de analizar y editar relaciones a partir de la vista de un diagrama. Base incorpora HSQLDB como su motor de bases de datos relacional por defecto. También puede utilizar dBASE, Microsoft Acces, MYSQL u ORACLE, o cualquier base de datos compatible con ODBC o JDBC. Base también ofrece compatibilidad con un subconjunto de ANSI-92 SQL.

### 1.13.1.6 Math

LibreOffice Math es el componente para edición de fórmulas o ecuaciones de LibreOffice. Math es el editor de fórmulas o editor de ecuaciones de LibreOffice. Puede utilizarlo para crear ecuaciones complejas que incluyan símbolos o caracteres no disponibles para el conjunto de fuentes estándar. Aunque se usa habitualmente para crear fórmulas en otros documentos, como por ejemplo archivos de Writer e Impress, Math también puede trabajar como aplicación independiente. Puede guardar fórmulas en otros documentos en formato de Lenguaje de Marcado Matemático Estándar (MathML) para incluirlas en páginas web y otros documentos que no hayan sido creados por LibreOffice.

## 1.13.2 Ventajas de LibreOffice

- No hay pago de licencia
- De código abierto
- Multiplataforma

## Temas Especiales

---

- Soporte extensivo de idiomas y corrector ortográfico
- Interfaz de usuario coherente
- Integración
- No necesita saber con qué aplicación se creó un archivo
- Compatibilidad de archivos
- No se ata a ningún proveedor (Formato de archivo OpenDocument – Es formato XML)
- Tiene versión portable y versión Visor para Android.

### 1.13.3 Requisitos mínimos de LibreOffice

#### 1.13.3.1 En Microsoft Windows

Los requisitos de hardware y software para instalar LibreOffice en sistemas Windows son los siguientes:

- Microsoft Windows 7 SP1 (con la actualización KB3063858), Windows 8, Windows Server 2012, Windows 10 o Windows 11;
- PC compatible con Pentium (Pentium III, Athlon, aunque se recomienda un sistema más reciente);
- 256 MB de RAM (se recomiendan 512 MB de RAM);
- Al menos 1,5 GB disponibles en el disco duro;
- Resolución de por lo menos 1024 × 768 (se recomienda más alta), con al menos 256 colores.

Es necesario contar con privilegios administrativos para el proceso de instalación. Se recomienda realizar una copia de seguridad del sistema y de sus datos antes de quitar o instalar software.

Para ciertas características del software —pero no para la mayor parte— se requiere Java. Resulta especialmente necesario para Base

#### 1.13.3.2 En Apple macOS (Mac OS X)

Los requisitos de software y hardware para instalar LibreOffice en sistemas Apple macOS son los siguientes:

- macOS 10.12 o superior
- Procesador Intel o Apple Silicon (vía Rosetta; la compatibilidad con Silicon está en pruebas)
- 512 MB de RAM;
- Al menos 800 MB disponibles en el disco duro;
- Resolución de por lo menos 1024 × 768 (se recomienda más alta), con al menos 256 colores.

Se recomienda realizar una copia de seguridad del sistema y de sus datos antes de quitar o instalar software.

Notas:

- Para ciertas características del software —pero no para la mayor parte— se requiere Java. Resulta especialmente necesario para Base.

- Debido a un problema, existen las siguientes restricciones con Java: en macOS 10.10 y posteriores, no se encuentra JRE, se requiere JDK.
- LibreOffice 4.3 aún puede ejecutarse bajo OS X 10.6+, pero sepá que su servicio técnico finalizó cuando la versión 4.3 fue retirada el 27 de mayo de 2015.

### 1.13.3.3 En GNU/Linux

Como regla general se recomienda instalar LibreOffice a través de los métodos de instalación recomendados por su distribución Linux (como el Centro de software, en el caso de Ubuntu Linux). Esto se debe a que suele ser la forma más sencilla de obtener una instalación que se integre de manera óptima en el sistema. De hecho, es posible que LibreOffice ya esté instalado de forma predeterminada cuando instale el sistema operativo Linux.

Los instaladores de LibreOffice suministrados por la comunidad se proporcionan para los usuarios con necesidades especiales, y para los casos fuera de lo común.

Los prerequisitos de software y hardware para la instalación en Linux son los siguientes:

- Núcleo Linux, versión 3.10 o superior;
- glibc2, versión 2.17 o superior;
- PC compatible con Pentium (Pentium III, Athlon, aunque se recomienda un sistema más reciente);
- 256 MB de RAM (se recomienda 512 MB de RAM);
- Al menos 1,55 GB disponibles en disco;
- Servidor X con resolución de 1024 × 768 (se recomienda más alta), con al menos 256 colores;
- Gnome 3.18 o más reciente, con el paquete at-spi 1.32 (necesario para la compatibilidad con las herramientas de tecnología de asistencia [AT]), u otra interfaz gráfica de usuario compatible (tal como KDE, entre otras).

Para ciertas características del software —pero no para la mayor parte— se requiere Java. Resulta especialmente necesario para Base.

Se recomienda realizar una copia de seguridad del sistema y de sus datos antes de quitar o instalar software.

## Capítulo 2. Acceso Remoto

### 2.1 Definición

Antes de entrar de lleno en la definición del término acceso remoto que nos ocupa es importante conocer el significado individual de cada palabra. En este caso, podemos establecer que este es el que poseen las dos palabras que le dan forma: “**Acceso** es el acto de alcanzar algo o de aproximarse. **Remoto**, por su parte, es aquello que se encuentra alejado o que es poco probable que suceda”.

En informática, Un acceso remoto es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet).

En el acceso remoto se ven implicados protocolos (En informática, un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes), y programas en ambas computadoras que permitan recibir/enviar los datos necesarios. Además, deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y los programas).

Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras. Se pueden acceder a archivos, dispositivos periféricos (como impresoras), configuraciones, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

Debemos tomar en cuenta que para poder tener acceso remoto desde un computador A (cliente) hacia otro computador B (servidor), ambos dispositivos además de estar comunicados a través de una red informática, deben disponer del software necesario para poder realizar dicha tarea. El dispositivo B debe tener habilitado un servicio que le permita a usted acceder a determinados recursos utilizando dicho servicio a través de una red y dispositivo A debe contar con el software cliente que le permita conectarse al servicio publicado por el dispositivo B.

Igunos ejemplos de acceso remoto son ssh, escritorios remotos y ftp.

### 2.2 SSH

SSH (**S**ecure **S**Hell, en español: intérprete de órdenes seguro) es un conjunto de estándares y protocolo de red que permite establecer una comunicación a través de un canal seguro entre un cliente local y un servidor remoto. Utiliza una llave pública para autenticar el servidor remoto y —de manera opcional— permitir al servidor remoto autenticar al usuario. SSH provee confidencialidad e integridad en la transferencia de los datos utilizando criptografía y MAC (Message Authentication Codes o Códigos de Autenticación de Mensaje). De modo predeterminado, escucha peticiones a través del puerto 22 por TCP.

Permite acceder a servidores donde esté dicho servicio habilitado para manejar por completo el servidor mediante un intérprete de comandos, y también permite redirigir el tráfico de X (Sistema de Ventanas X) para poder ejecutar programas gráficos si tenemos ejecutando un Servidor X (en sistemas Unix y Windows).

## Temas Especiales

---

SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas, a través de SFTP), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH a través de SCP.

- SFTP (SSH File Transfer Protocol), que es una de las funcionalidades que se incluye en SSH, es un protocolo que provee funcionalidad de transferencia y manipulación de archivos a través de un flujo confiable de datos. Comúnmente se utiliza con SSH para proveer a éste de transferencia segura de archivos.
- SCP (Secure Copy o Copia Segura), que también es una de las funcionalidades que se incluye en SSH, es un protocolo seguro para transferir archivos entre un anfitrión local y otro remoto. Básicamente, es idéntico a RCP (Remote Copy o Copia Remota), con la diferencia de que los datos son cifrados durante la transferencia para evitar la extracción potencial de información a través de programas de captura de las tramas de red (packet sniffers). SCP sólo implementa la transferencia de archivos, pues la autenticación requerida es realizada a través de SSH.

En un servidor donde se tiene instalado un sistema operativo GNU/Linux si se quiere habilitar la capacidad de acceder a dicho servidor de forma remota vía SSH, se hace uso de OpenSSH (Open Secure Shell), el cual es una alternativa de código fuente abierto, con licencia BSD, puesto que la versión original de SSH creada por Tatu Ylönen es propietaria y de código cerrado. OpenSSH es un proyecto creado por el equipo de desarrollo de OpenBSD y actualmente dirigido por Theo de Raadt. Se considera que es más segura que la versión privativa Ylönen, gracias a la constante auditoría que se realiza sobre el código fuente por parte de una enorme comunidad de desarrolladores, una ventaja que brinda el Software Libre.

OpenSSH incluye servicio y clientes para los protocolos SSH, SFTP y SCP.

### 2.2.1 Habilitar SSH con OpenSSH en Rocky Linux

**IMPORTANTE: EJECUTE EL PROCEDIMIENTO ABAJO DESCRITO, SOLO SI NO INSTALO SSH CUANDO INSTALO SU SISTEMA OPERATIVO**

- i. En una consola de comandos cambiar al root
- ii. Instalar los paquetes para que su servidor Rocky Linux pueda servir como servidor y como cliente ssh

```
dnf -y install openssh openssh-server openssh-clients openssl-libs
```

- iii. Si el servicio no está habilitado lo hacemos ejecutando el comando

```
systemctl enable sshd.service
```

- iv. Si el servicio no está iniciado lo hacemos ejecutando el comando

```
systemctl start sshd.service
```

## Temas Especiales

---

- v. Si el servicio no está habilitado en el firewall, dar permisos de acceso ejecutando  
`firewall-cmd --permanent --zone=public --add-service ssh`  
`firewall-cmd --reload`
- vi. (Opcional) Si deseamos cambiar la configuración por defecto del servicio, procedemos a:
  - a. Sacar copia de seguridad al archivo de configuración del servicio ssh  
`cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig`
  - b. Editamos y cambiamos el archivo de configuración del servicio  
`vi /etc/ssh/sshd_config`
  - c. Procedemos a realizar cambios en los parámetros de ssh, grabamos el archivo y salimos de dicho archivo.
  - d. Reiniciamos el servicio  
`systemctl restart sshd.service`

### 2.2.1.1 Algunos parámetros configuración del servicio ssh

- **Port.**- Permite establecer el puerto en que atiende el servicio. Por defecto el servicio atiende en el puerto 22. Si desea cambiar el puerto para ssh, edite el archivo /etc/ssh/sshd\_config, busque la linea donde esta #Port 22, quite el carácter # y cambie el 22 por el puerto deseado. Luego reinicie el servicio. (No se olvide de dar permisos en el firewall para este nuevo puerto)
- **PermitRootLogin.**- Permite establecer si se permite conectarse por ssh al servidor usando el usuario root. Si no desea que se accese al servidor con el usuario root usando ssh, ponga el valor no a este parámetro y luego reinicie el servicio.
- **LoginGraceTime.**- Este parámetro el tiempo que se demora la pantalla de login abierta a la espera de que el usuario se autentique. Si el usuario demora más de este tiempo en autenticarse el servidor no le permitirá acceder esa vez. Por ejemplo si queremos que la espera sea de 20 segundos pongamos el valor de este parámetro en **20s**
- **MaxAuthTries.**- Este parámetro establece el número de veces que nos podemos equivocar a la hora de ingresar la contraseña.
- **Banner.**- Con este parámetros establecemos el nombre del archivo que contiene el mensaje de bienvenida que queremos que se muestre a los usuarios al momento de que se conectan a nuestro servidor por ssh.
- **AllowUsers.**- Permite especificar que cuentas tienen permitido conectarse a nuestro servidor usando ssh
- **MaxStartups.**- Permite definir el número de usuarios conectados simultaneamente a tu servidor via ssh.
- **DenyUsers.**- Permite especificar que cuentas no tienen permitido conectarse a nuestro servidor usando ssh

### 2.2.1.2 Como conectarse a un servidor que tiene habilitado el servicio ssh

**NOTA:** Esto es solo un ejemplo ficticio de como acceder a un servidor con ssh

## Temas Especiales

A continuación, mostramos un ejemplo de como conectarse desde un equipo cualquiera que usa S.O. GNU/Linux a un servidor que tiene habilitado acceso por ssh (supongamos que ese servidor el que queremos conectarnos tiene la ip 192.168.0.116):

- i. Desde un computador que ejecuta S.O. GNU/Linux, abrir una consola
- ii. En la consola, ejecutar el comando cliente ssh para conectarse al servidor, para esto debemos tener un usuario en el servidor donde corre el servicio ssh y saber su ip. Por ejemplo:

The screenshot shows a terminal window titled 'estudiante@serverc7:~'. The window contains the following text:

```
File Edit View Search Terminal Help
carlosv@jester2:~> ssh estudiante@192.168.137.18
The authenticity of host '192.168.137.18 (192.168.137.18)' can't be established.
ECDSA key fingerprint is SHA256:eN6Fz4zbwQxCby5Lu8P+1Dwf9eNv0btfwRYkWNq0ncE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.137.18' (ECDSA) to the list of known hosts.
estudiante@192.168.137.18's password: [estudiante@serverc7 ~]$
```

Red arrows numbered 1 through 4 point to specific parts of the terminal output:

- Arrow 1 points to the command 'ssh estudiante@192.168.137.18'.
- Arrow 2 points to the user input 'yes' at the prompt 'Are you sure you want to continue connecting (yes/no)?'.
- Arrow 3 points to the user input 'estudiante' at the prompt 'estudiante@192.168.137.18's password:'.
- Arrow 4 points to the final prompt '[estudiante@serverc7 ~]\$'.

- 1) En la figura estamos trabajando en el servidor que tiene como nombre jester2 y en el cual estamos conectados con el usuario carlosv (el prompt de sistema nos lo confirma). Ahora para conectarnos al servidor, donde se tiene habilitado el servicio ssh. Este servidor supongamos que tiene la ip **192.168.0.116**, tiene el nombre serverc7 y que a ese servidor nos conectamos con un usuario que existe en dicho servidor el cual tiene la cuenta **estudiante**. Entonces ejecutamos el comando ssh:  
**ssh estudiante@192.168.0.116**
- 2) Como es la primera vez que nos conectamos nos pedirá confirmar conectarnos a dicho servidor. Ingresamos **yes** y luego **enter** para continuar. Esto hará que se guarde un registro de que ya hemos confirmado ingresar a este servidor con el usuario estudiante (Luego ya no nos pedirá confirmación a no ser que intentemos conectarnos con otro usuario o si intentamos conectarnos a otro servidor)
- 3) Ingresamos el password del usuario con el que nos estamos conectando. En la figura tendría que ser el password del usuario **estudiante**. Luego presionamos **enter** para continuar
- 4) Al ingresar ya vemos el prompt del sistema en el otro servidor y ya podemos ejecutar lo que le esté permitido al usuario estudiante en el servidor **192.168.0.116**

### RECORDATORIO:

Siempre que nos conectamos por primera vez con un usuario a un servidor ssh, nos aparece un mensaje para que confirmemos la autenticidad de la computadora a la que estamos

conectándonos, si confiamos en ese servidor, tecleamos yes y luego presionamos ENTER. Las siguientes veces que nos conectemos a ese mismo computador con el mismo usuario ya nos pedirá esta confirmación. Lo que siempre si nos pedirá será la contraseña del usuario que estamos usando para conectarnos.

Desde Windows la conexión a un servidor vía ssh, se lo puede realizar utilizando un programa cliente que permita conectarse a un servidor que tiene habilitado ssh. Por ejemplo, podemos utilizar el emulador de terminal llamado Putty para esta tarea.

Si nuestro sistema operativo cliente tiene soporte para sistemas de ventanas X y queremos que un programa esté instalado en el servidor se nos visualice en nuestra maquina cliente, solo deberemos ejecutar la conexión ssh al servido con el parámetro **-X**, luego de lo cual ya podremos ejecutar programas que no están instalado en nuestra maquina cliente, pero que si están en el servidor donde corre el servicio ssh. Cuando hacemos esto nuestra maquina cliente sirve para visualizar la ventana del programa que corre en el servidor y que reciba nuestras interacciones de teclado y mouse, pero si intentamos grabar algún documento que estemos elaborando se grabará en el servidor y no en nuestra maquina cliente. Entonces la conexión debería realizarse así:

```
ssh -X estudiante@192.168.0.116
```

### 2.2.1.3 Copia de archivos con scp

Adicionalmente ssh también tiene la capacidad de soportar copia de archivos desde nuestra maquina cliente hacia el servidor y viceversa, si que el usuario que utilizamos para la acción tiene los permisos debidos.

**NOTA:** Esto son solo ejemplos ficticio de como hacer copias usando ssh

Suponga que tenemos:

| Equipo Cliente                                                                                                                                                                                                                                                                                                                                                                                                                                              | Equipo servidor (Con Servicio ssh)                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Nombre de servidor: <b>jester2</b></li><li>Usuario: <b>carlosv</b></li><li>Directorio de trabajo: <b>/home/carlosv</b></li><li>Directorio de donde queremos copiar que está dentro del directorio de trabajo: <b>Documents</b>, es decir <b>/home/carlosv/Documents</b></li><li>Archivo a llevar al servidor: <b>lista.txt</b> que está en el directorio <b>Documents</b></li><li>IP: <b>192.168.137.11</b></li></ul> | <ul style="list-style-type: none"><li>Nombre de servidor: <b>serverc7</b></li><li>Usuario: <b>estudiante</b></li><li>Directorio de trabajo: <b>/home/estudiante</b></li><li>Directorio a donde queremos copiar que está dentro del directorio de trabajo: <b>personales</b>, es decir <b>/home/estudiante/personales</b></li><li>IP: <b>192.168.0.116</b></li></ul> |

Por ejemplo, supongamos que queremos llevar el archivo lista.txt del equipo cliente al directorio personales del equipo servidor, para esto ejecutamos

```
scp ./Documents/lista.txt estudiante@192.168.0.116:./personales/
```

## Temas Especiales

---

Una vez nos solicite la contraseña se realizará la copia. Tome en cuenta que, si nunca antes ejecuto ni ssh ni scp hacia el servidor, este le hará la consulta de verificación de conexión la primera vez que realice scp, de forma idéntica a como pasaría cuando ejecuta el comando ssh.

Ahora supongamos que queremos traer a nuestro equipo cliente, todos los archivos con extensión txt del directorio **cartas** del servidor al directorio **Downloads** del equipo cliente, bajo los siguientes supuestos:

| Equipo Cliente                                                                                                                                                                                                                                                                                                                                         | Equipo servidor (Con Servicio ssh)                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Nombre de servidor: <b>jester2</b></li><li>Usuario: <b>carlosv</b></li><li>Directorio de trabajo: <b>/home/carlosv</b></li><li>Directorio a donde queremos copiar que está dentro del directorio de trabajo: <b>Download</b>, es decir <b>/home/carlosv/Download</b></li><li>IP: <b>192.168.137.11</b></li></ul> | <ul style="list-style-type: none"><li>Nombre de servidor: <b>serverc7</b></li><li>Usuario: <b>estudiante</b></li><li>Directorio de trabajo: <b>/home/estudiante</b></li><li>Directorio de donde queremos copiar que está dentro del directorio de trabajo: <b>cartas</b>, es decir <b>/home/estudiante/cartas</b></li><li>IP: <b>192.168.0.116</b></li></ul> |

El comando a ejecutar sería:

```
scp estudiante@192.168.0.116:./cartas/*.txt ./Downloads/
```

### 2.2.2 Bitácoras del servicio SSH

Si en algún momento se desea revisar las bitácoras que el servicio ssh genera en su servidor, puede hacer un seguimiento de los archivos **secure** o **messages** que están disponibles en el directorio **/var/log**. Puede hacer seguimiento de estos archivos con el comando tail, more o cualquier otro comando o programa que usted prefira, siempre y cuando no edite el archivo. Además, recuerde que para poder mirar estos archivos debe hacerlo con el usuario **root**.

También recuerde que si está en una consola con el usuario root puede ejecutar el comando “**systemctl status sshd**” para ver el estado del servicio y algunos mensajes recientes generados por las interacciones con el servicio.

### 2.3 Escritorio remoto

Primero debemos recordar que en informática un **escritorio** es la ventana que aparece cada vez que se inicia nuestro sistema operativo cuando este tiene habilitado interfaz gráfica. Recordar su nombre es sencillo, realizando una comparación: el escritorio, se asemeja a una mesa de trabajo, donde se sitúa todo lo necesario a tener a mano para trabajar.

El escritorio puede contener accesos directos a los programas, documentos, carpetas e incluso, impresoras que utilice con más frecuencia.

Un **escritorio remoto** es una tecnología que permite a un usuario trabajar en una computadora a través de su escritorio gráfico desde otro computador ubicado en otro lugar.

## Temas Especiales

---

La tecnología de escritorio remoto permite la centralización de aquellas aplicaciones que generalmente se ejecutan en entorno de usuario (por ejemplo, procesador de textos o navegador). De esta manera, dicho entorno de usuario se transforma en meros terminales de entrada/salida.

### 2.3.1 Protocolo de comunicaciones

El elemento característico en cualquier implementación de escritorio remoto es su protocolo de comunicaciones, que varía dependiendo del programa que se use. Entre los diversos protocolos de comunicaciones que se conocen para trabajar con escritorios remotos se encuentran:

- Independent Computing Architecture (ICA), utilizado por MetaFrame.
- Remote Desktop Protocol (RDP), utilizado por Terminal Services.
- Adaptive Internet Protocol (AIP), utilizado por Secure Global Desktop.
- Virtual Network Computing, (VNC), utilizado por el producto del mismo nombre.
- X11, utilizado por el sistema de ventanas X.

### 2.3.2 VNC

VNC (Virtual Network Computing, el mismo nombre del protocolo que usa) es un programa de software libre basado en una estructura cliente-servidor que permite al servidor compartir una o más pantallas (concretamente hablando estas pantallas serían los escritorios remotos) para de esta manera desde el cliente, interactuar con dicha pantalla compartida como si se estuviera físicamente trabajando en el servidor y/u observar las acciones del servidor en dicha pantalla a través del protocolo. VNC no impone restricciones en el sistema operativo del ordenador servidor con respecto al del cliente: es posible compartir la pantalla de una máquina con cualquier sistema operativo que admita VNC conectándose desde otro ordenador o dispositivo que disponga de un cliente VNC.

#### 2.3.2.1 Instalar VNC Server en Rocky Linux

- i. Abrir una consola de comandos y cambiarse al root
- ii. Instalar tigervnc-server (es el software servidor) y tigervnc (es el software cliente)  
`dnf -y install tigervnc tigervnc-server`
- iii. Agregar un usuario para el vnc (o agregar los usuarios)
- iv. Agregar acceso a vnc en el firewall de Rocky Linux  
`firewall-cmd --permanent --zone=public --add-service=vnc-server`  
`firewall-cmd --reload`
- v. Este paso por cada puerto vnc al que se de permiso, por ejemplo si queremos habilitar el puerto 6 deberemos realizar.  
`firewall-cmd --permanent --zone=public --add-port=5906/tcp`  
`firewall-cmd --reload`
- vi. A partir de este paso se debe repetir por cada usuario al que quiera habilitarle un escritorio remoto con vnc, entonces, en otra consola donde tenga iniciada sesión con el usuario de interés (digamos que usted ya tiene creado el usuario usrvnc y tiene su sesión en una consola con ese usuario), ejecute el comando **vncserver**, pero solo si es la primera vez que lo hace con dicho usuario (o si procedio a borrar el directorio .vnc que hay en el directorio de trabajo de dicho usuario). Este comando nos pedirá que establezcamos el password para acceder al escritorio de este usuario, en la siguiente secuencia:

- 1) (**Password:**) Ingresamos la contraseña para acceder al escritorio remoto
  - 2) (**Verify:**) Confirmamos la contraseña para acceder al escritorio remoto
  - 3) (**Would you like to enter a view-only password (y/n)?**) Si en la pregunta ingresamos **y**, nos pedirá password para solo poder mirar el escritorio remoto, pero no podremos hacer nada. Si colocamos **n** a la pregunta no nos aparecerá la segunda solicitud de password. En ambos casos luego grabará la contraseña definida
- vii. A partir de este paso se debe repetir por cada usuario al que quiera habilitarle un escritorio remoto con vnc, entonces, en otra consola donde tenga iniciada sesión con el usuario de interés (digamos que usted ya tiene creado el usuario usrvncp y tiene su sesión en una consola con ese usuario), ejecute el comando **vncpasswd**. Este comando nos pedirá que establezcamos el password para acceder al escritorio de este usuario, en la siguiente secuencia:
- 1) (**Password:**) Ingresamos la contraseña para acceder al escritorio remoto
  - 2) (**Verify:**) Confirmamos la contraseña para acceder al escritorio remoto
  - 3) (**Would you like to enter a view-only password (y/n)?**) Si en la pregunta ingresamos **y**, nos pedirá password para solo poder mirar el escritorio remoto, pero no podremos hacer nada. Si colocamos **n** a la pregunta no nos aparecerá la segunda solicitud de password. En ambos casos luego grabará la contraseña definida
- viii. Como hemos ejecutado el comando vncserver esto creará un proceso que deberemos matar con el comando kill con el usuario con el que ejecutamos el comando vncserver, para esto buscamos el proceso ejecutando comando: **ps -fa | grep vnc** . Esto nos listará los procesos que tengan corriendo algun vnc, y por ejemplo para nuestro caso podría mostrarnos algunas finals como las siguientes:

```
usrvncp 2909 2067 2 22:26 pts/0 00:00:00 /usr/bin/Xvnc :2 -geometry 2560x1440
-securitytypes vncauth,tlsVNC -auth /home/usrvncp/.xauthnR4jn5 -desktop
rcvpcsrv.sof164.net:2 (usrvncp) -fp catalogue:/etc/X11/fontpath.d -pn -rfbauth
/home/usrvncp/.vnc/passwd -rfbport 5902
usrvncp 2914 2067 0 22:26 pts/0 00:00:00 /bin/sh /home/usrvncp/.vnc/xstartup
usrvncp 2961 2067 0 22:26 ? 00:00:00 /usr/libexec/gvfsd-fuse
/home/usrvncp/.cache/gvfs -f
usrvncp 3249 2876 0 22:26 pts/0 00:00:00 grep --color=auto usrvncp
```

La que nos interesa es una línea como la que esta marcada con rojo en este ejemplo y particularmente su número de proceso, que en el ejemplo esta marcado en azul, para materlo ejecutamos para este ejemplo el comando kill con el parámetro -9 y el nro de proceso (en este ejemplo seria 2909) es decir ejecutaríamos: **kill -9 2909**

- ix. Una vez hagamos esto ya existirá el directorio .vnc dentro del home del usuario (como estamos usando como ejemplo el usuario usrvncp, entonces creará el directorio .vnc dentro de la ruta absoluta /home/usrvncp), entonces nos cambiamos a este directorio ejecutando: **cd ~/vnc/**
- x. Seguros de que existe el archivo config en este directorio, lo editamos con un editor de texto plano y deberemos definir los parametros de sesión, tipo de seguridad y la resolución para el escritorio. Para nuestro usuario de ejemplo definiremos que su sesión es gnome, tipo de

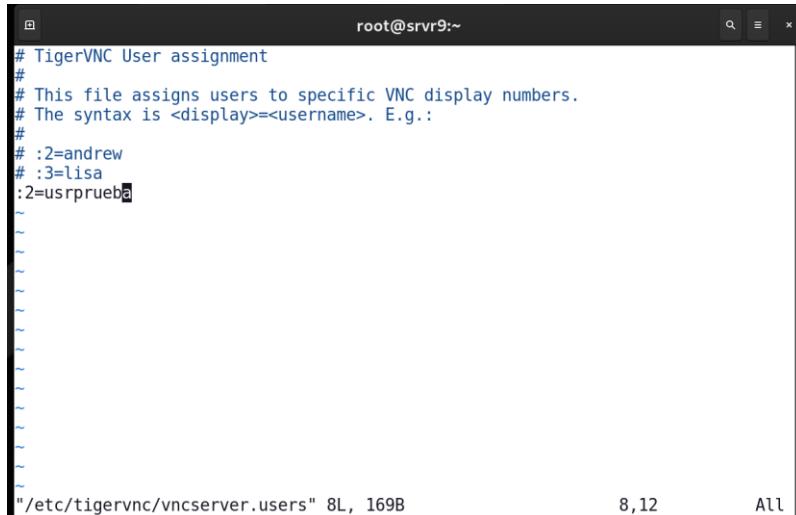
## Temas Especiales

seguridad **vncauth,tlsVNC** y para la resolución definiremos **1500x800** (Este ultimo lo debe definir de acuerdo a la resolución del monitor de su equipo desde donde accedera a su escritorio remoto). Una vez hecho los cambio grabamos el archivo. (Nuestro archivo podría verse así)



```
roberto@srvc9:~/vnc — /usr/bin/vim config
Supported server options to pass to vncserver upon invocation can be listed
in this file. See the following manpages for more: vncserver(1) Xvnc(1).
Several common ones are shown below. Uncomment and modify to your liking.
##
securitytypes=vncauth,tlsVNC
desktop=sandbox
geometry=2000x1200
localhost
alwaysshared
session=gnome
securitytypes=vncauth,tlsVNC
geometry=1500x800
~
```

- xi. Luego para este nuestro usuario de ejemplo (usrprueba) digamos que queremos habilitar su escritorio en el puerto 2 de vnc (equivalente al 5902 tcp) entonces en una consola donde estemos con root procederemos a editar el archivo **vncserver.users** que se encuentra en el directorio **/etc/tigervnc**. En dicho archivo agregaremos una entrada por puerto y usuario donde se quiera habilitar un escritorio remoto, por ejemplo puerto 2 para el usuario usrvncp:



```
TigerVNC User assignment
#
This file assigns users to specific VNC display numbers.
The syntax is <display>=<username>. E.g.:
#
:2=andrew
:3=lisa
:2=usrprueba
~
```

- xii. Finalmente deberemos para habilitar el inicio automático del escritorio remoto al iniciar nuestro servidor rocky Linux, deberemos ejecutar el comando: **systemctl enable --now vncserver@:2**
- xiii. En el comando anterior si no coloca el parámetro **--now** para que el escritorio inicie deberá reiniciar su servidor rocky Linux o ejecutar el comando: **systemctl start vncserver@:2**

**NOTA:**

## Temas Especiales

---

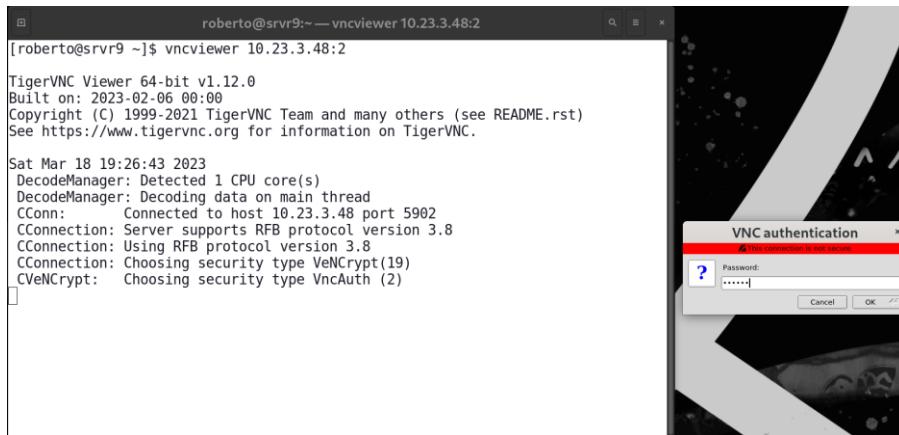
Si ya no queremos que nuestro escritorio inicie automáticamente, deberemos ejecutar el comando: **systemctl disable vncserver@:2** o el comando **systemctl disable --now vncserver@:2** (Si lo ejecutamos así el comando el servicio que habilita este escritorio será bajado y ya no iniciará al encender el computador.

### 2.3.2.2 Conexión al escritorio remoto desde Linux

**NOTA:** Lo que se muestra a continuación son ejemplos ficticios de como conectarse usando vnc. Usted tiene que usar como base estos ejemplos para intentar hacer lo mismo usando su instalación y la de otro compañero, con las IP's que les tocó.

Para conectarnos a nuestro escritorio remoto desde un equipo que tiene interfaz gráfica, este equipo debe tener instalado algún cliente vnc. Nosotros en Rocky Linux usaremos el programa vncviewer que instala el paquete tigervnc. Para ejecutarlo realizamos los siguiente:

- 1) Abrir una consola desde donde se quiera hacer la prueba (En equipo con Rocky Linux)
- 2) Ejecutar el comando: vncviewer ipDelServidorDeEscritorioRemoto:puerto (Ej: **vncviewer 10.23.3.48:2**)
- 3) Ingresamos la contraseña que hemos definido para ese escritorio remoto luego enter.

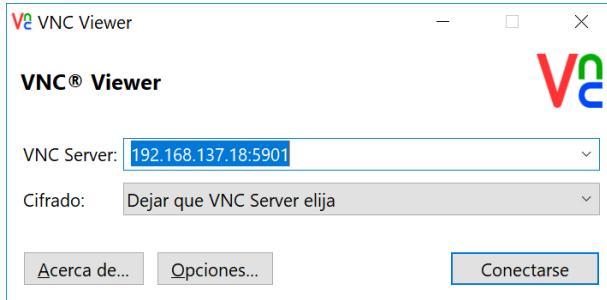


### 2.3.2.3 Conexión al escritorio remoto desde Windows

Para conectarnos a un escritorio remoto con vnc desde Windows, también necesitamos que el computador que corre Windows tenga instalado un cliente para vnc. Nosotros utilizaremos RealVnc Viewer.

En este caso supongamos que también queremos conectarnos al escritorio remoto que habilitamos en el servidor con ip 192.168.0.116 y que corre en el puerto 1. Para esto, ejecutamos el programa RealVnc Viewer y la ventana que se presenta colocamos la ip del servidor y el puerto del escritorio y luego hacemos clic en conectarse, tal como se muestra en la siguiente figura:

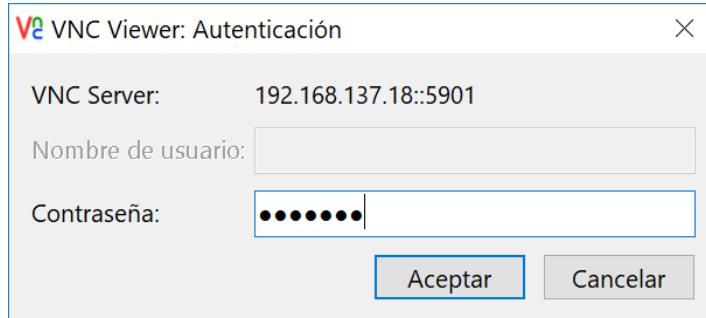
## Temas Especiales



En la siguiente ventana solo hacemos clic en **Continuar**



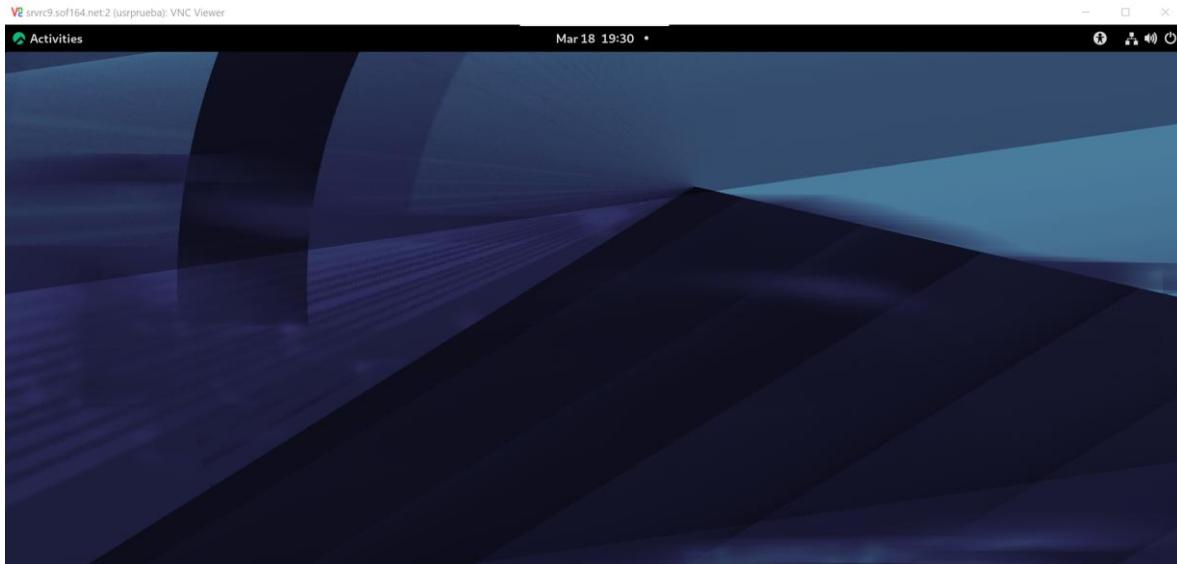
A continuación, en la siguiente ventana ingresamos el password que establecimos para el escritorio y luego hacemos clic en aceptar, tal como se muestra en la figura:



Ahora ya podremos ver el escritorio remoto corriendo dentro de su escritorio local en Windows, y lo que verá será lo mismo que si se conecta desde un equipo con Linux

## Temas Especiales

---



### 2.3.3 RDP y xRDP

Como otra alternativa para compartir escritorios de forma remota existe RDP (Remote Desktop Protocol), el cual es un protocolo propietario desarrollado por Microsoft que permite la comunicación entre una terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón ó el teclado).

Este servicio utiliza por defecto el puerto TCP 3389 en el servidor para recibir las peticiones. Una vez iniciada la sesión desde un punto remoto el ordenador servidor mostrará la pantalla de bienvenida de windows, no se verá lo que el usuario está realizando de forma remota.

**XRDП** es la implementación libre de RDP para sistemas GNU/Linux, el cual permite disponer de un escritorio remoto en servidor Linux donde se instala xrdp y se accede a este escritorio desde Windows con el programa Conexión a Escritorio Remoto que ya viene instalado en los sistemas operativos Windows.

#### 2.3.3.1 Instalar xrdp

- i. En una consola cambiarirse al super usuario
- ii. Agregar el repositorio epel  
`dnf -y install epel-release`
- iii. Instalar xrdp  
`dnf -y install xrdp`
- iv. Iniciar el servicio  
`systemctl start xrdp`
- v. Habilitar el servicio para inicio automatico  
`systemctl enable xrdp`
- vi. Dar acceso en el firewall  
`firewall-cmd --permanent --add-port=3389/tcp`  
`firewall-cmd --reload`
- vii. Conectarse con el cliente de escritorio remoto de Windows

#### NOTA

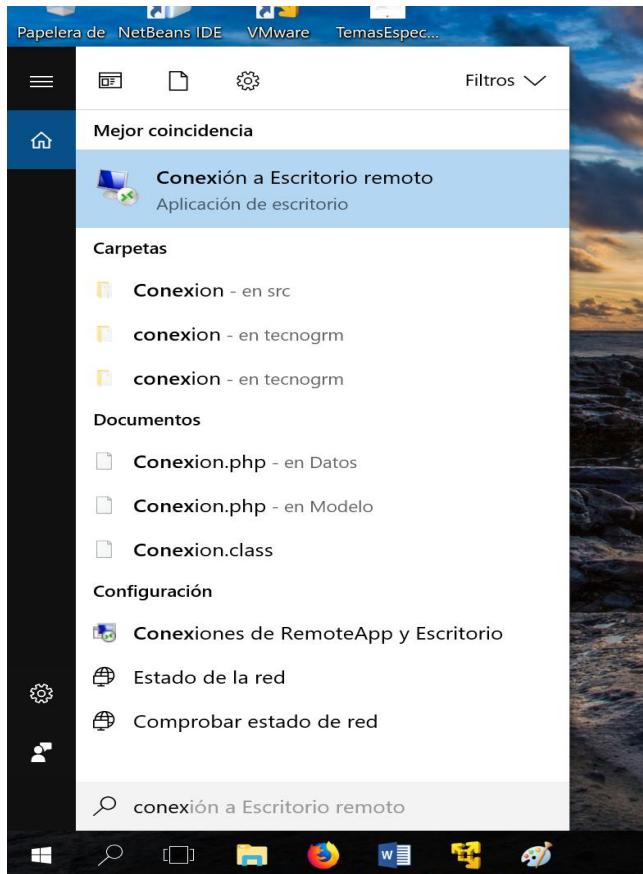
---

## Temas Especiales

- Tanto para conectar remote desktop por vnc o xrdp desde Rocky Linux puede instalarse el paquete remmina con el comando gestor de paquetes dnf, luego lo ejecutamos, solo variamos que, en lugar de elegir VNC en el protocolo, elegimos RDP.
- Otro punto muy importante no intente probar rdp con un usuario al que le haya habilitado escritorio vnc, ya que al intentar probar no mostrará el escritorio con xrdp. Tendrá el mismo efecto nocivo si ya inicio sesión xrdp con un usuario e intenta iniciar escritorio remoto con vnc y con el mismo usuario.
- Si necesita revisar alguna bitacora de este servicio, puede hacer seguimiento al archivo **xrdp.log** que se graba en el directorio **/var/log**

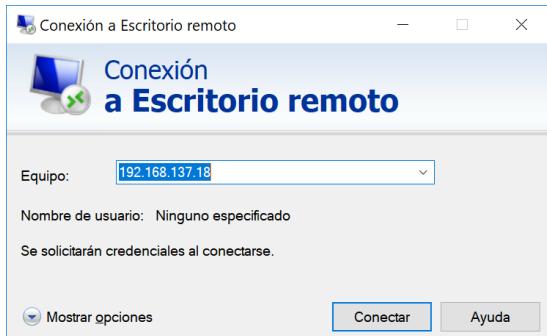
### 2.3.3.2 Conexión a escritorio remoto habilitado con xrdp desde cliente Windows

- Buscar el programa de conexión a escritorio remoto en Windows

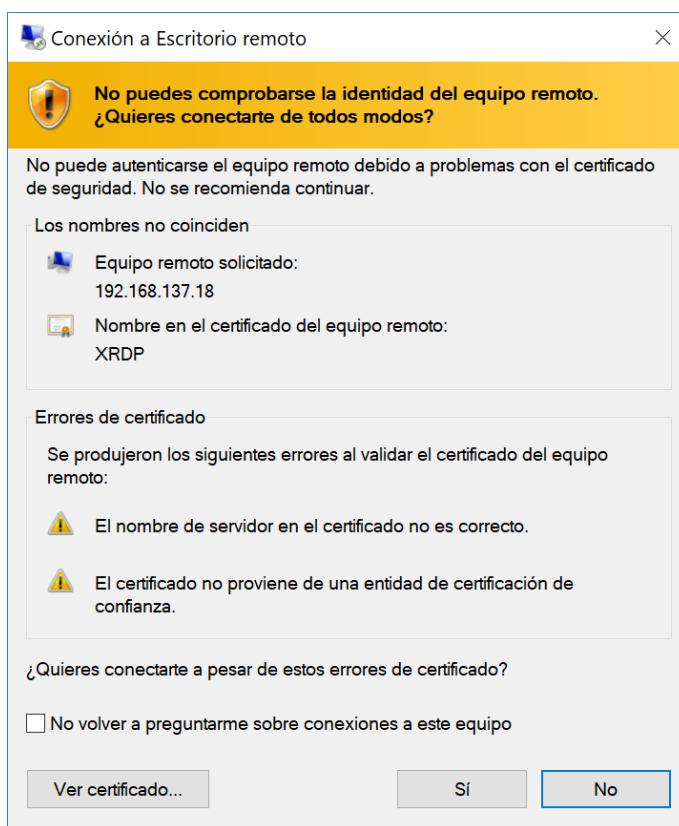


- Ingresar la ip del servidor remoto y hacer clic en el botón conectar

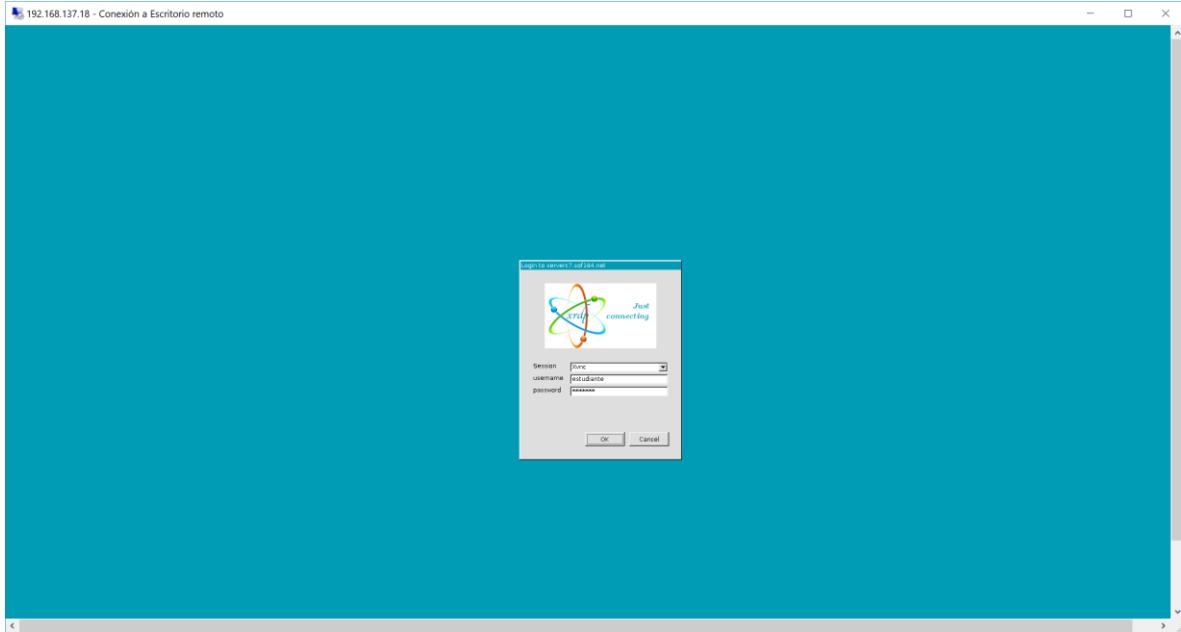
## Temas Especiales



- iii. Si reporta problemas con el certificado en la siguiente ventana, solo hacer clic en el botón **Si**



- iv. Escoger sesión Xvnc, ingresar usuario y password. Luego hacer clic en OK



- v. Luego se nos desplegará el escritorio remoto y si nos es más fácil maximizamos la ventana

### 2.4 Servidor ftp

FTP (File Transfer Protocol) o Protocolo de Transferencia de Archivos (o archivos informáticos) es uno de los protocolos estándar más utilizados en Internet siendo el más idóneo para la transferencia de grandes bloques de datos a través de redes que soporten TCP/IP. El servicio utiliza los puertos 20 y 21, exclusivamente sobre TCP. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizado para el envío de órdenes del cliente hacia el servidor. Prácticamente todos los sistemas operativos y plataformas incluyen soporte para FTP, lo que permite que cualquier computadora conectada a una red basada sobre TCP/IP pueda hacer uso de este servicio a través de un cliente FTP.

**Vsftpd** (Very Secure FTP Daemon) es un software utilizado para implementar servidores de archivos a través del protocolo FTP. Se distingue principalmente porque sus valores predeterminados son muy seguros y por la sencillez para su configuración cuando se le compara con otras alternativas como ProFTPD y Wu-ftpd. En la actualidad se estima que vsftpd podría ser quizás el servidor FTP más seguro del mundo.

Un **servidor FTP** es un programa especial que se ejecuta en un equipo servidor e conectado a una red (LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

#### 2.4.1 Habilitación de servidor ftp con vsftpd

- i. Abrir una consola de comandos y cambiarse al root
- ii. Instalar los paquetes para que su servidor Rocky Linux pueda servir como servidor ftp  
`dnf -y install vsftpd`
- iii. Si el servicio no está habilitado lo hacemos ejecutando el comando  
`systemctl enable vsftpd.service`

- iv. Si el servicio no está iniciado lo hacemos ejecutando el comando  
`systemctl start vsftpd.service`
- v. En el firewall es necesario abrir FTP-DATA los puertos 20 y 21 (FTP-DATA y FTP, respectivamente)  
`firewall-cmd --permanent --zone=public --add-service=ftp`  
`firewall-cmd --permanent --zone=public --add-port=20/tcp`  
`firewall-cmd --reload`

Una vez completado este procedimiento ya podremos conectarnos vía ftp a nuestro servidor desde consola de comandos o mediante algún programa en modo grafico que tenga soporte de cliente ftp como ser el explorador de Windows, los navegadores web, winscp, etc.

### IMPORTANTE:

Con la configuración por defecto, si desea hacer seguimiento de alguna bitácora, cada vez que descarguemos un archivo del servidor o subamos un archivo por ftp, se registrará que se está bajando o subiendo en el archivo bitacora del servidor ftp que tiene el nombre **xferlog** que existe en el directorio **/var/log**

### 2.4.2 Archivos de configuración de vsftpd

El principal archivo para cambiar la configuración de vsftpd está en el directorio /etc/vsftpd y tiene el nombre vsftpd.conf

En este archivo se encuentran parámetros como:

- **anonymous\_enable**, Esta opción viene incluida en la configuración predeterminada. Se utiliza para definir si se permitirán los accesos anónimos al servidor. Establezca como valor YES o NO de acuerdo a lo que se requiera. Establecer YES permitirá a cualquiera acceder libremente a los datos almacenados dentro del directorio /var/ftp, el cual está vacío de modo predeterminado. Decida qué hacer. Si tiene dudas, establezca NO.
- **local\_enable**, Esta opción viene incluida en la configuración predeterminada. Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema. Establezca como valor YES o NO de acuerdo a lo que se requiera. Decida qué hacer. salvo que sólo quiera permitir acceso anónimo, establezca YES, otro modo tendría poca utilidad el servicio.
- **write\_enable**, Esta opción viene incluida en la configuración predeterminada. Establece si se permite ejecutar write (escritura) en el servidor. Establezca como valor YES o NO de acuerdo a lo que se requiera.
- **anon\_upload\_enable**, especifica si los usuarios anónimos tendrán permitido subir contenido al servidor. Por lo general no es una función deseada, por lo que se acostumbra desactivar ésta.
- **anon\_mkdir\_write\_enable**, especifica si los usuarios anónimos tendrán permitido crear directorios en el servidor. Al igual que la anterior, por lo general no es una función deseada, por lo que se acostumbra desactivar ésta.
- **ftpd\_banner**, Esta opción viene incluida en la configuración predeterminada. Sirve para establecer el mensaje de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Puede establecerse cualquier frase breve que considere conveniente, pero sin signos de puntuación. Ej:

**ftpd\_banner=Bienvenido al servidor FTP de Ofimática**

- **userlist\_enable**, Toma los valores YES o NO, indica al servidor si debe utilizar el archivo user\_list que se encuentra en el directorio /etc/vsftpd para denegar acceso o no denegar el acceso por ftp a los usuarios que esten en dicho archivo

Así como estos existen otros parámetros que podrá modificar dentro del archivo vsftpd.conf, para hacer el cambio se le aconseja primero sacar una copia de este archivo, luego modificar el parámetro o parámetros que deseé y finalmente reiniciar el servicio vsftpd.

Si desea agregar más usuario para que no accedan por ftp solo adicione a la lista del archivo /etc/vsftpd/user\_list y reinicie el servicio vsftpd.

### 2.4.3 Conexión al servidor ftp

Para conectarnos al servidor ftp desde una maquina cliente, solo se necesita que en la maquina cliente existe algún cliente gráfico o de modo consola para acceso a ftp.

En Windows o en Linux normalmente por defecto en modo consola existe el programa cliente ftp, el cual podemos usar para conectarnos a un servidor ftp, solo tenemos que, en una consola de comandos, ejecutar el comando ftp acompañado de la ip del servidor, por ejemplo: **ftp 10.23.3.48**

Luego de ejecutar el comando, si el servidor acepta nuestra solicitud, primero nos pedirá un usuario que ya debe existir en el servidor y luego su password para poder acceder al servidor, para asi poder llevar o traer archivos. Si no sabemos un usuario y el servidor acepta conexiones anónimas, cuando nos pida el usuario para acceder, podemos escribir **anonymous** y solo presionar la tecla **ENTER** cuando nos solicite el password. Una vez conectados ya podremos hacer uso de los comandos para movernos dentro de la estructura de directorios a la que el servidor nos de acceso, así como también hacer uso de los comandos para traernos archivos que estén en el servidor o para llevar archivos al servidor que ofrece el cliente ftp para consola, aclarando que solo los que nos permita usar el servidor con el usuario con el que nos hemos conectado a él.

#### NOTA IMPORTANTE:

En nuestro caso como estamos usando Rocky Linux 9, con la instalación que hemos hecho, no tenemos habilitado el cliente ftp para consola. Si deseamos instalar el cliente ftp como root deberemos ejecutar en una consola (previo a esto, primero habilite su dvd como repositorio y luego recién ejecute el comando para instalar el cliente ftp de consola):

```
dnf -y install ftp
```

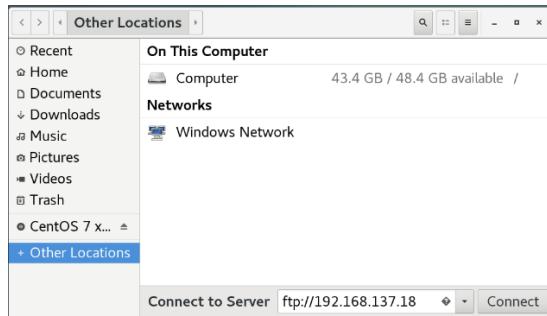
Desde Windows para conectarnos al servidor FTP en modo gráfico podemos utilizar el manejador de archivos de Windows que conocemos, es decir, el explorador de Windows. También podemos utilizar un navegador como mozilla Firefox o Google Chrome, o cualquier otro programa con soporte ftp, como por ejemplo WinScp.

Desde Linux para conectarnos al servidor FTP en modo gráfico, podemos utilizar un manejador de archivo, como por ejemplo Nautilus. También, podemos utilizar navegadores web, como Firefox o Chrome, o cualquier programa cliente con soporte FTP.

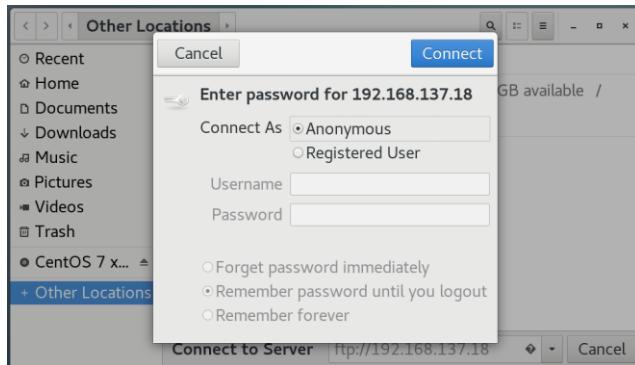
## Temas Especiales

---

Por ejemplo con Nautilus, abrimos el programa y hacemos clic en **Other Locations**, y en el cuadro de texto Connect to Server, ingresamos **ftp://ip\_del\_servidor** y luego hacemos clic en connect, como se muestra en la siguiente figura:



Esto hará que se nos presente la ventana para ingresar los datos del usuario con el que accedemos al servidor ftp. En este podremos elegir anonimo o la opción de ingresar un usuario y su password, para luego hacer clic en Connect. En la figura se muestra para acceder con un usuario anónimo.



Una vez validado nuestro acceso nos mostrará los archivos y carpetas a los que tenemos acceso.

El uso de los navegadores en Windows o en Linux para acceder a un servidor ftp es similar, solo basta con ingresar en el cuadro de direcciones: **ftp://ip\_servidor**, Ej: **ftp://10.23.3.48**. Lo anterior solo sirve para acceder en modo anónimo al servidor ftp desde un navegador, pero si queremos acceder al servidor ftp con un usuario deberemos poner en el cuadro de direcciones del navegador: **ftp://cuentaDeUsuario@ip\_servidor**. Por ejemplo, si queremos acceder al servidor ftp que tiene la ip 10.23.3.48 utilizando la cuenta de usuario estudiante, deberemos ingresar en el cuadro de direcciones del navegador lo siguiente: **ftp://estudiante@10.23.3.48**

## Capítulo 3. DNS y DHCP

### 3.1 DNS

Cuando se quiere acceder a una página web, conectarnos a un servidor ftp, o tener cualquier tipo de acceso remoto en internet o en una intranet, se necesita la dirección IP del servidor a donde se quiere llegar, pero, por regla general, el usuario solo conoce el nombre de dominio de dicho servidor. La razón no es otra que la dificultad de recordar las series numéricas del tipo 93.184.216.34 que componen una dirección IP, y que, además, constituyen la base de la comunicación en Internet. Es por este motivo por el que las direcciones IP se “traducen” en nombres de dominios que podemos recordar, por ejemplo:

Dirección IP: 200.87.195.238

Nombre de Dominio: www.uagrm.edu.bo

El proceso de traducción de los nombres de dominio en direcciones numéricas que las máquinas puedan entender es lo que se conoce como resolución de nombres, una labor que realiza el Domain Name System, en castellano Sistema de Nombres de Dominio, conocido por sus siglas DNS.

#### 3.1.1 Definición de DNS

DNS (acrónimo de Domain Name System) es una base de datos distribuida y jerárquica, que almacena la información necesaria para los nombres de dominio. Sus usos principales son la traducción de nombres de dominio a direcciones IP y la traducción de dirección IP a nombres de dominio. También es útil para realizar la localización de los servidores de correo electrónico correspondientes para cada dominio. El DNS nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección IP.

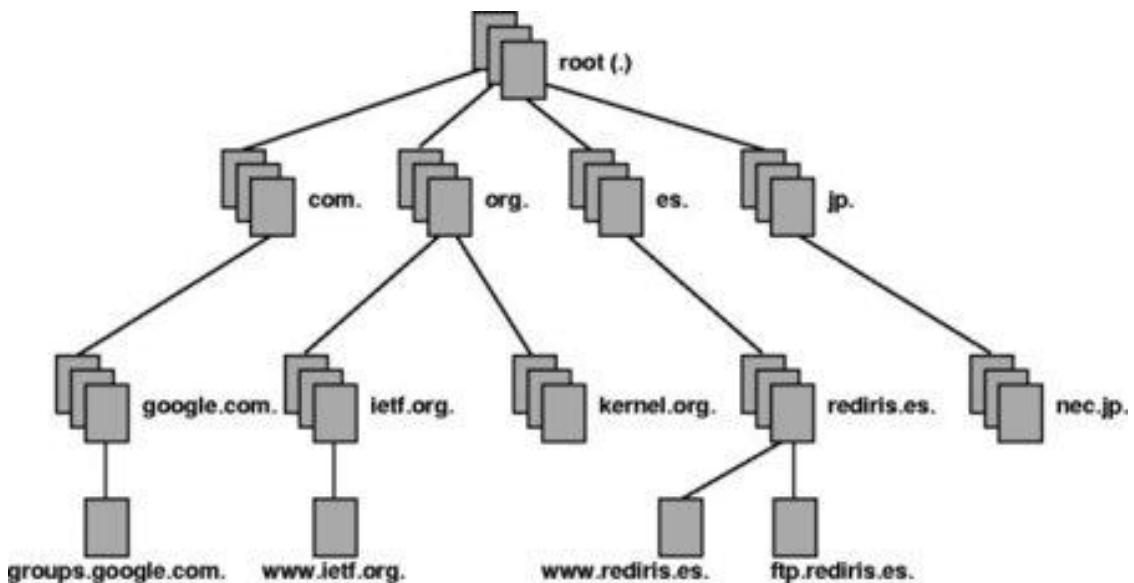
Los Servidores DNS utilizan TCP y UDP, en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud UDP desde un Cliente DNS, seguida por una sola respuesta UDP del servidor. Se realiza una conexión TCP cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como transferencia de zonas.

La creación este sistema de nombres de dominio en 1983, sustituyó al procedimiento anterior de resolución, muy propenso a errores y basado en un archivo local de hosts. Este archivo con nombre **hosts** puede encontrarse aún hoy en sistemas basados en UNIX o LINUX en el directorio /etc/ y, en computadores Windows, en %SystemRoot%\system32\drivers\etc.

El archivo hosts requería el mantenimiento manual y una actualización regular, un esfuerzo que, a medida que Internet iba creciendo de forma exponencial, ya no era posible realizar. Hoy, este archivo se usa exclusivamente para la clasificación de direcciones IP en redes locales. También permite bloquear servidores web desviando automáticamente su dirección hacia el alojamiento local (local host).

Normalmente La resolución de nombres utiliza una estructura en árbol, mediante la cual los diferentes servidores DNS de las zonas de autoridad se encargan de resolver las direcciones de su zona, y si no se lo solicitan a otro servidor que conoce la dirección. Un ejemplo del árbol

jerárquico que existe entre los servidores DNS podemos ver en la siguiente figura, donde el punto de partida es el dominio raíz (root), representado por el punto.



### 3.1.2 NIC (Network Information Center)

NIC (acrónimo de Network Information Center o Centro de Información sobre la Red) es un operador de registro de los dominios de nivel superior del sistema de nombres de dominio (DNS) de Internet, que mantiene todos los datos administrativos de un dominio DNS y genera un archivo de zona que contiene las direcciones de los servidores de nombres para cada dominio. Es una institución encargada de asignar los dominios en Internet ya sean nombres de dominio genéricos o por países, permitiendo personas o empresas, montar sitios de Internet a través de un proveedor de internet (ISP), mediante un DNS. Técnicamente existe un NIC por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país. Por ejemplo: NIC Bolivia es la entidad encargada de gestionar todos los dominios con terminación **.bo**, la cual es la terminación correspondiente asignada a los dominios de Bolivia.

También son conocidos como registradores de dominio.

### 3.1.3 Dominio

Un dominio es un conjunto de caracteres que conforman un nombre que identifica a un grupo de dispositivos conectados a una red. Entonces un dominio es una etiqueta que está dentro nivel del árbol jerárquico de la estructura de dominios mundial.

Un dominio lo podemos desglosar del siguiente modo:

- A la etiqueta ubicada más a la derecha se le llama dominio de nivel superior (en inglés top level domain). Como **.bo** en **uagrm.edu.bo** u **.org** en **wikipedia.org**
- Cada etiqueta a la izquierda especifica una subdivisión o subdominio. Nótese que "subdominio" expresa dependencia relativa, no dependencia absoluta.

- Por ejemplo, en el dominio **uagrm.edu.bo**, existe el subdominio **edu.bo** que es un subdominio del dominio de nivel superior **bo**. También existe el subdominio **uagrm.edu.bo**, que sería un subdominio del subdominio **edu.bo** (o dominio **edu.bo**, como se lo prefiera denominar).
- En un segundo ejemplo, en el nombre de dominio del host **wikipedia.org**, existe el subdominio **wikipedia.org**, el cual es un subdominio del dominio **org**
- Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (en inglés hostname) del cual hablaremos más adelante con más detalle.

Debe notar que un subdominio esta dentro de un dominio y notará que también se lo puede denominar dominio, ya que dentro de este también pueden existir subdominios y así sucesivamente, según usted lo necesite estructurar.

Debemos resaltar que, así como existen dominios de nivel superior, el dominio raíz de todos los dominios es “.” (el punto), por esta razón la forma correcta de ingresar un nombre de dominio es con un punto al final del mismo, solo que por costumbre no lo hacemos, pero las aplicaciones clientes asumen que, si usted no coloca el punto al final del nombre de dominio, la aplicación se lo coloca. Por ejemplo, para el FQDN del host **www.uagrm.edu.bo** la forma correcta de escribir este sería **www.uagrm.edu.bo.**, con el punto al final, solo que normalmente nosotros los usuarios no lo escribimos así, por lo cual las aplicaciones clientes asumen que existe el punto al final del nombre de dominio, si el usuario no lo colocó.

### 3.1.4 FQDN

FQDN (acrónimo de Fully Qualified Domain Name o Nombre de Dominio Plenamente Calificado) es un conjunto de caracteres que conforman un Nombre no ambiguo que identifica de forma única y absoluta un dispositivo de red (servidor, computador o dispositivo en la red) en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final (aunque en la práctica nosotros casi nunca ponemos el punto final, solo en configuración de servidores DNS como veremos más adelante).

Como ejemplo, supongamos que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y que su dominio es llamado «dominio.com», entonces su FQDN de este computador sería «maquina1.dominio.com.», así es que se define de forma única al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solamente puede haber uno llamado «maquina1.dominio.com.». La ausencia del punto al final definiría que se pudiera tratar solamente de un prefijo, es decir «maquina1.dominio.com» pudiera ser un dominio de otro más largo como «maquina1.dominio.com.bo».

La longitud máxima de un FQDN es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Solamente se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-» (guion medio). Sin distinción de mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar IDN (acrónimo de Internationalized Domain Name) que permite caracteres no-ASCII, codificando caracteres Unicode dentro de cadenas de bytes dentro del conjunto normal de caracteres de FQDN. Como resultado,

los límites de longitud de los nombres de dominio IDN dependen directamente del contenido mismo del nombre.

### 3.1.5 Datos necesarios para registrar un dominio

Los datos necesarios para registrar un dominio son:

- Registrador oficial de dominios: Empresa registradora oficial inscrita en ICANN la cual se encarga de preservar los datos de los registros.
- Nombre de dominio: Nombre de dominio seleccionado que esta disponible, es decir, que no esta registrado por otro persona o institución
- Propietario del dominio: Persona o entidad que figura como propietario y legítimo dueño por el periodo de registro.
- Contacto administrativo: Persona o entidad designada por el propietario que figura como administrador de los datos del dominio en favor del propietario.
- Contacto técnico: Persona o entidad que se encarga del mantenimiento de los números DNS del dominio para su correcto funcionamiento y enlace en la red.
- Contacto de financiero: Persona o entidad que se encargará de realizar el pago por las correspondientes renovaciones del dominio.
- DNS (Domain Name Servers) (Servidor de Nombres de Dominio): FQDN e IP de servidor DN maestro y esclavo (este segundo suele ser opcional). Son los servidores de nombre que se harán cargo de las peticiones de traducción al dominio y de redirigir las mismas a donde proceda según la naturaleza de cada petición.

### 3.1.6 Procedimiento de registro

El procedimiento es el siguiente:

- i. Elegir un registrador acreditado
- ii. Elegir un dominio teniendo cuidado dentro de que dominio de nivel superior estará el dominio seleccionado
- iii. Verificar la disponibilidad del nombre de dominio deseado en el sistema del registrador.
- iv. Crear una cuenta en el sistema del registrador (normalmente en línea vía web)
  - Ingresar los datos solicitados: Normalmente se solicita de forma obligatoria nombre y apellidos, correo electrónico, dirección física, teléfono, país y ciudad
- v. Registrar el dominio, para lo cual se solicitará datos adicionales aparte de lo que se ingreso en la creación de cuenta, entre ellos el periodo de tiempo que durará el registro del dominio, en años.
- vi. Pagar el dominio, normalmente con tarjeta de crédito (o también por transferencia bancaria) o el medio que permita usar el registrador elegido.
  - El registrador contacta con ICANN y realiza el proceso de forma transparente para el registrante.
  - Avisa al registrante del registro para confirmación de activación.

- vii. Confirmar y activar el dominio, para lo cual habrá que revisar el correo electrónico proporcionado en el registro, procediendo a realizar la confirmación a través del procedimiento explicado en el correo recibido.
- viii. Una vez registrado y activado el dominio, el registrante del dominio el servidor DNS (o los servidores DNS) que responderán a solicitudes de resolución para el dominio registrado. En caso de tener un hosting web, usar el panel de control provisto por el proveedor de hosting para hacer el uso del hosting en conjunto con el dominio registrado.

**Nota:**

El registrante del dominio debe esperar un tiempo para que el dominio sea reconocido en todos los servidores de Internet. Por ejemplo, para los dominios .com y .net la demora suele ser entre 4 y 8 horas, y para otros es generalmente entre 24 y 48 horas.

### 3.1.7 Componentes DNS

El protocolo DNS opera a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

#### 3.1.7.1 Clientes DNS

Son todos aquellos programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres y direcciones IP. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado. Prácticamente todas las aplicaciones que requieren definir un nombre de anfitrión entre sus argumentos se consideran clientes DNS.

Por ejemplo: un cliente SSH —aun siendo cliente de otro protocolo— realiza una consulta de DNS para determinar la dirección IP de un servidor al cual se va a conectar, si usted en lugar de colocar la IP al ejecutar el comando ssh, coloca el nombre de dominio del servidor al que desea conectarse.

#### 3.1.7.2 Servidores DNS

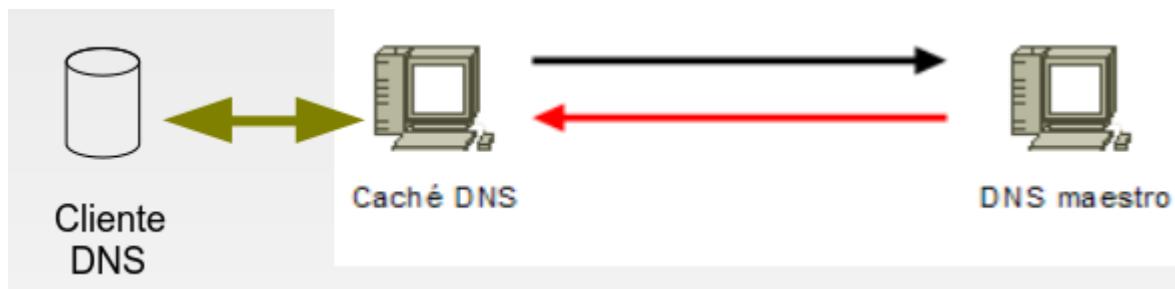
Son servicios que contestan las consultas realizadas por los Clientes DNS, es decir, son responsables de dar respuesta a las peticiones DNS, ¿tales como “cuál es la dirección IP para el nombre de dominio www.xxxxx.com?” y del mismo modo responden a peticiones DNS tales como “cuál es el nombre de dominio para la dirección IP XXX.XXX.XXX.XXX”.

Hay los siguientes tipos de servidores de nombres:

- Servidor primario (maestro): en él se llevan a cabo todas las modificaciones sobre una o varias zonas. Almacena la copia original de la BD de la zona y se le denomina autorizado.
- Servidor secundario (esclavo): contiene una copia de solo lectura de los archivos de zona que obtiene del servidor maestro (transferencia de zona), también es autorizado.



- Servidor caché: No contiene información acerca de la zona y se utiliza para acelerar las consultas, almacenando las últimas realizadas.



- Servidor reenviador (forwarder): Cuando un servidor DNS no tiene la respuesta a una consulta, puede acudir a este tipo de servidores que se utilizan para reducir el tráfico y las consultas DNS, ya que resuelven completamente la consulta y se comparte su caché.
- Servidor solo autorizado: Se trata de servidores que están autorizado en una o varias zonas, como primario o secundario, pero no preguntan a otros servidores para resolver la petición.
- Servidores raíz (root servers): En Internet existen un conjunto de servidores DNS autorizados para el dominio raíz «.», conocidos como servidores raíz (root servers). Contienen el fichero de la zona «.» que contiene información sobre los servidores DNS autorizados para cada uno de los dominios TLD

### 3.1.7.2.1 ¿Cuántos servidores DNS debe haber para resolver un dominio?

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para las zonas de DNS. Aunque podría funcionar con un solo servidor DNS primario, de acuerdo a la RFC 2182, el DNS requiere que al menos tres servidores existan para todos los dominios delegados (o zonas).

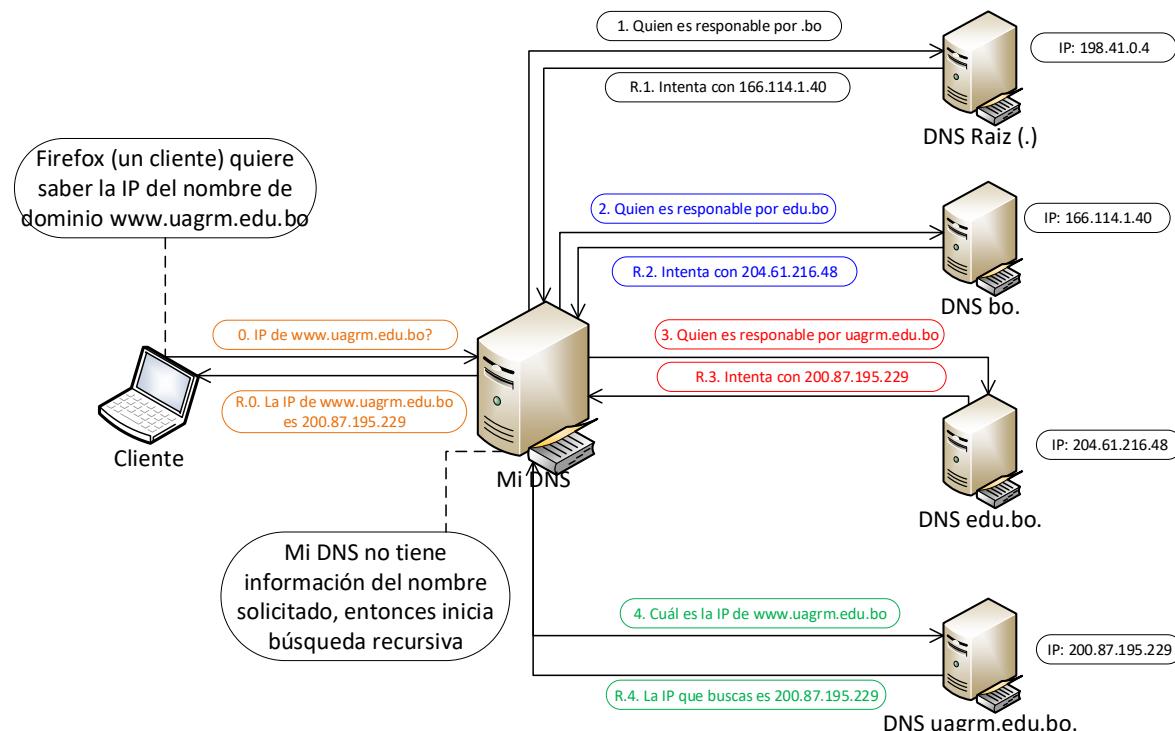
Una de las principales razones para tener al menos tres servidores para cada zona, es permitir que la información de la zona misma esté disponible siempre y de forma confiable, hacia los Clientes DNS, a través de Internet cuando un servidor DNS de dicha zona falle, esté fuera de servicio y/o esté inalcanzable.

Contar con múltiples servidores también facilita la propagación de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los Clientes DNS si acaso encontraran dificultades para realizar una consulta en un Servidor DNS. En otras palabras: tener múltiples servidores para una zona permite contar con redundancia y respaldo, del servicio.

Con múltiples servidores, por lo general uno actúa como Servidor Maestro o Primario y los demás como Servidores Esclavos o Secundarios. Correctamente configurados y una vez creados los datos para una zona, es innecesario copiarlos a cada Servidor Esclavo o Secundario, pues éste se encargará de transferir los datos de manera automática cada vez que sea necesario.

### 3.1.7.2.2 Tipos de resoluciones DNS

- **Resoluciones Iterativas (no recursivas):** El cliente hace una consulta al Servidor DNS y éste le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas consultando su base de datos local.
- **Resoluciones Recursivas:** El cliente hace una consulta al Servidor DNS y el servidor no tiene la información en su base de datos locales, por lo que busca y se pone en contacto con un servidor DNS raíz, y en caso de ser necesario repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la mejor respuesta a la pregunta. Veamos gráficamente la resolución recursiva de un servidor DNS cuando uno de sus clientes le pide traducir el nombre de dominio [www.uagrm.edu.bo](http://www.uagrm.edu.bo)



### 3.1.7.3 Tipos de búsqueda DNS

#### i. Búsqueda directa

## Temas Especiales

Devuelven direcciones IP para las búsquedas hechas para nombres FQDN (Fully Qualified Domain Name). También permite resolver consultas de registros especiales como el registro MX para los sistemas de correo electrónico. Estas zonas necesitan disponer de un archivo de configuración de zona en el servidor DNS maestro de la zona.

ii. **Búsqueda inversa**

Devuelven nombres FQDN (Fully Qualified Domain Name) para las búsquedas hechas para direcciones IP. Estas zonas, también necesitan disponer de un archivo de configuración de zona en el servidor DNS maestro de la zona.

### 3.1.7.4 Zonas de Autoridad

La zona de autoridad es una parte del espacio de nombre de dominios sobre la que es responsable un servidor DNS. La Zona de Autoridad de un servidor DNS abarca al menos un dominio y —posiblemente— sus sub-dominios, cuando estos últimos son imposibles de delegar a otras zonas de autoridad. La zona de autoridad de un Servidor Maestro o Primario la tiene almacenada en su base de datos de nombres de dominio.

Las zonas de autoridad se crean en archivos de texto simple o registros de una base de datos. Deben incluir el tiempo total de vida (TTL) predeterminado, la información del servidor DNS principal y los registros que componen la zona. El contenido mínimo de estos archivos debe ser el siguiente:

```
$TTL 3600
@ IN SOA dns1.dominio.com. usuario.gmail.com. (
 2016091901; número de serie. Se recomienda sea en formato de fecha.
 7200; tiempo de refresco del registro SOA.
 900; tiempo a esperar entre un intento de consulta fallido y otro.
 1209600; caducidad del registro SOA en otros servidores DNS.
 3600; tiempo total de vida del registro SOA en otros servidores DNS.
)
@ IN NS dns.dominio.com.
```

#### 3.1.7.4.1 Tipos de registros en las zonas de autoridad

La información de cada Zona de Autoridad es almacenada de forma local en un archivo en el Servidor DNS.

Este archivo puede incluir varios tipos de registros:

| Tipo de Registro       | Descripción                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A (Address)            | Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv4 de 32 bits.                                                            |
| AAAA (Address)         | Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv6 de 128 bits.                                                           |
| CNAME (Canonical Name) | Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los sub-dominios y registros DNS del dominio original. |
| MX (Mail Exchanger)    | Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.                  |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PTR</b> (Pointer)            | Registro de apuntador que resuelve direcciones IPv4 hacia los nombres anfitriones. Es decir, hace lo contrario al registro A. Se utiliza en zonas de Resolución Inversa.                                                                                                                                                                                                                                        |
| <b>NS</b> (Name Server)         | Registro de servidor de nombres, que sirve para definir una lista de servidores de nombres con autoridad para un dominio.                                                                                                                                                                                                                                                                                       |
| <b>SOA</b> (Start of Authority) | Registro de inicio de autoridad, encargado de especificar el Servidor DNS Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.                                                                                                             |
| <b>SRV</b> (Service)            | Registros de servicios, encargados de especificar información acerca de servicios disponibles a través del dominio. Protocolos como SIP (Session Initiation Protocol) y XMPP (Extensible Messaging and Presence Protocol) suelen requerir registros SRV en la zona para proporcionar información a los clientes.                                                                                                |
| <b>TXT</b> (Text)               | Registros de texto, encargados de permitir al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras DNSBL (DNS-based Blackhole List) para la filtración de Spam. Otro ejemplo de uso sería el caso de las VPN, donde suele requerirse un registro TXT, para definir una firma digital que será utilizada por los clientes |

En el caso de dominios públicos, la responsabilidad de que exista una Zona de Autoridad para cada Zona de búsqueda directa, corresponde a la autoridad misma del dominio, es decir quien esté registrado como autoridad del dominio la base de datos WHOIS donde esté registrado el dominio. Quienes adquieren dominios a través de un NIC (por ejemplo: www.nic.bo), son quienes deben hacerse cargo de las Zonas búsqueda directa ya sea a través de su propio Servidor DNS o bien a través de los Servidores DNS de su ISP.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un NIC, como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

Para búsquedas inversas, en el caso de segmentos de red públicos, la responsabilidad de que exista una Zona de Autoridad para cada Zona de búsqueda Inversa, corresponde a la autoridad misma del segmento, es decir, corresponde a quien esté registrado como autoridad del bloque de direcciones IP. Los grandes ISP y algunas empresas son quienes se hacen cargo de las Zonas de búsqueda Inversa.

### 3.1.8 Herramientas para probar un servidor DNS

Antes de ver cómo se instala y configura un servidor DNS en Rocky Linux, veremos algunas herramientas que sirven para probar si un servidor DNS está realizando su trabajo, con ellas podremos realizarle consultas a un servidor DNS para pedirle traducción de nombres de dominio a su respectiva dirección y viceversa, entre otras cosas.

### 3.1.8.1 Uso del comando host

El comando **host** es una herramienta simple para hacer consultas a Servidores DNS. Es utilizado para obtener las direcciones IP de los nombres de anfitrión y viceversa.

Como la gran mayoría de los programas clientes que utilizan un servidor DNS, el comando **host** realiza las consultas en los Servidores DNS que estén definidos en el archivo **/etc/resolv.conf** del anfitrión local, pudiendo definirse de manera opcional cualquier otro Servidor DNS. Los servidores DNS definidos en este archivo serían los servidores DNS que a los que por defecto los programas piden resoluciones DNS.

Por ejemplo:

```
host www.uagrm.edu.bo
```

Lo anterior solicita una traducción del nombre de dominio **www.uagrm.edu.bo** a los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado una dirección IP.

```
host www.uagrm.edu.bo 8.8.8.8
```

Lo anterior solicita una traducción del nombre de dominio **www.uagrm.edu.bo**, pero le pide, en específico, al servidor DNS con IP 8.8.8.8 que le haga dicha traducción. Luego de realizar la búsqueda del nombre **www.uagrm.edu.bo**, el servidor DNS con IP 8.8.8.8, devolverá la IP asociada al nombre de dominio **www.uagrm.edu.bo**

```
host 200.87.195.238
```

Lo anterior solicita una traducción inversa de la IP 200.87.195.238 a los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado un nombre de dominio (esto solo es posible si el servidor DNS responsable del dominio de la IP tiene configuradora la resolución inversa, caso contrario no habrá una respuesta exitosa).

### 3.1.8.2 Uso del comando dig

El comando **dig** (domain information groper) es una herramienta flexible para realizar consultas en Servidores DNS. Realiza búsquedas y muestra las respuestas que son regresadas por los servidores que fueron consultados. Debido a su flexibilidad y claridad en la salida, es que la mayoría de los administradores utilizan **dig** para diagnosticar problemas de DNS.

Al igual que el comando **host** y otros, el comando **dig** de modo predeterminado, realiza las búsquedas en los Servidores DNS definidos en el archivo **/etc/resolv.conf**, pudiendo definirse de manera opcional cualquier otro Servidor DNS. La sintaxis básica sería:

```
dig @servidor dominio.tld TIPO
```

Donde **servidor** corresponde al nombre o dirección IP del Servidor DNS a consultar, **dominio.tld** corresponde al nombre del registro del recurso que se está buscando y **TIPO** corresponde al tipo de consulta requerido (ANY, A, MX, SOA, NS, etc.)

Ejemplo:

```
dig @8.8.8.8 uagrm.edu.bo MX
```

## Temas Especiales

---

Lo anterior realiza una búsqueda en el Servidor DNS en la dirección IP **8.8.8.8** para los registros **MX** para el dominio **uagrm.edu.bo**.

```
dig uagrm.edu.bo NS
```

Lo anterior realiza una búsqueda en los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema para los registros NS para el dominio **uagrm.edu.bo**.

```
dig @8.8.8.8 uagrm.edu.bo NS
```

Lo anterior realiza una búsqueda en los Servidor DNS en la dirección IP 8.8.8.8 para los registros NS para el dominio **uagrm.edu.bo**.

```
dig www.uagrm.edu.bo
```

Lo anterior solicita una traducción del nombre de dominio **www.uagrm.edu.bo** a los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado una dirección IP.

```
dig @8.8.8.8 www.uagrm.edu.bo
```

Lo anterior solicita una traducción del nombre de dominio **www.uagrm.edu.bo**, pero le pide, en específico, al servidor DNS con IP 8.8.8.8 que le haga dicha traducción. Luego de realizar la búsqueda del nombre **www.uagrm.edu.bo**, el servidor DNS con IP 8.8.8.8, devolverá la IP asociada al nombre de dominio **www.uagrm.edu.bo**

```
dig -x 200.87.195.238
```

Lo anterior solicita una traducción inversa de la IP 200.87.195.238 a los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado un nombre de dominio (esto solo es posible si el servidor DNS responsable del dominio de la IP tiene configuradora la resolución inversa, caso contrario no habrá una respuesta exitosa).

### 3.1.8.3 Uso del comando nslookup

**nslookup** es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IPs. Se utiliza con el comando nslookup, que funciona tanto en Windows como en LINUX para obtener la dirección IP conociendo el nombre, y viceversa.

Por ejemplo:

Por ejemplo:

```
nslookup www.uagrm.edu.bo
```

Lo anterior solicita una traducción del nombre de dominio **www.uagrm.edu.bo** a los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado una dirección IP.

```
nslookup www.uagrm.edu.bo 8.8.8.8
```

Lo anterior solicita una traducción del nombre de dominio **www.uagrm.edu.bo**, pero le pide, en específico, al servidor DNS con IP 8.8.8.8 que le haga dicha traducción. Luego de realizar la búsqueda del nombre **www.uagrm.edu.bo**, el servidor DNS con IP 8.8.8.8, devolverá la IP asociada al nombre de dominio **www.uagrm.edu.bo**

```
nslookup 200.87.195.238
```

## Temas Especiales

---

Lo anterior solicita una traducción inversa de la IP 200.87.195.238 a los Servidores DNS definidos en el archivo **/etc/resolv.conf** del sistema, devolviendo como resultado un nombre de dominio (esto solo es posible si el servidor DNS responsable del dominio de la IP tiene configuradora la resolución inversa, caso contrario no habrá una respuesta exitosa).

### 3.1.9 BIND

BIND (acrónimo de Berkeley Internet Name Domain) es una implementación del protocolo DNS y provee una implementación libre de los principales componentes del Sistema de Nombres de Dominio, los cuales incluyen:

- Un servidor de sistema de nombres de dominio (named).
- Una biblioteca resolutoria de sistema de nombres de dominio.
- Herramientas para verificar la operación adecuada del servidor DNS (bind-utils).

El Servidor DNS BIND es utilizado de manera amplia en Internet en aproximadamente el 99% de los servidores DNS del mundo, proporcionando una robusta y estable solución.

### 3.1.10 Instalación y Configuración de servidor DNS maestro con BIND

Para habilitar el software necesario para poder configurar un servidor DNS en Rocky Linux 9, se puede instalar el grupo de paquetes '**DNS Name Server**' o en los paquetes **bind bind-chroot bind-utils**

#### 3.1.10.1 Procedimiento para instalar BIND

- i. Abrir una consola de comandos y cambiarse al root
- ii. Instalar bind:  
`dnf -y groupinstall 'DNS Name Server'`
- iii. Agregar al firewall la opción para que el servidor acepte las peticiones realizadas al servidor DNS:  
`firewall-cmd --permanent --zone=public --add-service=dns  
firewall-cmd --permanent --zone=home --add-service=dns  
firewall-cmd --reload`
- iv. Iniciar el servicio DNS (El servicio se llama named)  
`systemctl start named`
- v. Habilitar el servicio named para inicio automático  
`systemctl enable named`

#### 3.1.10.2 Configuración de servidor DNS primario con BIND

**NOTA:** Lo que se explica a continuación es solo un ejemplo ficticio, que usted debe usar como base para realizar con su propio nombre de dominio e IP respectiva y algunas otras IP's que decida utilizar para armar su servidor DNS de práctica.

Antes de empezar esta configuración usted debe tener ya definido cuál es su nombre de dominio, cuáles son los nombres de los host's que se tendrán dentro de su dominio y cuáles son las IP asignados a dichos nombres.

## Temas Especiales

Para la explicación se tomará como ejemplo la siguiente información, no olvide que usted deberá realizar su configuración son su propio dominio y sus nombres de host's.

|                                  |                    |                                                                             |
|----------------------------------|--------------------|-----------------------------------------------------------------------------|
| <b>Dominio:</b>                  | sof164.net         |                                                                             |
| <b>Correo del Administrador:</b> | roberto@sof164.net |                                                                             |
| <b>Nombre de host</b>            | <b>IP</b>          | <b>Aclaración</b>                                                           |
| dns1.sof164.net                  | 10.23.3.48         | Servidor DNS (Registro NS, registro A y registro PTR)                       |
| correo.sof164.net                | 10.23.3.48         | Servidor de correo (Registro MX con prioridad 4, registro A y registro PTR) |
| www.sof164.net                   | 10.23.3.48         | Servidor web (registro A y registro PTR)                                    |
| webserver.sof164.net             | 10.23.3.48         | Alias a www.sof164.net (Registro CNAME y registro PTR)                      |
| serverc7.sof164.net              | 10.23.3.48         | Alias a www.sof164.net (Registro CNAME)                                     |
| serveral98.sof164.net            | 10.23.3.98         | Servidor de alumno 98 (registro A y registro PTR)                           |
| serveral50.sof164.net            | 10.23.3.50         | Servidor de alumno 50 (registro A)                                          |
| serveral55.sof164.net            | 10.23.3.55         | Servidor de alumno 55 (registro A y registro PTR)                           |
| eqdamian.sof164.net              | 10.23.3.98         | Alias a serveral98.sof164.net (Registro CNAME y registro PTR)               |

Cuando usamos BIND para configurar un servidor DNS, podemos realizar de forma por defecto sin uso de vistas o utilizando vistas. Usamos vistas normalmente cuando queremos que nuestro servidor DNS de respuestas diferentes para las mismas zonas dependiente de quien es el cliente que hace la consulta, es decir desde que IP viene la consulta a nuestro servidor DNS.

### 3.1.10.2.1 Configuración de servidor DNS sin uso de vistas

- i. Abrir una consola de comandos y cambiarse al root
- ii. Cambiarse al directorio /etc  
`cd /etc`
- iii. Sacar copia de seguridad del archivo de configuración named.conf  
`cp named.conf named.conf.20200410`
- iv. El archivo **named.conf** por defecto viene con la siguiente información

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.

options {
 listen-on port 53 { 127.0.0.1; };
 listen-on-v6 port 53 { ::1; };
 directory "/var/named";
 dump-file "/var/named/data/cache_dump.db";
 statistics-file "/var/named/data/named_stats.txt";
 memstatistics-file "/var/named/data/named_mem_stats.txt";
 secroots-file "/var/named/data/named.secroots";
 recursing-file "/var/named/data/named.recurising";
```

## Temas Especiales

```
allow-query { localhost; };

/*
- If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
- If you are building a RECURSIVE (caching) DNS server, you need to enable
recursion.
- If your recursive DNS server has a public IP address, you MUST enable access
control to limit queries to your legitimate users. Failing to do so will
cause your server to become part of large scale DNS amplification
attacks. Implementing BCP38 within your network would greatly
reduce such attack surface
*/
recursion yes;

dnssec-validation yes;

managed-keys-directory "/var/named/dynamic";
geoip-directory "/usr/share/GeoIP";

pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";

/* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
include "/etc/crypto-policies/back-ends/bind.config";
};

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

zone "." IN {
 type hint;
 file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

En este archivo todo lo que esta después de // es ignorado por el servidor y lo que está dentro de /\* \*/ también, es decir que son comentarios.

- v. Editar el archivo **named.conf** con un editor de texto plano, como vi, nano o gedit y cambiamos su configuración a necesidad. Para este ejemplo este archivo quedaría así:

| Linea | Texto del archivo de configuracion                                             |
|-------|--------------------------------------------------------------------------------|
| 1     | //                                                                             |
| 2     | // named.conf                                                                  |
| 3     | //                                                                             |
| 4     | // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS     |
| 5     | // server as a caching only nameserver (as a localhost DNS resolver only).     |
| 6     | //                                                                             |
| 7     | // See /usr/share/doc/bind*/sample/ for example named configuration files.     |
| 8     | //                                                                             |
| 9     |                                                                                |
| 10    | options {                                                                      |
| 11    | listen-on port 53 { 127.0.0.1; 10.23.3.48; };                                  |
| 12    | listen-on-v6 port 53 { ::1; };                                                 |
| 13    | directory      "/var/named";                                                   |
| 14    | dump-file     "/var/named/data/cache_dump.db";                                 |
| 15    | statistics-file "/var/named/data/named_stats.txt";                             |
| 16    | memstatistics-file "/var/named/data/named_mem_stats.txt";                      |
| 17    | secroots-file  "/var/named/data/named.secroots";                               |
| 18    | recursing-file "/var/named/data/named.recurising";                             |
| 19    | allow-query    { localhost; 10.23.3.0/24; };                                   |
| 20    | allow-transfer { localhost; 10.23.3.48; };                                     |
| 21    |                                                                                |
| 22    | /*                                                                             |
| 23    | - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.    |
| 24    | - If you are building a RECURSIVE (caching) DNS server, you need to enable     |
| 25    | recursion.                                                                     |
| 26    | - If your recursive DNS server has a public IP address, you MUST enable access |
| 27    | control to limit queries to your legitimate users. Failing to do so will       |
| 28    | cause your server to become part of large scale DNS amplification              |
| 29    | attacks. Implementing BCP38 within your network would greatly                  |
| 30    | reduce such attack surface                                                     |

```

31 */
32 recursion yes;
33
34 dnssec-validation no;
35
36 managed-keys-directory "/var/named/dynamic";
37 geoip-directory "/usr/share/GeoIP";
38
39 pid-file "/run/named/named.pid";
40 session-keyfile "/run/named/session.key";
41
42 /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
43 include "/etc/crypto-policies/back-ends/bind.config";
44
45 };
46
47 logging {
48 channel default_debug {
49 file "data/named.run";
50 severity dynamic;
51 };
52
53 zone "." IN {
54 type hint;
55 file "named.ca";
56 };
57
58 include "/etc/named.rfc1912.zones";
59 include "/etc/named.root.key";
60 zone "sof164.net" {
61 type master;
62 file "sof164.net.zone";
63 allow-update { none; };
64 };
65 zone "3.23.10.in-addr.arpa" {
66 type master;
67 file "10.23.3.zone";
68 allow-update { none; };
69 };

```

Los cambios realizados:

- **Línea 11:** listen-on port 53 { 127.0.0.1; **10.23.3.48;** }; .- Esto es para que el servidor DNS también escuche por su tarjeta de red que tiene la IP 10.23.3.48, si no hacemos esto, el servidor no habilitara el servicio DNS solo para el mismo
- **Línea 19:** allow-query { localhost;**10.23.3.0/24;** }; .- Esto hace que el servidor DNS permita consultas DNS desde el mismo servidor y desde cualquier cliente que este en la red 10.23.3.0/24. Si no hacemos estos el servidor solo aceptará peticiones solo si lo hacen programas instalados en el mismo servidor DNS no desde otros equipos y si instalamos un servidor DNS es para que atienda peticiones de resolución realizadas por otros computadores.
- **Línea 20:** allow-transfer { localhost; **10.23.3.48;** }; .- Eso hace que cuando se haga una solicitud de transferencia de zona, solo se acepte si la solicitud viene del mismo servidor DNS o de computador que tenga la IP 10.23.3.48. Si queremos que otros equipos tambien puedan solicitarle que el servidor DNS le pase la zona completa, entonces agregamos la IP de dicho equipo en esta lista.
- **Lineas 60 a 64:** En la zona de resolución directa estamos indicando que el servidor DNS es autoridad de esta zona y que el archivo de configuración de esta zona está ubicado en **/var/named/** y que el archivo tiene como nombre **sof164.net.zone**. No se olvide que usted decide que nombre le pone a este archivo, porque usted lo tendrá que crear.

```

zone "sof164.net" {
 type master;

```

```
 file "sof164.net.zone";
 allow-update { none; };
};
```

- **Línea 60:** Nombre de la zona de resolución directa (usamos el nombre de dominio)
- **Línea 61:** Tipo de la zona. En este caso como estamos configurando un servidor primario, definimos la zona como maestra.
- **Línea 62:** Nombre del archivo que debemos crear para la configuración de zona directa y donde pondremos toda la configuración de esta zona. No se olvide, como solo coloco el nombre del archivo, este debe crearse en el directorio /var/named
- **Línea 63:** Especificamos que nadie puede actualizar esta configuración en forma dinámica. Si algún equipo tiene permitido modificar esta configuración en forma dinámica, en lugar de none, pondremos la IP de dicho equipo.

- **Lineas 65 a 69:** En la zona de resolución inversa estamos indicando que el servidor DNS es autoridad de esta zona y que el archivo de configuración de esta zona está ubicado en **/var/named/** y que el archivo tiene como nombre **10.23.3.zone**. No se olvide que usted decide que nombre le pone a este archivo, porque usted lo tendrá que crear.

```
zone "3.23.10.in-addr.arpa" {
 type master;
 file "10.23.3.zone";
 allow-update { none; };
};
```

- **Línea 65:** Nombre de la zona de resolución inversa. Como para el ejemplo estamos usando la red 10.23.3.0/24 entonces nuestro nombre de zona inversa hemos colocado la parte de la IP que define la red pero volcada y terminada en in-addr.arpa, es decir .3.23.10.in-addr.arpa. Esto siempre es así, para la inversa, de la IP que estamos utilizando, la parte que corresponde a la red (según la máscara que estemos usando), la colocamos invertida y que termine en in-addr.arpa. Así que para su práctica fíjese bien que IP esta usando su red.
- **Línea 66:** Tipo de la zona. En este caso como estamos configurando un servidor primario, definimos la zona como maestra.
- **Línea 67:** Nombre del archivo que debemos crear para la configuración de zona inversa y donde pondremos toda la configuración de esta zona. No se olvide, como solo coloco el nombre del archivo, este debe crearse en el directorio /var/named
- **Línea 68:** Especificamos que nadie puede actualizar esta configuración en forma dinámica. Si algún equipo tiene permitido modificar esta configuración en forma dinámica, en lugar de none, pondremos la IP de dicho equipo.

- vi. Ahora clarificamos que como la directiva **directory** (vea la linea 13) de esta configuración especifica la ruta **/var/named**, esto indica el directorio donde se buscarán los archivos para

los que en nuestra configuración solo coloquemos el nombre del archivo o alguna ruta relativa. Fijese la definición de zonas hemos solo colocado **sof164.net.zone** y **10.23.3.zone**. Esto quiere decir que dentro del directorio **/var/named** deberemos crear los archivos **sof164.net.zone** y **10.23.3.zone**.

- vii. Cambiemosnos al directorio **/var/named**, porque ahora nos toca hacer la configuración de las zonas. Ejecutemos para cambiarnos a este directorio:

```
cd /var/named/
```

- viii. Creamos el archivo de configuración para traducción de la directa del dominio **sof164.net**, para esto con un editor como vi, nano o gedit creamos el archivo, por ejemplo, con el editor vi:

```
vi sof164.net.zone
```

Dentro del archivo de este archivo colocamos la configuración de traducción de la directa de nuestro dominio, vea que se hizo según el detalle que pusimos en la tabla al principio de este apartado:

| Linea | Valor                                           |
|-------|-------------------------------------------------|
| 1.    | \$TTL 604800                                    |
| 2.    | @ IN SOA dns1.sof164.net. roberto.sof164.net. ( |
| 3.    | 2020041601; número de serie                     |
| 4.    | 604800 ; tiempo de refresco                     |
| 5.    | 86400 ; tiempo entre reintentos de consulta     |
| 6.    | 2419200 ; tiempo tras el cual expira la zona    |
| 7.    | 604800; tiempo total de vida                    |
| 8.    | )                                               |
| 9.    | @ IN NS dns1.sof164.net.                        |
| 10.   | @ IN MX 10 correo.sof164.net                    |
| 11.   | @ IN TXT "v=spf1 a mx -all"                     |
| 12.   | @ IN A 10.23.3.48                               |
| 13.   | dns1 IN A 10.23.3.48                            |
| 14.   | correo IN A 10.23.3.48                          |
| 15.   | www IN A 10.23.3.48                             |
| 16.   | serveral98 IN A 10.23.3.98                      |
| 17.   | serveral50 IN A 10.23.3.50                      |
| 18.   | serveral55 IN A 10.23.3.55                      |
| 19.   | webserver IN CNAME www                          |
| 20.   | serverc7 IN CNAME dns1                          |
| 21.   | eqdamian IN CNAME serveral98                    |

Luego grabamos y cerramos el archivo. Ahora entendamos que hemos puesto:

- **Línea 1.-** Nos indica el tiempo de vida de cada registro en el archivo. En este caso estamos indicando que la validez de cada registro son 7 días
- **Líneas 2 a la 8.-** Estamos definiendo el registro SOA de nuestra zona, donde:
  - **Línea 2 - @,** significa el nombre de nuestro dominio, es decir, **sof164.net**. con el punto al final.
  - **Línea 2 - dns1.sof164.net.** , es el nombre del servidor dns responsable de esta zona
  - **Línea 2 - roberto.sof164.net.** , es el correo electrónico del administrador del servidor DNS (es decir roberto@sof164.net). Note que acá no podemos usar @ porque en este archivo ya se explicó que significa @, entonces el primer punto el servidor entiende como que hemos colocado @.
  - **Línea 3 - 2020041601** , número de serie del registro, mejor si se usa un formato de fecha acompañado de un numero de 2 dígitos.

- **Línea 4 - 604800**, tiempo en el que los servidores secundarios de nuestro dominio (si hubieran), deben refrescar su información desde el servidor maestro. Hemos puesto 7 días.
- **Línea 5 - 86400**, tiempo en el que los servidores secundarios de nuestro dominio (si hubieran), deben refrescar su información desde el servidor maestro cuando una solicitud previa de refresco de información de zona falla. Hemos puesto 1 día.
- **Línea 6 - 2419200**, es el tiempo antes que un servidor secundario de nuestra zona (si hubiera) deje de responder a las búsquedas una vez se haya producido un intervalo de actualización de la zona. Hemos puesto 28 días.
- **Línea 7 - 604800**, Indica el intervalo de tiempo que se mantendrá una consulta no resuelta en la caché de los servidores de nombres. Hemos puesto 7 días.
- **Línea 9** – Registro NS indicando el FQDN del servidor DNS.
- **Línea 10** – Registro MX indicando el nombre del servidor de correo del dominio y su prioridad, en este caso es 10.
- **Línea 11** – Registro de tipo TXT, para ayudar a reducir los SPAM, especificando que solo las IP's de los registros de tipo A y MX están autorizados a enviar correos a través del servidor de correo definido en el registro MX.
- **Línea 12** – Registro A para la traducción directa del nombre de nuestro dominio hacia una IP
- **Líneas 13 a la 18** - Registros de tipo A para especificar la traducción directa de los nombres de host en nuestro dominio hacia una IP.
- **Líneas 19 a la 21** – Alias (apodos) para nombres host ya definidos con registros de tipo A o de tipo CNAME

Al finalizar la configuración de la zona de reenvío, el archivo que hemos creado deberemos cambiarle el propietario ejecutando en este nuestro ejemplo, el comando: **chown root.named sof164.net.zone**

Note en este ejemplo que se asume que usted ya se encuentra ubicado en el directorio /var/named que es donde acabamos de crear el archivo **sof164.net.zone**

- ix. Creamos el archivo de configuración para traducción de la inversa del dominio **10.23.3.zone**, para esto con un editor como vi, nano o gedit creamos el archivo, por ejemplo, con el editor vi haríamos algo así:

**vi 10.23.3.zone**

Dentro del archivo de este archivo colocamos la configuración de traducción de la inversa de nuestro dominio, según lo colocado en la tabla al principio de este apartado:

| Linea | Valor                                           |
|-------|-------------------------------------------------|
| 1.    | \$TTL 604800                                    |
| 2.    | @ IN SOA dns1.sof164.net. roberto.sof164.net. ( |
| 3.    | 2020041601; número de serie                     |
| 4.    | 604800 ; tiempo de refresco                     |
| 5.    | 86400 ; tiempo entre reintentos de consulta     |
| 6.    | 2419200 ; tiempo tras el cual expira la zona    |
| 7.    | 604800 ; tiempo total de vida                   |
| 8.    | )                                               |
| 9.    | @ IN NS dns1.sof164.net.                        |
| 10.   | 48 IN PTR dns1.sof164.net.                      |

|     |    |    |     |                        |
|-----|----|----|-----|------------------------|
| 11. | 48 | IN | PTR | www.sof164.net.        |
| 12. | 48 | IN | PTR | correo.sof164.net.     |
| 13. | 48 | IN | PTR | webserver.sof164.net.  |
| 14. | 98 | IN | PTR | serveral98.sof164.net. |
| 15. | 55 | IN | PTR | serveral55.sof164.net. |
| 16. | 55 | IN | PTR | eqdamian.sof164.net.   |

Luego grabamos y cerramos el archivo. Ahora entendamos que hemos puesto:

- **Línea 1.**- Nos indica el tiempo de vida de cada registro en el archivo. En este caso estamos indicando que la validez de cada registro son 7 días
- **Líneas 2 a la 8.**- Estamos definiendo el registro SOA de nuestra zona, donde:
  - **Línea 2 - @,** significa el nombre de nuestro dominio, es decir, **3.23.10.in-addr.arpa.** con el punto al final.
  - **Línea 2 - dns1.sof164.net.**, es el nombre del servidor dns responsable de esta zona
  - **Línea 2 - roberto.sof164.net.**, es el correo electrónico del administrador del servidor DNS (es decir roberto@sof164.net). Note que acá no podemos usar @ porque en este archivo ya se explicó que significa @, entonces el primer punto el servidor entiende como que hemos colocado @.
  - **Línea 3 - 2020041601**, número de serie del registro, mejor si se usa un formato de fecha acompañado de un numero de 2 digitos.
  - **Línea 4 - 604800**, tiempo en el que los servidores secundarios de nuestro dominio (si hubieran), deben refrescar su información desde el servidor maestro. Hemos puesto 7 días.
  - **Línea 5 - 86400**, tiempo en el que los servidores secundarios de nuestro dominio (si hubieran), deben refrescar su información desde el servidor maestro cuando una solicitud previa de refresco de información de zona falla. Hemos puesto 1 día.
  - **Línea 6 - 2419200**, es el tiempo antes que un servidor secundario de nuestra zona (si hubiera) deje de responder a las búsquedas una vez se haya producido un intervalo de actualización de la zona. Hemos puesto 28 días.
  - **Línea 7 - 604800**, Indica el intervalo de tiempo que se mantendrá una consulta no resuelta en la caché de los servidores de nombres. Hemos puesto 7 días.
- **Línea 9 – Registro NS** indicando el FQDN del servidor DNS.
- **Línea 10 a la 16 – Registros PTR** indicando la parte faltante de la dirección de red para poder hacer resolución inversa. En nuestro caso como nuestra red es la **10.23.3.0/24**, entonces en la definición de la zona usamos la parte **10.23.3** de la dirección de red, pero al revés, es decir, **3.23.10**, por lo tanto, acá solo completamos la parte de la IP que falta para cada nombre de host. Por ejemplo, para el nombre de dominio **www.sof164.net.** que hemos especificado que su IP es la **10.23.3.48**, en este archivo de resolución inversa solo hemos especificado el número **48**, es decir, **48 IN PTR www.sof164.net.**, por que el saldo se usó al definir la zona de traducción inversa en el inciso v. Lo mismo se hace con el resto de los nombres de host que queramos que haya resolución inversa.

Al finalizar la configuración de la zona de reenvío, el archivo que hemos creado deberemos cambiarle el propietario ejecutando en este nuestro ejemplo, el comando: **chown root.named 10.23.3.zone**

Note en este ejemplo que se asume que usted ya se encuentra ubicado en el directorio /var/named que es donde acabamos de crear el archivo **10.23.zone**

### NOTAS:

- Note que el carácter @ tiene un significado en el archivo de definición de zona de traducción directa y otro significado en el archivo de definición de zona de traducción inversa
- Para el caso de traducción de la inversa, si nuestra red fuera **10.23.0.0/16** entonces en la definición de zona de traducción inversa hubiéramos escrito **23.10.in-addr.arpa** y en el archivo de definición de esta zona para completar por ejemplo el mismo caso de **www.sof164.net.** como su IP es la **10.23.3.48**, la parte de la red solo es **10.23** por lo que para hacer la inversa la parte del faltante de la IP del host es **3.48**, por lo que el registro de inversa para este host hubiera sido:

**48.3 IN PTR www.sof164.net.**

Fíjese se coloca la parte faltante de la IP pero volcada.

- En el archivo de resolución directa cuando usted solo coloca el nombre canónico del host, por ejemplo, usted solo escribe el nombre canónico **www**, entonces, el servidor DNS entenderá que quiso escribir **www.sof164.net.**, fíjese que con el punto al final
- En el archivo de resolución directa cuando usted coloca el nombre FQDN del host, por ejemplo, usted escribe el nombre **www.sof164.net.**, entonces, el servidor DNS entenderá que quiso escribir **www.sof164.net.**, es decir lo mismo sin ningún cambio.
- En el archivo de resolución directa cuando usted coloca el nombre FQDN del host, por ejemplo, usted escribe el nombre **www.sof164.net**, entonces, el servidor DNS entenderá que quiso escribir **www.sof164.net.sof164.net.**, el aumento **sof164.net.**, porque cuando usted quiere especificar un nombre FQDN de un host tiene que ponerle el punto al final, si no lo hace, el servidor aumentara el nombre del dominio, por tanto, tenga cuidado con esto.
- En el archivo de resolución inversa, es mejor usar nombres FQDN todo el tiempo, porque cuando usted solo coloca el nombre canónico del host, en nuestro ejemplo (donde nuestra red es **10.23.3.0/24**), si usted solo escribe el nombre canónico **www**, entonces, el servidor DNS entenderá que quiso escribir **www.3.23.10.in-addr.arpa.**, entonces en los archivos de resolución inversa no use nombres canónicos, use FQDN, para el caso de **www** usted deberá escribir **www.sof164.net.** (OJO no se olvide el punto al final)

- x. Reiniciamos el servicio **named**  
**systemctl restart named**
- xi. Procedemos a cambiar el DNS que usan nuestros programas clientes, para eso la forma más fácil es abrir la configuración de nuestra tarjeta de red, tal como se explicó en el punto **1.9.2**

- de esta guía y como dns ya no usamos el 8.8.8.8, ahora deberemos poner como DNS la IP de nuestro servidor DNS.
- xii. Finalmente, cuando estemos seguro que nuestra configuración del paso anterior ya está habilitada, procedemos a probar en una consulta con alguno de los comandos explicados en el punto 3.1.6, por ejemplo, con dig para el host webserver.sof164.net, es decir:
- ```
dig webserver.sof164.net
```

NOTA: Para cualquier equipo al que necesitemos que use nuestro servidor DNS como su servidor de resolución de nombres, si el equipo es un Rocky Linux, repetiremos en ese equipo ultimo paso (inciso xii). Si el equipo tiene otro sistema operativo como por ejemplo Windows, procesa accediendo al administrador de recursos de red, y cambie la configuración de su tarjeta de red para el protocolo TPC/IP versión 4 y coloque como DNS la IP de su servidor DNS que acaba de finalizar de configurar

3.1.10.2.2 Configuración de servidor DNS con uso de vistas

- i. Abrir una consola de comandos y cambiarse al root
- ii. Cambiarse al directorio /etc

```
cd /etc
```
- iii. Sacar copia de seguridad del archivo de configuración named.conf

```
cp named.conf named.conf.20180416
```
- iv. El archivo **named.conf** por defecto viene con la siguiente información

```
//  
// named.conf  
//  
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS  
// server as a caching only nameserver (as a localhost DNS resolver only).  
//  
// See /usr/share/doc/bind*/sample/ for example named configuration files.  
//  
// See the BIND Administrator's Reference Manual (ARM) for details about the  
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html  
  
options {  
    listen-on port 53 { 127.0.0.1; };  
    listen-on-v6 port 53 { ::1; };  
    directory      "/var/named";  
    dump-file     "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    allow-query    { localhost; };  
  
    /*  
     * If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.  
     * If you are building a RECURSIVE (caching) DNS server, you need to enable  
     * recursion.  
     * If your recursive DNS server has a public IP address, you MUST enable access  
     * control to limit queries to your legitimate users. Failing to do so will  
     * cause your server to become part of large scale DNS amplification  
     * attacks. Implementing BCP38 within your network would greatly  
     * reduce such attack surface  
    */  
    recursion yes;  
  
    dnssec-validation yes;  
  
    /* Path to ISC DLV key */  
    bindkeys-file "/etc/named.iscdlv.key";  
  
    managed-keys-directory "/var/named/dynamic";
```

Temas Especiales

```
        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
    };

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

zone "." IN {
    type hint;
    file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

En este archivo todo lo que esta después de // es ignorado por el servidor y lo que está dentro de /* */ también, es decir que son comentarios.

- v. Editar el archivo **named.conf** con un editor de texto plano, como vi, nano o gedit y cambiamos su configuración a necesidad. Para este ejemplo este archivo quedaría así:

```
/*
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
    listen-on port 53 { 127.0.0.1; 10.23.3.48; 192.168.0.116; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file      "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query { localhost;10.23.3.0/24; 192.168.0.0/24; };
    allow-transfer { localhost; 10.23.3.48; 192.168.0.116; };

    /*
     - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
     - If you are building a RECURSIVE (caching) DNS server, you need to enable
       recursion.
     - If your recursive DNS server has a public IP address, you MUST enable access
       control to limit queries to your legitimate users. Failing to do so will
       cause your server to become part of large scale DNS amplification
       attacks. Implementing BCP38 within your network would greatly
       reduce such attack surface
    */
    recursion yes;

    dnssec-validation no;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";

    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
};

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

include "/etc/named.root.key";
```

```
view "local" {
    match-clients {
        127.0.0.0/8;
        10.23.3.0/24;
    };
    include "/etc/named.rfc1912.zones";
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "sof164.net" {
        type master;
        file "local/sof164.net.zone";
        allow-update { none; };
    };
    zone "3.23.10.in-addr.arpa" {
        type master;
        file "local/10.23.3.zone";
        allow-update { none; };
    };
};
view "publico" {
    match-clients { any; };
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "sof164.net" {
        type master;
        file "publico/sof164.net.zone";
        allow-update { none; };
    };
};
```

Los cambios realizados:

- **listen-on port 53 { 127.0.0.1; 10.23.3.48; 192.168.0.116; };** .- Esto es para que el servidor DNS también escuche por su tarjeta de red que tiene la IP 10.23.3.48 y en la tarjeta que tenga la ip 192.168.0.116
- **allow-query { localhost;10.23.3.0/24; 192.168.0.0/24; };** .- esto hace que el servidor DNS permita consultas DNS desde el mismo servidor y desde cualquier cliente que este en la red 10.23.3.0/24 o desde la red 192.168.0.0/24
- **allow-transfer { localhost; 10.23.3.48; 192.168.0.116; };** .- Eso hace que cuando se haga una solicitud de transferencia de zona, solo se acepte si la solicitud viene del mismo servidor o de computador que tenga la IP 10.23.3.48 o la ip 192.168.0.116
- Se tienen dos vistas, la vista local y la vista publico

```
view "local" { .... }
view "publico" { .... }
```

- La sección que se ha marcado en violeta en el texto dentro de la vista publico y local, sirve para que el DNS sepa a que servidores va realizar consultas cuando necesite hacer búsquedas recursivas

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

- La sección marcada en celeste dentro de las vistas publico y local, hace saber al servidor DNS para que clientes aplica dicha vista, por ejemplo, el bloque en celeste de la vista **local**, indica que la configuración de la vista **local** solo aplica a solicitudes del propio servidor y de la red 10.23.3.0/25

```
match-clients {
    127.0.0.0/8;
    10.23.3.0/24;
};
```

- Para la vista local se ha definido una zona de resolución directa para el dominio **sof164.net** y una zona de resolución inversa.

En la zona de resolución directa estamos indicando que el servidor DNS es autoridad de esta zona y que el archivo de configuración de esta zona está ubicado en **/var/named/local** y que el archivo tiene como nombre **sof164.net.zone**. No se olvide que usted decide que nombre le pone a este archivo, porque usted lo tendrá que crear.

```
zone "sof164.net" {
    type master;
    file "local/sof164.net.zone";
    allow-update { none; };
};
```

En la zona de resolución inversa estamos indicando que el servidor DNS es autoridad de esta zona y que el archivo de configuración de esta zona está ubicado en **/var/named/local** y que el archivo tiene como nombre **10.23.3.zone**. No se olvide que usted decide que nombre le pone a este archivo, porque usted lo tendrá que crear.

```
zone "3.23.10.in-addr.arpa" {
    type master;
    file "local/10.23.3.zone";
    allow-update { none; };
};
```

- Para la vista publico, solo estamos configurando un zona de resolución directa, pero no una inversa.

En la zona de resolución directa estamos indicando que el servidor DNS es autoridad de esta zona y que el archivo de configuración de esta zona está ubicado en **/var/named/publico** y que el archivo tiene como nombre **sof164.net.zone**. No se olvide que usted decide que nombre le pone a este archivo, porque usted lo tendrá que crear.

```
zone "sof164.net" {
    type master;
    file "publico/sof164.net.zone";
    allow-update { none; };
};
```

Temas Especiales

- vi. Ahora clarificamos que como la directiva **directory** de esta configuración especifica la ruta **/var/named**, esto indica el directorio donde se buscarán los archivos para los que en nuestra configuración solo coloquemos el nombre del archivo o alguna ruta relativa. Fijese que en la vista **local** tenemos configurado 2 archivos: **local/sof164.net.zone** y **local/10.23.3.zone**; y en la vista **publico** tenemos configurado el archivo: **publico/sof164.net.zone**. Esto quiere decir que dentro del directorio **/var/named** deberemos crear, si es que aún no existen, los directorios: **local** y **publico**; y luego dentro de local deberemos crear los archivos **sof164.net.zone** y **10.23.3.zone**. Procedemos primero a crear los directorios solo si no existen ejecutando los siguientes comandos:

```
cd /var/named  
mkdir local publico
```

- vii. Ahora nos cambiamos al directorio local, ejecutando, porque ahora nos toca hacer la configuración de las zonas de la vista local:

```
cd /var/named/local
```

- viii. Creamos el archivo de configuración para traducción de la directa del dominio **sof164.net**, para esto con un editor como vi, nano o gedit creamos el archivo, por ejemplo, con el editor vi:

```
vi sof164.net.zone
```

Dentro del archivo de este archivo colocamos la configuración de traducción de la directa de nuestro dominio, vea que se hizo según el detalle que pusimos en la tabla al principio de este apartado:

Linea	Valor
1.	\$TTL 604800
2.	@ IN SOA dns1.sof164.net. roberto.sof164.net. (
3.	2020041601; número de serie
4.	604800 ; tiempo de refresco
5.	86400 ; tiempo entre reintentos de consulta
6.	2419200 ; tiempo tras el cual expira la zona
7.	604800; tiempo total de vida
8.)
9.	@ IN NS dns1.sof164.net.
10.	@ IN MX 10 correo
11.	@ IN TXT "v=spf1 a mx -all"
12.	@ IN A 10.23.3.48
13.	dns1 IN A 10.23.3.48
14.	correo IN A 10.23.3.48
15.	www IN A 10.23.3.48
16.	serveral98 IN A 10.23.3.98
17.	serveral50 IN A 10.23.3.50
18.	serveral55 IN A 10.23.3.55
19.	webserver IN CNAME www
20.	serverc7 IN CNAME dns1
21.	eqdamian IN CNAME serveral98

Vea la explicación de este punto en el inciso **viii** del apartado 3.1.8.2.1, ya que es la misma.

- ix. Creamos el archivo de configuración para traducción de la inversa del dominio **10.23.3.zone**, para esto con un editor como vi, nano o gedit creamos el archivo, por ejemplo, con el editor vi haríamos algo así:

```
vi 10.23.3.zone
```

Dentro del archivo de este archivo colocamos la configuración de traducción de la inversa de nuestro dominio, según lo colocado en la tabla al principio de este apartado:

Temas Especiales

Linea	Valor
1.	\$TTL 604800
2.	@ IN SOA dns1.sof164.net. roberto.sof164.net. (
3.	2020041601; número de serie
4.	604800 ; tiempo de refresco
5.	86400 ; tiempo entre reintentos de consulta
6.	2419200 ; tiempo tras el cual expira la zona
7.	604800 ; tiempo total de vida
8.)
9.	@ IN NS dns1.sof164.net.
10.	48 IN PTR dns1.sof164.net.
11.	48 IN PTR www.sof164.net.
12.	48 IN PTR correo.sof164.net.
13.	48 IN PTR webserver.sof164.net.
14.	98 IN PTR serveral98.sof164.net.
15.	55 IN PTR serveral55.sof164.net.
16.	55 IN PTR eqdamian.sof164.net.

Vea la explicación de este punto en el inciso **ix** del apartado 3.1.8.2.1, ya que es la misma.

- x. Ahora configuraremos el archivo de traducción directa para la vista **publico**, para esto nos cambiamos al directorio **publico** que creamos en el inciso **vi**
cd /var/named/publico
- xi. Con editor de texto plano creamos el archivo **sof164.net.zone** que tendrá la resolución directa que nuestro DNS dará cuando el cliente solicitante no sea de la red 127.0.0.0/8 o de la red 10.23.3.0/24:
vi sof164.net.zone

Dentro de este archivo colocamos la configuración de traducción directa de nuestro DNS para el dominio **sof164.net** en la vista **publico**:

\$TTL 604800					
@	IN	SOA	dns1.sof164.net.	roberto.sof164.net.	(
	2020041601; número de serie				
	604800 ; tiempo de refresco				
	86400 ; tiempo entre reintentos de consulta				
	2419200 ; tiempo tras el cual expira la zona				
	604800 ; tiempo total de vida				
)				
@	IN	NS	dns1.sof164.net.		
@	IN	MX	10 correo		
@	IN	TXT	"v=spf1 a mx -all"		
@	IN	A	192.168.0.116		
dns1	IN	A	192.168.0.116		
correo	IN	A	192.168.0.116		
www	IN	A	192.168.0.116		
cliente10	IN	A	192.168.0.34		

Fíjese que en este archivo hemos colocado la traducción directa de menos host's que lo que colocamos para la vista **local**, porque así lo hemos decidido, y si se fija ahora para esta vista la traducción será para otra red, ya no para la 10.23.3.0.

- xii. Reiniciamos el servicio **named**
systemctl restart named
- xiii. Procedemos a cambiar el DNS que usan nuestros programas clientes, para eso la forma más fácil es abrir la configuración de nuestra tarjeta de red, tal como se explicó en el punto **1.9.2** de esta guía y como dns ya no usamos el 8.8.8.8, ahora deberemos poner como DNS la IP de nuestro servidor DNS.

- xiv. Finalmente, cuando estemos seguro que nuestra configuración del paso anterior ya está habilitada, procedemos a probar en una consulta con alguno de los comandos explicados en el punto 3.1.6, por ejemplo, con dig para el host webserver.sof164.net, es decir:
`dig webserver.sof164.net`

NOTA: Para cualquier equipo al que necesitemos que use nuestro servidor DNS como su servidor de resolución de nombres, si el equipo es un Rocky Linux, repetiremos en ese equipo el inciso **xiii**. Si el equipo tiene otro sistema operativo como por ejemplo Windows, procesa accediendo al administrador de recursos de red, y cambie la configuración de su tarjeta de red para el protocolo TPC/IP versión 4 y coloque como DNS la IP de su servidor DNS que acaba de finalizar de configurar.

IMPORTANTE:

Si desea que el servidor dns registre en bitacora las respuestas a solicitudes de resoluciones, agregar en la sección options del archivo named.conf lo siguiente: **querylog yes;**

Luego reinicie el servidor DNS y podrá hacer seguimiento del archivo **messages** que se encuentra en **/var/log**

3.2 DHCP

Cuando trabajamos con dispositivos que se comunican por red utilizando el conjunto de protocolos TCP/IP, cada uno de estos dispositivos debe tener asignada al menos una dirección IP y su máscara, para de esta manera poder comunicarse con los otros dispositivos dentro de la misma red. Esta asignación de IP a los dispositivos, se la puede realizar manualmente o en forma dinámica a través del uso DHCP, para de esta manera asegurarnos de una u otra forma que los dispositivos en la red pueden conversar.

3.2.1 Definición de DHCP

DHCP (acrónimo de Dynamic Host Configuration Protocol, que se traduce Protocolo de configuración dinámica de servidores) es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de sub-red, puerta de enlace, etc.) a partir de un servidor DHCP. Su propósito principal es hacer más fáciles de administrar las redes grandes. DHCP existe desde 1993 como protocolo estándar y se describe a detalle en la RFC 2131.

Sin la ayuda de un servidor DHCP, tendrían que configurarse de forma manual cada dirección IP de cada anfitrión que pertenezca a una Red de Área Local. Si un anfitrión se traslada hacia otra ubicación donde existe otra Red de Área Local, se tendrá que configurar otra dirección IP diferente para poder unirse a esta nueva Red de Área Local. Un servidor DHCP entonces supervisa y distribuye, las direcciones IP de una Red de Área Local asignando una dirección IP a cada anfitrión que se une a la Red de Área Local. Cuando, por mencionar un ejemplo, una computadora portátil se configura para utilizar DHCP, a ésta le será asignada una dirección IP y las variables de red, necesarios para unirse a cada Red de Área Local donde se localice.

Existen tres métodos de asignación en el protocolo DHCP:

Temas Especiales

- Asignación manual: La asignación utiliza una tabla con direcciones MAC (acrónimo de Media Access Control Address, que se traduce como dirección de Control de Acceso al Medio). Sólo los anfitriones con una dirección MAC definida en dicha tabla recibirán el IP asignada en la misma tabla. Esto se hace a través de la opción hardware ethernet combinado con deny unknown-clients.
- Asignación automática: Una dirección de IP disponible dentro de un rango determinado se asigna permanentemente al anfitrión que la requiera.
- Asignación dinámica: Se determina arbitrariamente un rango de direcciones IP y cada anfitrión conectado a la red está configurada para solicitar su dirección IP al servidor cuando se inicia el dispositivo de red, utilizando un intervalo de tiempo controlable (opciones default-lease-time y max-lease-time), de modo que la asignación de direcciones IP es de manera temporal y éstas se reutilizan de forma dinámica.

3.2.2 ¿Por qué usar DHCP?

Cada dispositivo de una red basada en TCP/IP debe tener una dirección IP de unidifusión única para acceder a la red y sus recursos. Sin DHCP, las direcciones IP de los equipos nuevos o de los equipos que se mueven de una subred a otra deben configurarse manualmente, mientras que las direcciones IP de los equipos que se quitan de la red deben recuperarse manualmente.

Con DHCP, todo este proceso está automatizado y se administra de forma centralizada. El servidor DHCP mantiene un grupo de direcciones IP y concede una dirección a cualquier cliente habilitado para DHCP cuando se inicia en la red. Dado que las direcciones IP son dinámicas (concedidas) en lugar de estáticas (asignadas permanentemente), las direcciones que ya no están en uso se devuelven automáticamente al grupo para la reasignación.

El administrador de red establece servidores DHCP que mantienen la información de configuración de TCP/IP y proporcionan la configuración de direcciones a los clientes habilitados para DHCP en forma de oferta de concesión. El servidor DHCP almacena la información de configuración en una base de datos que incluye lo siguiente:

- Parámetros de configuración de TCP/IP válidos para todos los clientes de la red.
- Direcciones IP válidas, mantenidas en un grupo para la asignación a clientes, así como direcciones excluidas.
- Direcciones IP reservadas asociadas a determinados clientes DHCP. Esto permite una asignación coherente de una única dirección IP a un único cliente DHCP.
- La duración de la concesión, o el período de tiempo durante el que se puede usar la dirección IP antes de que se requiera una renovación de la concesión.

Cuando un cliente habilitado para DHCP acepta una oferta de concesión, recibe lo siguiente:

- Una dirección IP válida para la subred a la que se conecta.
- Las opciones DHCP solicitadas, que son parámetros adicionales que un servidor DHCP está configurado para asignar a los clientes. Algunos ejemplos de opciones DHCP son Enrutador (puerta de enlace predeterminada), Servidores DNS y Nombre de dominio DNS.

3.2.3 Ventajas de DHCP

DHCP proporciona las ventajas siguientes.

- **Configuración fiable de la dirección IP.** DHCP minimiza los errores de configuración causados por la configuración manual de direcciones IP, como errores tipográficos o conflictos de direcciones causados por la asignación de una dirección IP a más de un equipo al mismo tiempo.
- **Administración de red reducida.** DHCP incluye las características siguientes para reducir la administración de red:
 - Configuración de TCP/IP centralizada y automatizada.
 - Capacidad de definir configuraciones TCP/IP desde una ubicación central.
 - Capacidad de asignar un intervalo completo de valores de configuración de TCP/IP adicionales mediante opciones DHCP.
 - Control eficaz de los cambios de dirección IP para los clientes que deben actualizarse con frecuencia, como los de dispositivos portátiles que se mueven a ubicaciones diferentes en una red inalámbrica.
 - Reenvío de mensajes DHCP iniciales mediante un agente de retransmisión DHCP, lo que elimina la necesidad de un servidor DHCP en cada subred.

3.2.4 DHCP por Internet Software Consortium, Inc.

El programa utilizado para las funciones de DHCP se denomina ISC DHCP.

Fundado en 1994, Internet Software Consortium, Inc., distribuye un conjunto de herramientas para el protocolo DHCP, las cuales consisten en:

- Servidor DHCP.
- Cliente DHCP.
- Agente de retransmisión.

Dichas herramientas utilizan un API (Application Programming Interface o Interfaz de Programación de Aplicaciones) modular diseñado para ser lo suficientemente general para ser utilizado con facilidad en los sistemas operativos que cumplen el estándar POSIX (Portable Operating System Interface for UNIX o interfaz portable de sistema operativo para Unix) y no-POSIX, como Windows.

3.2.5 Anatomía del protocolo

El protocolo trabaja en el puerto UDP 67 para computadoras servidor y en el puerto UDP 68 para computadoras clientes. La secuencia de intercambio de mensajes entre el cliente DHCP y el servidor DHCP es:

DHCP Discovery

Temas Especiales

DHCP Discovery es una solicitud DHCP realizada por un cliente de este protocolo para que el servidor DHCP de dicha red de computadoras le asigne una dirección IP y otros Parámetros DHCP como la máscara de red o el nombre DNS. La solicitud va contenida en un mensaje de descubrimiento que se difunde a todas las máquinas en la red.

DHCP Offer

DHCP Offer es el paquete de respuesta del Servidor DHCP a un cliente DHCP ante su petición de la asignación de los Parámetros DHCP. Para ello involucra su dirección MAC (Media Access Control). Este mensaje contiene una dirección IP disponible que el servidor está dispuesto a asignar al cliente, junto con los otros parámetros de configuración. El servidor puede enviar múltiples ofertas de asignación de direcciones IP y otros parámetros de configuración al cliente.

DHCP Request

Después de recibir las ofertas, el cliente DHCP selecciona una oferta específica de los paquetes recibidos de DHCP Offer. El cliente envía un mensaje de solicitud al servidor DHCP correspondiente, indicando que desea aceptar esa oferta en particular. El mensaje contiene la dirección IP de la oferta seleccionada.

DHCP Acknowledge

Al recibir el mensaje de solicitud del cliente, el servidor la reconoce y le envía un acuse de recibo o mensaje de aceptación DHCP, se inicia la fase final del proceso de configuración. Esta fase implica el reconocimiento con el envío de un paquete al cliente. Este paquete confirma que la dirección IP solicitada ha sido asignada al cliente e incluye la duración de la conexión y cualquier otra información de configuración que el cliente pueda tener solicitada. En este punto, el proceso de configuración TCP/IP se ha completado. El servidor reconoce la solicitud y la envía acuse de recibo al cliente. El sistema en su conjunto espera que el cliente configure su interfaz de red con las opciones suministradas. El servidor DHCP responde a la DHCPREQUEST con un DHCPACK, completando así el ciclo de iniciación. La dirección origen es la dirección IP del servidor de DHCP y la dirección de destino es todavía 255.255.255.255. El campo YIADDR contiene la dirección del cliente, y los campos CHADDR y DHCP: Client Identifier campos son la dirección física de la tarjeta de red en el cliente. La sección de opciones del DHCP identifica el paquete como un ACK.

3.2.6 Instalación de servidor DHCP

- i. Abrir una consola como root
- ii. Instale el paquete dhcp
`dnf -y install dhcp-server`
- iii. Dar permiso en el firewall para los puertos que usa el servidor DHCP
`firewall-cmd --permanent --zone=public --add-port=67-68/udp`
`firewall-cmd --reload`

3.2.7 Configuración de servidor DHCP

Supongamos que se trabaja bajo el siguiente caso hipotético:

Parámetro	Valor
-----------	-------

Temas Especiales

Dirección de segmento de red	10.23.3.0
Dirección de difusión (Broadcast)	10.23.3.255
Mascara de red	255.255.255.0 (24 bits)
Puerta de Enlace (Gateway)	10.23.3.1
Servidor de nombres (DNS)	10.23.3.48
Servidores de tiempo (NTP)	Usaremos ntp.org - es decir 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org y 3.pool.ntp.org - los cuales son confiables y de acceso gratuito.
Rango de direcciones IP a asignar de modo dinámico	10.23.3.100 hasta 10.23.3.120
Nombre de dominio	sof164.net

- i. Abra una consola como root en el servidor DHCP
- ii. (Opcional) Si su servidor DHCP tiene más de una tarjeta de red, por ejemplo, la tarjeta **ens33** y **ens34**, y solo deseamos que el servidor DHCP acepte solicitudes DHCP para la tarjeta de red **ens34** entonces deberemos editar el archivo **dhcpd** que se encuentra en el directorio **/etc/sysconfig**. En este archivo agregaremos la línea: **DHCPDARGS=ens34** (Si no le interesa eso no haga este paso, deje que su DHCP trabaje para todas sus tarjetas de red).
- iii. Para lograr la configuración de nuestro caso hipotético que describimos en la tabla al inicio de este apartado, deberemos editar el archivo **dhcpd.conf**, que está en el directorio **/etc/dhcp** y adicionar el siguiente contenido. (Si desea antes de empezar saque backup de este archivo).

Linea	Valor
1	#
2	# DHCP Server Configuration file.
3	# see /usr/share/doc/dhcp*/dhcpd.conf.example
4	# see dhcpd.conf(5) man page
5	#
6	ddns-update-style none;
7	ignore client-updates;
8	authoritative;
9	default-lease-time 900;
10	max-lease-time 7200;
11	option ip-forwarding off;
12	option domain-name "sof164.net";
13	subnet 10.23.3.0 netmask 255.255.255.0 {
14	option routers 10.23.3.1;
15	option subnet-mask 255.255.255.0;
16	option broadcast-address 10.23.3.255;
17	option domain-name-servers 10.23.3.48;
18	range 10.23.3.100 10.23.3.120;
19	}

Ahora analicemos lo que hemos hecho:

- **Línea 1 a la 5:** Comentarios
- **Línea 6:** Indicamos que el dhcp no hará actualizaciones DNS
- **Línea 7:** Indicamos que los clientes no podrán hacer ellos su actualización de registro A en el DNS

- **Línea 8:** Le indicamos al servidor DHCP que es autoritativo, es decir que podrá enviar mensajes DHCPNACK a aquellos clientes que envían un DHCPREQUEST con una propuesta de IP no válida, debido a que al cliente se le ha cambiado de segmento de red. Si no hacemos esto, en estos casos un servidor no autoritativo no contesta.
 - **Línea 9:** Indicamos que el tiempo que la IP se le concede al cliente es de 900 segundos, cuando el cliente no especifica por cuanto tiempo quiere la IP.
 - **Línea 10:** Indicamos el tiempo máximo que se puede prestar una IP a un cliente en 7200 segundos, cuando el cliente pide la IP por un tiempo mayor a este parámetro.
 - **Línea 11:** Indicamos que el cliente no puede configurar su IP para reenvío de paquetes.
 - **Línea 12:** Indicamos el nombre de dominio que los clientes usarán cuando resuelven nombres de hosts vía DNS, en este caso hemos puesto sof164.net
 - **Línea 13:** Especificamos la sub red que se usará y su máscara.
 - **Línea 14:** Indicamos la puerta de enlace
 - **Línea 15:** Indicamos la máscara de red.
 - **Línea 16:** Indicamos la dirección IP de difusión (broadcast)
 - **Línea 17:** Indicamos la IP del servidor DNS de nuestra red (o las IP's si fueran varios servidores DNS)
 - **Línea 18:** Especificamos el rango de IP en nuestra sub red que el servidor DNS puede utilizar para asignar a los clientes que piden IP en forma dinámica.
 - **Línea 19:** Fin del bloque iniciado en la línea 13
- iv. Habilitamos el servicio dhcp
systemctl enable dhcpcd.service
- v. Iniciamos el servicio
systemctl start dhcpcd.service
- vi. Para probar que nuestro servidor DHCP funciona en otro computador donde tengamos instalado Rocky Linux, utilicemos la interfaz gráfica para configurar la tarjeta de ese equipo como DHCP, siguiendo el procedimiento del apartado 1.9.2, donde aprendimos a configurar la IP en forma manual, pero esta vez le pondremos DHCP y dejaremos la tarjeta de red como desconectada.
En general, para verificar que nuestro servidor dhcp esta distribuyendo IP, en cualquier otro computador (real o virtual) conectado a la red, sin importar que sistema operativo tiene, iremos al gestor de red de dicho equipo y en lugar de configurar IP manualmente procederemos a configurar IP dinámica o vía DHCP (dependiendo de como funcione el gestor de red) para que, al confirmar la configuración, dicho computador comience a buscar un servidor dhcp funcionando en la red. De esta manera podrá verificar que el servidor DHCP (si es el único en la red que da el servicio o si no el único pero responde primero a la solicitud de un equipo cliente) responde y brinda IP a equipos clientes que lo soliciten y que estén conectados al a red dentro del rango de distribución de IP.

3.2.7.1 Asignación de direcciones IP estáticas

Supongamos que tenemos una pc, la cual tiene la dirección MAC 00:50:BF:27:1C:1C y queremos que el servidor DHCP le asigne siempre la IP 10.23.3.121, entonces tendremos que agregar algo como lo siguiente al archivo **/etc/dhcp/dhcpcd.conf**

Temas Especiales

```
host pc51 {  
    option host-name "pc51.sof164.net";  
    hardware ethernet 00:50:BF:27:1C:1C;  
    fixed-address 10.23.3.121;  
}
```

Además queremos que le asigne el nombre pc51.sof164.net. Esta misma configuración tendremos que agregar por cada computador que queramos que se le asigne la misma IP siempre. Con este cambio nuestro archivo **/etc/dhcp/dhcpd.conf** quedaría así:

```
#  
# DHCP Server Configuration file.  
#   see /usr/share/doc/dhcp*/dhcpd.conf.example  
#   see dhcpd.conf(5) man page  
  
#  
ddns-update-style none;  
ignore client-updates;  
authoritative;  
default-lease-time 900;  
max-lease-time 7200;  
option ip-forwarding off;  
option domain-name "sof164.net";  
subnet 10.23.3.0 netmask 255.255.255.0 {  
    option routers 10.23.3.1;  
    option subnet-mask 255.255.255.0;  
    option broadcast-address 10.23.3.255;  
    option domain-name-servers 10.23.3.48;  
    option netbios-name-servers 10.23.3.48;  
    range 10.23.3.100 10.23.3.120;  
}  
# Equipos con IP fija.  
host pc51 {  
    option host-name "pc51.sof164.net";  
    hardware ethernet 00:50:BF:27:1C:1C;  
    fixed-address 10.23.3.122;  
}  
host pcalumno53 {  
    option host-name "alumno53.sof164.net";  
    hardware ethernet 00:0C:29:76:CC:27;  
    fixed-address 10.23.3.121;  
}
```

En rojo también agregamos un segundo host al que queremos darle el mismo trato.

Ahora solo reiniciamos el servicio DHCP y podremos probar.

3.2.7.2 Limitar el acceso por dirección MAC

Es posible limitar el acceso al servidor DHCP a través de la opción deny con el valor unknown-clients y definiendo una lista de direcciones físicas o MAC. De tal modo, a los anfitriones que estén ausentes en dicha lista les será denegado el servicio. Ejemplo, limitemos a que solo dos computadores puedan usar nuestro servidor DHCP:

```
deny unknown-clients;  
host pc1 {  
    hardware ethernet 00:0C:29:83:21:7D;  
}  
host pc2 {  
    hardware ethernet F4:C7:14:70:FA:AC;  
}
```

Temas Especiales

Nuestro archivo de configuración entonces quedaría así:

```
#  
# DHCP Server Configuration file.  
#   see /usr/share/doc/dhcp*/dhcpd.conf.example  
#   see dhcpcd.conf(5) man page  
  
#  
ddns-update-style none;  
ignore client-updates;  
authoritative;  
default-lease-time 900;  
max-lease-time 7200;  
option ip-forwarding off;  
option domain-name "sof164.net";  
subnet 10.23.3.0 netmask 255.255.255.0 {  
    option routers 10.23.3.1;  
    option subnet-mask 255.255.255.0;  
    option broadcast-address 10.23.3.255;  
    option domain-name-servers 10.23.3.48;  
    option netbios-name-servers 10.23.3.48;  
    range 10.23.3.100 10.23.3.120;  
}  
# deny unknown-clients impide que equipos fuera de esta lista puedan  
# utilizar el servicio.  
deny unknown-clients;  
# Lista de direcciones MAC que tendrán permitido utilizar el servidor DHCP.  
host pc1 {  
    hardware ethernet 00:0C:29:83:21:7D;  
}  
host pc2 {  
    hardware ethernet F4:C7:14:70:FA:AC;  
}
```

Reiniciamos el servicio DHCP y podremos probar.

También podemos combinar el hecho que se acepte solo algunos equipos usar el servidor DHCP y de ese conjunto que a algunos se les de IP estatica, por ejemplo podríamos hacer la siguiente configuración:

```
#  
# DHCP Server Configuration file.  
#   see /usr/share/doc/dhcp*/dhcpd.conf.example  
#   see dhcpcd.conf(5) man page  
  
#  
ddns-update-style none;  
ignore client-updates;  
authoritative;  
default-lease-time 900;  
max-lease-time 7200;  
option ip-forwarding off;  
option domain-name "sof164.net";  
subnet 10.23.3.0 netmask 255.255.255.0 {  
    option routers 10.23.3.1;  
    option subnet-mask 255.255.255.0;  
    option broadcast-address 10.23.3.255;  
    option domain-name-servers 10.23.3.48;  
    option netbios-name-servers 10.23.3.48;  
    range 10.23.3.100 10.23.3.120;  
}  
# deny unknown-clients impide que equipos fuera de esta lista puedan
```

Temas Especiales

```
# utilizar el servicio.
deny unknown-clients;
# Lista de direcciones MAC que tendrán permitido utilizar el servidor DHCP.
# Equipos con IP fija.
host pcalumno53 {
    option host-name "alumno53.sof164.net";
    hardware ethernet 00:0C:29:76:CC:27;
    fixed-address 10.23.3.121;
}
host pc51 {
    option host-name "pc51.sof164.net";
    hardware ethernet 00:50:BF:27:1C:1C;
    fixed-address 10.23.3.122;
}
host impresora {
    hardware ethernet 00:24:2B:65:54:84;
}
host pcl {
    hardware ethernet 00:0C:29:83:21:7D;
}
host pc2 {
    hardware ethernet F4:C7:14:70:FA:AC;
}
host laptop1 {
    hardware ethernet 00:24:2B:65:54:84;
}
host laptop2 {
    hardware ethernet 70:F1:A1:9F:70:3B;
}
```

Reiniciamos el servicio y probamos.

NOTA:

Puede hacer seguimiento del archivo **messages** que se encuentra en el directorio **/var/log** para ver la bitácora de su servidor **dhcp**

Capítulo 4. Servidores Web y Servidores de Base de Datos

4.1 Servidor Web

4.1.1 Introducción

El éxito espectacular de la web se basa en dos pilares fundamentales: el protocolo HTTP y el lenguaje HTML.

El protocolo HTTP, es el protocolo de comunicación que permite las transferencias de información en la red informática mundial (internet). HTTP permite una implementación simple y sencilla de un sistema de comunicaciones que nos permite enviar cualquier tipo de ficheros de una forma fácil, simplificando el funcionamiento del servidor y permitiendo que servidores poco potentes atiendan miles de peticiones y reduzcan los costes de despliegue.

El lenguaje HTML, es un lenguaje de marcas que nos permite representar de forma rica el contenido de un documento y también referenciar otros recursos (imágenes, videos, audio, etc), enlaces a otros documentos (la característica más destacada), mostrar formularios para posteriormente procesarlos, etc. Por tanto, este lenguaje nos proporciona un mecanismo de composición de páginas enlazadas simple y fácil, altamente eficiente y de uso muy simple.

4.1.2 ¿Qué es un servidor web?

Un servidor web (o servidor HTTP) es un programa que atiende y responde a las diversas peticiones de los programas clientes (estos programas web clientes en su mayoría son navegadores), proporcionándoles los recursos que solicitan mediante el protocolo HTTP o el protocolo HTTPS (la versión segura, cifrada y autenticada de HTTP). Un servidor web básico tiene un esquema de funcionamiento muy sencillo, ejecutando de forma infinita el bucle siguiente:

1. Espera peticiones en el puerto TCP asignado (el estándar para HTTP es el 80).
2. Recibe una petición.
3. Busca el recurso en la cadena de petición.
4. Envía el recurso por la misma conexión por donde ha recibido la petición.
5. Vuelve al punto 2.

Este esquema también puede funcionar usando el protocolo HTTPS, que, por lo general, trabaja en el puerto 443 del computador donde está instalado el servidor web, a no ser que el administrador decida cambiar dicho puerto, al igual que lo puede hacer con el puerto 80 del protocolo HTTP.

4.1.3 Características generales de los Servidores Web

Los servidores pueden presentar una serie de características, que, dependiendo del fabricante del servidor web, puede ser incluida o no en dicho servidor.

4.1.3.1 Servicio de archivos estáticos

Todos los servidores web deben incluir, como mínimo, la capacidad para servir los archivos estáticos (documentos cuyo contenido no varía) que se encuentren en alguna parte concreta del disco donde se tiene instalado el servidor web.

4.1.3.2 Seguridad y autenticación

La mayoría de los servidores web modernos nos permiten controlar desde el programa servidor aquellos aspectos relacionados con la seguridad y la autenticación de los usuarios, es decir, nos permiten controlar quienes pueden acceder al servidor web y una vez han accedido al servidor, también nos permiten controlar a que recursos pueden tener acceso y a que recursos no pueden acceder. Cuando hablamos de recursos a los que puede acceder usuario en el servidor web, nos referimos a archivos: Documentos HTML, hojas de estilos, imágenes, videos, archivos Javascript y otros.

4.1.3.3 Contenido dinámico

Es la capacidad que presenta un servidor web de generar páginas web cuyo contenido varía dependiendo de la petición que realiza el usuario a través de su navegador web. Esta capacidad de los servidores web, conocida también como servicio de páginas web dinámicas, los servidores la proveen haciendo uso de otros lenguajes de programación que se ejecutan en el servidor web, permitiendo realizar funciones y características, que generan páginas web cuyo contenido varía dependiendo como realiza su petición el usuario. El medio más usado por los servidores web para ofrecer contenido dinámico es PHP (PHP es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web de contenido dinámico y que puede ser incrustado en HTML).

4.1.3.4 Servidores virtuales

Capacidad de algunos servidores web de proporcionar múltiples dominios con sólo una dirección IP, discriminando entre los diversos dominios alojados por el nombre de dominio enviado en la cabecera de la petición HTTP.

Esta prestación permite administrar de una forma más racional y ahorrativa las direcciones IP públicas.

4.1.3.5 Servidores Intermedios

Algunos servidores web, permiten ser usados como servidores intermedios entre el cliente y los servidores web finales con propósitos como:

- Para servir de aceleradores de navegación de nuestros usuarios (uso como proxy-cache).
- Para servir como aceleradores de acceso frontales para un servidor web, instalando diversos servidores web que repliquen los accesos a un servidor maestro (reverse-proxy o HTTP server acceleration).
- Como frontales a algún servidor o protocolo.

4.1.3.6 Protocolos Adicionales

Algunos servidores, además de atender y servir peticiones HTTP (y HTTPS), pueden atender y servir peticiones de otros protocolos o de protocolos implementados sobre HTTP. Algunos de estos protocolos pueden convertirse en requisitos fundamentales de nuestro sistema y, por ello, su existencia en el del servidor web puede ser imprescindible.

4.1.4 Servidor Web Apache

El servidor web (Servidor HTTP) Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual según la normativa RFC 2616. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que alguien quería que tuviese la connotación de algo que es firme y energético, pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de Estados Unidos, y en esos momentos la preocupación de su grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de internet [cita requerida]. Además, Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. En inglés, a patchy server (un servidor "parcheado") suena igual que Apache Server.

El servidor Apache es desarrollado y mantenido por una comunidad de usuarios bajo la supervisión de la Apache Software Foundation dentro del proyecto HTTP Server (httpd).

Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Apache tiene amplia aceptación en la red: desde 1996, Apache es el servidor HTTP más usado. Jugó un papel fundamental en el desarrollo de la World Wide Web y alcanzó su máxima cuota de mercado en 2005, siendo el servidor empleado en el 70% de los sitios web en el mundo. Sin embargo, ha sufrido un descenso en su cuota de mercado en los últimos años (estadísticas históricas y de uso diario proporcionadas por Netcraft²). En 2009, se convirtió en el primer servidor web que alojó más de 100 millones de sitios web.

4.1.4.1 Ventajas

- Modular
- Código abierto
- Multi-plataforma
- Extensible
- Popular (fácil conseguir ayuda/sopporte)

4.1.4.2 Configuración

La configuración de Apache se realiza principalmente en el archivo de configuración apache2.conf en Ubuntu o httpd.conf en otros sistemas. Cualquier modificación en este archivo requiere reiniciar el servidor o forzar la lectura de los archivos de configuración.

También se utilizan archivos de configuración de los hosts virtuales para establecer configuraciones específicas para cada dominio o sitio web alojado en el servidor.

Estos archivos permiten establecer reglas de reescritura, configurar autenticación, habilitar compresión y manejar otros aspectos de la configuración del servidor.

4.1.4.3 Licencia

La licencia de software bajo la cual la fundación Apache es distribuido es una parte distintiva de la historia de Apache HTTP Server y de la comunidad de código abierto. La Licencia Apache permite la distribución de derivados de código abierto y cerrado a partir de su código fuente original.

4.1.4.4 Instalación de Apache en Rocky Linux

- i. Abrir una consola de comandos y cambiarse al root
- ii. Instalar Servidor HTTP Apache:
`dnf -y install httpd`
- vi. Iniciar el servidor apache (El servicio se llama httpd)
`systemctl start httpd`
- vii. Habilitar el servicio httpd para inicio automático
`systemctl enable httpd`
- viii. En el firewall para cada puerto que usted vaya habilitar para apache agregue la respectiva regla. Por ejemplo, supongamos que damos acceso a los puertos estándares de http y https (puertos 80 y 443 respectivamente), deberemos ejecutar:
`firewall-cmd --permanent --zone=public --add-port=80/tcp`
`firewall-cmd --permanent --zone=public --add-port=443/tcp`
`firewall-cmd --reload`
- ix. Ahora podremos probar que nuestro servidor web ya responde desde cualquier navegador colocando la ip de nuestro servidor (o su nombre de dominio si hay un DNS funcionando y configurado que resuelva dicho nombre)

4.1.4.5 SELinux y apache

SELinux es un módulo de seguridad para el kernel Linux que proporciona el mecanismo para soportar políticas de seguridad para el control de acceso, incluyendo controles de acceso obligatorios. En la práctica, el kernel linux pregunta a SELinux antes de cada llamada al sistema para saber si un proceso está autorizado a realizar una determinada operación. SELinux utiliza una serie de políticas para autorizar o denegar cualquier operación a realizar a un proceso o a un usuario.

En Rocky Linux y Red Hat™ Enterprise Linux, de modo predeterminado SELinux viene activo en modo obligatorio. Éste añade seguridad y protección adicional. Algunas opciones impedirán utilizar ciertas funciones, como directorios virtuales fuera del directorio /var/www, directorios ~/public_html, el envío de correo electrónico desde aplicaciones basadas sobre HTTP, etc.

Se puede deshabilitar SELinux por completo, pero esto en un servidor en producción sería irresponsable, es mejor aprender a usarlo, por lo cual veremos que ejecutar para el caso que necesite activar o desactivar algunas políticas dentro de SELinux para Apache.

IMPORTANTE: LOS SIGUIENTE COMANDOS, SON SOLO EJEMPLOS DE ALGUNOS PARAMETROS QUE PODRIA NECESITAR HABILITAR O DESHABILITAR EN SELINUX PARA PERMITIR QUE SU SERVIDOR WEB PUEDA O NO UTILIZAR CIERTAS CARACTERISTICAS

- Para permitir el envío de correo electrónico a través de Apache:
`setsebool -P httpd_can_sendmail 1`
- Para permitir que Apache pueda leer contenidos localizados en los directorios de inicio de los usuarios locales:
`setsebool -P httpd_read_user_content 1`
- Para habilitar el uso de los directorios ~/public_html de los usuarios regulares o anfitriones virtuales asignados a usuarios regulares:
`setsebool -P httpd_enable_homedirs 1`
- Para permitir administrar a través de FTP o FTPS cualquier directorio gestionado por Apache o bien permitir a Apache funcionar como un servidor FTP escuchando peticiones a través del puerto de FTP:
`setsebool -P httpd_enable_ftp_server 1`
- Para desactivar la ejecución de guiones CGI:
`setsebool -P httpd_enable_cgi 0`
- Para permitir las inclusiones del lado del servidor (SSI, Server Side Includes):
`setsebool -P httpd_ssi_exec 1`
- Para permitir conexiones hacia bases de datos localizada en otros servidores:
`setsebool -P httpd_can_network_connect_db 1`
- para permitir conexiones de red hacia otros servicios —como por ejemplo sieve en Round Cube Mail— locales o remotos:
`setsebool -P httpd_can_network_connect 1`
- Para desactivar la ejecución de PHP y otros lenguajes de programación:
`setsebool -P httpd_builtin_scripting 0`

Adicionalmente puede revisar que políticas de seguridad existen para apache y ver si están activas o inactivas se puede ejecutar:

```
getsebool -a |grep httpd
```

O también puede ejecutar:

```
semanage boolean -l |grep httpd
```

En sistemas que corren SELinux, todos los procesos y archivos se etiquetan con una etiqueta que contiene información de seguridad relevante. Esta información se llama contexto de SELinux. Si estas etiquetas están mal, el acceso puede ser negado. Si una aplicación se etiqueta incorrectamente, el proceso al que transiciona puede no tener la etiqueta correcta, causando negaciones de acceso de SELinux, y los procesos pueden crear archivo con las etiquetas incorrectas.

El contexto por defecto que usa apache en los archivos colocados dentro de /var/www es, **httpd_sys_content_t**. Si usted necesita habilitar otro directorio para que trabaje de forma similar al directorio /var/www, antes de hacer las configuraciones en Apache, primero debe establecer este contexto al directorio, por ejemplo, si quiere que el directorio /srv/www/dominio/public_html trabaje con el mismo contexto que /var/www, debe primero ejecutar:

```
chcon -t httpd_sys_content_t /srv/www/dominio/public_html
```

Temas Especiales

Para definir que un archivo hipotético /srv/www/dominio/public_html/lee.php pueda ser utilizado con permisos de sólo lectura de datos estando localizado fuera del directorio /var/www:

```
chcon -t httpd_sys_script_ro_t /srv/www/dominio/public_html/lee.php
```

Para definir que un archivo hipotético /srv/www/dominio/public_html/escribir.php pueda ser utilizado con permisos de lectura y escritura de datos estando localizado fuera del directorio /var/www:

```
chcon -t httpd_sys_script_rw_t /srv/www/dominio/public_html/escribir.php
```

Este contexto es requerido para archivos de configuración y directorios de cache, complementos, datos, extensiones, módulos, plantillas, temas o temporales de aplicaciones como Joomla, Wordpress, Moodle, vTigerCRM, Group-Office, etc. cuando éstos utilizan componentes fuera de /var/www y se requieren permisos de lectura y escritura.

Ejecute semanage con fcontext como argumento, la opción -a, la opción -t con httpd_sys_content_t como argumento y el directorio o archivo de destino como último argumento para establecer este contexto como el predeterminado para éste:

```
semanage fcontext -a -t httpd_sys_rw_content_t /srv/www/dominio/public_html/leer.php
```

Lo anterior permitirá establecer los contextos establecidos como los predeterminados para cada directorio o archivo definido. Es decir, se restaurarán estos mismos contextos al ejecutar restorecon sobre estos archivos o directorios. Puede aplicarse también con cualquiera de los otros contextos descritos arriba.

4.1.4.6 Inicio rápido de uso de Apache

El servidor web apache, por defecto, requiere que los archivos de las páginas web que usted desea que su servidor disponga para los usuarios, se pongan en el directorio /var/www/html. Por tanto, sin mayor esfuerzo para probar su servidor web, puede crear o copiar archivos html dentro de este directorio junto con los recursos que estos archivos html usan (imágenes, videos, estilos, etc). También puede organizarla en carpetas.

4.1.4.7 Host Virtuales

Apache permite mostrar el contenido de diferentes directorios dependiendo del nombre de host utilizado. Es decir, permite configurar host (anfitriones) virtuales.

El término “host virtual” se refiere en si a la práctica de hospedar más de un sitio web en un mismo host. Los host's virtuales pueden estar basados sobre dirección IP —es decir cada sitio Web tiene una dirección IP propia— o bien basado sobre nombres. En cualquiera de los casos los usuarios finales jamás se percatan que hay más de un sitio Web en el mismo servidor.

No olvidemos que el host virtual predeterminado muestra el contenido que se encuentre dentro del directorio /var/www/html, por lo cual conviene colocar un contenido genérico que sirva como cortinilla en lugar de mostrarse la página de bienvenida de Apache.

La plantilla general a utilizar para crear un host virtual es:

```
<VirtualHost [dirección IP|*] [:Número Puerto]>
  ServerName [nombre.dominio.com]
```

Temas Especiales

```
DocumentRoot [/srv/www/dominio/public_html]
[ServerAdmin [alguien@algo.com]]
[ErrorLog [logs/dominio-error_log]]
[CustomLog [logs/dominio-access_log] [combined]]
DirectoryIndex index.html
<Directory "[/srv/www/dominio/public_html]">
    [AllowOverride [all|none|tipo-de-directiva]]
    [Require local]
    [Require all granted]
</Directory>
</Virtualhost>
```

La configuración de un host virtual requiere los siguientes datos:

- VirtualHost: para definir la dirección IP y puerto a utilizar.
- ServerName: para definir el nombre de anfitrión.
- DocumentRoot: para definir el directorio raíz del anfitrión virtual. Es decir, el directorio donde se deben colocar las páginas web y sus recursos (videos, audios, imágenes, estilos, etc) de su sitio web para el host virtual definido
- ServerAdmin: la dirección de correo del administrador del servidor.
- ErrorLog: ruta del archivo de registro de errores.
- CustomLog: ruta del archivo de registro de accesos combinados
- DirectoryIndex: nombre del archivo html a devolver por defecto
- Directory: opciones de configuración para el directorio raíz que incluye:
 - AllowOverride all: para activar el soporte para archivos .htaccess
 - Require local: para permitir el acceso al anfitrión local
 - Requires all granted: para permitir el acceso al resto del mundo.

Cabe destacar que si deseamos mantener el acceso sin ningún problema al directorio de páginas web por defecto de apache, debemos editar el archivo httpd.conf que está en el directorio /etc/httpd/conf y agregar antes de la línea final (**IncludeOptional conf.d/*.conf**) un host virtual con cualquiera de los nombres que tenga nuestro servidor y que no vayamos a usar para los otros hosts virtuales. En nuestro ejemplo utilizaremos el nombre dns1.sof164.net y solo utilizaremos una mínima parte reducida de la plantilla para configuración de host virtual que hemos mostrado más arriba. Esta configuración servirá como host virtual por defecto, para que si utilizamos algún nombre host para acceder a nuestro servidor web, que no se está utilizando en ningún host virtual, entonces nuestro servidor responderá con las páginas de la carpeta por defecto. Note que solo me puse la directiva VirtualHost y dentro la directiva ServerName, pero no colocamos más nada porque el resto de la configuración de esta plantilla ya existe en el archivo httpd.conf y colocarla de nuevo sería redundante. Es así que en las últimas líneas nuestro archivo httpd.conf deberá verse así:

```
# esto es comentario y encima está el texto original del archivo que fue puesto
# por el instalador
<VirtualHost *:80>
    ServerName dns1.sof164.net
</Virtualhost>

IncludeOptional conf.d/*.conf
```

Ahora definiremos como ejemplo dos hosts virtuales adicionales y creemos los hosts virtuales solo para http utilizando el Puerto 80, para esto realizaremos los siguientes pasos:

Temas Especiales

- i. Como para las practicas estamos usando el dominio sof164.net y queremos 2 host virtuales, agreguemos en nuestro dns 2 nombres hacia la ip de nuestro servidor web. Si ya no lo tenemos entonces agreguemos en nuestro servidor DNS los nombres: **inter.sof164.net** y **webserver.sof164.net**
- ii. Creemos el directorio raiz de cada host virtual, como son 2 host virtuales, creamos los directorios: **/srv/www/inter.sof164.net/public_html** y **/srv/www/webserver.sof164.net/public_html**. Esto quiere decir que en estos directorios deberemos colocar los archivos de las paginas web y sus recursos de cada host virtual que estamos configurando.
- iii. Deberemos crear las configuraciones de cada host virtual en apache, pero para ser ordenados y no poner todo dentro del archivo httpd.conf, nos cambiamos al directorio **/etc/httpd/conf.d** y en este directorio crearemos en archivos donde colocaremos las configuraciones de cada uno de los hosts virtuales que vayamos a crear. Entonces cambiase al directorio antes mencionado.
- iv. Una vez nos cambiamos al directorio que citamos en el paso anterior, dentro de este directorio, creamos el archivo de configuración para el primer host virtual, lo llamaremos **inter.sof164.net.conf** con el siguiente contenido:

```
<VirtualHost *:5100>
    ServerName inter.sof164.net
    DocumentRoot /srv/www/inter.sof164.net/public_html
    ServerAdmin estudiante@sof164.net
    ErrorLog logs/inter.sof164.net-error_log
    CustomLog logs/inter.sof164.net-access_log combined
    DirectoryIndex index.html
    <Directory "/srv/www/inter.sof164.net/public_html">
        AllowOverride all
        Require all granted
    </Directory>
</Virtualhost>
```

- v. Luego, dentro del mismo directorio que ya estamos (**/etc/httpd/conf.d**) creamos el archivo de configuración para el segundo host virtual, lo llamaremos **webserver.sof164.net.conf** con el siguiente contenido:

```
<VirtualHost *:80>
    ServerName webserver.sof164.net
    DocumentRoot /srv/www/webserver.sof164.net/public_html
    ServerAdmin estudiante@sof164.net
    ErrorLog logs/webserver.sof164.net-error_log
    CustomLog logs/webserver.sof164.net-access_log combined
    DirectoryIndex index.html
    <Directory "/srv/www/webserver.sof164.net/public_html">
        AllowOverride all
        Require all granted
    </Directory>
</Virtualhost>
```

- vi. Ahora debemos ver si estos directorios que hemos creado tienen el contexto adecuado. Primero para el directorio raíz del host virtual **inter.sof164.net**, verificamos que el contexto del directorio que usaremos para este host tenga el contexto: **httpd_sys_content_t**; para esto ejecutamos:

```
ls -Zd /srv/www/inter.sof164.net/public_html/
```

Temas Especiales

Si obtenemos que el contexto de esta carpeta nos es **unconfined_u:object_r:httpd_sys_content_t:s0** (Fijese el texto en rojo debe aparecer, aunque no aparezca lo demas igual), entonces corregimos esto ejecutando:

```
chcon -R -t httpd_sys_content_t /srv/www/inter.sof164.net/public_html/
```

Ahora, con este cambio realizado, volvemos a ejecutar:

```
ls -Zd /srv/www/inter.sof164.net/public_html/
```

y deberíamos ver que nos muestra **unconfined_u:object_r:httpd_sys_content_t:s0** como parte de la respuesta del comando ls ejecutado. Esto nos indica el nuevo contexto de este directorio

- vii. Seguido, para el directorio asociado al otro host virtual, debemos ver si este directorio tiene el contexto adecuado, es decir, validamos que el contexto del directorio raíz que asocioamos al host virtual **webserver.sof164.net**, debe ser: **httpd_sys_content_t**, para esto ejecutamos:

```
ls -Zd /srv/www/webserver.sof164.net/public_html/
```

Si obtenemos que el contexto de esta carpeta nos es **unconfined_u:object_r:httpd_sys_content_t:s0**, entonces corregimos esto ejecutando:

```
chcon -R -t httpd_sys_content_t /srv/www/webserver.sof164.net/public_html/
```

Ahora volvemos a ejecutar

```
ls -Zd /srv/www/webserver.sof164.net/public_html/
```

y ya deberíamos ver que nos muestra **unconfined_u:object_r:httpd_sys_content_t:s0** como parte de la respuesta del comando ls ejecutado.

- viii. (**Opcional**) Si no tenemos paginas en las carpetas de estos hosts virtuales, para probar podemos crear un archivo simple con un contenido diferente en cada carpeta ejecutando:

- echo "Pagina de prueba del dominio inter.sof164.net" > /srv/www/inter.sof164.net/public_html/index.html
- echo "Pagina de prueba del dominio webserver.sof164.net" > /srv/www/webserver.sof164.net/public_html/index.html

OJO: Esto es opcional, por que si usted tiene paginas web ya creadas para cada uno de sus host virtuales copielas con todo dentro de estos directorios. Es decir, para su host virtual inter.sof164.net, copie sus paginas web y sus recursos en el directorio /srv/www/inter.sof164.net/public_html/ y para el host virtual webserver.sof164.net, copie sus paginas web y sus recursos en el directorio /srv/www/webserver.sof164.net/public_html/

- ix. Reiniciamos el servicio de apache ejecutando: `systemctl restart httpd`
- x. Ahora abramos un navegador en cualquier computador que esté usando como DNS nuestro servidor dns y luego ingresemos el nombre de cada uno de estos nombres de dominios utilizados para estos hosts virtuales y comprobemos la diferencia.

4.1.4.8 Restricción de acceso basada en ip y/o host

Se puede restringir acceso a nuestros hosts virtuales desde algún otro servidor se puede restringir por ip, agregando:

- Require not ip xxx.xxx.xxxx.xxxx

Temas Especiales

o por host utilizando el FQDN de dicho host, agregando:

- `Require not host nombrehostFQDN`

Si queremos restringir que a nuestro host virtual inter.sof164.net no acceda ningun usuario cuando quiera acceder desde el computador con ip 10.23.3.55, entonces agregamos debajo del Require all granted, la directiva `Require not ip 10.23.3.55`, entonces nuestro archivo inter.sof164.net.conf se verá asi:

```
<VirtualHost *:80>
    ServerName inter.sof164.net
    DocumentRoot /srv/www/inter.sof164.net/public_html
    ServerAdmin estudiante@sof164.net
    ErrorLog logs/inter.sof164.net-error_log
    CustomLog logs/inter.sof164.net-access_log combined
    DirectoryIndex index.html
    <Directory "/srv/www/inter.sof164.net/public_html">
        AllowOverride all
        <RequireAll>
            Require all granted
            Require not ip 10.23.3.55
        </RequireAll>
    </Directory>
</Virtualhost>
```

Ahora reiniciamos el servidor apache y verificamos que cuando queramos acceder desde el computador con ip 10.23.3.55, no se nos permitirá el acceso.

4.1.4.9 Restricción de acceso basada en usuario

Se puede restringir acceso a nuestros hosts virtuales por usuario, para esto deberemos crear una base de datos de usuario y modificar el archivo de configuración de nuestro host virtual para que se restrinja el acceso por usuario.

Por ejemplo, si queremos que solo usuarios validos accedan a nuestro virtual host webserver.sof164.net, primero creamos nuestra base de datos de usuarios. Para nuestro ejemplo creamos los usuarios: estudiante, prueba y profesor. Estos serán agregados al archivo de usuarios dentro del directorio no publicado a la web de nuestro host virtual.

i. Entonces creamos los usuarios ejecutando en una consola como root:

- `htpasswd -c /srv/www/webserver.sof164.net/usuarios estudiante`
- `htpasswd /srv/www/webserver.sof164.net/usuarios prueba`
- `htpasswd /srv/www/webserver.sof164.net/usuarios profesor`

Note que estamos usando el comando htpasswd y como el archivo aún no existe la primera vez lo ejecutamos con el parámetro `-c`. El resto ya no es necesario.

ii. Cambiamos el contexto de este archivo:

```
chcon -R -t httpd_sys_content_t /srv/www/webserver.sof164.net/usuarios
```

iii. Y cambiamos nuestro archivo de configuración webserver.sof164.net.conf. Si queremos que cualquier usuario valido acceda a nuestro sitio web, nuestro archivo deberá lucir asi:

```
<VirtualHost *:80>
```

Temas Especiales

```
ServerName webserver.sof164.net
DocumentRoot /srv/www/webserver.sof164.net/public_html
ServerAdmin estudiante@sof164.net
ErrorLog logs/webserver.sof164.net-error_log
CustomLog logs/webserver.sof164.net-access_log combined
<Directory "/srv/www/webserver.sof164.net/public_html">
    AllowOverride all
    AuthType Basic
    AuthName "Restricted Access"
    AuthUserFile "/srv/www/webserver.sof164.net/usuarios"
    Require valid-user
</Directory>
</Virtualhost>
```

Pero si queremos solo restringir que el usuario estudiante sea el que acceda entonces nuestro archivo de configuración deberá lucir así:

```
<VirtualHost *:80>
    ServerName webserver.sof164.net
    DocumentRoot /srv/www/webserver.sof164.net/public_html
    ServerAdmin estudiante@sof164.net
    ErrorLog logs/webserver.sof164.net-error_log
    CustomLog logs/webserver.sof164.net-access_log combined
    <Directory "/srv/www/webserver.sof164.net/public_html">
        AllowOverride all
        AuthType Basic
        AuthName "Restricted Access"
        AuthUserFile "/srv/www/webserver.sof164.net/usuarios"
        Require user estudiante
    </Directory>
</Virtualhost>
```

- iv. Reiniciamos el servidor apache y probamos desde un navegador. Si hemos hecho todo bien, el navegador al tratar de ingresar a <http://webserver.sof164.net> debería lanzarnos su ventana para ingresar usuario y password antes de dejarnos ingresar a ver las páginas web.

4.1.4.10 Configuración de apache con soporte SSL/TLS

4.1.4.10.1 Acerta de HTTPS

HTTPS es la versión segura del protocolo HTTP, es así que es un protocolo dependiente de HTTP, consistiendo de una combinación de éste, con un mecanismo de transporte SSL o TLS, garantizando así una protección razonable durante la comunicación cliente-servidor. Es ampliamente utilizado en la red mundial (WWW o World Wide Web) para comunicaciones como transacciones bancarias y pago de bienes y servicios. También recordemos, que a no ser que se cambie esta configuración en el servidor web, https trabaja en el puerto 443.

En Rocky Linux 9 para poder configurar apache para soporte SSL/TLS, primero debemos instalar el paquete **mod_ssl**, el cual, es un módulo para el servidor HTTP Apache que provee soporte para SSL versiones 2 y 3 y TLS versión 1.

Para preparar un servidor web que acepte conexiones HTTPS, debemos primero crear un certificado de clave pública para el servidor web. Este certificado debe estar firmado por una autoridad de

certificación para que el navegador web lo acepte. La autoridad certifica que el titular del certificado es quien dice ser. Los navegadores web generalmente son distribuidos con los certificados raíz firmados por la mayoría de las autoridades de certificación por lo que estos pueden verificar certificados firmados por ellos.

4.1.4.10.2 Acerca de SSL y TLS

SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas).

SSL utiliza tecnología de cifrado de claves públicas para la autenticación. En el cifrado de claves públicas, se generan una clave pública y una clave privada para una aplicación. Los datos cifrados con la clave pública sólo se pueden descifrar utilizando la clave privada correspondiente. Del mismo modo, los datos cifrados con la clave privada sólo se pueden descifrar utilizando la clave pública correspondiente. La clave privada está protegida por contraseña en un archivo de base de datos de manera que sólo el propietario pueda acceder a ésta para descifrar mensajes cifrados utilizando la clave pública correspondiente.

Un certificado digital firmado es un método estándar del sector para verificar la autenticidad de una entidad, como un servidor, cliente o aplicación. Para garantizar la máxima seguridad, una entidad emisora de certificados emite un certificado.

Puede utilizar certificados autofirmados para probar una configuración SSL antes de crear e instalar un certificado firmado emitido por una entidad emisora de certificados.

Un certificado autofirmado contiene una clave pública, información sobre el propietario del certificado y la firma del propietario. Tiene una clave privada asociada, pero no verifica el origen del certificado mediante una entidad emisora de certificados. Cuando se genera un certificado autofirmado en una aplicación de servidor SSL, se debe extraer y agregar al registro de certificados de la aplicación del cliente SSL.

El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA.

4.1.4.10.3 Certificados digitales

Un certificado digital (también conocido como certificado de clave pública) es un tipo de documento digital firmado por una entidad llamada Autoridad de certificación que asocia una clave pública a unos datos que representan la identidad de una entidad (por ejemplo, una persona física, organismo, empresa o un servidor) que posee la clave privada asociada a dicha clave pública. De esta forma, cuando se usa la clave privada asociada a dicha clave pública se puede asegurar que ha

sido usada por la entidad asociada, claro está, esto se valida atendiendo a la autoridad de la Autoridad de certificación que firmo la clave pública.

4.1.4.10.4 Acerca de RSA

RSA, acrónimo de los apellidos de sus autores, Ron Rivest, Adi Shamir y Len Adleman, es un sistema criptográfico de clave pública desarrollado en 1979, que utiliza factorización de números enteros. El cifrado RSA es uno de esos criptosistemas para el descifrado de mensajes privados que utiliza un algoritmo de clave pública. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente. El algoritmo consta de tres pasos: generación de claves, cifrado y descifrado.

El cifrado de datos implica disfrazar la información como texto cifrado. El texto cifrado es ininteligible para personas no autorizadas. Por el contrario, descifrar implica convertir texto cifrado en el formato original. El cifrado manual se remonta al Imperio Romano. Sin embargo, hoy en día el cifrado es un proceso básico de criptología y es sinónimo de ocultar información a través de métodos electrónicos.

Las computadoras aplican un algoritmo para cifrar los datos. Un algoritmo es un conjunto de instrucciones o procedimientos para realizar tareas específicas en bloques de datos. Una clave es un nombre de cifrado personal que solo conocen el usuario o transmisor del mensaje y el destinatario previsto.

En la actualidad, existen dos tipos principales de cifrado:

- El cifrado simétrico utiliza la misma clave para cifrar y descifrar datos, como el estándar de cifrado avanzado (AES).
- El cifrado asimétrico también se denomina criptografía de clave pública porque requiere un par de claves, una pública para el cifrado y una privada para la descifrado. El algoritmo Rivest Shamir Adleman es un ejemplo común.

RSA funciona porque las claves de cifrado seleccionadas aleatoriamente de longitud suficiente son casi inexpugnable. El algoritmo asimétrico asigna a cada emisor un par de claves:

- Una clave pública para el cifrado
- Una clave privada para descifrar datos

Aunque las dos claves están vinculadas, es imposible derivar la clave privada de la pública o descifrar los datos mediante una clave pública. Como su nombre indica, la clave pública es bien conocida, pero las claves privadas son secretas y solo están disponibles para los usuarios que las poseen. En resumen, todos pueden enviar mensajes al usuario usando sus claves públicas, pero solo el destinatario previsto puede descifrar los mensajes usando su clave privada.

Muchos protocolos, como Secure Shell (SSH), SSL-TLS, S/MIME y OpenPGP, dependen del cifrado RSA y de las funciones seguras de firma digital.

4.1.4.10.5 Certificados X.509

Es un formato de certificados, el cual es un estándar ITU-T (estandarización de Telecomunicaciones de la International Telecommunication Union) para infraestructura de claves públicas (PKI o Public Key Infrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (CA o Certification Authority).

4.1.4.10.6 Acerca de OpenSSL

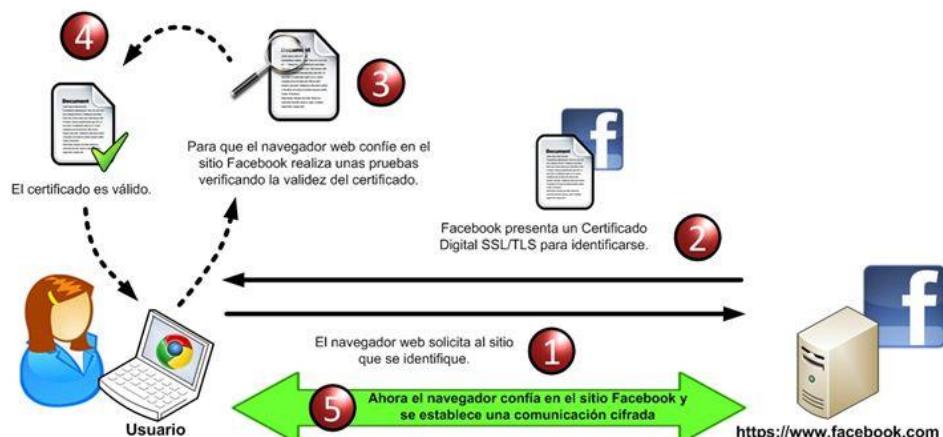
OpenSSL es una implementación libre, de código abierto, de los protocolos SSL (Secure Sockets Layer o Nivel de Zócalo Seguro) y TLS (Transport Layer Security o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto SSLeay, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

4.1.4.10.7 Acerca de las autoridades de certificadoras

Una Autoridad Certificadora (AC, en inglés CA) es una entidad confiable que se encarga de garantizar que el poseedor de un certificado digital sea quien dice ser, brindando confianza a ambas partes de una comunicación segura SSL/TLS.

4.1.4.10.8 Validación de un certificado digital

En la siguiente figura ponemos como ejemplo la forma en que un navegador verifica la validez de un certificado digital al tratar de iniciar una conexión https (en el ejemplo con Facebook). Este procedimiento es el que se realiza cada vez que se trata de establecer una conexión segura, por ejemplo: entre un navegador y un servidor web, un cliente de correo y un servidor de correo, o en general desde cualquier tipo de cliente hacia un servidor que acepte estas conexiones seguras.



Iniciando comunicación segura

Temas Especiales

En el punto dos de la figura, cuando el navegador hace una petición al sitio seguro de Facebook, éste envía un mensaje donde indica que quiere establecer una conexión segura y envía datos sobre la versión del protocolo SSL/TLS que soporta y otros parámetros necesarios para la conexión.

En base a esta información enviada por el navegador, el servidor web de Facebook responde con un mensaje informando que está de acuerdo en establecer la conexión segura con los datos de SSL/TLS proporcionados.

Una vez que ambos conocen los parámetros de conexión, el sitio de Facebook presenta su certificado digital al navegador web para identificarse como un sitio confiable.

Verificación de validez del certificado

Una vez que el navegador tiene el certificado del sitio web de Facebook, realiza algunas verificaciones antes de confiar en el sitio:

- **Integridad del certificado:** Verifica que el certificado se encuentre íntegro, esto lo hace descifrando la firma digital incluida en él mediante la llave pública de la AC y comparándola con una firma del certificado generada en ese momento, si ambas son iguales entonces el certificado es válido.
- **Vigencia del certificado:** Revisa el periodo de validez del certificado, es decir, la fecha de emisión y la fecha de expiración incluidos en él.
- **Verifica emisor del certificado:** Hace uso de una lista de Certificados Raíz almacenados en su computadora y que contienen las llaves públicas de las ACs conocidas y de confianza. Puedes acceder a esta lista desde las opciones avanzadas de tu navegador.

Con base a esta lista, el navegador revisa que la AC del certificado sea de confianza, de no serlo, el navegador mostrará una advertencia indicando que el certificado fue emitido por una entidad en la cual no confía.

Una vez el certificado es validado se inicia la conexión segura, caso contrario no se realiza la conexión.

4.1.4.10.9 Habilitar apache para soporte SSL/TLS

NOTA:

Cuando una organización quiere solicitar un certificado a una Autoridad de Certificación (CA) necesitará enviar una petición de firma de certificado (CSR = certificate-signing request), lo cual tiene un costo dependiendo entre otras cosas, del tiempo de validez del certificado. En nuestro caso como estamos realizando una práctica, lo que haremos será crearnos un certificado de clave publica (certificado publico + llave privada) que sea autofirmada (firmada por nosotros mismos) para que no tengamos que incurrir en este gasto, pero no olvide que esto hará que el navegador no reconozca nuestro certificado y nos pida agregar una excepción, para dejar pasar este certificado autofirmado y también recuerdo que esto en una práctica real no se debería hacer.

Supongamos que queremos que el host virtual webserver.sof164.net trabaje también con https, entonces realizamos los siguientes pasos:

Temas Especiales

- i. Como root en una consola, nos aseguramos de tener instalado el paquete mod_ssl.
- ii. Deberemos crear un certificado de clave pública para nuestro servidor. Para esto realizamos los siguientes pasos:
 - a. Se debe crear una clave con algoritmo RSA de 4096 octetos y estructura x509 ejecutando el siguiente comando:

```
openssl req -x509 -nodes -days 1000 -newkey rsa:4096 -keyout
/etc/pki/tls/private/webserver.sof164.net.pem
-out
/etc/pki/tls/certs/webserver.sof164.net.crt
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del host. Debe ser el nombre con el que se accederá hacia el servidor y dicho nombre deberá estar resuelto en un DNS.
- Dirección de correo electrónico válida del administrador del sistema.

Osea que al ejecutar el comando openssl para generar el certificado de clave pública, podríamos ver que se nos pida información del siguiente modo (En letra negrita la información que se ingresó para este ejemplo):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:BO
State or Province Name (full name) []:Santa Cruz
Locality Name (eg, city) [Default City]:Santa Cruz de la Sierra
Organization Name (eg, company) [Default Company Ltd]:U.A.G.R.M.
Organizational Unit Name (eg, section) []:Ofimatica
Common Name (eg, your name or your server's hostname) []:webserver.sof164.net
Email Address []:admin@sof164.net
```

IMPORTANTE: Cuando generamos la llave y el certificado para nuestro servidor hay que asegurarnos que estos 2 archivos tengan el contexto **cert_t**, si no tiene este contexto hay que cambiarlo usando el comando **chcon**, es decir, ejecutando lo siguiente:

```
chcon -t cert_t /ruta/de/archivo/nombreArchivo
```

Esto no será necesario si al ejecutar el comando openssl los archivos se generan en los directorios **/etc/pki/tls/private/** o **/etc/pki/tls/certs/**

- iii. Luego procederemos a modificar nuestro archivo webserver.sof164.net.conf, para que se vea del siguiente modo:

```
<VirtualHost *:80>
ServerName webserver.sof164.net
DocumentRoot /srv/www/webserver.sof164.net/public_html
```

Temas Especiales

```
ServerAdmin estudiante@sof164.net
ErrorLog logs/webserver.sof164.net-error_log
CustomLog logs/webserver.sof164.net-access_log combined
<Directory "/srv/www/webserver.sof164.net/public_html">
    AllowOverride all
    AuthType Basic
    AuthName "Restricted Access"
    AuthUserFile "/srv/www/webserver.sof164.net/usuarios"
    Require valid-user
</Directory>
</VirtualHost>
<VirtualHost *:443>
    ServerName webserver.sof164.net
    DocumentRoot /srv/www/webserver.sof164.net/public_html
    ServerAdmin estudiante@sof164.net
    ErrorLog logs/webserver.sof164.net-error_log
    CustomLog logs/webserver.sof164.net-access_log combined
    <Directory "/srv/www/webserver.sof164.net/public_html">
        AllowOverride all
        AuthType Basic
        AuthName "Restricted Access"
        AuthUserFile "/srv/www/webserver.sof164.net/usuarios"
        Require valid-user
    </Directory>
    SSLEngine on
    SSLProtocol all -SSLv2
    SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEALOW
    SSLCertificateFile /etc/pki/tls/certs/webserver.sof164.net.crt
    SSLCertificateKeyFile /etc/pki/tls/private/webserver.sof164.net.pem
</Virtualhost>
```

- iv. Ahora podremos reiniciar nuestro servidor web apache y verificar usando un navegador el acceso por <https://webserver.sof164.net>. Veremos que como se trata de un certificado autofirmado deberemos agregar una excepción para este certificado en nuestro navegador.

4.1.4.11 Host virtual para redirección de URL's

Cuando los recursos HTTP o las páginas web cambian de ubicación, a menudo es importante proveer algún medio para alertar a los usuarios que estos recursos han sido movidos. HTTP provee un número de códigos de "redirección" que pueden ser usados para facilitar este proceso, comunicando con la aplicación del cliente sin interferir con la experiencia de usuario.

En el siguiente ejemplo puede ver una configuración de host virtual que redirige las peticiones que llega via http por el puerto 80 hacia https por el puerto 443

```
<VirtualHost *:80>
    ServerName webserver.sof164.net
    Redirect permanent / https://webserver.sof164.net
</Virtualhost>
<VirtualHost *:443>
    ServerName webserver.sof164.net
    DocumentRoot /srv/www/webserver.sof164.net/public_html
    ServerAdmin estudiante@sof164.net
    ErrorLog logs/webserver.sof164.net-error_log
    CustomLog logs/webserver.sof164.net-access_log combined
    <Directory "/srv/www/webserver.sof164.net/public_html">
        AllowOverride all
        AuthType Basic
```

```
AuthName "Restricted Access"
AuthUserFile "/srv/www/webserver.sof164.net/usuarios"
Require valid-user
</Directory>
SSLEngine on
SSLProtocol all -SSLv2
SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEALOW
SSLCertificateFile /etc/pki/tls/certs/webserver.sof164.net.crt
SSLCertificateKeyFile /etc/pki/tls/private/webserver.sof164.net.pem
</Virtualhost>
```

4.1.4.12 Habilitar otros puertos en apache

Para habilitar otros puertos en apache además del puerto 80 y el puerto 443, primero debemos asegurarnos que está habilitado en SELinux, para esto ejecutamos como root el siguiente comando:

```
semanage port -l | grep http
```

Si no se lista nuestro puerto de interés, pues entonces hay que agregarlo. Por ejemplo, supongamos que queremos agregar el puerto 3200 como puerto para http deberemos realizar los siguientes pasos:

- i. Agregar el puerto 3200 entre los puertos permitidos por SELinux para http:

```
semanage port -a -t http_port_t -p tcp 3200
```
- ii. Agregar el puerto a los puertos permitidos en el firewall de Linux

```
firewall-cmd --permanent --zone=public --add-port=3200/tcp
firewall-cmd --reload
```
- iii. Modificar el archivo httpd.conf que se encuentra en el directorio /etc/httpd/conf y agregar debajo de la línea Listen 80, la línea Listen 3200.
- iv. Luego si deseamos podemos agregar hosts virtuales para este puerto o dejar que use la configuración por defecto.
- v. Reiniciamos el servidor apache

NOTA IMPORTANTE

En caso de necesitar habilitar otro puerto para https, el procedimiento es el mismo, lo único que debemos hacer diferentes es el paso iii, en donde por ejemplo si queremos el puerto 4001 como puerto para https, realizamos el mismo procedimiento con el puerto 4001, pero en el paso iii, modificaremos el archivo ssl.conf que esta en el directorio /etc/httpd/conf.d y debajo de la línea Listen 443 https, agregaremos la línea Listen 4001 https.

Para mayor detalle de administración de apache http Server puede acceder al sitio de servidor: <https://httpd.apache.org/docs/2.4/>

4.2 Servidor de Base de Datos

4.2.1 Introducción

Un servidor de base de datos o Sistema de gestión de base de datos, es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información en una base de datos, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos. Los

Temas Especiales

usuarios pueden acceder a la información usando herramientas específicas de consulta y de generación de informes, o bien mediante aplicaciones al efecto.

En la actualidad existen un gran número de servidor de base de datos pagos y gratuitos, entre los que podemos nombrar: Oracle, MariaDb, MySQL, MongoDB, PostgreSQL y otros, de los cuales muchos de ellos pueden instalarse en servidor que tienen instalados sistemas operativo GNU/Linux.

4.2.2 MySQL

MySQL™ es un DBMS (DataBase Management System) o sistema de gestión de base de datos SQL (Structured Query Language o Lenguaje Estructurado de Consulta) multiusuario y multihilo con licencia GNU/GPL. Fue propiedad y patrocinio de MySQL AB, compañía fundada por David Axmark, Allan Larsson y Michael Widenius, con base de operaciones en Suecia, la cual poseía los derechos de autor de prácticamente todo el código que lo integraba. MySQL AB desarrolló y se encargó del mantenimiento de MySQL vendiendo servicios de soporte y otros valores agregados, así como también licenciamientos privativos para los desarrollos de equipamiento lógico que requieren mantener cerrado su código fuente. MySQL™ AB fue adquirido en 2008 por Sun Microsystems, que a su vez fue adquirido por Oracle Corporation en 2009.

MySQL™ es actualmente el servidor de base de datos más popular para los desarrollos a través de la red mundial, principalmente sitios de Internet. Es célebre y casi legendario, por considerarse rápido y sólido.

4.2.3 MariaDB

MariaDB™ es un sistema de gestión de bases de datos relacionales de código abierto, es un proyecto derivado de MySQL™ con licencia GNU/GPLv2, desarrollado por Michael Widenius y una comunidad de desarrolladores de software libre. Se diferencia de MySQL™ en que incluye dos nuevos motores de almacenamiento: Aria —que reemplazo para MyISAM— y XtraDB —reemplazo para InnoDB. Es completamente compatible con MySQL™ gracias a que utiliza las mismas órdenes, interfaces, APIs y bibliotecas, siendo su objetivo poder reemplazar de manera transparente a MySQL.

MariaDB está escrito en C y C++ y es compatible con varios lenguajes de programación, incluidos C, C#, Java, Python, PHP y Perl. MariaDB también es compatible con todos los principales sistemas operativos, incluidos Windows, Linux y macOS.

MariaDB ofrece las mismas características que MySQL y se puede usar como sustituto directo del servidor de base de datos MySQL (es decir, MySQL se puede desinstalar e instalar MariaDB sin ningún otro cambio). Diseñado para brindar velocidad, fiabilidad y facilidad de uso, MariaDB se puede utilizar para tareas de procesamiento tanto pequeñas como a nivel empresarial.

4.2.3.1 ¿En qué casos sería recomendable usar MariaDB?

- **Procesamiento de Transacciones**

MariaDB es ideal para aplicaciones transaccionales empresariales que requieren soporte para consultas frecuentes, tiempos de respuesta rápidos y capacidad para procesar pequeñas cantidades de datos. Su motor de almacenamiento InnoDB admite transacciones compatibles con ACID y garantiza que cada transacción se trate como una sola unidad.

- **Aplicaciones Web**

MariaDB funciona bien con las aplicaciones web y las plataformas de comercio electrónico, y sus mecanismos de subprocessos múltiples le permiten gestionar cargas más altas que otros sistemas de bases de datos. Debido a su modelo de subprocessos múltiples y su alto rendimiento, MariaDB puede adaptarse para permitir que su aplicación o sitio gestione los picos de tráfico o el rápido crecimiento del negocio.

4.2.3.2 ¿Cuánto cuesta MariaDB?

MariaDB Community Server se publica bajo la licencia pública GNU v2 y se garantiza que será gratuito y de código abierto para siempre. MariaDB Community Server cuenta con soporte para SQL en JSON, compatibilidad con Oracle y MySQL, soporte para múltiples motores de almacenamiento y análisis en tiempo real.

MariaDB también está disponible en versiones empresariales y en la nube. MariaDB Enterprise incluye MariaDB MaxScale, conectores de aplicación e integración, herramientas de gestión y soporte técnico. Puede adquirir MariaDB Enterprise solicitando un presupuesto personalizado.

SkySQL, la versión en la nube de MariaDB, ofrece la alta disponibilidad, escalabilidad y seguridad de los entornos en la nube. Cuenta con soporte para múltiples cargas de trabajo, recuperación ante desastres y monitoreo proactivo.

4.2.3.3 ¿Por qué debería usar MariaDB en lugar de MySQL?

Si bien MariaDB conserva muchas de las funciones de MySQL, tiene varias funciones integradas potentes y mejoras de rendimiento frente a MySQL, que incluyen:

- **Modelo de licencia:** tanto MariaDB como MySQL están disponibles como bases de datos de código abierto con ediciones comunitarias en GPLv2. Mientras que MariaDB ofrece un paquete completo con su edición comunitaria, MySQL solo ofrece algunas características como la agrupación de subprocessos en su edición para empresas.
- **Rendimiento:** MariaDB ofrece un rendimiento mejorado sobre MySQL cuando se consultan las vistas y se maneja el almacenamiento flash. MySQL consulta todas las tablas conectadas a la vista. MariaDB optimiza el proceso consultando solo las tablas que requiere la consulta. MariaDB también proporciona el motor de almacenamiento MyRocks y RocksDB, que están diseñados para un mejor rendimiento con almacenamiento flash.
- **Subprocesos múltiples:** la función de agrupación de subprocessos de MariaDB puede manejar hasta 200 000 conexiones simultáneas. Esta función solo está disponible en la edición MySQL Enterprise.
- **Más motores de almacenamiento:** MariaDB incluye más motores de almacenamiento y complementos que MySQL, incluidos Aria, Connect, Spider para fragmentación y TokuDB para el manejo de macrodatos.

4.2.4 Instalación de MariaDB en Rocky Linux

- i. Abrir una consola de comandos y cambiarse al root
- ii. Instalar Servidor MariaDB:
`dnf -y install mariadb-server`

Temas Especiales

- iii. Iniciar el servidor mariadb (El servicio se llama mariadb)
`systemctl start mariadb`
- iv. Habilitar el servicio mariadb para inicio automático
`systemctl enable mariadb`
- v. En el firewall habilitamos el puerto de mariadb (3306) para que el firewall acepte peticiones dirigidas a este puerto:
`firewall-cmd --permanent --zone=public --add-port=3306/tcp`
`firewall-cmd -reload`
- vi. Configurar seguridad en el acceso al servidor de base de datos, para ello ejecutamos:
`mysql_secure_installation (si no está, puede estar como`
`mariadb-secure-installation)`

Posterior a esto, como es la primera vez cuento la consola nos muestre el mensaje “**Enter current password for root (enter for none):**” solamente presionamos enter para que nos permita ingresar el password para el usuario root de mariadb, para ello seguiremos el asistente que se nos visualiza. Luego de finalizar este asistente ya no podremos ingresar al sistema sin especificar contraseña para el root y si hemos elegido eliminar el usuario anónimo, tampoco podremos ingresar sin usuario y password.

- vii. Ahora podremos ingresar a la consola de mariadb por ejemplo usando el usuario root, ejecutando:

```
mysql -u root -p
```

luego nos pedirá el password y para poder ingresar. Podremos ver algo como:

```
[root@serverc7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 24
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

IMPORTANTE:

- El archivo de configuración de MariaDB está dentro del directorio /etc y tiene el nombre **my.cnf**
- Este archivo también permite cargar configuraciones adicionales que están en el directorio /etc/my.cnf.d
- Si revisamos el archivo my.cnf veremos que el directorio donde almacena las bases de datos es **/var/lib/mysql** y que su archivo de los es **/var/log/mariadb/mariadb.log**

4.2.5 Creación y eliminación de base de datos en MariaDB

Existe más de una forma de realizar este par de tareas. Una de las formas de realizarlas la detallamos a continuación:

Para crear una nueva base de datos, ejecute mysqladmin con create como argumento, la opción -u con root como usuario y la opción -p para indicar que se ingresará una contraseña:

```
mysqladmin -u root -p create basedatos
```

Temas Especiales

Para eliminar una base de datos, ejecute mysqladmin con drop como argumento en lugar de create, la opción -u con root como usuario y la opción -p para indicar que se ingresará una contraseña:

```
mysqladmin -u root -p drop basedatos
```

4.2.6 Cambios de configuración

Ya mencionamos que el archivo de configuración de mariadb es el archivo my.cnf que se encuentra en el directorio /etc; en este archivo se hace referencias a configuraciones que se cargan de archivos que se encuentran en el directorio /etc/my.cnf.d. Si queremos hacer cambios de configuración en nuestro servidor MariaDB deberemos realizar los cambios en el archivo server.cnf.

4.2.6.1 Ejemplo 1:

Para cambiar el puerto en el que mariadb atiende las peticiones de los clientes sea el puerto por ejemplo 40000 y ya no el puerto 3306 deberemos realizar lo siguiente:

- a) Ubicar el archivo server.cnf antes comentado y sacarle backup
- b) En este archivo buscar la sección [mysqld]
- c) En esta sección si no existe el parámetro port=3306, agregar en esta sección el parámetro y fijar el nuevo puerto del siguiente modo:
port=40000
- d) Usar el comando semanage explicado en la sección de apache, para avisarle a selinux que debe permitir usar al sistema el puerto, en este caso el 40000:
semanage port -a -t mysqld_port_t -p tcp 40000
- e) Reiniciar el servicio mariadb

NOTA:

Partir de ahora sus clientes deben especificar que la conexión es al puerto 40000. Por ejemplo el comando del inciso viii del punto 4.2.5 deberá ser ejecutado ya no así:

```
mysql -u root -p
```

si no del siguiente modo:

```
mysql -u root -p -P 40000
```

El parámetro -P (en mayúscula) le permite al programa cliente en consola especificar que el servidor atiende las peticiones en el puerto especificado (40000 en este caso), si no se hace así no podrá conectarse al servidor.

4.2.6.2 Ejemplo 2:

Cambio del parámetro que especifica resolución de nombres se debe cambiar el parámetro **skip-name-resolve**. Esto nos ayudará a acelerar el tiempo de respuesta cuando el servidor mariadb trate de verificar los permisos de nuestros usuarios, pues nos evitará que el servidor mariadb no pierda tiempo intentando convertir nombres de dominio a IP. El único inconveniente será que sus clientes deberán usar solamente direcciones IP para definir los permisos. Procedimiento

- a) Ubicar el archivo server.cnf antes comentado y sacarle backup

- b) En este archivo buscar la sección [mysqld]
- c) En esta sección si no existe el parámetro port=3306, agregar en esta sección el parámetro y fijar el nuevo puerto del siguiente modo:
skip-name-resolve
- d) Reiniciar el servicio mariadb

4.2.6.3 Ejemplo 3

Para habilitar el servidor mariadb para permitir conexión segura usando cifrado SSL. Para este procedimiento se asume que usted ya habilito el modo seguro de su servidor mariaDB.

- a) Verificamos si esta habilitado ssl en nuestro servidor, para lo cual nos conectamos como root
- b) Una vez conectados verificamos en las variables de sistema de mariadb el estado ssl:
SHOW VARIABLES LIKE '%ssl%';
- c) Este comando en mariadb nos arrojara el siguiente resultado si hay soporte SSL pero no esta habilitado:

Variable_name	Value
have_openssl	YES
have_ssl	DISABLED
ssl_ca	
ssl_capath	
ssl_cert	
ssl_cipher	
ssl_crl	
ssl_crlpath	
ssl_key	
version_ssl_library	OpenSSL 1.0.2k-fips 26 Jan 2017

Vemos que SSL esta deshabilitado pero que tiene openssl. Procedamos a habilitar para soporte conexión seguro por SSL

- d) Ubicar el archivo server.cnf antes comentado y sacarle backup.
- e) Crear un directorio donde se tendrá el certificado público de la autoridad certificadora (que la simularemos) y el certificado y llave de su servidor mariaDB. Para nuestro caso crearemos el directorio mariadb-pki dentro del directorio /etc
- f) Nos cambiamos al directorio creado (/etc/mariadb-pki)
- g) Crear llave para CA (autoridad certificadora) simulada:
openssl genrsa -out ca-key.pem 4096
- h) Crear certificado de autoridad certificadora simulada (Llenar los datos para su autoridad simulada):
openssl req -new -x509 -nodes 1500 -key ca-key.pem -out ca-cert.pem
- i) Crear certificado y llave para nuestro servidor mariadb, ejecutando el comando:
openssl req -newkey rsa:4096 -days 365 -nodes -keyout mariadb-key.pem -out mariadb-req.pem
- j) Crearemos el certificado para le servidor mariadb, ejecutando el siguiente comando:
openssl x509 -req -in mariadb-req.pem -days 350 -CA ca-cert.pem -CAkey ca-key.pem -set_serial 01 -out mariadb-cert.crt

Temas Especiales

- k) Cambiamos los privilegios de acceso a todas las llaves y certificados creados con el comando chmod, del siguiente modo (no se olvide que aun sigue dentro del directorio /etc/mariadb-pki):
chmod 755 *
- l) Ahora nos cambiamos al directorio donde estan los archivos de configuración de mariadb (/etc/my.cnf.d) ejecutando:
cd /etc/my.cnf.d
- m) Estado en este directorio abrimos el archivo (server.cnf) buscamos la sección [mysqld]
- n) En esta sección (justo debajo) en el archivo mencionado en el inciso previo, procederemos a especificar el archivo con el certificado de la autoridad certificadora que firma el certificado del servidor, la llave privada y el certificado public del servidor mariadb, habilitando o agregando (si no están ya puestos los parametros) los siguientes parámetros:
ssl-ca=/etc/mariadb-pki/ca-cert.pem
ssl-cert=/etc/mariadb-pki/mariadb-cert.crt
ssl-key=/etc/mariadb-pki/mariadb-key.pem
- o) Reiniciamos servidor mariadb.
- p) Si volvemos a conectarnos al servidor y vemos las variables de sistema que tienen que ver con ssl: **SHOW VARIABLES LIKE '%ssl%';** obtendremos la siguiente respuesta:

Variable_name	Value
have_openssl	YES
have_ssl	YES
ssl_ca	/etc/mariadb-pki/ca-cert.pem
ssl_capath	
ssl_cert	/etc/mariadb-pki/mariadb-cert.pem
ssl_cipher	
ssl_crl	
ssl_crlpath	
ssl_key	/etc/mariadb-pki/mariadb-key.pem
version_ssl_library	OpenSSL 1.0.2k-fips 26 Jan 2017

- q) Además, estando conectado al servidor ejecutamos el comando **status** obtenemos la siguiente respuesta:

```
mariadb Ver 15.1 Distrib 10.8.3-MariaDB, for Linux (x86_64) using readline 5.1

Connection id:          3
Current database:
Current user:          root@localhost
SSL:                  Not in use
Current pager:         stdout
Using outfile:
Using delimiter:       ;
Server:                MariaDB
Server version:        10.8.3-MariaDB MariaDB Server
Protocol version:      10
Connection:             Localhost via UNIX socket
Server characterset:   latin1
Db     characterset:   latin1
Client characterset:   utf8mb3
Conn. characterset:    utf8mb3
UNIX socket:           /var/lib/mysql/mysql.sock
Uptime:                1 hour 51 min 58 sec

Threads: 1  Questions: 5  Slow queries: 0  Opens: 17  Open tables: 10  Queries per second avg: 0.000
```

Temas Especiales

Si vemos esta respuesta la línea SSL dice Not in use. Esto es porque aún en nuestra conexión no solicitamos conexión usando SSL.

- r) Para conectarnos usando conexión SSL, el cliente debe solicitar conexión con SSL. Por ejemplo usando el comando mysql (o mariadb) se deberá hacer de la siguiente manera (se asume que el servidor esta funcionando en el puerto por defecto)

mysql -u root -p --ssl

- s) Una vez conectados con el comando anterior, volvemos a ejecutar el comando **status** obtendremos la siguiente respuesta:

```
mariadb Ver 15.1 Distrib 10.8.3-MariaDB, for Linux (x86_64) using readline 5.1

Connection id:          4
Current database:
Current user:           root@localhost
SSL:                   Cipher in use is DHE-RSA-AES256-GCM-SHA384
Current pager:          stdout
Using outfile:
Using delimiter:        ;
Server:                 MariaDB
Server version:         10.8.3-MariaDB MariaDB Server
Protocol version:       10
Connection:              Localhost via UNIX socket
Server characterset:    latin1
Db     characterset:    latin1
Client characterset:   utf8mb3
Conn. characterset:    utf8mb3
UNIX socket:            /var/lib/mysql/mysql.sock
Uptime:                 1 hour 57 min 1 sec

Threads: 1  Questions: 9  Slow queries: 0  Opens: 17  Open tables: 10  Queries per second avg: 0.001
```

Si vemos la línea SSL ya no dice Not in use, ya informa que algoritmo de cifrado se está utilizando en la conexión SSL

NOTA

Es importante tomar en cuenta que dependiendo de donde instale mariadb en Rocky Linux, el archivo de configuración que necesitamos tocar para este ejemplo en lugar de llamarse server.cnf podría llamarse mariadb-server.cnf o mysql_server.cnf

Para mayor detalle de administración de mariaDB puede acceder al sitio de mariaDB en la sección de administración: <https://mariadb.com/kb/en/mariadb-administration/>

4.2.7 Respaldo y restauración de bases de datos

Para respaldar una base de datos desde el servidor local, ejecute `mysqldump` con las opciones `--opt` (que añade automáticamente las opciones `--add-drop-table`, `--add-locks`, `--create-options`, `--quick`, `--extended-insert`, `--lock-tables`, `--set-charset` y `--disable-keys`), la opción `-u` con el nombre de usuario a utilizar, la opción `-p` para indicar que se ingresará una contraseña, el nombre de la base de datos, `>` para guardar la salida estándar (STDOUT) en un archivo y el nombre del archivo donde se guardará el respaldo. Ejemplo:

```
mysqldump --opt -u root -p basedatos > respaldo.sql
```

Temas Especiales

Para restaurar un respaldo, ejecute mysql con las opciones -u con el nombre de usuario con privilegios sobre la base de datos a restaurar, -p para indicar que se utilizará contraseña, el nombre de la base de datos a restaurar, < para indicar que la entrada estándar (STDIN) será un archivo y el nombre del archivo con el respaldo de la base de datos. Ejemplo:

```
mysql -u root -p basedatos < respaldo.sql
```

Para respaldar todas las bases de datos almacenadas en MariaDB ejecute mysqldump con las opciones --opt, --all-databases para indicar que se respaldarán todas las bases de datos, la opción -u con root como usuario, la opción -p para indicar que se utilizará contraseña, el símbolo > para guardar la salida estándar (STDOUT) en un archivo y el nombre del archivo donde se guardará el respaldo. Ejemplo:

```
mysqldump --opt --all-databases -u root -p > respaldo-todo.sql
```

Para restaurar todas las bases de datos a partir de un único archivo de respaldo, ejecute mysql con la opción -u con root como usuario, la opción -p para indicar que se utilizará contraseña, el símbolo < para indicar que la entrada estándar (STDIN) será un archivo y el nombre del archivo con el respaldo de todas las bases de datos. Ejemplo:

```
mysql -u root -p < respaldo-todo.sql
```

Capítulo 5. Servidor de Correos Electrónicos

5.1 Definición

El correo electrónico (en inglés: electronic mail, comúnmente abreviado e-mail o email) es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica. El término “correo electrónico” proviene de la analogía con el correo postal: ambos sirven para enviar y recibir mensajes, y se utilizan “buzones” intermedios (servidores de correo). Por medio del correo electrónico se puede enviar no solamente texto, sino todo tipo de archivos digitales, si bien suelen existir limitaciones al tamaño de los archivos adjuntos.

Los sistemas de correo electrónico se basan en un modelo de almacenamiento y reenvío, de modo que no es necesario que ambos extremos se encuentren conectados simultáneamente. Para ello se emplea un servidor de correo que hace las funciones de intermediario, guardando temporalmente los mensajes antes de enviarse a sus destinatarios. En Internet, existen multitud de estos servidores, que incluyen a empresas, proveedores de servicios de internet y proveedores de correo tanto libres como de pago.

5.2 Términos y Protocolos Utilizados

5.2.1 Agente de Usuario de Correo - MUA

El Agente de Usuario de Correo (MUA por su acrónimo en inglés) o cliente de correo electrónico, es el programa que le va a permitir a un usuario (como mínimo) leer y escribir mensajes de correo electrónico. Típicamente, esto se hace a través de una interfaz que puede ser gráfica (Ximena Evolution, Outlook, Wemail, ThunderBird, etc) o en texto (Pine, Mutt, etc). Debe tener funcionalidades de agente de acceso a correo para permitir la recuperación de correo a través de POP ó IMAP y debe tener funcionalidad MIME (Multipurpose Internet Mail Extensions, Extensiones de Correo de Internet Multipropósito).

5.2.2 Agente de transferencia de correo – MTA

El Agente de transferencia de correo (MTA por su acrónimo en inglés) se encarga de la transferencia de los mensajes de correo electrónico entre las máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar al destino final. En GNU/Linux tenemos más de una alternativa para instalar y habilitar el protocolo SMTP, entre los que podemos citar: postfix, exim4, sendmail, etc.

5.2.3 Agente de entrega de correo – MDA

El Agente de entrega de correo (MDA por su acrónimo en inglés) se encarga de realizar la entrega del correo electrónico al buzón de un usuario concreto. En GNU/Linux Podemos instalar Dovecot para poder disponer de un MDA, pues nos permite habilitar el protocolo POP3 o IMAP.

5.2.4 Protocolo SMTP

SMTP (simple mail transfer protocol): es el protocolo que se emplea para que dos servidores de correo intercambien mensajes. También se emplea para que los clientes envíen correos al servidor.

5.2.5 Protocolo POP3

POP (post office protocol) se usa para obtener los mensajes almacenados en el servidor y que el destinatario los pueda consultar. Actualmente se usa la versión 3, POP3.

5.2.6 Protocolo IMAP

IMAP (internet message access protocol) tiene la misma finalidad que la de POP, pero con un funcionamiento y unas funcionalidades un poco diferente.

Ventajas sobre IMAP

- Soporte para operación en línea y fuera de línea
- Soporte para la conexión de múltiples clientes simultáneos a un mismo destinatario.
- Soporte para acceso a partes MIME de los mensajes y obtención parcial.
- Soporte para que la información de estado del mensaje se mantenga en el servidor.
- Soporte para accesos múltiples a los buzones de correo en el servidor.
- Soporte para búsquedas de parte del servidor.
- Soporte para un mecanismo de extensión definido.

5.2.7 Multipurpose Internet Mail Extensions – MIME

Serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. El uso de MIME amplia la capacidad del servicio de correo electrónico a no solo poder enviar mensajes de texto, si no también audio, video, imágenes, etc.

5.2.8 Direcciones de correo electrónico

Para poder enviar o recibir mensajes de un correo electrónico es necesario disponer de una cuenta de correo. Dicha cuenta es un buzón virtual identificado por una dirección de correo electrónico de la forma “juan_perez@ejemplo.com”. Cada dirección se compone de una parte local (en este caso juan_perez), el símbolo separador @ y una parte que identifica un dominio (en este caso ejemplo.com).

5.2.9 Proveedores de correo electrónico

Son los encargados de brindarnos acceso al servicio de correo electrónico, proporcionándonos de una cuenta de correo electrónico y el soporte para utilizar dicha cuenta para enviar correos electrónicos a otros usuarios. Existen diversos modos de obtener una cuenta de correo electrónico:

- las empresas y administraciones suelen proporcionar una cuenta de correo corporativo a sus empleados.
- los centros educativos, especialmente los universitarios, hacen lo propio con empleados y alumnos.

Temas Especiales

- en el ámbito doméstico, los proveedores de servicios de internet suelen facilitar una o varias cuentas por cada contrato.
- existen proveedores de correo que proporcionan este servicio a cambio de una cuota.
- finalmente, es posible obtener gratuitamente una cuenta de correo en servicios tales como GMail, Yahoo Mail, Outlook.com y muchos otros.

5.2.10 Postfix

Postfix, originalmente conocido por los nombres VMailer e IBM Secure Mailer, es un popular agente de transporte de correo (MTA o Mail Transport Agent), creado con la principal intención de ser una alternativa más rápida, fácil de administrar y segura que Sendmail. Fue originalmente escrito por Wietse Venema durante su estancia en el Thomas J. Watson Research Center de IBM.

5.2.11 Dovecot

Dovecot es un servidor de POP3 e IMAP de fuente abierta que funciona en Linux y sistemas basados sobre Unix™ y diseñado con la seguridad como principal objetivo. Dovecot puede utilizar tanto el formato mbox como maildir y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.

5.2.12 Buzón de correo

El buzón de correo electrónico es lugar asociado a una cuenta (dirección) de correo electrónico por defecto, donde se almacenan todos los correos electrónicos que el usuario ha enviado y recibido desde y hacia su dirección de correo electrónico.

Para acceder a este buzón necesita una dirección de correo electrónico, así como un programa de cliente de correo electrónico como Webmail, Outlook, Thunderbird o una aplicación para smartphones.

Cada buzón de correo electrónico tiene un espacio de almacenamiento específico en el servidor donde se creó la cuenta de correo electrónico, en el que se almacenan los correos electrónicos. El tamaño de este espacio de almacenamiento depende del proveedor y de la tarifa - no existe una regulación uniforme. Los correos electrónicos enviados y recibidos se almacenan allí hasta ser eliminados por el usuario.

5.2.13 Tipos de buzones de correo

Maildir y MBOX son simplemente dos tipos de formatos de buzón de correo electrónico que se utilizan para almacenar los mensajes en las aplicaciones de correo electrónico.

MBOX coloca todos los mensajes del servidor en el mismo archivo, mientras que Maildir almacena los mensajes con nombres únicos en archivos individuales.

es el formato tradicional de Unix para almacenar los mensajes. Esto agrega los correos a un solo archivo de manera secuencial. Este archivo debe estar bloqueado por cualquier aplicación para escribir en él. En servidores con un alto uso, puede haber problemas de bloqueo y rendimiento si se utiliza el formato MBOX, ya que solo una aplicación a la vez puede leer y escribir el archivo al mismo tiempo. De manera predeterminada, Postfix entrega el correo al objeto de archivo en el directorio

Temas Especiales

de spool. (Por ejemplo: para el usuario root, el archivo MBOX es /var/spool/mail/root). La mayoría de las tecnologías de recuperación de correo, como los servidores base IMAP y POP3, siguen esta estructura de directorio de manera predeterminada.

Maildir es el estándar Unix más nuevo para enrutar el correo a una estructura de directorio. Maildir proporciona una escalabilidad superior y no presenta problemas de bloqueo. Crea un subdirectorio en el directorio de inicio de cada usuario llamado Maildir. Debajo de este directorio se encuentra la estructura que contiene los mensajes. Maildir es introducido por Qmail y reconocido y soportado por casi todos los MUAs. Dentro del directorio Maildir de cada se crean los directorios tmp, new y cur. En el directorio tmp es usado por el servicio de correo electrónico cuando un mensaje se almacena en cola, copiando el mensaje a ese directorio. El directorio "new" contiene los correos no leídos. En el directorio cur se encuentran los correos que el usuario ya ha leído.

5.2.14 SASL

SASL (Simple Authentication and Security Layer) es una estructura para la seguridad de datos en protocolos de Internet. Desempareja mecanismos de la autenticación desde protocolos de aplicaciones, permitiendo, en teoría, cualquier mecanismo de autenticación soportado por SASL para ser utilizado en cualquier protocolo de aplicación que capaz de utilizar SASL

5.3 Formato Básico de un mensaje de Correo Electrónico

Un mensaje de correo mínimamente este compuesto de los siguientes campos para poder enviarse:

- Cuenta emisor: Cuenta de correo que envía el mensaje
- Cuenta Destinatario: cuenta de correo a quien va dirigido el mensaje.
- Asunto: Descripción corta de lo que vera el destinatario en el mensaje
- Mensaje: El mensaje en si. (Opcional). Solo texto en un SMTP básico

Además, se suele dar la opción de incluir archivos adjuntos al mensaje. Por otro lado además del campo Cuenta Destinatario, existen los campos:

- CC (Copia de Carbón) en donde se puede colocar la lista de cuentas de correos electrónicos a quienes también les llegará el mensaje, pero verán que no va dirigido a ellos.
- CCO (Copia de Carbón Oculta): una variante del campo CC, en la que especificaremos la cuenta o cuentas de correos electrónicos a quienes queremos que también les llegue el mensaje sin que aparezca en el correo que el mensaje también le (les) llegó.

5.4 Funcionamiento

En forma resumida para el envío de un mensaje de correo electrónico, el remitente utiliza un Agente de Usuario de Correo (MUA) o cliente de correo electrónico, para enviar el mensaje a través de uno o más agentes de transferencia de correo (MTA), el último de los cuales será el encargado de pasarlo a un Agente de entrega de correo (MDA) para la entrega a la buzón de correo del destinatario, de la que va a ser recuperada por el cliente de correo electrónico del destinatario, por lo general a través de un servidor POP3 o IMAP.

Para entender mejor el funcionamiento, supongamos que Ana (ana@a.org) envía un correo electrónico a Bea (bea@b.com). Cada una de ellas tiene su cuenta de correo electrónico en un

servidor distinto (una en a.org, otra en b.com), pero estos se pondrán en contacto para transferir el mensaje.

Secuencialmente, son ejecutados los siguientes pasos:

- i. Ana escribe el correo con la ayuda de su cliente de correo electrónico (MUA). Cuando envía el mensaje, el programa hace contacto con el servidor de correo usado por Ana (en este caso supongamos, smtp.a.org). Se comunica usando un lenguaje conocido como protocolo SMTP (MTA). Le transfiere el correo, y le da la orden de enviarlo.
- ii. El servidor smtp.a.org debe entregar un correo a un usuario del dominio b.com, pero no sabe con qué ordenador tiene que conectarse. Para ello, efectúa una consulta al servidor DNS de su red, usando el protocolo DNS, y le pregunta qué servidor es el encargado de gestionar el correo del dominio b.com. Técnicamente, le está preguntando el registro MX asociado a ese dominio.
- iii. Como respuesta a esta petición, el servidor DNS contesta con el nombre de dominio del servidor de correo de Bea. En este caso supongamos tiene el nombre email.b.com; que en este caso en particular es un servidor gestionado por el proveedor de Internet de Bea.
- iv. El servidor SMTP (smtp.a.org) ya puede conectarse con emial.b.com y transferirle el mensaje, que quedará guardado en este servidor. Se usa otra vez el protocolo SMTP.
- v. Posteriormente, cuando Bea inicie su programa cliente de correo electrónico, su ordenador inicia una conexión, mediante el protocolo POP3 o IMAP (MDA), al servidor que guarda los correos nuevos que le han llegado. Este servidor es el mismo que el del paso anterior (email.b.com), ya que se encarga tanto de recibir correos del exterior como de entregárselos a sus usuarios. En el esquema, Bea se descarga el mensaje de Ana mediante el protocolo POP3 o IMAP.

Así pues, un servidor de correo suele ser en realidad una combinación de dos servicios. Un servicio SMTP, que es el encargado de enviar y recibir los mensajes, y un servicio POP/IMAP, que permite a los usuarios obtener los mensajes.

Estos protocolos de correo electrónico usan los puertos:

- SMTP utiliza el puerto 25/TCP (SMTP sobre TLS utiliza el puerto 465/TCP y el puerto 587/TCP).
- POP utiliza el puerto 110/TCP (POP sobre SSL utiliza el puerto 995/TCP).
- IMAP utiliza el puerto 143/TCP (IMAP sobre SSL utiliza el puerto 993/TCP).

5.5 Software para habilitar servidor de correo en Rocky Linux

El nombre de los paquetes que deberemos tener instalados para poder habilitar un servidor de correo electrónico en nuestro servidor Rocky Linux es: openssl, postfix y dovecot. Postfix nos servirá como MTA, dovecot será nuestro MDA (que además que cuanta con una capa SASL que también puede utilizarse con Postfix) y openssl nuestra herramienta para la generación de firmas y certificados digitales que se necesitan cuando se habilitará un servicio con soporte de conexión segura.

En una consola como root verifique si están instalados estos paquetes y en caso de no estar instalados, instálelos. Puede verificar si un paquete esta instalado ejecutando:

```
dnf list nombrePaquete
```

Por ejemplo si quiero verificar si el paquete postfix está o no instalado ejecutariamos:

```
dnf list postfix
```

Si se nos muestra el mensaje **Installed Packages**, entonces el paquete ya esta instalado, pero si se nos visualiza el mensaje **Available Packages**, entonces deberemos instalar el paquete.

Adicionalmente en caso de querer realizar algunas pruebas al momento de configurar nuestro servidor, deberemos instalar los paquetes mailx y telnet.

Habilitar los servicios: **postfix** y **dovecot** para que puedan iniciar en forma automática.

5.6 Pasos para configurar el servidor de correo

Luego de instalar los paquetes requeridos, deberemos realizar el siguiente procedimiento:

5.6.1 Creación de la firma y certificado digital para el servidor de correo

Realizaremos el mismo procedimiento que utilizamos en el apartado donde creamos el certificado de clave publica para el servidor web cuando habilitamos soporte SSL/TLS, es decir:

```
i. openssl req -x509 -nodes -days 1000 -newkey rsa:4096 -keyout
   /etc/pki/tls/private/correo.sof164.net.key
   -out
   /etc/pki/tls/certs/correo.sof164.net.crt
```

5.6.2 Habilitación de puertos en el firewall para servicios de correo

- `firewall-cmd --permanent --add-service={http,https,smtp-submission,smtp,smtps,imap,imaps,pop3,pop3s}`
- `firewall-cmd --reload`

5.6.3 Configuración de Postfix

Para configurar Postfix, debemos realizar los siguientes pasos:

- i. Abrir una consola como superusuario (root)
- ii. Sacamos copia de seguridad los archivos de configuración de postfix que se modificarán:
 - `cp /etc/postfix/main.cf /etc/postfix/main.cf.bkp`
 - `cp /etc/postfix/master.cf /etc/postfix/master.cf.bkp`
- iii. Habilitares para postfix el tipo de buzon Maildir, autenticación a través de dovecot y uso de conexión segura, para esto deberemos ejecutar los siguientes comandos:
 - `postconf -e 'home_mailbox = Maildir/'`
 - `postconf -e 'inet_interfaces = all'`
 - `postconf -e 'inet_protocols = all'`
 - `postconf -e 'mydomain = sof164.net'`
 - `postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain'`
 - `postconf -e 'myhostname = correo.sof164.net'`
 - `postconf -e 'myorigin = $mydomain'`
 - `postconf -e 'mynetworks = 127.0.0.0/8'`
 - `postconf -e 'smtpd_sasl_type = dovecot'`
 - `postconf -e 'smtpd_sasl_path = private/auth'`

Temas Especiales

- `postconf -e 'smtpd_sasl_auth_enable = yes'`
 - `postconf -e 'smtpd_sasl_local_domain = '`
 - `postconf -e 'smtpd_sasl_security_options = noanonymous'`
 - `postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination'`
 - `postconf -e 'smtpd_tls_received_header = yes'`
 - `postconf -e 'smtp_tls_note_starttls_offer = yes'`
 - `postconf -e 'smtp_tls_security_level = may'`
 - `postconf -e 'smtpd_tls_security_level = may'`
 - `postconf -e 'smtpd_use_tls = yes'`
 - `postconf -e 'smtpd_tls_cert_file = /etc/pki/tls/certs/correo.sof164.net.crt'`
 - `postconf -e 'smtpd_tls_key_file = /etc/pki/tls/private/correo.sof164.net.key'`
- iv. Para que se habilite smtps (smtp por el puerto 465), editamos el archivo `/etc/postfix/master.cf` y buscaremos las líneas que se muestran en la primera fila de la siguiente tabla y haremos que se vean como están en la segunda fila

<code>smtp inet n - n - - smtspd</code>
<code>#smtp inet n - n - 1 postscreen</code>
<code>#smtspd pass - - n - - smtspd</code>
<code>#dnsblog unix - - n - 0 dnsblog</code>
<code>#tlsproxy unix - - n - 0 tlsproxy</code>
<code>#submission inet n - n - - - smtspd</code>
<code> # -o syslog_name=postfix/submission</code>
<code> # -o smtpd_tls_security_level=encrypt</code>
<code> # -o smtpd_sasl_auth_enable=yes</code>
<code> # -o smtpd_reject_unlisted_recipient=no</code>
<code> # -o smtpd_client_restrictions=\$mua_client_restrictions</code>
<code> # -o smtpd_helo_restrictions=\$mua_helo_restrictions</code>
<code> # -o smtpd_sender_restrictions=\$mua_sender_restrictions</code>
<code> # -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject</code>
<code> # -o milter_macro_daemon_name=ORIGINATING</code>
<code>#smtps inet n - n - - smtspd</code>
<code> # -o syslog_name=postfix/smtps</code>
<code> # -o smtpd_tls_wrappermode=yes</code>
<code> # -o smtpd_sasl_auth_enable=yes</code>
<code> # -o smtpd_reject_unlisted_recipient=no</code>
<code> # -o smtpd_client_restrictions=\$mua_client_restrictions</code>
<code> # -o smtpd_helo_restrictions=\$mua_helo_restrictions</code>
<code> # -o smtpd_sender_restrictions=\$mua_sender_restrictions</code>
<code> # -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject</code>
<code> # -o milter macro daemon name=ORIGINATING</code>
<code>smtp inet n - n - - smtspd</code>
<code>#smtp inet n - n - 1 postscreen</code>
<code>#smtspd pass - - n - - smtspd</code>
<code>#dnsblog unix - - n - 0 dnsblog</code>
<code>#tlsproxy unix - - n - 0 tlsproxy</code>
<code>submission inet n - n - - - smtspd</code>
<code> -o syslog_name=postfix/submission</code>
<code> -o smtpd_tls_security_level=encrypt</code>
<code> -o smtpd_tls_wrappermode=no</code>
<code> -o smtpd_sasl_auth_enable=yes</code>
<code> -o smtpd_relay_restrictions=permit_sasl_authenticated,reject</code>
<code> -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject</code>
<code> -o smtpd_sasl_type=dovecot</code>
<code> -o smtpd_sasl_path=private/auth</code>
<code>smtps inet n - n - - smtspd</code>
<code> -o syslog_name=postfix/smtps</code>
<code> -o smtpd_tls_wrappermode=yes</code>
<code> -o smtpd_sasl_auth_enable=yes</code>
<code> -o smtpd_relay_restrictions=permit_sasl_authenticated,reject</code>
<code> -o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,reject</code>
<code> -o smtpd_sasl_type=dovecot</code>
<code> -o smtpd_sasl_path=private/auth</code>

- v. Reiniciar el servicio de postfix

5.6.4 Configuración de Dovecot

Para configurar dovecot, debemos realizar los siguientes pasos:

Temas Especiales

- i. Abrir una consola como superusuario (root)
- ii. Sacar copia de seguridad a los archivos que se va a modificar
 - cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.bkp
 - cp /etc/dovecot/conf.d/10-mail.conf /etc/dovecot/conf.d/10-mail.conf.bkp
 - cp /etc/dovecot/conf.d/10-master.conf /etc/dovecot/conf.d/10-master.conf.bkp
 - cp /etc/dovecot/conf.d/10-auth.conf /etc/dovecot/conf.d/10-auth.conf.bkp
 - cp /etc/dovecot/conf.d/10-ssl.conf /etc/dovecot/conf.d/10-ssl.conf.bkp
 - cp /etc/dovecot/conf.d/20-pop3.conf /etc/dovecot/conf.d/20-pop3.conf.bkp
- iii. Como estamos usando certificados autofirmados, para evitar que el servidor de correo bloquee inicios de sesión desde algunas aplicaciones web, editamos el archivo /etc/dovecot/dovecot.conf en el cual buscamos el parámetro **login_trusted_networks** lo descomentamos y le asignamos separados por espacios las ip de los servidores o clientes que son de confianza o en nuestro caso podríamos poner toda nuestra red (ejemplo para la red del lab49)
`login_trusted_networks = 10.23.3.0/24`
- iv. Para asegurarnos que usamos el mismo buzón que postfix (maildir), debemos editar el archivo /etc/dovecot/conf.d/10-mail.conf y asegurarse que la variable **mail_location** tiene el valor **maildir:~/Maildir** y que no está comentado, es decir, debe tener una línea con lo siguiente:
`mail_location = maildir:~/Maildir`
- v. Para asegurarnos que postfix puede utilizar el mecanismo de autenticación de dovecot, editamos el archivo /etc/dovecot/conf.d/10-master.conf y buscamos en este archivo la línea comentada “**# Postfix smtp-auth**”. Debajo de esta línea debemos colocar los siguientes parámetros de configuración:
`unix_listener /var/spool/postfix/private/auth {
 mode = 0666
 user = postfix
 group = postfix
}`
- vi. Por si tenemos que usar alguna aplicación que utiliza como mecanismos de autenticación texto plano o login, modificaremos el archivo /etc/dovecot/conf.d/10-auth.conf y buscaremos la línea con el valor “**auth_mechanisms = plain**” y lo modificaremos por el valor “**auth_mechanisms = plain login**”. Adicionalmente descomentamos la línea con el texto “**#auth_username_format = %Lu**” cambiando su valor %n, es decir quedaría así: “**#auth_username_format = %n**”, esto para que dovecot trabaje con el tipo de cuenta que estamos usando que es una cuenta de usuario de correo canónico, ya que para autenticarnos no estamos usando el formato cuenta de correo electrónico. Luego grabamos el archivo.
- vii. Para asegurarnos que cualquier usuario que se conecte por pop3 solo se le permite una sesión activa a la vez, editamos el archivo /etc/dovecot/conf.d/20-pop3.conf y buscamos la línea “**#pop3_lock_session = no**” y la modificamos por “**pop3_lock_session = yes**”. Note que debemos quitar el carácter # para descomentar esta línea y ponerle el valor yes. Luego grabamos el archivo.
- viii. Por último, para que nuestro servidor MDA pueda trabajar con soporte para conexión asegurada, editamos el archivo /etc/dovecot/conf.d/10-ssl.conf y realizamos los siguientes cambios:
 - a. Primero buscamos la línea “**ssl = required**” y lo cambiamos a “**ssl = yes**”

- b. Buscamos la línea “`ssl_cert = </etc/pki/dovecot/certs/dovecot.pem`” y la modificamos utilizando como valor el mismo certificado digital que utilizamos para postfix, es decir, `/etc/pki/tls/certs/correo.sof164.net.crt`, por lo cual esta línea quedaría así: “`ssl_cert = </etc/pki/tls/certs/correo.sof164.net.crt`”.
 - c. Buscamos la línea “`ssl_key = < /etc/pki/dovecot/private/dovecot.pem`” y la modificamos utilizando como valor la misma llave privada que utilizamos para postfix, es decir, `/etc/pki/tls/private/email.sof164.net.pem`, por lo cual esta línea quedaría así: “`ssl_key = < /etc/pki/tls/private/correo.sof164.net.key`”.
 - d. Grabar el archivo
- ix. Reiniciar el servicio dovecot.

NOTA:

Si desea hacer seguimiento del servicio de correo electrónico puede usar los archivos **maillog** o **messages** que se encuentran el directorio **/var/log**

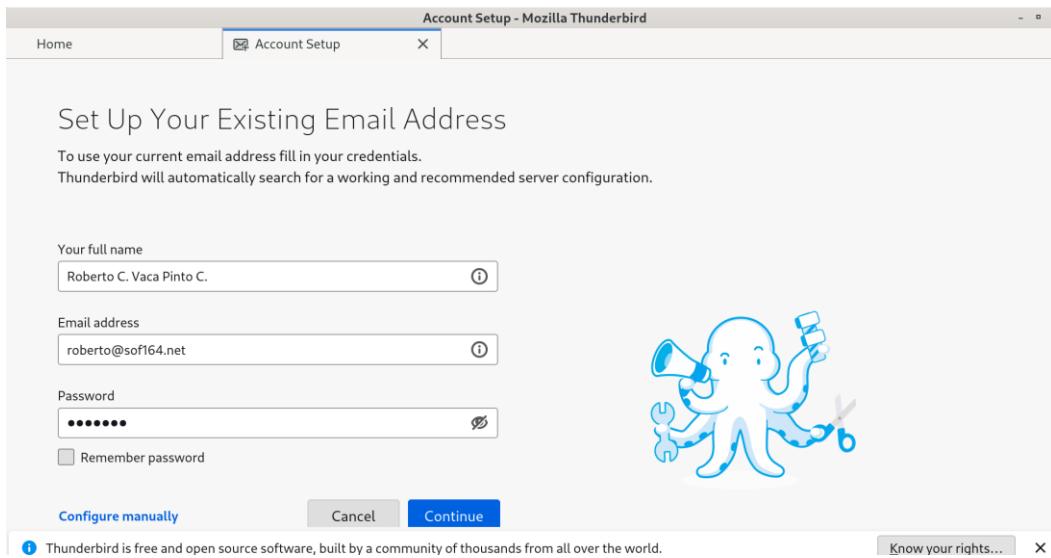
5.6.5 Configuración de cliente de correo de escritorio

Las cuentas de nuestro servidor de correo son las mismas que tenemos habilitadas en el sistema operativo, es decir que, si tenemos una cuenta de usuario, cuyo login es estudiante, entonces, también existe el buzón de correo estudiante@sof164.net. Para probar que nuestro servidor funciona, probaremos configurar un cliente de correo, en nuestro caso utilizaremos como MUA al programa de escritorio Thunderbird, el cual es un cliente de correo electrónico desarrollado por mozilla. Para instalar thunderbird en Rocky Linux en una consola como root instalamos el paquete **thunderbird**.

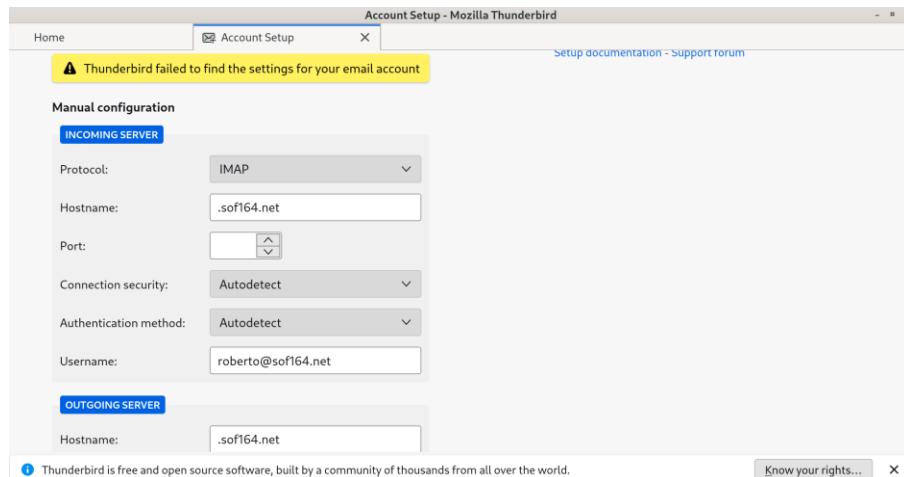
Para nuestro ejemplo supongamos que contamos con el usuario **roberto** y el usuario **estudiante**. Verificaremos que podemos enviar correo desde una cuenta y que la otra cuenta recibirá el correo en su buzón de correo.

- i. En su sesión gráfica con el otro usuario, en nuestro ejemplo, el usuario roberto, lanzamos Thunderbird.
- ii. Se lanzará en su escritorio el programa thunderbird. Como no tienen ninguna cuenta configurada le aparecerá como se muestra en la siguiente figura. En la ventana que se mostrará ingrese cualquier descripción en el campo Your Full Name. En el campo Email address, ingrese el correo electrónico para el que se está habilitando el programa cliente (esta cuenta ya debe existir en el sistema operativo, ya sea que se haya creado con el comando adduser o con la interfaz gráfica para gestión de usuario). Y en el campo password, ingrese la contraseña del usuario. En nuestro ejemplo usaremos el usuario roberto, por lo cual ingresaremos el correo roberto@sof164.net, por que estamos trabajando con el dominio sof164.net, tal como muestra la figura:

Temas Especiales

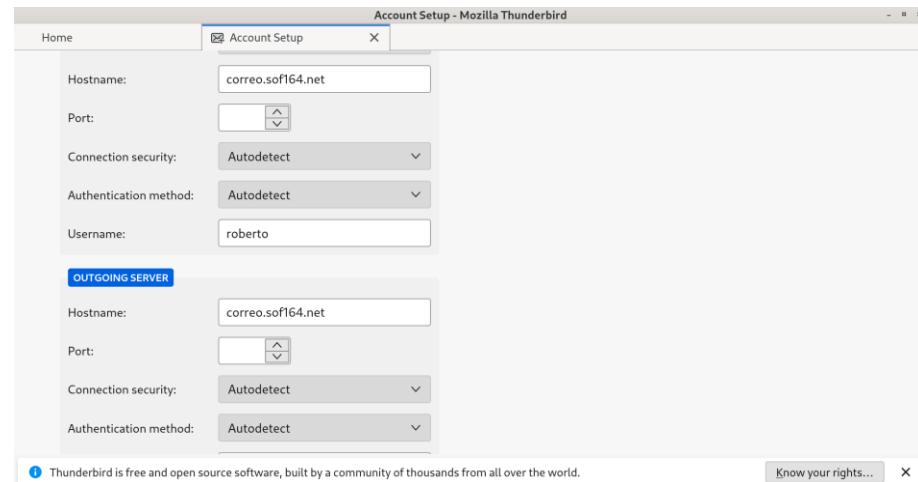


- iii. Una vez metida la información hacemos clic en el botón **Continue**, esperamos unos segundos que trata de encontrar la configuración sugerida. Puede pasar que el asistente de ThunderBird no encuentre una configuración ideal, por lo cual podría mostrarse la siguiente pantalla.

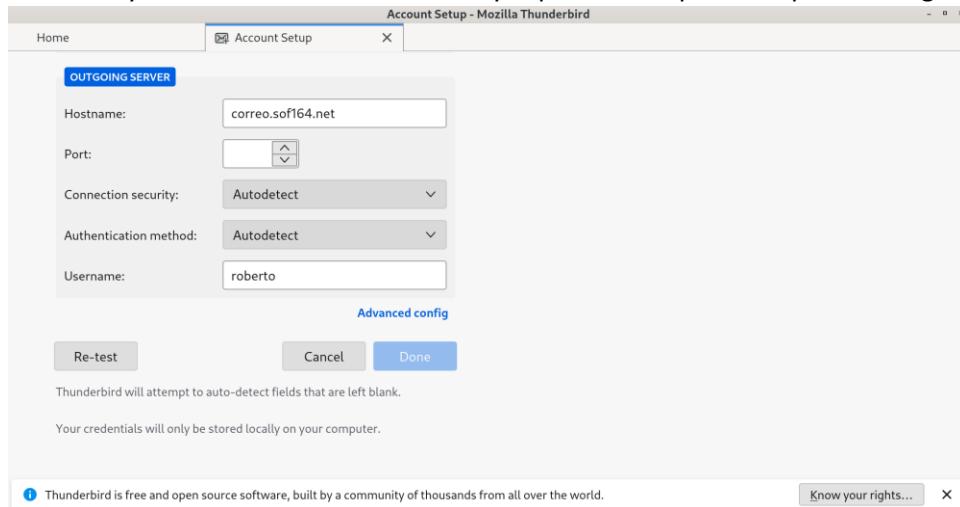


- iv. Si se nos presenta la pantalla anterior, llenaremos los datos correctos. En la sección **INCOMING SERVER** y en la sección **OUTCOMING SERVER** del siguiente modo: En el campo Hostname colocaremos el FQDN del servidor de correo o su IP (en nuestro hemos usado como FQDN correo.sof164.net ejemplo del servidor correo, además también nos aseguraremos que en el campo username de las dos secciones colocar solo la cuenta a nivel de sistema operativo no la cuenta de correo electrónico, entonces para nuestro ejemplo deberemos asegurarnos que en este solo el valor roberto (o su caso la cuenta que este configurando para su ejercicio):

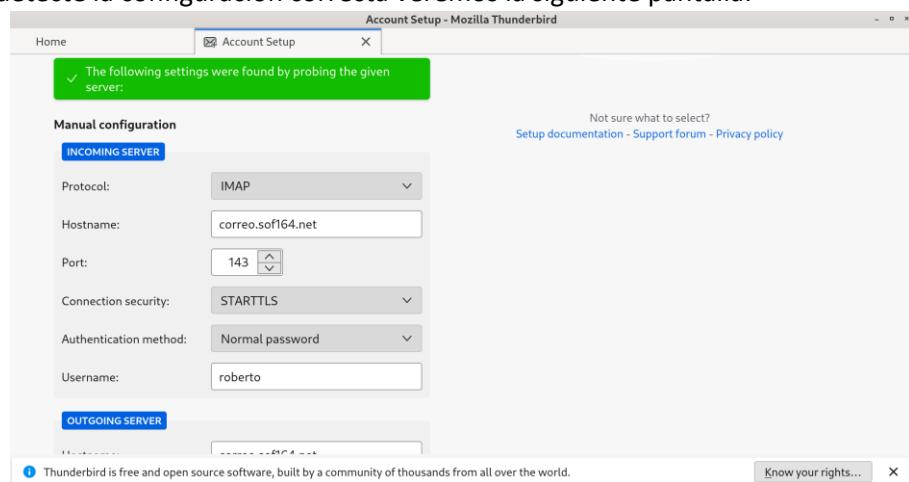
Temas Especiales



- v. Ahora para poder ver el botón Re-test, nos movemos abajo con el scroll que habilita ThunderBird y hacemos clic en dicho botón y esperamos a que verifique la configuración:

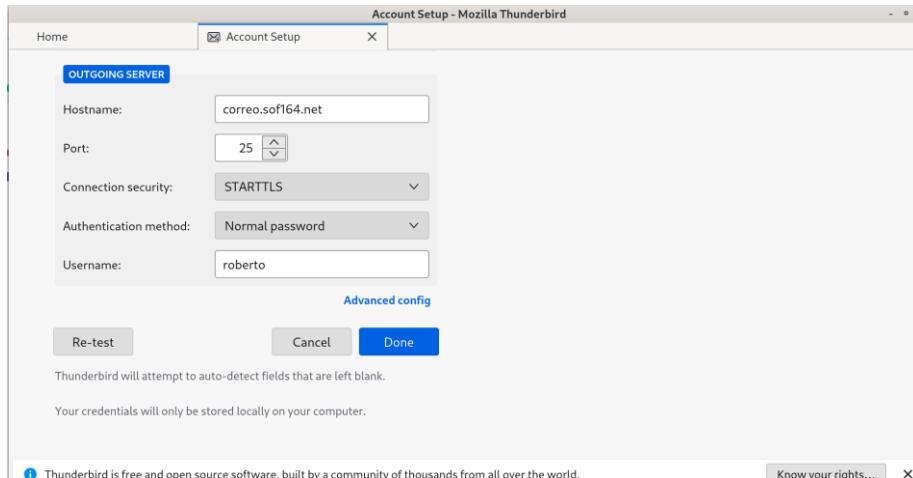


Cuando detecte la configuración correcta veremos la siguiente pantalla:

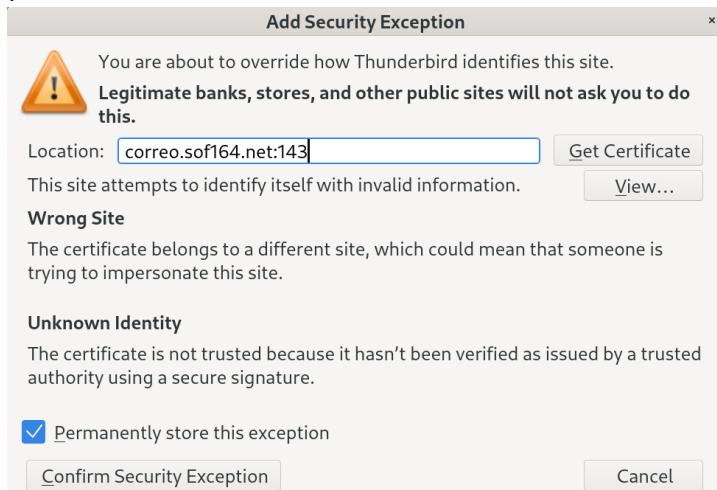


En esta pantalla la cual volveremos a bajar en la pantalla para buscar el botón Done y hacer clic sobre dicho botón:

Temas Especiales

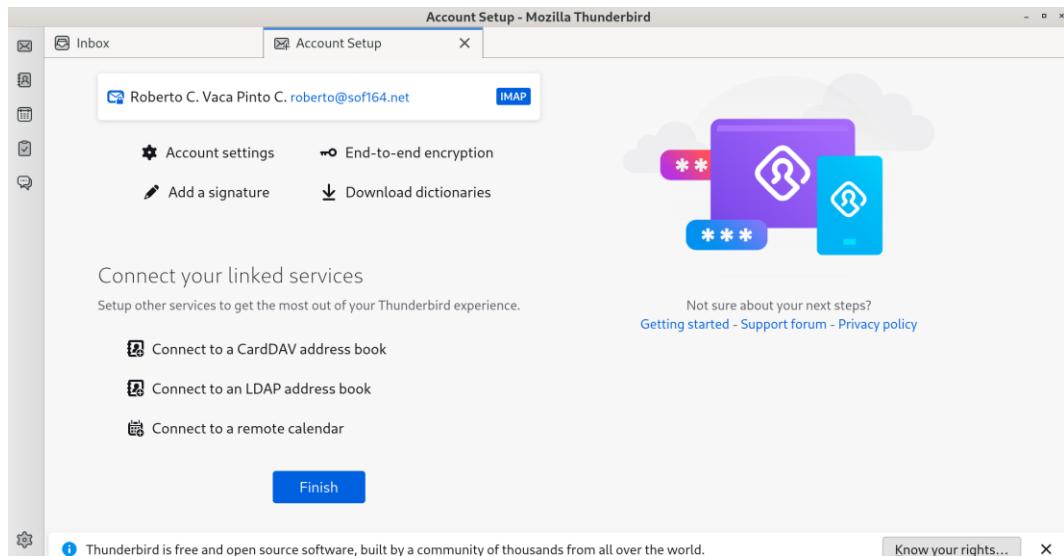


- vi. En esta ventana corregimos los datos que pudieran faltar (generalmente en IMAP y SMTP no mostrara el nombre de nuestro servidor de correo) y luego hacemos clic en **Re-test** y esperamos a que se nos habilite el botón **Done**.
- vii. En nuestro ejercicio como estamos usando un certificado autofirmado para el servidor de correo, al hacer clic en el botón **Done**, se nos mostrará una ventana pidiendo agregar una excepción por el certificado. Simplemente hacemos clic en el botón **Confirm Security Exception** como se muestra en la figura siguiente (Puede que esta ventana se nos muestre más de una vez):

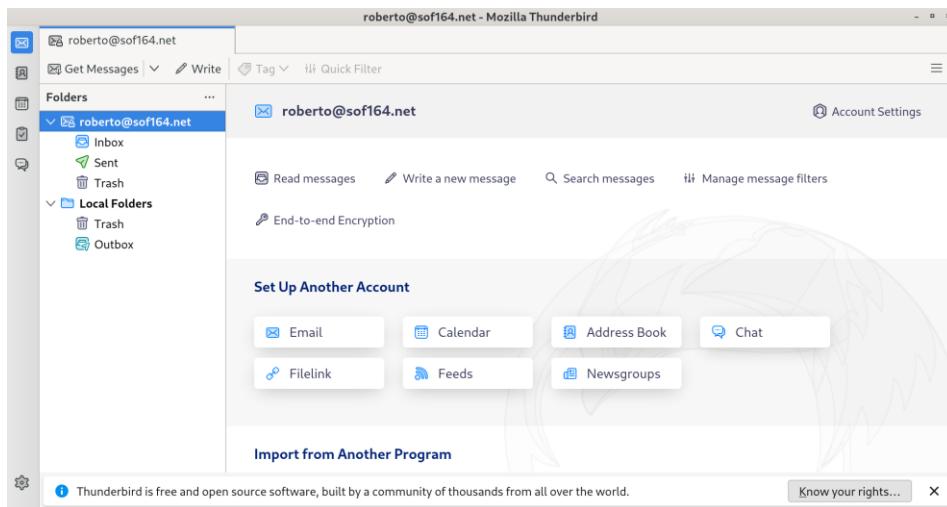


Luego haremos clic en el botón **Finish** que veremos en la siguiente pantalla

Temas Especiales

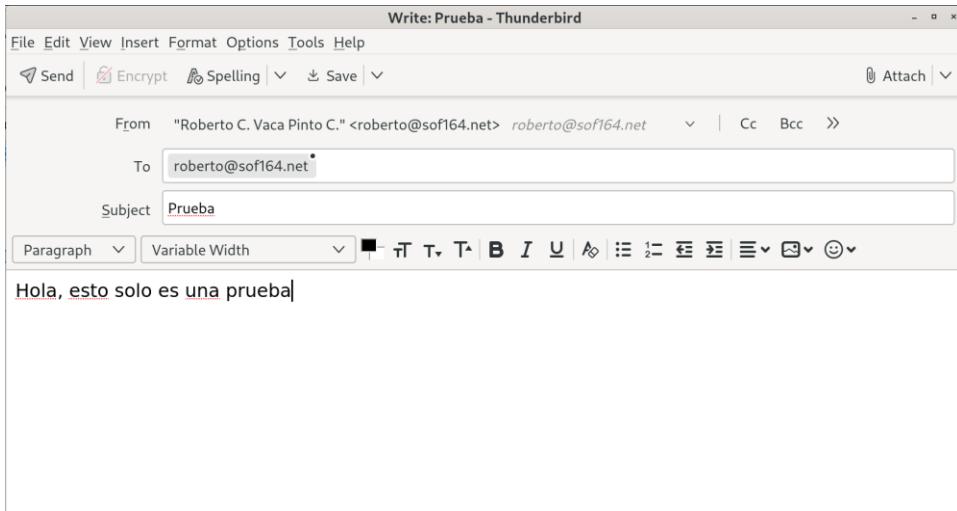


- viii. Luego esto se nos visualizará thunderbird con la cuenta en la lista del lado izquierdo y al hacer clic en la carpeta **inbox** de nuestra cuenta veremos que recibiremos el correo que enviamos con el otro usuario en el inciso i.



- ix. Puede probar el funcionamiento correcto haciendo clic en el botón Write, redactar un correo, enviándolo y verificando que llega usando como destinatario la cuenta de correo electrónico que acabamos de configurar.

Temas Especiales



NOTA IMPORTANTE:

- Si está usando certificados SSL autofirmados, las aplicaciones clientes normalmente en la actualidad no reciben bien el uso de este tipo de certificados por no estar validados por una autoridad reconocida, por lo cual en aplicaciones cliente de correo como thunderbird y otros tenga registrar excepciones al uso de este tipo de certificados, ya que para un servidor de correo institucional se pueda usar sin inconvenientes no deberíamos usar certificados ssl autofirmados
- Para el caso del cliente de correo electrónico Thunderbird, al usar certificados autofirmados en su servidor de correo, la primera vez que trata de enviar un correo nuevo o de responder uno que haya recibido, notará que le dará un mensaje de error y le pedirá agregar una excepción por el certificado autofirmado del servidor de correo (Este puede pasar de dos a 3 veces). Simplemente agregue la excepción y luego vuelva a intentar enviar su correo. Adicionalmente puede que en ajustes de thunderbird necesite desmarcar la casilla OCSP para confirmar la validez actual de los certificados. En Windows adicionalmente para hacer sus pruebas deshabilite su antivirus y/o firewall.

5.6.6 Configuración de cliente de correo Web

Existen múltiples aplicaciones web que son clientes de correo web que pueden instalarse bajo linux utilizando apache como servidor web. Una de estas aplicaciones es Roundcube. Para instalarla y configurarla seguimos los siguientes pasos:

- i. Se asume que ya tiene instalado y funcionando apache como su servidor web y mariadb
- ii. Abrir una consola de commandos como root.
- iii. Instalaremos las herramientas de desarrollo que se necesitan para habilitar Roundcube:
dnf -y groupinstall "Development Tools"
- iv. Instalamos php y los paquetes adicionales para hacer funcionar Roundcube, además de habilitar los servicios y repositorios adicionales necesarios:
dnf install -y php
dnf install -y php-common php-cli php-gd php-curl php-intl
dnf install -y php-mysqlnd
dnf install -y php-bz2 php-curl

```
dnf install -y php-gd
dnf install -y php-mbstring
dnf install -y php-xml
dnf install -y php-json
dnf install -y php-bcmath
dnf install -y php-pear
dnf install -y php-snmp
dnf install -y php-ldap
dnf install -y php-opcache
dnf install -y php-mysqli
dnf install -y php-pdo
dnf install -y php-devel
dnf install -y php-zip
dnf install -y php-fpm make
systemctl enable --now php-fpm
dnf makecache
dnf install -y ImageMagick ImageMagick-devel
pecl install imagick
#En el comando de la linea anterior cuando le pida detectar el prefijo
#de instalacion de ImageMagick solo presione enter en el teclado para
#autodetectarlo
echo "extension=imagick.so" > /etc/php.d/20-imagick.ini
systemctl restart httpd php-fpm
```

- v. Como sabemos ya existe un directorio /var/www/html que es el repositorio por defecto de su servidor apache. Lo que haremos será crear una carpeta con cualquier nombre dentro de la carpeta /var/www. La carpeta que crearemos en este ejemplo la llamaremos correo, dentro de esta crearemos la carpeta public y nos ubicamos dentro de esta carpeta public

```
cd /var/www
mkdir correo
chmod -R 777 correo
cd correo
mkdir public
cd public
```

- vi. Descargamos roundcube, para esto buscamos el enlace de la descarga de roundcube el paquete completo, copiamos la url y en la consola donde estamos dentro del directorio public usando el comando wget descargamos roundcube así (no de enter ingrese todo en una sola linea separando wget con https un espacio):

```
wget
https://github.com/roundcube/roundcubemail/releases/download/1.6.1/roundcubemail-
1.6.1-complete.tar.gz
```

- vii. Descomprimimos el archivo descargado del siguiente modo (luego de descomprimir si desea puede eliminar el archivo descargado, es decir el archivo **roundcubemail-1.6.1-complete.tar.gz**):

```
tar zxvf roundcubemail-1.6.1-complete.tar.gz
```

- viii. Hacemos propietario de la carpeta public al usuario apache y al grupo apache, cambios tambien los permisos y el contexto. Para no cambiarnos de directorio podemos usar ruta absoluta, del siguiente modo:

```
chown -R apache.apache /var/www/correo/public
chmod -R 777 /var/www/correo/public
```

Temas Especiales

```
chcon -R -t httpd_sys_rw_content_t /var/www/correo/public
```

- ix. Cuando descomprimimos roundcube en el paso vii, se creó la carpeta **roundcubeemail-1.6.1**. En una de las carpetas dentro de esta carpeta hay un archivo que tiene el script para crear las tablas necesarias en mariadb para hacer funcionar roundcube, antes de usarlo ingresamos a mariadb con el usuario root, una vez conectados a maria db procedemos a crear el usuario, con los permisos respectivos y la base de datos (crearemos el usuario dbuser y la base de datos db) En la figura esta con flecha verde el comando para conectarse a mariadb y con flecha roja los comandos a ejecutar una vez conectado a mariadb

```
root@srvr9rc public]# ls -l
total 4
drwxr-xr-x. 13 501 80 4096 Jan 23 16:03 roundcubeemail-1.6.1
[root@srvr9rc public]# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 12
Server version: 10.11.2-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database db;
Query OK, 1 row affected (0.005 sec)

MariaDB [(none)]> create user dbuser@'localhost' identified by 'abc123';
Query OK, 0 rows affected (0.023 sec)

MariaDB [(none)]> grant all on db.* to dbuser@'localhost';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> exit
Bye
[root@srvr9rc public]#
```

- x. Procedemos a crear las tablas en mariadb como se muestra en la siguiente figura:

```
root@srvr9rc public]# mariadb -u dbuser -p db < /var/www/correo/public/roundcubeemail-1.6.1/SQL/mysql.initial.sql
Enter password:
[root@srvr9rc public]#
```

- xi. Ahora procedemos a configurar apache. Para esto nos cambiamos al directorio **conf.d** que existe dentro del directorio **/etc/httpd**. Dentro de ese directorio conf.d creamos un archivo con cualquier nombre que termine en .conf, por ejemplo **correo.conf**, dentro del cual incluimos la siguiente configuración de host virtual que necesitamos para hacer funcionar roundcube con apache (La configuración está hecha tomando en cuenta los directorios que antes estuvimos trabajando y asume que usted ya creo en su servidor DNS la resolución para su FQDN clienteweb.sof164.net y que creo la llave y certificado público para el hostvirtual para ese FQDN):

```
<VirtualHost *:80>
```

Temas Especiales

```
ServerName clienteweb.sof164.net
DocumentRoot /var/www/correo/public/roundcubemail-1.6.1/
ServerAdmin roberto@sof164.net
ErrorLog logs/correo.sof164.net-error_log
CustomLog logs/correo.sof164.net-access_log combined
DirectoryIndex index.php
<Directory "/var/www/correo/public/roundcubemail-1.6.1/">
    Options -Indexes +FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
</VirtualHost>
<VirtualHost *:443>
    ServerName clienteweb.sof164.net
    DocumentRoot /var/www/correo/public/roundcubemail-1.6.1/
    ServerAdmin roberto@sof164.net
    ErrorLog logs/correo.sof164.net-error_log
    CustomLog logs/correo.sof164.net-access_log combined
    DirectoryIndex index.php
    <Directory "/var/www/correo/public/roundcubemail-1.6.1/">
        Options -Indexes +FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/clienteweb.sof164.net.crt
    SSLCertificateKeyFile /etc/pki/tls/private/clienteweb.sof164.net.key
</VirtualHost>
```

- xii. Establecemos los parámetros para permitir conexión de su apache con servidor de correo, conexión con mariadb y conexión de red:

```
setsebool -P httpd_can_sendmail 1
setsebool -P httpd_can_network_connect 1
setsebool -P httpd_can_network_connect_db 1
setsebool -P mysql_connect_http 1
setsebool -P httpd_read_user_content 1
setsebool -P httpd_builtin_scripting 1
```

- xiii. Reiniciar el servidor apache

- xiv. Abrir un navegador en su servidor rocky Linux y en la barra de direcciones cargue la url <http://clienteweb.sof164.net/installer> lo que hara que veamos la siguiente pagina:

Temas Especiales

The screenshot shows a web browser window titled "Roundcube Webmail Installer". The URL in the address bar is "clienteweb.sof164.net/installer/". The page content is titled "Roundcube Webmail Installer" and includes a navigation bar with three items: "1. Check environment" (which is highlighted), "2. Create config", and "3. Test config". Below the navigation bar, there are two sections: "Checking PHP version" and "Checking PHP extensions". The "PHP version" section states "Version: OK (PHP 8.0.27 detected)". The "PHP extensions" section lists several required modules: PCRE: OK, DOM: OK, Session: OK, XML: OK, Intl: OK, JSON: OK, PDO: OK, and Mcrypt: OK.

Si en esta página vemos algún NOT OK en rojo, deberemos resolverla para poder hacer clic en el botón Next que esta al final de la página. Si no tenemos ese problema hacemos clic en Next

- xv. Luego dar clic en Next se nos presentará una pagina bastante larga y solo cambiaremos algunos cambios que deberemos buscar:

- El campo `producto_name` puede no modificarlo o puede ponerle cualquier texto que deseé que aparezca al ingresar a su correo.
- En la sección cambiar por los siguientes valores de servidor (127.0.0.1 si el servidor de base de datos esta en el mismo servidor web o la ip donde este instalado su servidor de base de datos), base de datos (db), usuario (dbuser) y contraseña de usuario (abc123)

The screenshot shows a "Database setup" configuration form. It has a section titled "db_dsnw" with the sub-section "db_prefix". The "db_prefix" field contains the value "correo.". Below this, there is a note: "Optional prefix that will be added to database object names". The main configuration area is titled "Database settings for read/write operations:" and includes the following fields:

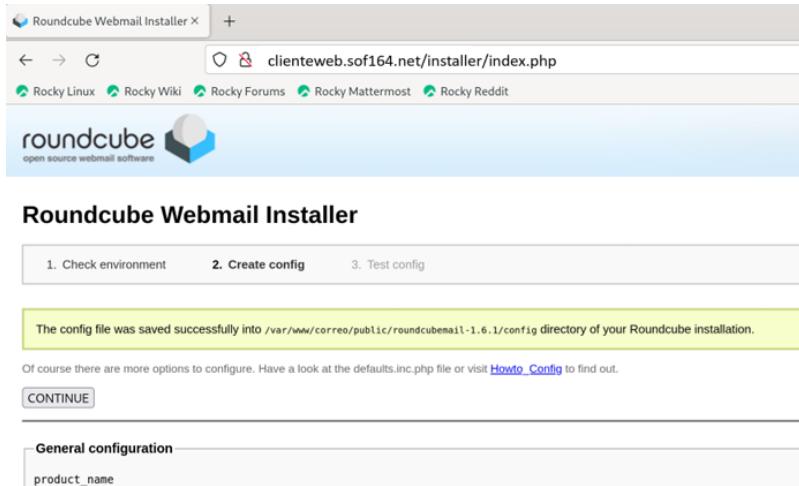
- "Database type": MySQL (selected from a dropdown menu).
- "Database server (omit)": 127.0.0.1
- "Database name (use a)": db
- "Database user name (use a)": dbuser
- "Database password (use a)": abc123

- En la sección IMAP Setting colocaremos como `imap_host` el valor **correo.sof164.net:143**

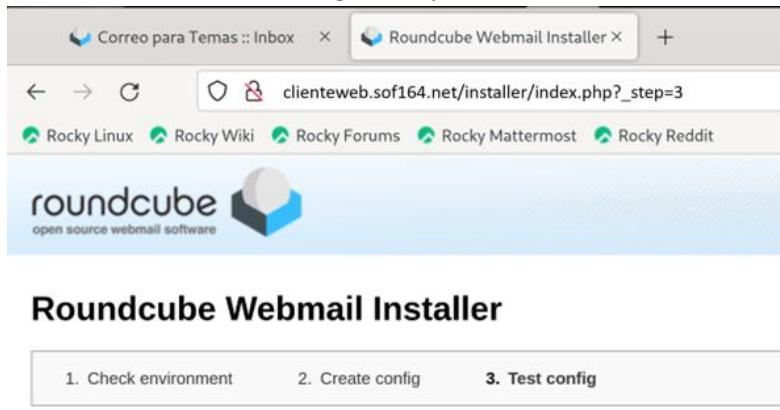
Temas Especiales

- En la sección SMTP Setting colocaremos como smtp_host el valor **correo.sof164.net:25**

Luego hacemos clic en el botón CREATE CONFIG que esta al final de la página. Esto hará que la pagina se actualice y al inicio se muestre un mensaje avisando que se creo el archivo de configuración, como se ve en la figura:

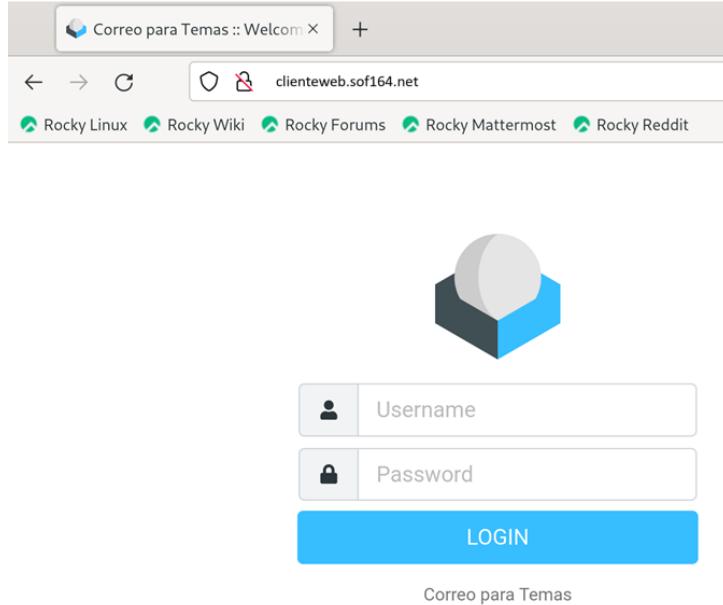


- xvi. Hecho esto si todo va bien veremos la siguiente pantalla:



- xvii. Ahora estaremos listos para iniciar sesión con la aplicación, para esto pondremos en nuestro navegador la URL <http://clienteweb.sof164.net> (es el FQDN que hemos estado usando y con el protocolo http o si lo prefiere con https), lo que hará que veamos lo siguiente

Temas Especiales



Nota:

Antes de probar por primera vez su roundcube, para Establecer el dominio de las cuentas en el archivo config.inc.php (En este ejemplo el archivo está en la ruta /var/www/correo/public/roundcubemail-1.6.1/config) antes de la línea siguiente:

```
$config['imap_host'] = 'correo.sof164.net:143';
```

Agregar el parametro para el dominio que debe manejar roundcube para sus cuentas:

```
$config['mail_domain'] = 'sof164.net';
```

Ahora pondremos algun usuario y su contraseña que ya tengamos creado. No olvide que nuestros usuarios son los mismos que ya existen en el sistema operativo.

Capítulo 6. Samba

6.1 Protocolo SMB

SMB (acrónimo de Server Message Block) es un protocolo de red que permite compartir archivos, impresoras, etcétera, entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows. Este protocolo pertenece a la capa de aplicación en el modelo OSI. Es utilizado principalmente en computadoras con sistemas operativos: Microsoft Windows y DOS.

SMB fue desarrollado originalmente por IBM, pero la versión más común es la modificada ampliamente por Microsoft. En 1998, Microsoft renombró SMB a Common Internet File System (CIFS) y añadió más características, que incluyen: soporte para enlaces simbólicos, enlaces duros (hard links), y mayores tamaños de archivo. Hay características en la implementación SMB de Microsoft que no son parte del protocolo SMB original.

Con los años, CIFS ganó una mala reputación. Las interacciones cliente/servidor estaban bugeadas, las extensiones propietarias y el bajo rendimiento en redes de alta latencia (especialmente, irónicamente, Internet) ensuciaron su reputación. Mucho de esto se lo merecía: CIFS simplemente no estaba destinado a este tipo de uso, y las muchas y frecuentes modificaciones hechas por Microsoft y otros no ayudaron a las cosas.

Microsoft se propuso escribir una versión completamente nueva del bloque de mensajes del servidor (SMB), liberando el resultado con Windows Vista en 2006. El protocolo resultante, SMB 2.0 es radicalmente diferente de CIFS. SMB2 se ha simplificado drásticamente. La canalización permite realizar varias solicitudes por lotes, lo que mejora el rendimiento en vínculos de alta latencia, y las manijas de archivos duraderas sobreviven a breves interrupciones de la red, lo que ocurre frecuentemente con las redes inalámbricas, por ejemplo.

SMB 2.0 también añade una funcionalidad importante: se introducen vínculos simbólicos, los identificadores de archivos de 128 bits mejoran el rendimiento y permiten archivos más grandes, se mejora la seguridad y el cliente puede almacenar en caché las propiedades de los archivos. A medida que los clientes de Windows adoptaron Vista y se implementó Windows Server 2008, SMB 2.0 se hizo cargo gradualmente del mundo de Windows.

Aunque las diversas implementaciones del CIFS continuaron en un uso generalizado, sus días fueron contados. SMB 2.0 era simplemente demasiado bueno para ignorarlo, y Microsoft publicó suficientes detalles de implantación para permitir que aparecieran clientes y servidores de terceros totalmente compatibles.

Hoy en día, la gran mayoría de los servidores NAS y clientes soportan SMB 2.0, aunque CIFS generalmente todavía se ofrece como reserva. Apple hizo ondas cuando Mac OS X 10.7 «Lion» volcó sin contemplaciones el soporte CIFS, pero la mayoría de los dispositivos eran totalmente capaces de soportar SMB 2.0 de todos modos. Desde entonces, Microsoft ha introducido SMB 2.1 (en Windows 7 y Server 2008 R2), luego lanzó SMB 3 como parte de Windows 8 y Windows Server 2012, pero eso es una historia para otro día.

En la actualidad, los servicios de impresión y el SMB para compartir archivos son el pilar de las redes de Microsoft.

SMB fue originalmente diseñado para trabajar a través del protocolo NetBIOS, el cual a su vez trabaja sobre NetBEUI, IPX/SPX o NBT, aunque también puede trabajar directamente sobre TCP/IP.

6.2 Funcionamiento de SMB

Se basa en la estructura cliente-servidor, donde el cliente formula una solicitud y el servidor envía su respuesta. El servidor tiene su sistema de archivos y otros recursos, disponibles para los clientes sobre la red. Por su parte los clientes, independiente de su almacenamiento interno, pueden tener acceso al sistema de archivos e impresoras del servidor. Los clientes se conectan al servidor usando TCP/IP, NetBIOS e IPX/SPX. Una vez que la conexión está establecida, el cliente envía comandos (llamados SMB's) al servidor para trabajar con el sistema de archivos.

6.3 Samba

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que computadoras con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows.

Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

Entre los sistemas tipo Unix en los que se puede ejecutar Samba, están las distribuciones GNU/Linux, Solaris y las diferentes variantes BSD entre las que podemos encontrar el Mac OS X Server de Apple.

6.4 Características de samba

Samba es una implementación de servicios y protocolos, entre los que están: NetBIOS sobre TCP/IP (NetBT), SMB (también conocido como CIFS), DCE/RPC o más concretamente, MSRPC, el servidor WINS también conocido como el servidor de nombres NetBIOS (NBNS), la suite de protocolos del dominio NT, con su Logon de entrada a dominio, la base de datos del gestor de cuentas seguras (SAM), el servicio Local Security Authority (LSA) o autoridad de seguridad local, el servicio de impresoras de NT y recientemente el Logon de entrada de Active Directory, que incluye una versión modificada de Kerberos y una versión modificada de LDAP. Todos estos servicios y protocolos son frecuentemente referidos de un modo incorrecto como NetBIOS o SMB.

A partir de la versión 4.10.0 ofrece soporte completo para Python 3 y aunque mantiene compatibilidad con Python 2, esta debe ser configurada de manera explícita; sin embargo, a futuro, dicho soporte a Python 2 será retirado.

6.5 Que ofrece samba

SAMBA nos ofrece múltiples posibilidades como ser:

- Acceso a carpetas compartidos por otras máquinas y compartir carpetas de la propia máquina
- Compartir impresoras a través de la red y acceder a las que estén compartidas

Temas Especiales

- Inicio de sesión mediante Active Directory
- Ejercer el rol de controlador de dominio o de un cliente más en redes Windows

Es tan completo que hasta permite que un equipo con Linux... ¡sea Controlador de Dominio de una red Windows! Por supuesto también funciona como un simple miembro del Dominio, ya sea de una red estilo NT o de una basada en Active Directory. Sin embargo, para un uso simple, a veces, es conveniente prescindir del Dominio y utilizar una red del tipo "Grupo de Trabajo", mucho más sencilla y, por lo tanto, más adecuada para este fin, pero sin olvidar que podemos usarla del otro modo.

6.6 Funcionamiento de samba

Samba implementa los protocolos NetBIOS y SMB. A su vez utiliza dos demonios (programas que se ejecutan en segundo plano): smb y nmb.

- **smb** (Samba Daemon): Permite la compartición de archivos e impresoras sobre una red SMB, y proporciona autentificación y autorización de acceso para clientes SMB; ofrece los dos modos de compartición de recursos existentes en Windows:
 - Modo basado en usuarios o modo user (propio de los dominios Windows NT o 2000 y posteriores)
 - Modo basado en recursos o modo share (propio de Windows 3.11/95/98/Milenium y posteriores)
- **nmb** (Network Management DataBase): Permite que el sistema Unix participe en los mecanismos de resolución de nombres propios de Windows (WINS), lo que incluye:
 - Anuncio en el grupo de trabajo.
 - Gestión de la lista de ordenadores del grupo de trabajo.
 - Contestación a peticiones de resolución de nombres.
 - Anuncio de los recursos compartidos.

6.7 Uso de Samba

Para usar Samba se deben configurar los directorios de Unix/GNU-Linux como recursos compartidos a través de una red, para así permitir que los clientes puedan acceder a la información.

Para poder compartir archivos y impresoras, para que otros usuarios puedan acceder a estos desde otros equipos, deberemos:

- Instalar al menos el software común de cliente y servidor y el software servidor de samba
- Dar permiso de acceso a los puertos que usa samba.
- Habilitar y levantar los dos demonios (servicios) que usa samba bajo Gnu/Linux.
- Crear las carpetas que queremos compartir y cambiarles el contexto al contexto que reconoce samba
- Colocar dentro de esas carpetas lo que queremos compartir (archivos y directorios).
- De ser necesario, si quiere restringir el acceso por usuario, crear en el sistema operativos los usuarios a los que se les permitirá acceder a estos recursos compartidos, para luego asignar contraseña a nivel de samba a estos usuarios. Pero si su carpeta será de acceso público, no necesita hacer esto.

Temas Especiales

- De ser necesario, dar los permisos de acceso que se requieran a estas carpetas que vamos a compartir.
- Finalmente publicar las carpetas que se esta compartiendo y los permisos de acceso que debe controlar samba a través del archivo /etc/samba/smb.conf.

Si queremos poder acceder a recursos compartidos en otros equipos que usan Windows (con smb) o en con otros equipos que usan o Gnu/Linux (con SAMBA) deberemos instalar el software común de cliente y servidor; y el software para cliente samba. Luego podremos acceder usando el manejador de archivo Nautilus disponible en Rocky Linux, o desde consola utilizando el comando smbclient o el comando mount.

6.8 Inconvenientes de SMB y Samba

Compartir archivos con otros ordenadores conectados a la red a través de cualquiera de estos protocolos es muy sencillo y cómodo. Sin embargo, también es realmente peligroso. Lo primero que debemos tener en cuenta es que el tráfico SAMBA/SMB/CIFS no está cifrado. Cualquiera capaz de interceptar nuestras comunicaciones, como un pirata en un ataque MITM o incluso nuestro ISP, puede interceptar todos los archivos que enviamos y recibimos. Además, si no usamos contraseña para controlar el acceso al servidor cualquiera podría acceder a él, lo mismo que si la usamos esta viajará por la red en texto plano, sin cifrar. Por estas razones y algunos otros huecos de seguridad de estos protocolos, a lo sumo solo se aconseja utilizar en redes local privadas, pero no en redes públicas y menos en internet.

6.9 Paquetes a instalar en Rocky Linux

Si queremos trabajar con samba en un servidor que corre Rocky Linux, deberemos instalar los siguientes paquetes: samba, samba-client y samba-common. Estos paquetes están en el DVD todo en uno que hemos estado usando.

- samba: Servidor SMB.
- samba-client: Diversos clientes para el protocolo SMB.
- samba-common: Archivos necesarios para cliente y servidor.

6.10 Permisos en firewall de Rocky Linux

En el firewall para la zona de seguridad que requiera (en nuestro caso utilizaremos la zona **public**) si esta configurando un servidor es necesario abrir los puertos 137/udp, 138/udp, 139/tcp y 445/tcp. Si esta configurando un cliente es necesario abrir los puertos 137/udp y 138/udp. La forma más fácil es agregando el servicio samba al firewall del siguiente modo:

- `firewall-cmd --permanent --zone=public --add-service=samba`
- `firewall-cmd --reload`

6.11 Iniciar el servicio y añadirlo al arranque del sistema

Los servicios que debemos iniciar y agregar en el Sistema de arranque automático son: smb y nmb

- `systemctl start smb`
- `systemctl start nmb`
- `systemctl enable smb`

- `systemctl enable nmb`

6.12 Cuentas de usuario en samba

La gestión de usuarios de samba se realiza con el comando `smbpasswd`. Con dicho comando, entre otras cosas podremos crear y eliminar usuarios, cambiar su contraseña, etc.

6.12.1 Creación de un usuario de samba

Para crear un usuario de samba debemos utilizar el comando `smbpasswd`, pero antes debemos haber creado el usuario en Linux. Ejemplo, supongamos que queremos crear en Linux al usuario `pepe`, para esto en una consola de comandos donde estemos con el usuario `root` ejecutamos:

```
useradd pepe
```

Esto creará solo el usuario Linux y le permitirá acceder al sistema por ejemplo por `ssh`, claro que previamente deberemos asignarle un password. Pero si queremos crear el usuario `pepe`, pero que no pueda ingresar al sistema Linux, entonces no deberemos crearlo de la anterior manera, si no así:

```
useradd -s /sbin/nologin pepe
```

Sin importar de que forma creamos el usuario `pepe`, si deseamos que `pepe` pueda disfrutar de los servicios samba, debemos crear a `pepe` como usuario de samba ejecutando el siguiente comando en una consola donde estemos con el usuario `root`:

```
smbpasswd -a pepe
```

Con la opción `-a` indicamos que añada al usuario. Acto seguido nos preguntará dos veces la contraseña que deseamos poner al usuario. Lo razonable es que sea la misma contraseña que tiene el usuario en Linux, pero puede ser otra.

6.12.2 Eliminar un usuario de samba

Para eliminar un usuario de samba debemos ejecutar `smbpasswd` con la opción `-x`, ejemplo queremos eliminar el usuario samba `pepe`:

```
smbpasswd -x pepe
```

Inmediatamente el usuario habrá desaparecido de la base de datos de 'usuarios samba' aunque seguirá siendo un usuario de Linux.

6.12.3 Modificación de password de usuario samba

Para modificar el password de un usuario samba que ya existe, también utilizamos el comando `smbpasswd`, pero ya esta vez sin parámetros. Por ejemplo queremos cambiar el password del usuario `pepe` solo a nivel de samba, entonces ejecutamos:

```
smbpasswd pepe
```

Acto seguido nos preguntará dos veces la contraseña que deseamos poner al usuario.

6.13 Grupos de usuarios en samba

Para poder hacer uso de los grupos de usuarios en samba, simplemente creamos un grupo de usuario Linux y luego le agregamos usuarios, que a su vez sean o vayan a ser usuarios samba. Con esto ya podremos usar los grupos para dar acceso a recursos compartidos en nuestro servidor. Por ejemplo, queremos tener los grupos rrhh y contabilidad, entonces ejecutamos como root:

- `groupadd rrhh`
- `groupadd contabilidad`

Ahora queremos tener los usuarios nuevos juan, pablo, maria, yaquelin y pedro, pero no queremos que maria pueda loguearse al sistema. Entonces ejecutamos como root:

- `useradd juan`
- `useradd pablo`
- `useradd -s /sbin/nologin maria`
- `useradd yaquelin`
- `useradd pedro`

Le asignamos usuarios a todos. Si queremos a maria no le ponemos password por que ya la creamos para que no pueda loguearse al sistema operativo. Ejecutamos entonces, como root:

- `passwd juan`
- `passwd pablo`
- `passwd yaquelin`
- `passwd pedro`
- Este seria opcional, si queremos lo hacemos o si no no, porque no hace falta: `passwd maria`

Queremos que juan, maria y pedro sean parte del grupo rrhh, entonces ejecutamos como root:

- `usermod juan -G rrhh`
- `usermod maria -G rrhh`
- `usermod pedro -G rrhh`

Queremos que yaquelin y pablo sean parte del grupo contabilidad, ejecutamos como root:

- `usermod yaquelin -G contabilidad`
- `usermod pablo -G contabilidad`

Finalmente queremos que sean usuarios samba maria, juan y pablo. Entonces como root ejecutamos:

- `smbpasswd -a maria`
- `smbpasswd -a juan`
- `smbpasswd -a pablo`

Con esto ya podremos disponer dar acceso por usuario o grupo a los usuarios maria, juan y pablo cuando quieran usar samba.

6.14 Contexto y permiso de los directorios a compartir con Samba

Para compartir directorios con samba, debemos cambiar el contexto de SELinux para dichos directorios a fin de que este directorio sea considerado como contenido Samba, asignandoles el contexto `samba_share_t`.

Por ejemplo, supongamos que ya existe el directorio `/srv/samba/ejemplo` y también supongamos que queremos compartir con samba este directorio y todo su contenido, para esto antes de hacer las configuraciones necesarias en el archivo de configuración de samba, primero deberemos cambiar el contexto del directorio en SELinux a `samba_share_t` y hacer el cambio permanente. Para esto ejecutamos estas 2 secuencias de comandos:

- `chcon -R -t samba_share_t /srv/samba/ejemplo`
- `semanage fcontext -a -t samba_share_t /srv/samba/ejemplo`

También, supongamos que ya existen los usuarios **estudiante** y **profesor** y el grupo **gruposmb**. Ahora supongamos que queremos darle accesos de lectura, escritura y acceso a estos usuarios a través de samba al directorio `/srv/samba/ejemplo`, para esto ejecutaremos lo siguiente:

- `setfacl -R -m u:estudiante:rwx,u:profesor:rwx,g:gruposmb:rwx /srv/samba/ejemplo`

6.15 Compartir carpetas en samba

En el mismo archivo de configuración de Samba encontrará distintos ejemplos para distintas situaciones particulares. Lo siguiente corresponde a un ejemplo básico:

```
[lo_que_sea]
    comment = Comentario que se le ocurra
    path = /cualquier/ruta/que/desea/compartir
```

Procure que los nombres de los recursos a compartir tengan un máximo de 12 caracteres, utilizando sólo caracteres alfanuméricos de la tabla de caracteres ASCII.

Para compartir una carpeta puede utilizar cualquiera de las siguientes opciones:

- guest ok.- Define si se permitirá el acceso como usuario invitado. El valor puede ser Yes o No.
- public.- Es un equivalente de guest ok, es decir define si se permitirá el acceso como usuario invitado. El valor puede ser Yes o No.
- browsable.- Define si se permitirá mostrar este recurso en las listas de recursos compartidos. El valor puede ser Yes o No.
- writable.- Define si se permitirá la escritura. Es la opción contraria de read only. El valor puede ser Yes o No. Ejemplos: «writable = Yes» es lo mismo que «read only = No». Obviamente «writable = No» es lo mismo que «read only = Yes»
- valid users.- Define los usuarios o grupos, que podrán acceder al recurso compartido. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: fulano, mengano, @administradores
- write list.- Define los usuarios o grupos, que podrán acceder con permiso de escritura. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: fulano, mengano, @administradores

Temas Especiales

- admin users.- Define los usuarios o grupos, que podrán acceder con permisos administrativos para el recurso. Es decir, podrán acceder hacia el recurso realizando todas las operaciones como super-usuarios. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: fulano, mengano, @administradores
- directory mask.- Es lo mismo que directory mode. Define qué permiso en el sistema tendrán los subdirectorios creados dentro del recurso. Ejemplos: 1777
- create mask.- Define que permiso en el sistema tendrán los nuevos archivos creados dentro del recurso. Ejemplo: 0644
- hosts allow.- Define los host's que tienen permitido acceder al recurso compartido. Se puede colocar la lista de ip's permitidas separadas por un espacio o la ip de red con su máscara. Puede usar este parámetro a nivel global si lo desea
- hosts deny.- Define los host's que no tienen permitido acceder al recurso compartido. Se puede colocar la lista de ip's permitidas separadas por un espacio o la ip de red con su máscara. Puede usar este parámetro a nivel global si lo desea

6.15.1 Ejemplo de compartir una carpeta al público con acceso total

Deberemos crear la carpeta a compartir, por ejemplo:

```
mkdir -p /srv/samba/ejemplo
```

Cambiamos al contexto que necesita samba:

- chcon -R -t samba_share_t /srv/samba/ejemplo
- semanage fcontext -a -t samba_share_t /srv/samba/ejemplo

Asignamos los permisos que queramos a la carpeta, por ejemplo Todo al dueño, lectura y acceso al grupo y lectura y acceso a los demás:

```
chmod -R 0755 /srv/samba/ejemplo
```

Como será de acceso público, asignamos la propiedad de la carpeta al usuario nobody y al grupo nobody:

```
chown -R nobody:nobody /srv/samba/ejemplo
```

Copiamos en esta carpeta todo lo que se quiera compartir.

Sacamos backup al archivo /etc/samba/smb.conf

Editamos el archivo smb.conf y nos aseguramos que:

- i. En la sección [global]
 - a. Si existe el parámetro **workgroup** en esta sección, nos aseguramos tenga el valor del nombre del grupo que queremos de computadores que queremos usar. Si no existe el parámetro en esta sección lo agregamos y le ponemos su valor. Si no sabe que grupo ponerle y quiere usar el mismo grupo que las computadoras Windows, fíjese en la siguiente sección como ver el nombre de grupo de un equipo Windows por consola.

Temas Especiales

- b. Si existe el parámetro **netbios name** en esta sección, nos aseguramos que tenga el nombre con que queremos que aparezca nuestro servidor en la red Windows. Si no existe el parámetro agregarlo y poner el valor que deseemos usar como nombre de computador en la red Windows.
 - c. Si no existe el parámetro **map to guest** en esta sección, nos aseguramos que tenga el valor **bad user** para que nos permita utilizar usuarios invitados para acceder a los recursos así configurados. Si no existe el parámetro en la sección global, agregarlo y poner el valor ya mencionado.
 - d. Si existe el parámetro **security** en esta sección, nos aseguramos tenga el valor del **user**, porque utilizaremos usuarios como mecanismo de validación de acceso. Si no existe el parámetro en esta sección lo agregamos y le ponemos su valor ya mencionado.
 - e. Si existe el parámetro **dns proxy** en esta sección, nos aseguramos tenga el valor del **No**, porque no queremos que samba use el servidor dns, pero si queremos que lo use le ponemos **Yes**. Si no existe el parámetro en esta sección lo agregamos y le ponemos su valor ya mencionado.
 - f. Grabamos el archivo
- ii. Supongamos que queremos compartir la carpeta con el nombre público. Entonces editamos el archivo, nos vamos al final del mismo y le agregamos

```
1 [publico]
2     comment = Carpeta compartida a todos
3     browseable = Yes
4     path = /srv/samba/ejemplo
5     guest ok = Yes
6     read only = No
7     create mask = 0755
```

Que estamos haciendo:

- a. Línea 1: Nombre con el que aparece el recurso compartido
- b. Línea 2: Comentario que aparecerá como descripción
- c. Línea 3: Para que el recurso compartido sea listado al usuario. Si no hacemos esto el usuario no lo verá, pero si sabe cómo se llama el recurso compartido aun así podrá acceder
- d. Línea 4: Indicamos que carpeta es la que estamos compartiendo en nuestro servidor
- e. Línea 5: Indicamos que está permitido el acceso a los usuarios invitados, es decir, los no autenticados
- f. Línea 6: Para decirle que no solo podrá llevarse archivos, sino que también podrá agregar a la carpeta más archivos y/o carpetas. Si solo queremos que pueda copiarse el contenido le damos el valor **Yes**
- g. Línea 7: Los permisos sobre la carpeta: Acceso total al dueño, Lectura y Acceso al Grupo y Lectura y Acceso a los demás

- iii. Reiniciamos el servidor samba y probamos. Recuerdo en samba se reinician 2 servicios.

NOTA: Si desea verificar que configuración está tomando samba, antes de reiniciar los servicios, ejecute como root el comando **testparm**, verifica lo que se imprime en pantalla si es lo que usted desea configurar. Si está bien reinicia los servicios, si no está bien, primero deberá corregir la configuración antes de reiniciar los servicios.

6.15.2 Ejemplo de compartir una carpeta restringida a usuarios validos

Deberemos crear la carpeta a compartir, por ejemplo:

```
mkdir -p /srv/otro/ejemplo
```

Cambiamos al contexto que necesita samba:

- `chcon -R -t samba_share_t /srv/otro/ejemplo`
- `semanage fcontext -a -t samba_share_t /srv/otro/ejemplo`

Creamos el grupo de usuario, luego creamos usuarios Linux y luego creamos sus usuarios samba asignándole el respectivo password. Creemos por ejemplo el grupo **gruposmb1** y los usuarios samba **estudiante, juan, pepe y cato**. Agreguemos los usuarios **estudiante** y **juan** al grupo **gruposmb1**.

Utilizamos el comando setfacl como se explico en el apartado **6.8** para darle acceso total al grupo **gruposmb1** y al usuario **pepe**.

Asignamos acceso total como permisos a la carpeta:

```
chmod -R 0777 /srv/otro/ejemplo
```

Y luego utilizamos el comando setfacl para dar establecer los permisos de acceso al directorio a compartir para los usuarios y grupos que vamos a utilizar en nuestra configuración de samba para este directorio. En nuestro ejemplo serian para el grupo **gruposmb1** y el usuario **pepe**

Copiamos en esta carpeta todo lo que se quiera compartir o la dejamos vacia.

Sacamos backup al archivo /etc/samba/smb.conf

Editamos el archivo smb.conf y nos aseguramos que:

- i. En la sección [global]
 - a. Si existe el parámetro **workgroup** en esta sección, nos aseguramos tenga el valor del nombre del grupo que queremos de computadores que queremos usar. Si no existe el parámetro en esta sección lo agregamos y le ponemos su valor. Si no sabe que grupo ponerle y quiere usar el mismo grupo que las computadoras Windows, fíjese en la siguiente sección como ver el nombre de grupo de un equipo Windows por consola.
 - b. Si existe el parámetro **netbios name** en esta sección, nos aseguramos que tenga el nombre con que queremos que aparezca nuestro servidor en la red Windows. Si no existe el parámetro agregarlo y poner el valor que deseemos usar como nombre de computador en la red Windows.
 - c. Si no existe el parámetro **map to guest** en esta sección, nos aseguramos que tenga el valor **bad user** para que nos permita utilizar usuarios invitados para acceder a los recursos así configurados. Si no existe el parámetro en la sección global, agregarlo y poner el valor ya mencionado.
 - d. Si existe el parámetro **security** en esta sección, nos aseguramos tenga el valor del **user**, porque utilizaremos usuarios como mecanismo de validación de acceso. Si no

- existe el parámetro en esta sección lo agregamos y le ponemos su valor ya mencionado.
- e. Si existe el parámetro **dns proxy** en esta sección, nos aseguramos tenga el valor del **No**, porque no queremos que samba use el servidor dns, pero si queremos que lo use le ponemos **Yes**. Si no existe el parámetro en esta sección lo agregamos y le ponemos su valor ya mencionado.
 - f. Grabamos el archivo
- ii. Supongamos que queremos compartir la carpeta con el nombre protegido. Entonces editamos el archivo, nos vamos al final del mismo y le agregamos

```
1 [protegido]
2   path = /srv/otro/ejemplo
3   valid users = @gruposmb1 pepe marta
4   guest ok = No
5   writable = Yes
6   browsable = Yes
```

Que estamos haciendo:

- a. Linea 1: Nombre con el que aparece el recurso compartido
 - b. Linea 2: Indicamos que carpeta es la que estamos compartiendo en nuestro servidor
 - c. Linea 3: Para indicarle quienes tiene acceso. En este caso el gruposmb1 y el usuario pepe. Los grupos se especifican con @por delante y los usuarios sin @
 - d. Linea 4: Indicamos que no está permitido el acceso a los usuarios invitados, es decir, los no autenticados
 - e. Linea 5: Para decirle que no solo podrá llevarse archivos, sino que también podrá agregar a la carpeta más archivos y/o carpetas.
 - f. Linea 6: Para que el recurso compartido sea listado al usuario. Si no hacemos esto el usuario no lo verá, pero si sabe cómo se llama el recurso compartido aun así podrá acceder
- iii. Reiniciamos el servidor samba y probamos. Recuerdo en samba se reinician 2 servicios.

NOTA: Si desea verificar que configuración está tomando samba, antes de reiniciar los servicios, ejecute como root el comando **testparm**, verifica lo que se imprime en pantalla si es lo que usted desea configurar. Si esta bien reinicia los servicios, si no esta bien, primero deberá corregir la configuración antes de reiniciar los servicios.

6.16 Ocultando archivos que inician con punto.

Es poco conveniente que los usuarios puedan acceder, notando la presencia de archivos ocultos (archivos de configuración, por lo general), es decir archivos cuyo nombre comienza con un punto, como es el caso del directorio de inicio del usuario en el servidor Samba (.bashrc, .bash_profile, .bash_history, etc.). Puede utilizarse la opción **hide dot files**, con el valor Yes, para mantenerlos ocultos en la sección del recurso compartido donde quiera ocultar los archivos cuyo nombre inician con punto.

6.17 Compartir el directorio de inicio de un usuario

Esta configuración viene establecida por defecto en el archivo de configuración de samba, pero para que tenga efecto debe habilitar la directiva respectiva en SELinux de su servidor samba. Para esto como root ejecutamos:

```
setsebool -P samba_enable_home_dirs=1
```

Luego reiniciamos los servicios samba y cuando probemos acceder con un usuario veremos que también nos mostrara su directorio de inicio en el servidor samba.

Si quiere deshabilitar esto, siemplemente ejecute:

```
setsebool -P samba_enable_home_dirs=0
```

Si desea ver como hace samba para compartir los directorios de inicio de los usuarios busque la sección **homes** en el archivo de configuración de samba.

6.18 Compartir impresoras en samba

Las impresoras se comparten de modo predeterminado y sólo hay que realizar algunos ajustes. Si se desea que se pueda acceder hacia la impresora como usuario invitado sin contraseña, añada **public = Yes** — es lo mismo que agregar **guest ok = Yes**— en la sección de impresoras. La sección impresora esta identificado asi: [printers]

Es decir, edite el archivo /etc/samba/smb.conf:

```
[printers]
comment = El comentario que guste.
path = /var/spool/samba
printable = Yes
browseable = No
writable = No
printable = yes
public = Yes
```

Luego simplemente reinicie los servicios de samba

6.19 Conectarse a un recurso compartido desde Rocky Linux

Para hacer la prueba necesitamos de otro equipo con Linux. Supongamos que contamos con un servidor 2 que tiene instalado Rocky Linux y que también ya tiene instalado el software cliente de samba (samba-client). Supongamos que ya estamos en ese otro servidor.

No olvide que para acceder al servidor samba debe usar las cuentas sambas que creo en el servidor samba, no las que tiene en el segundo servidor.

6.19.1 Cliente Linux samba usando mount

Una primera forma es montando el recurso compartido en nuestro servidor samba, dentro de una carpeta de nuestro segundo servidor. Para esto podemos realizar en una consola como root lo siguiente:

- i. Crear una carpeta donde montar el recurso compartido, por ejemplo:
`mkdir /mnt/protegido_compartido`
- ii. Luego ejecutamos el comando mount para montar el recurso compartido en esta carpeta. Supongamos que queremos compartir el recurso protegido que esta compartido por samba en el servidor samba que tiene la ip 10.23.3.48, utilizando el usuario pepe. Entonces para hacer esto en nuestro servidor 2, ejecutamos como root:

Temas Especiales

- ```
mount -t cifs -o username=pepe //10.23.3.48/protegido /mnt/protegido_compartido
```
- iii. El comando anterior nos pedirá el password de pepe
  - iv. Una vez montado el recurso, podemos ir al directorio creado en el punto i. y veremos que podremos ver todo lo que nos han compartido y si tenemos permisos podremos poner otros archivos y/o carpetas

Para desmontar el recurso salgase de la carpeta y ejecute como root el comando:

```
umount /mnt/protegido_compartido
```

### 6.19.2 Cliente Linux samba usando smbclient

Una segunda forma es utilizando el comando smbclient, para lo cual deberemos ejecutar:

```
smbclient //servidor/recurso -U usuario
```

Donde:

- servidor, es el nombre o ip del servidor samba
- recurso, es el nombre con el que se comparte el recurso al que queremos acceder
- usuario, es el login de la cuenta con la que queremos acceder al servidor samba.

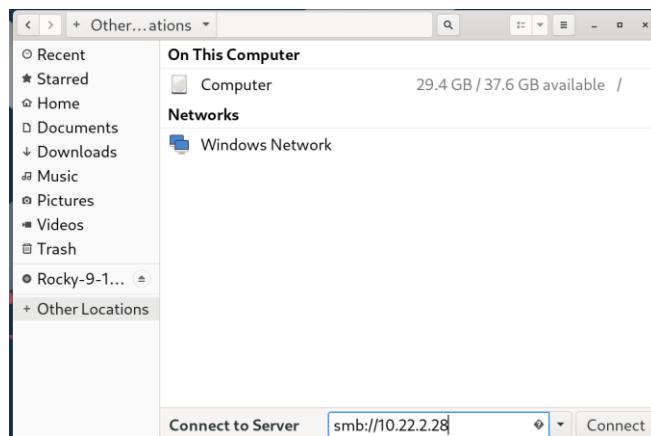
Luego de ejecutar este comando nos pedirá la contraseña del usuario y estaremos conectados si aparece el prompt **smb: \>**

Una vez conectados podremos trabajar como se lo hace cuando trabajamos con ftp. Para salir del recurso, solo digitamos exit y luego presionamos la tecla ENTER.

### 6.19.3 Cliente Linux para samba usando Nautilus

Desde Linux para conectarnos a un servidor samba en modo gráfico, podemos utilizar el manejador de archivo disponible en Rocky Linux, conocido como Nautilus o algún otro cliente samba disponible para este sistema.

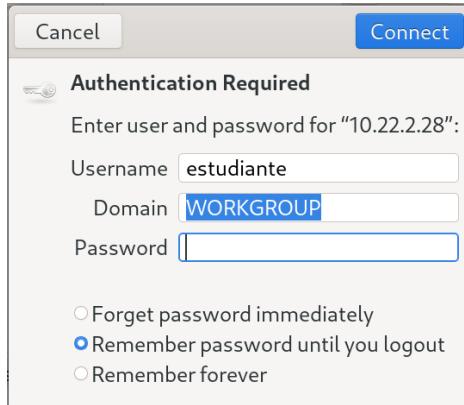
Por ejemplo con Nautilus, abrimos el programa y hacemos clic en **Other Locations**, y en el cuadro de texto Connect to Server, ingresamos **smb://ip\_del\_servidor** y luego hacemos clic en connect, como se muestra en la siguiente figura:



## Temas Especiales

---

Esto hará que se nos presente la ventana para ingresar los datos del usuario con el que accedemos al servidor samba. Ingresamos la cuenta de usuario con el que queremos ingresar, el grupo o dominio al que pertenece la cuenta de usuario, el password del usuario y el tipo tiempo en que se recordará la contraseña, para luego hacer clic en Connect. Por ejemplo:



Una vez validado nuestro acceso nos mostrará los archivos y carpetas a los que tenemos acceso.

Al seleccionar alguna de las carpetas validará el acceso dependiendo de que cuenta ingresamos en la ventana de validación de acceso.

### 6.20 Conectarse a un recurso compartido desde Windows

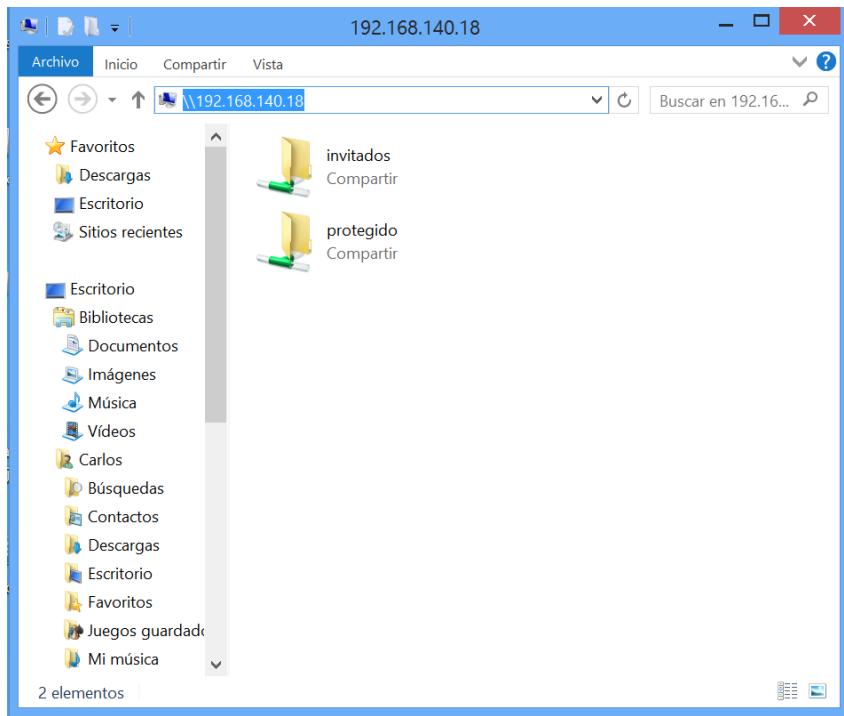
Podemos usar 2 formas de acceder a un recurso compartido desde Windows. Una es con el explorador de windows y otra desde la consola

#### 6.20.1 Cliente Windows Samba usando explorador de Windows

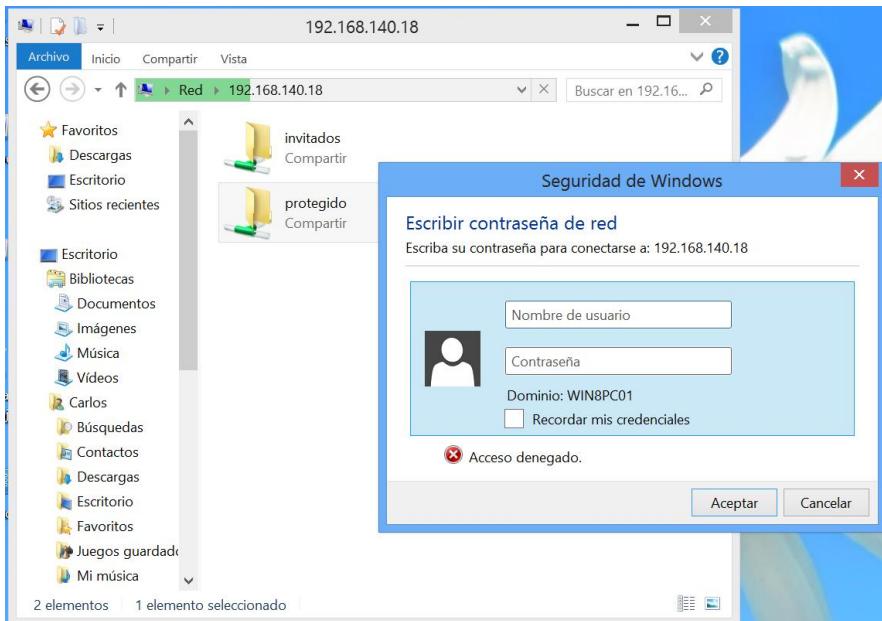
En windows usted podrá usar el explorador de windows para acceder a un recurso. Basta iniciar el explorador de windows y colocar la dirección del servidor samba para acceder a la lista de recursos o la dirección del servidor y el recurso para acceder directo al recurso. En cualquier caso, si la carpeta requiere validación de usuario nos lanzara la Ventana para ingresar usuario y password.

Por ejemplo:

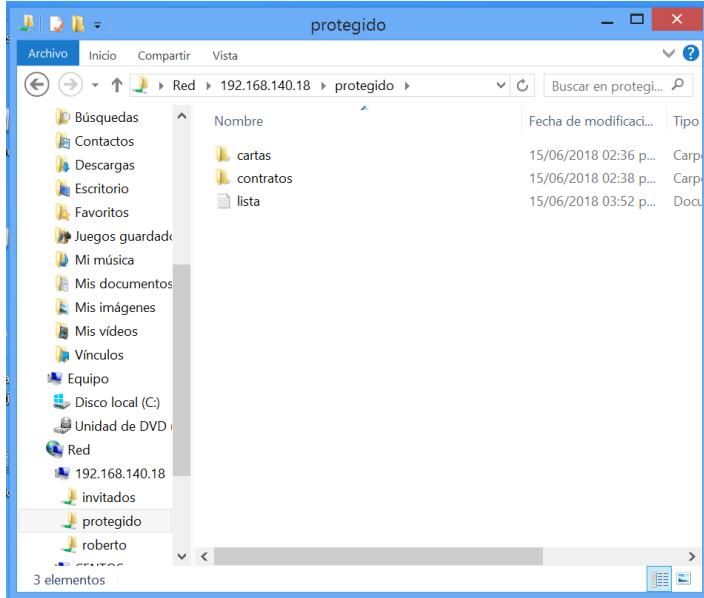
## Temas Especiales



Si hacemos clic en uno de los recursos y este requiere validación de usuario, entonces Windows nos mostrará lo siguiente para ingresar usuario y password:



Una vez ingresamos los datos del usuario a utilizar, hacemos clic en aceptar y el servidor samba valida nuestro acceso, entonces el explorador de Windows nos mostrará lo que hay dentro del recurso compartido



### 6.20.2 Cliente Windows Samba usando consola de comandos

Por comandos en Windows podemos conectarnos a un recurso conocido en un servidor. Para esto usamos en consola de Windows el comando **net use** del siguiente modo:

```
net use unidad: \\servidor\recurso /user:usuario
```

Donde:

- unidad, es la letra de la unidad en la que se quiere habilitar en Windows el recurso compartido al que queremos tener acceso
- servidor, es el nombre o ip del servidor samba
- recurso, es el nombre con el que se comparte el recurso al que queremos acceder
- usuario, es el login de la cuenta con la que queremos acceder al servidor samba.

Por ejemplo supongamos que queremos acceder al recurso protegido que esta compartido en el servidor con ip 10.23.3.48, con el usuario samba pepe y queremos habilitar la unidad H con este recurso (se asume que la unidad H no esta ocupada), entonces ejecutaríamos en una consola de Windows:

```
net use H: \\10.23.3.48\protegido /user:pepe
```

Esto nos pedirá el password de pepe, una vez ingresado presionamos ENTER y ya podremos ir a la unidad H por consola o con el explorador de Windows para ver que tenemos dentro del recurso compartido.

Si luego ejecutamos en consola de Windows, solo: **net use** la consola nos mostrará que recursos compartidos en otros computadores tenemos disponibles y en que unidad.

Si queremos desactivar un recurso compartido en Windows por consola ejecutamos:

```
net use unidad: /delete
```

## Temas Especiales

---

Donde:

- unidad, es la letra de la unidad donde esta ya habilitada un recurso compartido y queremos proceder a deshabilitar.

### NOTA:

Para este servicio puede hacer seguimiento a traves del archivo **messages** que esta en el directorio **/var/log**

## Bibliografía

- (1) Configuración De Servidores Con GNU/Linux, Joel Barrios Dueñas, 2017
- (2) <https://docs.rockylinux.org/>
- (3) <http://www.pathname.com/fhs/pub/fhs-2.3.pdf>
- (4) [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9)
- (5) <https://es.wikipedia.org/wiki/LibreOffice>
- (6) Primeros Pasos con LibreOffice, Juan C. Sanz y Jorge A. Guzman Soriano, 2012
- (7) <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-bind-namedconf.html>
- (8) <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-samba-servers.html>