



Servidor DNS

Despliegue de Aplicaciones Web

Contenido

1	Bind (Berkeley Internet Name Domain).....	1
2	DNS (DomainNameSystem)	1
3	NIC (Network Information Center).	1
4	FQDN (Fully Qualified Domain Name).	1
5	Componentes de un DNS.	2
5.1	Clientes DNS.....	2
5.2	Servidores DNS.....	2
6	Herramientas de búsqueda y consulta.	4
6.1	Mandato host.....	4
6.2	Mandato dig.....	5
6.3	Mandato jwhois (whois).	5
6.4	Software necesario	6
7	Procedimientos.	6
8	DNS con Webmin	7
8.1	Crear zona primaria	8
8.1.1	Crear dirección (A)	11
8.1.2	Crear alias (CNAME).....	14
8.1.3	Crear Servidor de correo (MX)	16
8.2	Verificar los registros	17
8.3	Crear zona inversa.....	18
8.3.1	Crear puntero (PTR)	21
9	Reiniciar el servicio DNS.....	23
10	Verificar funcionamiento DNS	24
11	DDNS	27

Índice de ilustraciones

ILUSTRACIÓN 1: ACCESO A WEBMIN	7
ILUSTRACIÓN 2: OPCIÓN SERVIDORES.....	8
ILUSTRACIÓN 3: OPCIÓN SERVIDOR DE DNS BIND	8
ILUSTRACIÓN 4: CREAR UNA NUEVA ZONA MAESTRA.....	9
ILUSTRACIÓN 5: CREAR ZONA MAESTRA	9
ILUSTRACIÓN 6: ZONA CREADA.....	10
ILUSTRACIÓN 7 EDITCONFIG FILE.....	10

ILUSTRACIÓN 8 ZONA PRIMARIA EN NAMED.CONF.LOCAL.....	11
ILUSTRACIÓN 9: EDITAR ZONA MAESTRA	11
ILUSTRACIÓN 10 CREAR DIRECCIÓN	12
ILUSTRACIÓN 11 DIRECCIÓN CREADA.....	12
ILUSTRACIÓN 12 ICONO DIRECCIÓN ACTUALIZADO	13
ILUSTRACIÓN 13 EDITAR ARCHIVO DE REGISTROS	13
ILUSTRACIÓN 14 EDICIÓN DEL ARCHIVO DE REGISTRO.....	14
ILUSTRACIÓN 15 ALIAS DE NOMBRE.....	15
ILUSTRACIÓN 16 EDITAR NOMBRE DE ALIAS	15
ILUSTRACIÓN 17 CREACIÓN DE ALIAS	15
ILUSTRACIÓN 18 FICHERO /VAR/LIB/BIND/SERVERDAW.INF.HOSTS	16
ILUSTRACIÓN 19 SERVIDOR DE CORREO	16
ILUSTRACIÓN 20 CREAR REGISTRO MX	16
ILUSTRACIÓN 21 CREADO SERVIDOR DE CORREO	17
ILUSTRACIÓN 22 FICHERO /VAR/LIB/BIND/SERVERDAW.INF.HOSTS	17
ILUSTRACIÓN 23 BOTÓN VERIFICAR REGISTROS.	18
ILUSTRACIÓN 24 MENSAJE DE VERIFICAR REGISTROS	18
ILUSTRACIÓN 25 CREAR ZONA INVERSA	19
ILUSTRACIÓN 26 ZONA INVERSA CREADA.....	19
ILUSTRACIÓN 27 ZONA INVERSA EN /ETC/BIND/NAMED.CONF.LOCAL	20
ILUSTRACIÓN 28 EDITAR ZONA INVERSA	21
ILUSTRACIÓN 29 CREAR DIRECCIÓN INVERSA REGISTROS.....	21
ILUSTRACIÓN 30 DIRECCIÓN INVERSA CREADA.....	22
ILUSTRACIÓN 31 ICONO DIRECCIÓN INVERSA ACTUALIZADO	22
ILUSTRACIÓN 32 EDITAR ARCHIVO DE REGISTRO.....	23
ILUSTRACIÓN 33 EDICIÓN FICHERO /VAR/LIB/BIND/192.168.1.REV.....	23
ILUSTRACIÓN 34 APPLY CONFIGURATION	24
ILUSTRACIÓN 35 REINICIAR EL SERVICIO DNS POR CONSOLA	24
ILUSTRACIÓN 36 COMANDO DIG.....	25
ILUSTRACIÓN 37 COMANDO NSLOOKUP	25
ILUSTRACIÓN 39: ACTIVAR DDNS ROUTER.....	28
ILUSTRACIÓN 40: ABRIR PUERTOS.....	28
ILUSTRACIÓN 41: CREAR CUENTA EN NO-IP.....	28
ILUSTRACIÓN 42: DESCARGAR CLIENTE NO-IP.....	29
ILUSTRACIÓN 43: PROGRAMA CLIENTE NO-IP EN EJECUCIÓN.....	29
ILUSTRACIÓN 44: ACCESO AL SERVIDOR WEB.....	29

1 Bind (Berkeley Internet Name Domain)

BIND (acrónimo de **Berkeley InternetNameDomain**) 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 ampliamente utilizado en la Internet (99% de los servidores DNS) proporcionando una robusta y estable solución.

2 DNS (DomainNameSystem)

DNS (acrónimo de **DomainNameSystem**) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombres de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y 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 **Ciente DNS** seguida por una sola respuesta **UDP** del servidor. **TCP** interviene cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como **transferencia de zonas**.

3 NIC (Network Information Center).

NIC (acrónimo de **NetworkInformation Center** o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominio genérico o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un **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 México es la entidad encargada de gestionar todos los dominios con terminación **.mx**, la cual es la terminación correspondiente asignada a los dominios de México.

4 FQDN (Fully Qualified Domain Name).

FQDN (acrónimo de **FullyQualifiedDomainName** o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

EJEMPLO: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio llamado «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», así es que se define de forma única al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solo puede haber uno llamado «**maquina1.dominio.com.**». La ausencia del punto al final definiría que

se pudiera tratar tan solo de un prefijo, es decir «**maquina1.dominio.com**» pudiera ser un dominio de otro más largo como «**maquina1.dominio.com.mx**».

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. Solo se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-». No se distinguen mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar **IDN** (acrónimo de **I**nternationalized**D**omain**N**ame) 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.

5 Componentes de un DNS.

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

5.1 Clientes DNS.

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

5.2 Servidores DNS.

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

- **Servidor Maestro:** También denominado **Primario**. Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.
- **Servidor Esclavo:** También denominado **Secundario**. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado **transferencia de zona**.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para las zonas de DNS. De acuerdo al [RFC2182](#), 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 forma confiable hacia los **Clientes DNS** a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible 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, no será necesario copiarlos a cada **Servidor Esclavo o Secundario**, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los **Servidores DNS** responden dos tipos de consultas:

- Consultas Iterativas (no recursivas): El cliente hace una consulta al

Servidor DNS y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al **Servidor DNS** que tiene la **Zona de Autoridad** capaz de resolver la consulta.

- **Consultas Recursivas:** El **Servidor DNS** asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el

Cliente DNS. El **Servidor DNS** desarrolla entonces **Consultas Iterativas** separadas hacia otros **Servidores DNS** (en lugar de hacerlo el **Cliente DNS**) para obtener la respuesta solicitada.

5.3 Zonas de Autoridad.

Permiten al **Servidor Maestro o Primario** cargar la información de una zona. Cada **Zona de Autoridad** abarca al menos un dominio y posiblemente sus sub-dominios, si estos últimos no son delegados a otras zonas de autoridad.

La información de cada **Zona de Autoridad** es almacenada de forma local en un fichero en el **Servidor DNS**. Este fichero puede incluir varios tipos de registros:

Tipos de registro	Descripción
A (Address)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv4 de 32 bits.
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv6 de 128 bits.
CNAME (CanonicalName)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtienen los subdominios 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.
PTR (Pointer)	Registro de apuntador que resuelve direcciones IPv4 hacia el nombre anfitriones. Es decir, hace lo contrario al registro A. Se utiliza en zonas de Resolución Inversa
NS (Name Server)	Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio
SOA (Start of Authority)	Registro de inicio de autoridad que especifica 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.

SRV (Service)	Registro de servicios que especifica información acerca de servicios disponibles a través del dominio. Protocolos como SIP (SessionInitiationProtocol) y XMPP (Extensible Messaging and presenceProtocol) suelen requerir registros SRV en la zona para proporcionar información a los clientes.
TXT (Text)	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de registro es muy utilizado por los servidores de listas negras DNSBL (DNS-basedBlackholeList) para la filtración de Spam. Otro ejemplo de uso son las VPN , donde suele requerirse un registro TXT para definir una llave que será utilizada por los clientes.

Las zonas que se pueden resolver son:

Zonas de Reenvío.

Devuelven **direcciones IP** para las búsquedas hechas para nombres **FQDN (Fully Qualified Domain Name)**.

En el caso de dominios públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Reenvío** corresponde a la autoridad misma del dominio, es decir, y por lo general, quien esté registrado como autoridad del dominio tras consultar una base de datos **WHOIS**. Quienes compran dominios a través de un **NIC** (por ejemplo ejemplo: www.nic.mx) son quienes se hacen cargo de las **Zonas de Reenvío**, 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.

Zonas de Resolución Inversa.

Devuelven nombres **FQDN (Fully Qualified Domain Name)** para las búsquedas hechas para **direcciones IP**.

En el caso de segmentos de red públicos, la responsabilidad de que exista de que exista una **Zona de Autoridad** para cada **Zona de Resolución Inversa** corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos.

Los grandes **ISP**, y en algunos casos algunas empresas, son quienes se hacen cargo de las **Zonas de Resolución Inversa**.

6 Herramientas de búsqueda y consulta.

6.1 Mandato host.

El mandato **host** una herramienta simple para hacer búsquedas en **Servidores DNS**. Es utilizada para convertir nombres en direcciones IP y viceversa.

De modo predefinido realiza las búsquedas en las **Servidores DNS** definidos en el fichero **/etc/resolv.conf**, pudiendo definirse opcionalmente el **Servidor DNS** a consultar.

```
host www.cisco.com
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el fichero `/etc/resolv.conf` del sistema, devolviendo como resultado una dirección IP.

```
host www.linuxparatodos.net 200.33.146.217
```

Lo anterior realiza una búsqueda en los **Servidor DNS** en la dirección IP 200.33.146.217, devolviendo una dirección IP como resultado.

6.2 Mandato dig.

El mandato **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.

De modo predefinido realiza las búsquedas en las **Servidores DNS** definidos en el fichero `/etc/resolv.conf`, pudiendo definirse opcionalmente el **Servidor DNS** a consultar. La sintaxis básica sería:

```
dig @servidor nombre TIPO
```

Donde **servidor** corresponde al nombre o dirección IP del **Servidor DNS** a consultar, **nombre** 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 @200.33.146.209 linuxparatodos.net MX
```

Lo anterior realiza una búsqueda en el **Servidor DNS** en la dirección IP 200.33.146.209 para los registros **MX** para el dominio *linuxparatodos.net*.

```
dig linuxparatodos.net NS
```

Lo anterior realiza una búsqueda en los **Servidores DNS** definidos en el fichero `/etc/resolv.conf` del sistema para los registros **NS** para el dominio *linuxparatodos.net*.

```
dig @200.33.146.217 linuxparatodos.net NS
```

Lo anterior realiza una búsqueda en los **Servidor DNS** en la dirección IP 200.33.146.217 para los registros **NS** para el dominio *linuxparatodos.net*.

6.3 Mandato jwhois (whois).

El mandato **jwhois** es una herramienta de consulta a través de servidores **WHOIS**. La sintaxis básica es:

```
jwhois dominio
```


Ejemplo:

```
jwhois linuxparatodos.net
```

Lo anterior regresa la información correspondiente al dominio *linuxparatodos.net*.

6.4 Software necesario

Paquete	Descripción
bind	Incluye el Servidor DNS (named) y herramientas para verificar su funcionamiento.
bind-libs	Biblioteca compartida que consiste en rutinas para aplicaciones para utilizarse cuando se interactúe con Servidores DNS.
bind-chroot	Contiene un árbol de ficheros que puede ser utilizado como una jaula chroot para named añadiendo seguridad adicional al servicio.
bind-utils	Colección de herramientas para consultar Servidores DNS
caching-nameserver	Ficheros de configuración que harán que el Servidor DNS actúe como un caché para el servidor de nombres.

7 Procedimientos.

Idealmente se deben definir primero los siguientes datos:

1. Dominio a resolver.
2. Servidor de nombres principal (SOA). Éste debe ser un nombre que ya esté plenamente resuelto, y debe ser un FQDN (Fully Qualified Domain Name).
3. Lista de todos los servidores de nombres (NS) que se utilizarán por efectos de redundancia. Éstos deben ser nombres que ya estén plenamente resueltos, y deben ser además FQDN (Fully Qualified Domain Name).
4. Cuenta de correo del administrador responsable de esta zona. Dicha cuenta debe existir y no debe pertenecer a la misma zona que se está tratando de resolver.
5. Al menos un servidor de correo (MX), con un registro A, nunca CNAME.
6. IP predeterminada del dominio.

Subdominios dentro del dominio (www, mail, ftp, ns, etc.) y las direcciones IP que estarán asociadas a estos.

Es importante tener bien en claro que los puntos 2, 3 y 4 involucran datos que **deben existir previamente** y estar plenamente resueltos por otro servidor DNS; Lo anterior quiere decir no pueden utilizar datos que sean parte o dependan del mismo dominio que se pretende resolver. De igual modo, el servidor donde se implementará el **DNS** deberá contar con un nombre **FQDN** y que esté previa y plenamente resuelto en otro DNS.

Como regla general se generará una zona de reenvío por cada dominio sobre el cual se tenga autoridad plena y absoluta y se generará una zona de resolución inversa por cada red sobre la cual se tenga plena y absoluta autoridad. es decir, si se es propietario del dominio «*cualquiercosa.com*», se deberá generar el fichero de zona correspondiente a fin de resolver dicho dominio. Por cada red con direcciones IP

privadas sobre la cual se tenga control y plena y absoluta autoridad, se deberá generar un fichero de zona de resolución inversa a fin de resolver inversamente las direcciones IP de dicha zona. Regularmente la resolución inversa de las direcciones es IP públicas es responsabilidad de los proveedores de servicio ya que son estos quienes tienen la autoridad plena y absoluta sobre dichas direcciones IP.

Todos los ficheros de zona deben pertenecer al usuario «named» a fin de que el servicio **named** pueda acceder a estos o bien modificarlos en el caso de tratarse de zonas esclavas.

8 DNS con Webmin

En el explorador de internet pondremos la dirección IP de la máquina Servidor y el puerto de acceso a la aplicación Webmin, 10000.

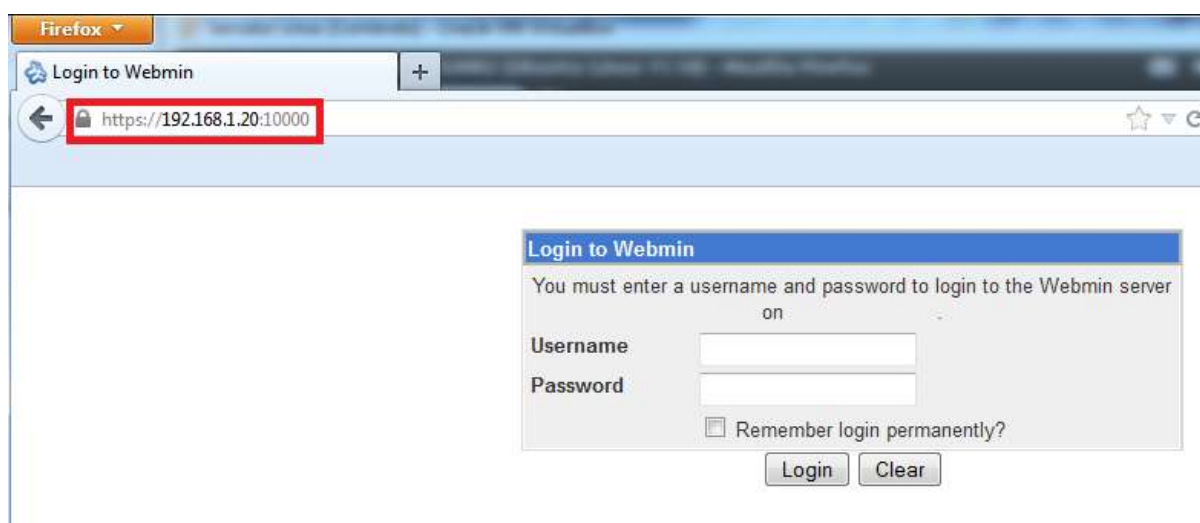


Ilustración 1: Acceso a Webmin

Introducimos el usuario y la contraseña. Aparecerá la pantalla de la *Ilustración 2: Opción Servidores* y se hará click en la opción *Servidores*.

Una vez en la opción de *Servidores*, selecciona *Servidor de DNS BIND* como se muestra en la *Ilustración 3: Opción Servidor de DNS BIND*. Se muestran dos secciones: *Opciones globales del servidor* y *Zonas DNS existentes*.

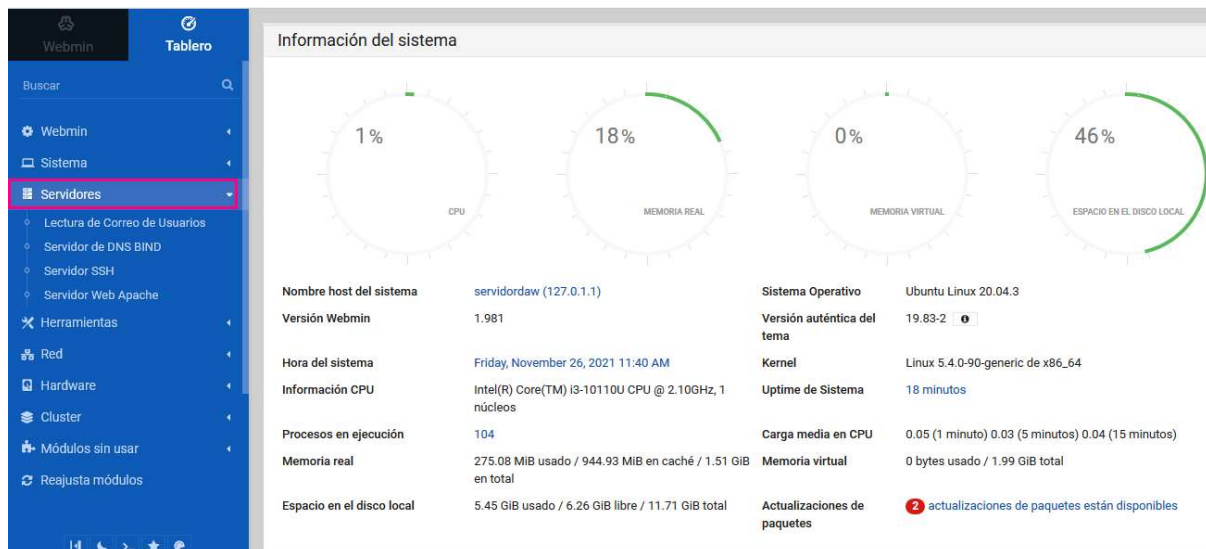


Ilustración 2: Opción Servidores



Ilustración 3: Opción Servidor de DNS BIND

8.1 Crear zona primaria

Para crear una zona primaria se selecciona de la sección *Zonas DNS Existentes* la opción *Crear una nueva zona maestra*, al igual que se muestra en la *Ilustración 4: Crear una nueva zona maestra*.

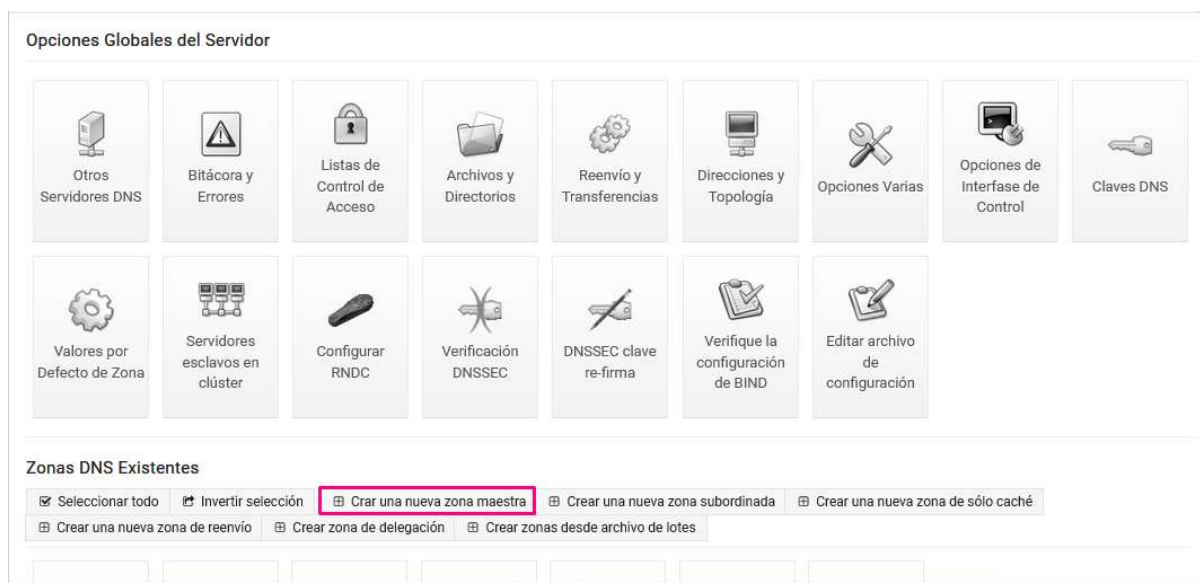


Ilustración 4: Crear una nueva zona maestra

A continuación, se rellenará los campos *Nombre de Dominio/Red* y *Dirección de Correo* y se hará clic en *Crear*, como muestra la *Ilustración 5: Crear Zona Maestra*.



Ilustración 5: Crear Zona Maestra

Si ahora se vuelve a la sección *Zonas DNS Existentes*, aparecerá la zona creada (*Ilustración 6: Zona creada*).



Ilustración 6: Zona creada

Ver cómo se va modificando el fichero `/etc/bind/named.conf.local`. Para ello en la sección *Opciones Globales del Servidor* pulsamos en el icono *Editar archivo de configuración* (Ilustración 7 EditConfig File).

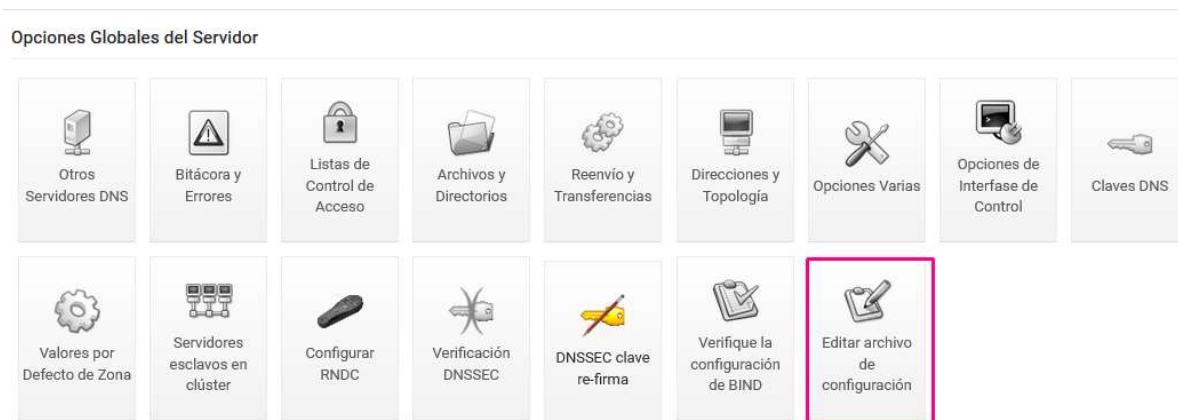


Ilustración 7 EditConfig File

En la pantalla aparecerá un combo con 4 opciones:

- `/etc/bind/named.conf`
- `/etc/bind/named.conf.options`
- `/etc/bind/named.conf.local`
- `/etc/bind/named.conf.default-zones`

Seleccionar el fichero `/etc/bind/named.conf.local` que es el fichero modificado para insertar la zona creada y pulsar botón *Edit* (Ilustración 8 Zona primaria en `named.conf.local`).

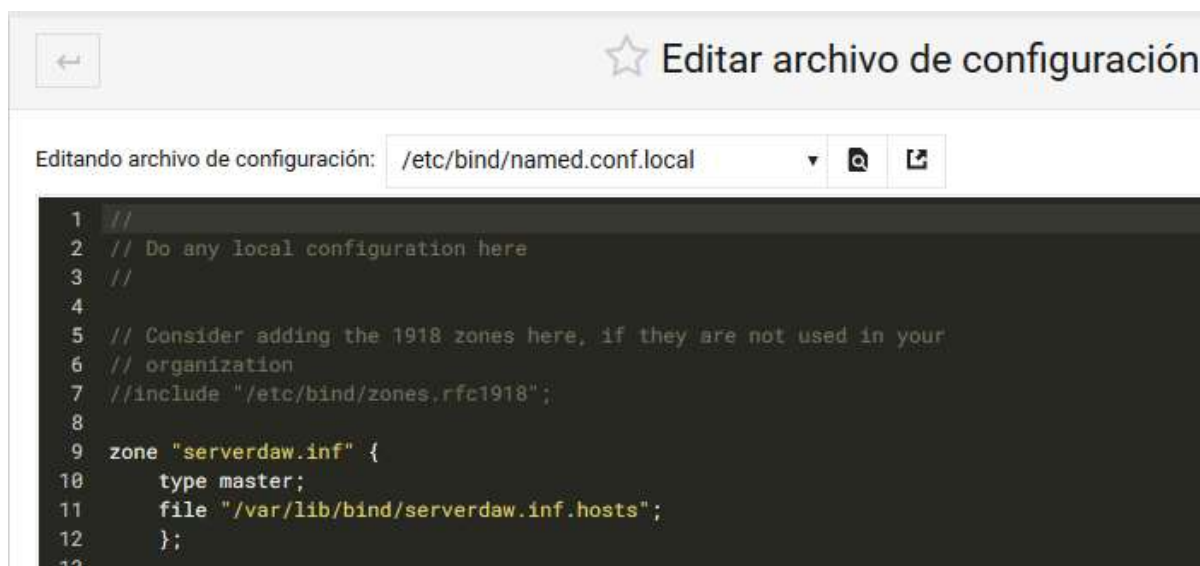


Ilustración 8 Zona primaria en named.conf.local

Observa que la zona es aulasmr2.org (zone “sererdaw.inf”), de tipo maestro (type master) y el fichero de la base de datos de dicha zona será /var/lib/bind/aulasmr2.org.hosts.

8.1.1 Crear dirección (A)

Acceda a la zona creada para añadir direcciones. Las direcciones permiten la conversión de nombres a direcciones IP.



Ilustración 9: Editar Zona Maestra

Hacer click en el icono *Dirección* dónde se podrán el nombre del equipo y su dirección IP (Se podrán crear tantos como se necesiten), para acabar, hacer clic en *Crear*. (Ilustración 10 Crear dirección).

☆ Dirección Registros
En serverdaw.inf

Añadir Registro Dirección

Nombre

Tiempo de vida ☒ Por defecto ☐

Dirección

¿Actualizar Inversas? ☒ Si ☐ No (y reemplazar las existentes)

☐ No

Mostrar registros coincidentes:

Ilustración 10 Crear dirección

Observa la *Ilustración 11 Dirección creada*, como se puede ver, aparece la dirección creada. Se crearan algunas direcciones más. Una vez creada el icono de *Dirección* se actualizará (*Ilustración 12 Icono Dirección actualizado*).

☆ Dirección Registros
En serverdaw.inf

Añadir Registro Dirección

Nombre

Tiempo de vida ☒ Por defecto ☐

Dirección

¿Actualizar Inversas? ☒ Si ☐ No (y reemplazar las existentes)

☐ No

Mostrar registros coincidentes:

☒ Seleccionar todo ☐ Invertir selección

Nombre	TTL	Dirección
<input type="checkbox"/> w10.serverdaw.inf	Por defecto	192.168.0.10

☒ Seleccionar todo ☐ Invertir selección

Ilustración 11 Dirección creada



Ilustración 12 Icono Dirección actualizado

También se puede ver cómo va quedando el fichero de base de datos de la zona directa que se está creando. Para ello haz clic en el icono *Editar Archivo de Registro* de *Editar Zona Maestra* (Ilustración 13 *Editar Archivo de Registros*). Aparecerá la Ilustración 14 *Edición del archivo de registro*, en ella está resaltado en rojo el fichero que se está editando, en este caso es el fichero `aulasmr2.org.hosts` que se encuentra en el directorio `/var/lib/bind`. Este es el directorio por defecto dónde Webmin crea los archivos de base de datos del DNS.

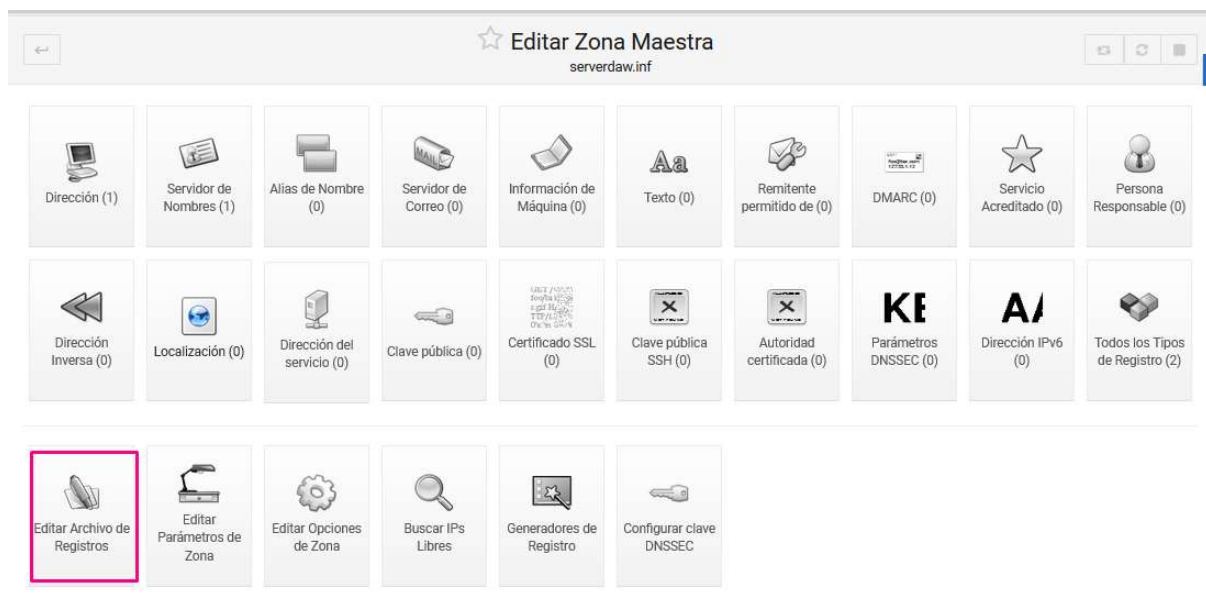


Ilustración 13 Editar Archivo de Registros



Ilustración 14 Edición del archivo de registro

Se pueden observar los tiempos de refresco, reintento, expiración y el mínimo expresados en segundos:

- 10800 es el tiempo de refresco
- 3600 tiempo de reintento de transferencia
- 604800 tiempo de expiración
- 38400 tiempo mínimo, ttl (time to live)

8.1.2 Crear alias (CNAME)

El alias es un sobrenombre de una dirección. Asignaremos el alias *www* a nuestra dirección principal para que todas las llamadas a *www.aulasmr2.org* se redirijan. Para ello se hará click en el icono Alias de Nombre como aparece en la *Ilustración 15 Alias de Nombre*.

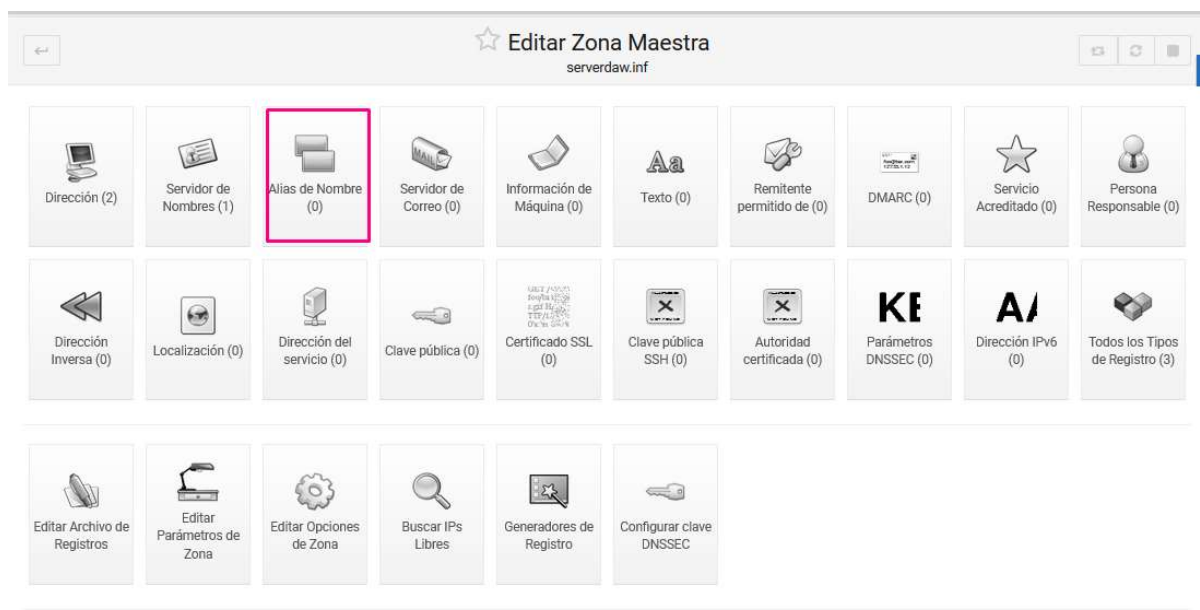


Ilustración 15 Alias de Nombre

Se crea el alias al igual que aparece en la *Ilustración 16 Editar Nombre de Alias*.



Ilustración 16 Editar Nombre de Alias

Al pulsar en salvar se crea el alias. (*Ilustración 17 Creación de Alias*).



Ilustración 17 Creación de Alias

El fichero de la base de datos de la Zona Directa o Primaria, es decir, el archivo `/var/lib/bind/serverdaw.inf.hosts` quedaría como en la Ilustración 18 Fichero `/var/lib/bind/serverdaw.inf.hosts`.

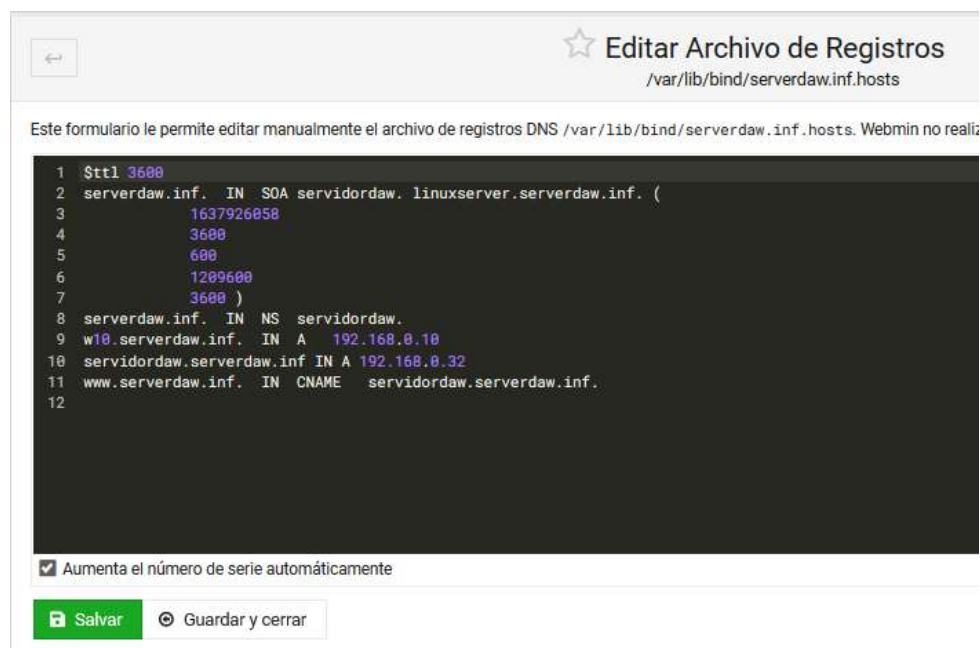


Ilustración 18 Fichero /var/lib/bind/serverdaw.inf.hosts

8.1.3 Crear Servidor de correo (MX)

Hacer click en *Servidor de Correo* (Ilustración 19 Servidor de Correo) para crear un registro MX cuya prioridad será 10 (Ilustración 20 Crear registro MX).

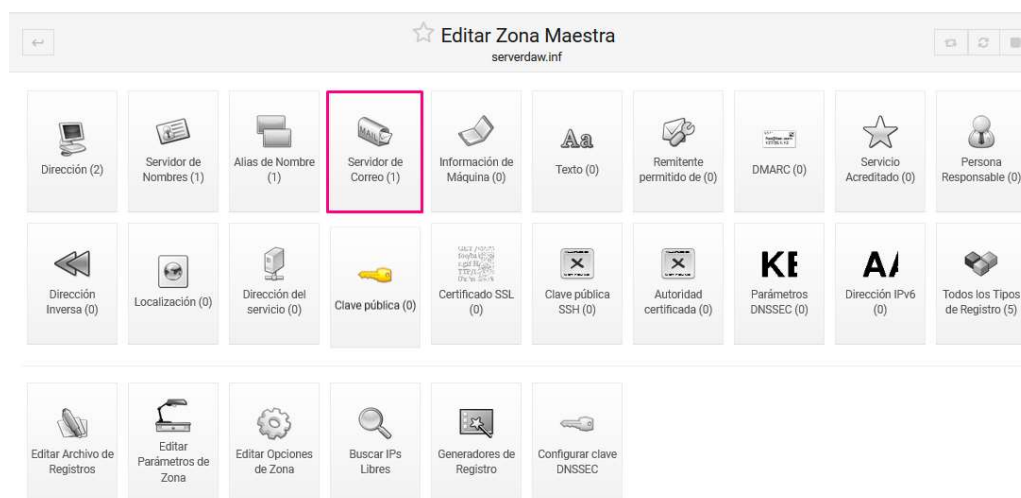


Ilustración 19 Servidor de Correo



Ilustración 20 Crear registro MX

Servidor de Correo Registros
En serverdaw.inf

Añadir Registro Servidor de Correo

Nombre: Tiempo de vida: ☐ segundos

Servidor de Correo: Prioridad:

Mostrar registros coincidentes:

☐ Seleccionar todo ☐ Invertir selección

Nombre	TTL	Prioridad	Servidor de Correo
<input type="checkbox"/> servidordaw.serverdaw.inf.	Por defecto	10	192.168.0.32

☐ Seleccionar todo ☐ Invertir selección

Ilustración 21 Creado Servidor de Correo

El fichero de la base de datos de la Zona Directa o Primaria después de la creación del registro MX quedaría como en la *Ilustración 22 Fichero /var/lib/bind/serverdaw.inf.hosts*.

Editar Archivo de Registros
/var/lib/bind/serverdaw.inf.hosts

Este formulario le permite editar manualmente el archivo de registros DNS /var/lib/bind/serverdaw.inf.hosts. Webmin no realizará

```

1 $ttl 3600
2 serverdaw.inf. IN SOA servidordaw. linuxserver.serverdaw.inf. (
3     1637926059
4     3600
5     600
6     1209600
7     3600 )
8 serverdaw.inf. IN NS servidordaw.
9 w10.serverdaw.inf. IN A 192.168.0.10
10 servidordaw.serverdaw.inf IN A 192.168.0.32
11 www.serverdaw.inf. IN CNAME servidordaw.serverdaw.inf.
12 servidordaw.serverdaw.inf. IN MX 10 192.168.0.32
13

```

☒ Aumenta el número de serie automáticamente

Ilustración 22 Fichero /var/lib/bind/serverdaw.inf.hosts

8.2 Verificar los registros

Para comprobar que los registros creados no tienen errores hacer click en *Verificar registros* dentro de *Editar Zona Maestra*(*Ilustración 23 Botón*).

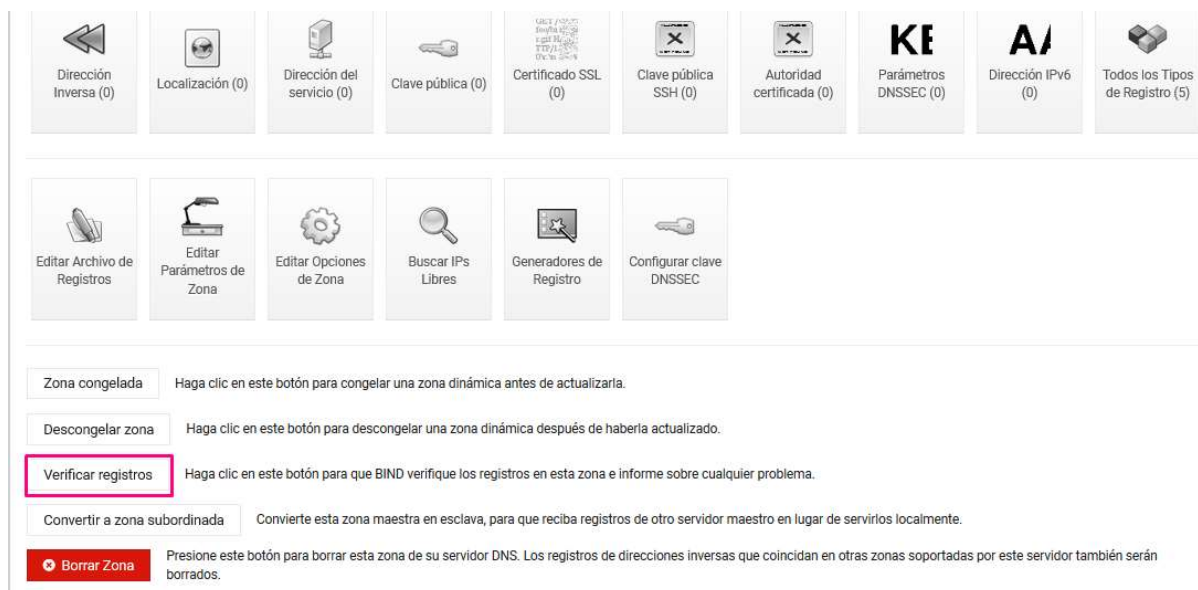


Ilustración 23 Botón Verificar registros.

Si no hay errores aparecerá un mensaje como el de la *Ilustración 24 Mensaje de* .



Ilustración 24 Mensaje de Verificar registros

8.3 Crear zona inversa

Para crear una zona inversa se selecciona de la sección *Zonas DNS Existentes* la opción *Crear una nueva zona maestra*, al igual que se muestra en la *Ilustración 4: Crear una nueva zona maestra*.

A continuación, se seleccionará la opción *Inversas (direcciones a Nombres)* y se rellenará los campos *Nombre de Dominio/Red*, *con la porción de red*, y *Dirección de Correo* y para finalizar pulsar *Crear*, como muestra la *Ilustración 25 Crear Zona Inversa*.

Ilustración 25 Crear Zona Inversa

Si ahora se vuelve a la sección *Zonas DNS Existentes*, aparecerá la zona creada (*Ilustración 26 Zona Inversa creada*)

Ilustración 26 Zona Inversa creada

Ver cómo se va modificando el fichero `/etc/bind/named.conf.local`. Para ello en la sección *Opciones Globales del Servidor* pulsamos en el icono *EditConfig File* (*Ilustración 7 EditConfig File*).

En la pantalla aparecerá un desplegable con 4 opciones:

- `/etc/bind/named.conf`
- `/etc/bind/named.conf.options`
- `/etc/bind/named.conf.local`
- `/etc/bind/named.conf.default-zones`

Seleccionar el fichero `/etc/bind/named.conf.local`, que es el fichero modificado para insertar la zona creada, y pulsar botón *Edit* (*Ilustración 27 Zona inversa en /etc/bind/named.conf.local*).

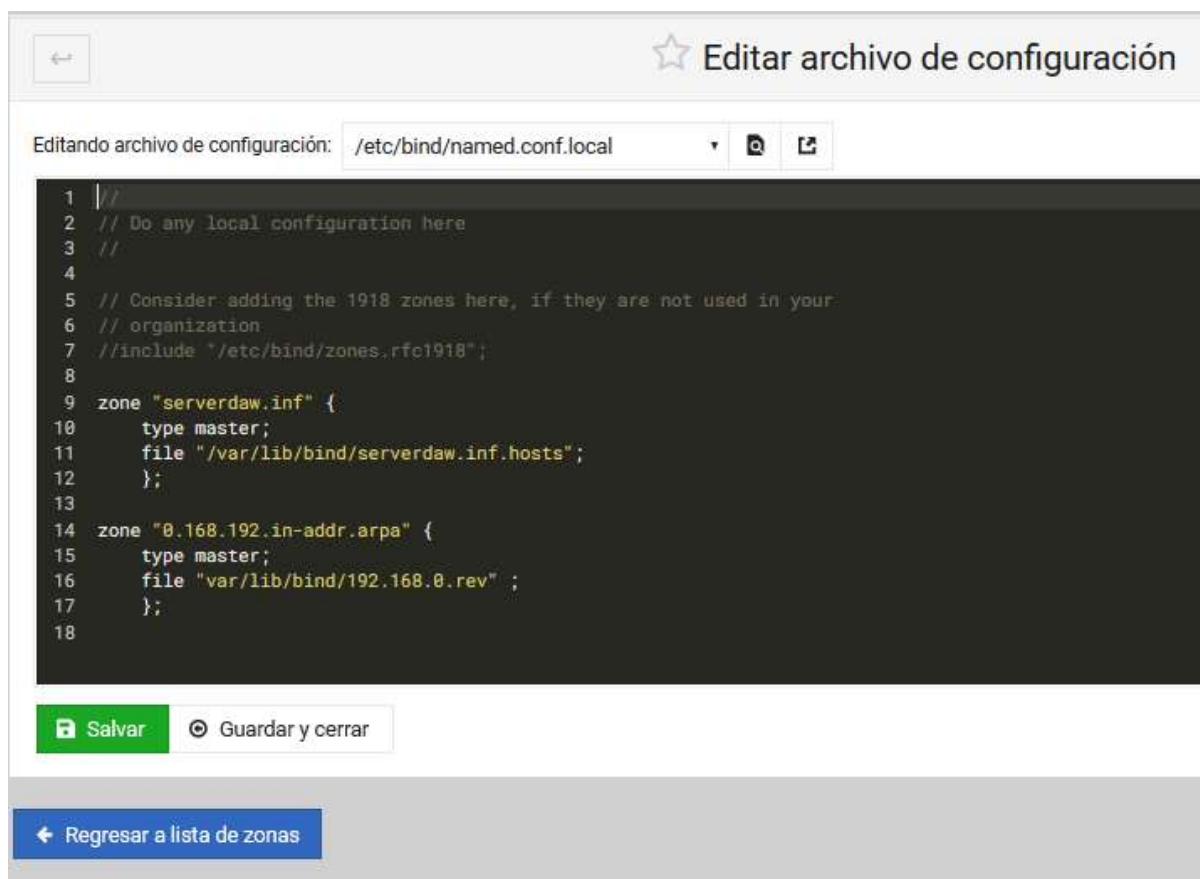


Ilustración 27 Zona inversa en /etc/bind/named.conf.local

Se puede observar que con respecto a la *Ilustración 8 Zona primaria en named.conf.local* se ha añadido 3 nuevas líneas:

- zone "1.168.192.in-addr.arpa": declara la zona inversa. Tener en cuenta que la dirección de la red se pone al revés.
- type master: tipo maestro.
- file "/var/lib/bind/192.168.1.rev": fichero de la base de datos de la zona inversa.

8.3.1 Crear puntero (PTR)

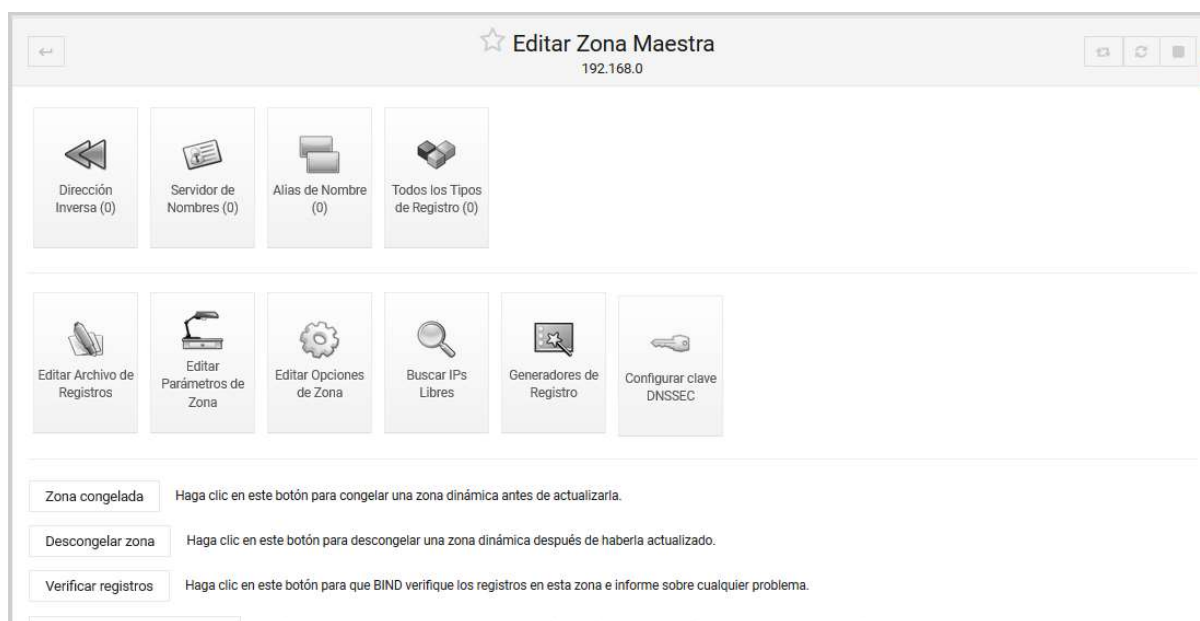


Ilustración 28 Editar Zona Inversa

Acceda a la zona inversa creada para añadir punteros (*Ilustración 26 Zona Inversa creada*). Los punteros permiten la conversión de direcciones IP a nombres.

Hacer click en el icono *Dirección inversa* dónde se podrán el nombre del equipo y su dirección IP (Se podrán crear tantos como se necesiten), para acabar, hacer clic en *Crear*. (*Ilustración 29 Crear Dirección Inversa Registros*)



Ilustración 29 Crear Dirección Inversa Registros

Ilustración 30 Dirección Inversa creada

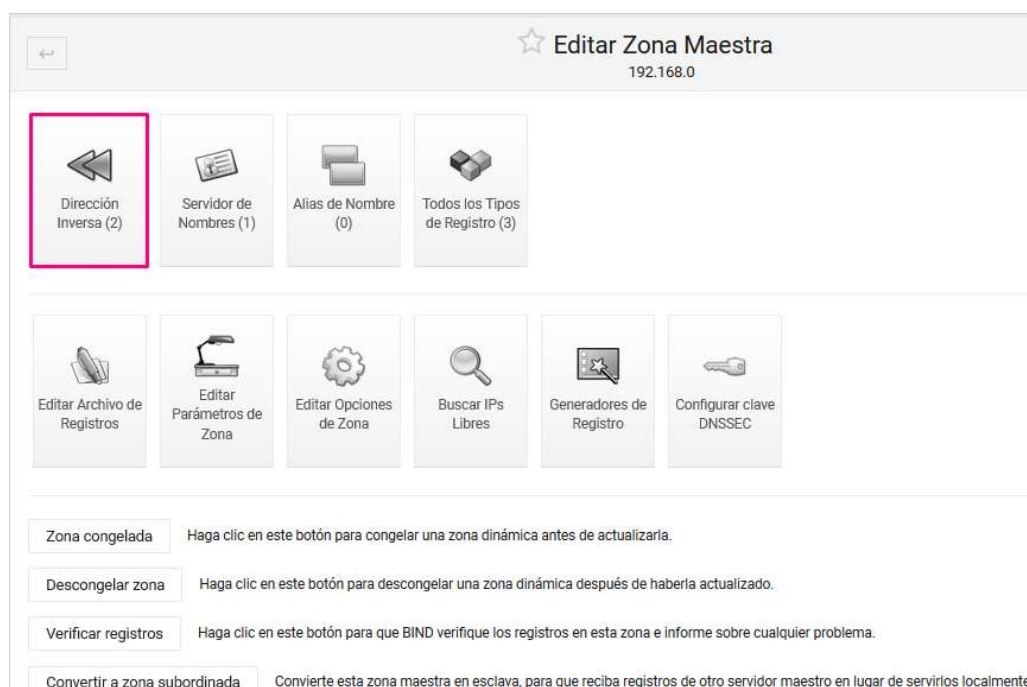


Ilustración 31 Icono Dirección Inversa actualizado

Observa la Ilustración 30 Dirección Inversa creada Ilustración 11 Dirección creada, como se puede ver, aparece la dirección inversa creada. Se crearan algunas direcciones más. Una vez creada el icono de *Dirección Inversa* se actualizará (Ilustración 31 Icono Dirección Inversa actualizado).

Se puede ver cómo va quedando el fichero de base de datos de la zona inversa que se está creando. Para ello haz clic en el icono *Editar Archivo de Registro* de *Editar Zona Maestra* (Ilustración 32 *Editar Archivo de Registro* Ilustración 13 *Editar Archivo de Registros*). Aparecerá la Ilustración 33 *Edición fichero /var/lib/bind/192.168.1.rev*, el fichero 192.168.1.rev que se encuentra en el directorio /var/lib/bind. Este es el directorio por defecto dónde Webmin crea los archivos de base de datos del DNS.

Hacer hincapié en que las direcciones IP están escritas al revés.

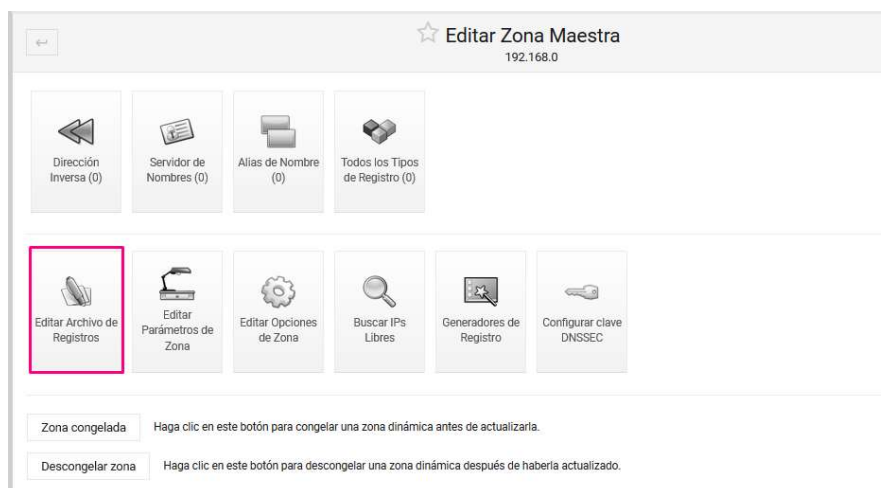


Ilustración 32 Editar Archivo de Registro

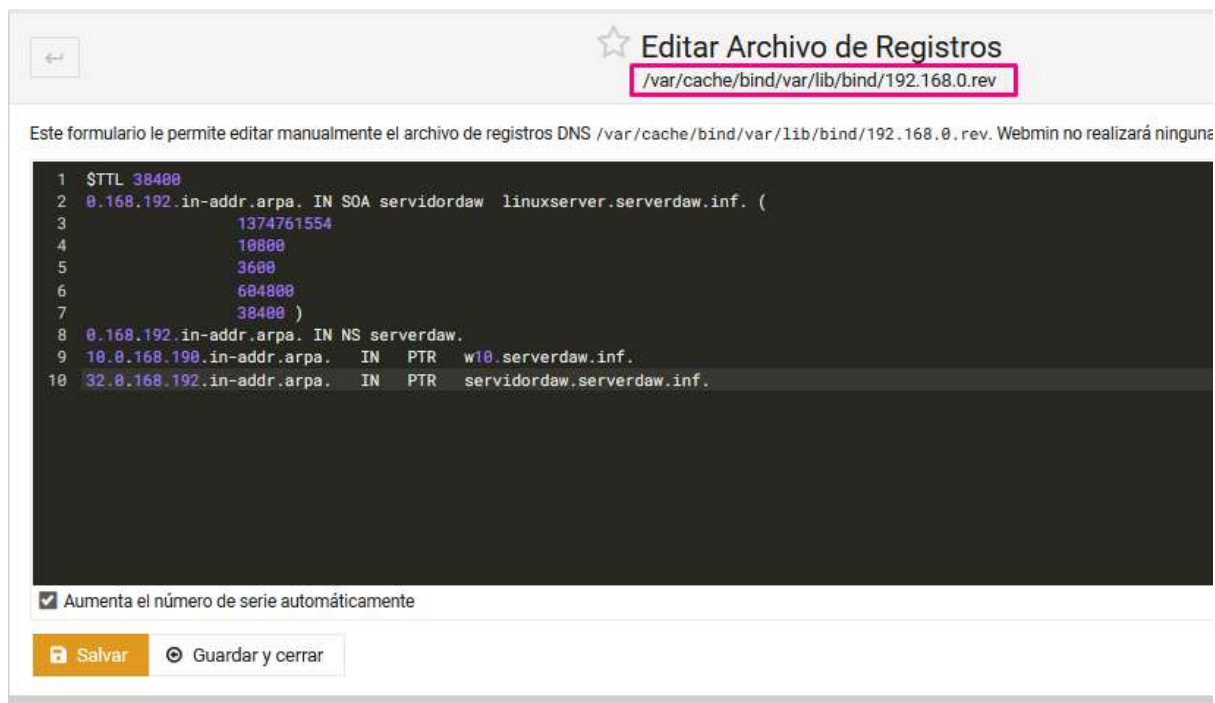


Ilustración 33 Edición fichero /var/lib/bind/192.168.1.rev

9 Reiniciar el servicio DNS

Una vez que se han realizado todos los cambios se debe reiniciar el servicio DNS, para ello tenemos 2 opciones:

- **Webmin:** hacer clic en *Apply Configuration* (Ilustración 34 Apply Configuration).



Ilustración 34 Apply Configuration

- **Consola:** se abre un terminal y en modo privilegio (*root*) reiniciamos el servicio (*Ilustración 35 Reiniciar el servicio DNS por consola*).

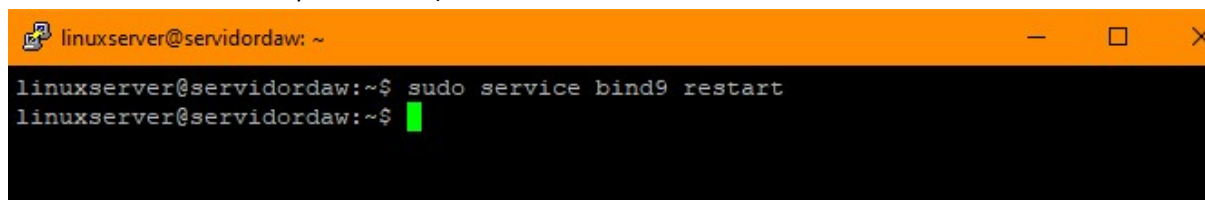
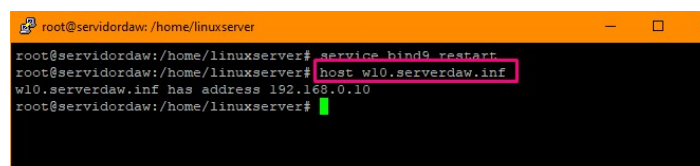


Ilustración 35 Reiniciar el servicio DNS por consola

10 Verificar funcionamiento DNS

Pasos a seguir para verificar el buen comportamiento del DNS creado:

1. Primero habrá que comprobar que el DNS que se esté utilizando es el creado, en este ejemplo sería el 192.168.0.32.
2. Utiliza el comando `host`



3. Utiliza el comando `dig`

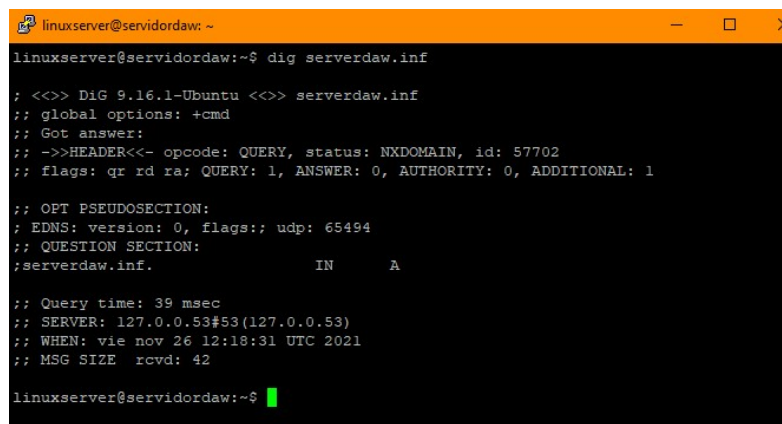
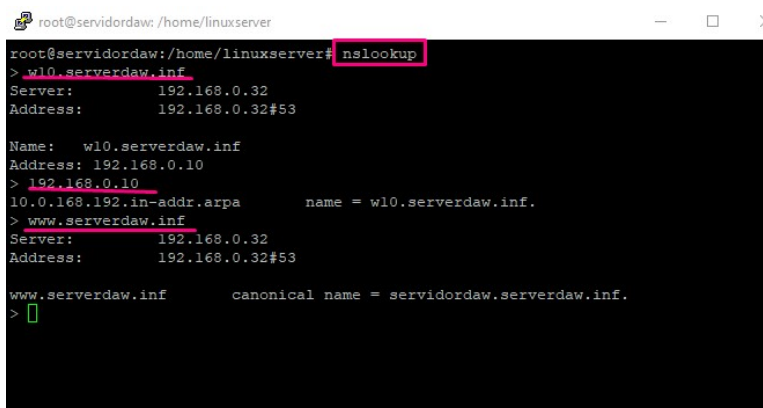


Ilustración 36 Comando dig

4. Utiliza el comando `nslookup`: se usa para consultar, obtener información, probar y solucionar problemas de los servidores DNS que usa una conexión. En la *Ilustración 37 Comando nslookup* se puede observar el funcionamiento del DNS creado en el apartado anterior.



```

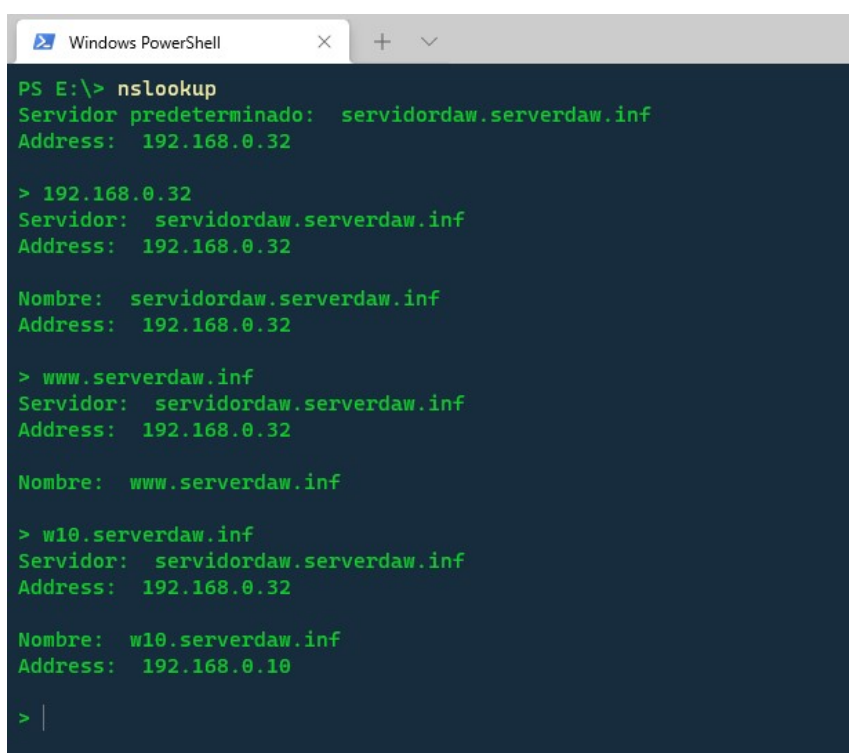
root@servidordaw: /home/linuxserver# nslookup
> w10.serverdaw.inf
Server:      192.168.0.32
Address:     192.168.0.32#53

Name:   w10.serverdaw.inf
Address: 192.168.0.10
> 192.168.0.10
10.0.168.192.in-addr.arpa      name = w10.serverdaw.inf.
> www.serverdaw.inf
Server:      192.168.0.32
Address:     192.168.0.32#53

www.serverdaw.inf      canonical name = servidordaw.serverdaw.inf.
>

```

Ilustración 37 Comando nslookup



```

PS E:\> nslookup
Servidor predeterminado:  servidordaw.serverdaw.inf
Address:  192.168.0.32

> 192.168.0.32
Servidor:  servidordaw.serverdaw.inf
Address:   192.168.0.32

Nombre:   servidordaw.serverdaw.inf
Address:  192.168.0.32

> www.serverdaw.inf
Servidor:  servidordaw.serverdaw.inf
Address:   192.168.0.32

Nombre:   www.serverdaw.inf

> w10.serverdaw.inf
Servidor:  servidordaw.serverdaw.inf
Address:   192.168.0.32

Nombre:   w10.serverdaw.inf
Address:  192.168.0.10

>

```

Ilustración 38 Comando nslookup desde windows

Para salir del comando `nslookup` escribir `exit`.

5. Para comprobar el servidor de correo electrónico seguir la *Ilustración 39 nslookup para Servidor de correo*

```

root@servidordaw:/home/linuxserver# nslookup
> w10.serverdaw.inf
Server:      192.168.0.32
Address:     192.168.0.32#53

Name:   w10.serverdaw.inf
Address: 192.168.0.10
> 192.168.0.10
10.0.168.192.in-addr.arpa      name = w10.serverdaw.inf.
> www.serverdaw.inf
Server:      192.168.0.32
Address:     192.168.0.32#53

www.serverdaw.inf      canonical name = servidordaw.serverdaw.inf.
> set q=MX
> servidordaw.serverdaw.inf
Server:      192.168.0.32
Address:     192.168.0.32#53

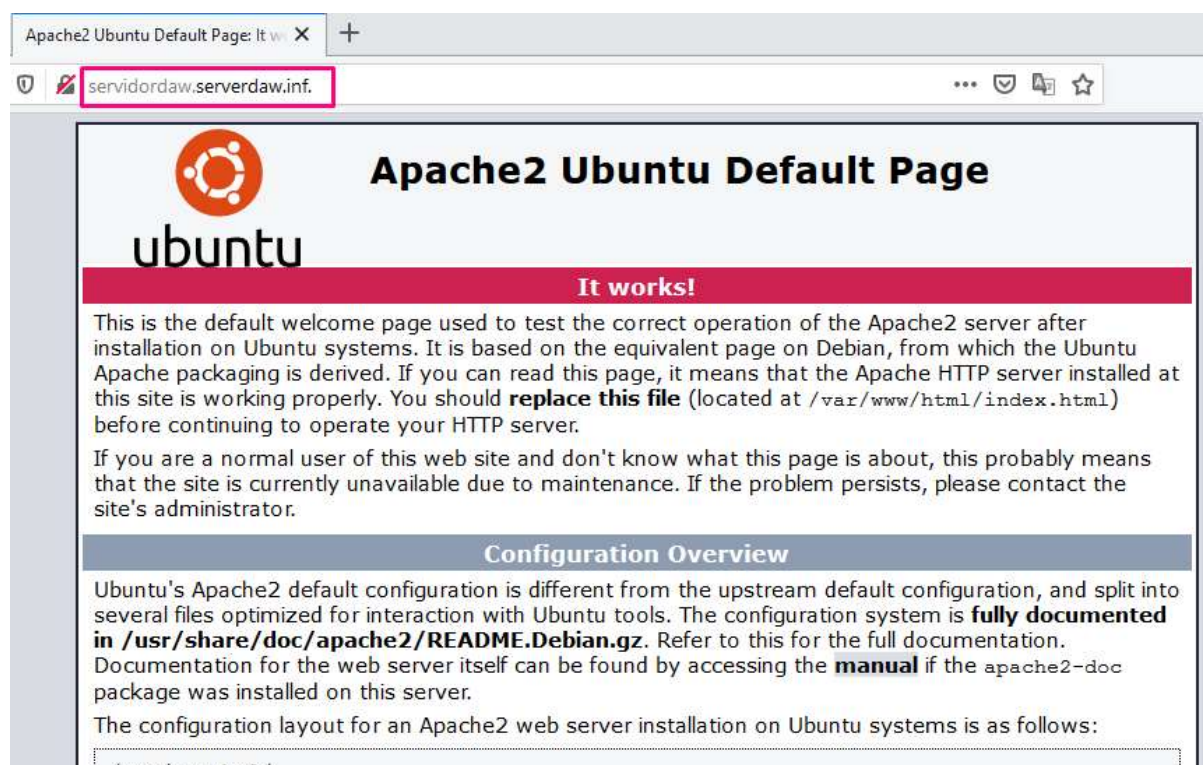
servidordaw.serverdaw.inf      mail exchanger = 10 192.168.0.32.serverdaw.inf.
>

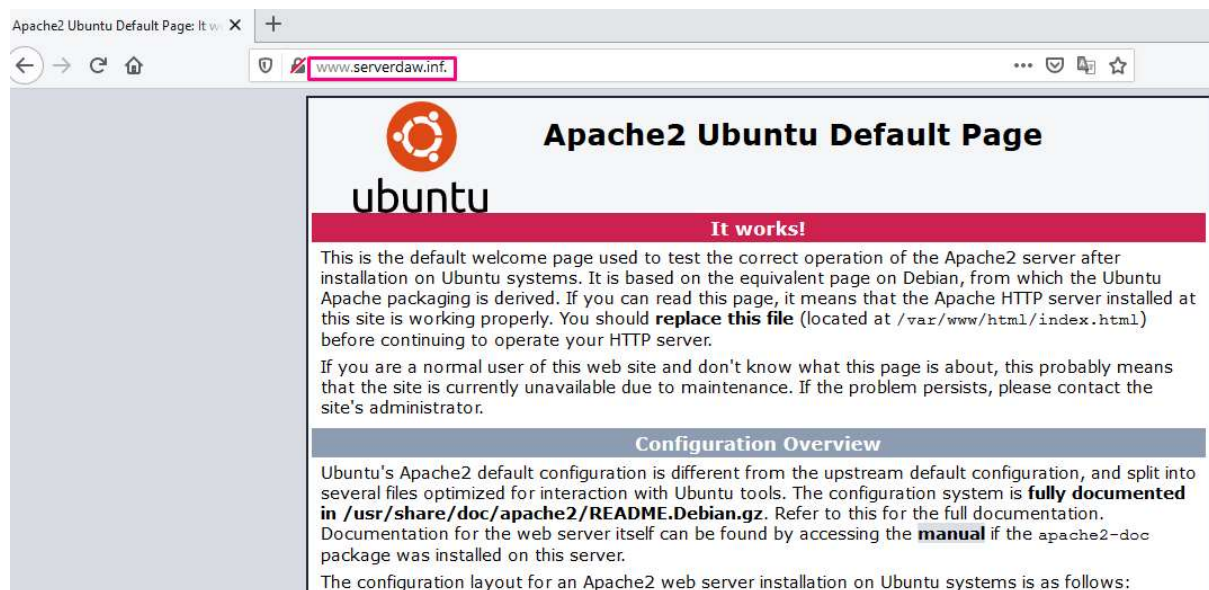
```

Ilustración 39 nslookup para Servidor de correo

6. Funcionamiento del alias desde Windows para petición de página web

Comprueba que tienes Apache instalado.





11 DDNS

Las siglas DDNS significan el sistema dinámico de nombres de dominio, que permite la asignación de un nombre de dominio a una máquina con dirección IP dinámica. Es una herramienta muy útil cuando la línea ADSL tiene un direccionamiento dinámico, es decir, el proveedor de Internet asigna una IP pública diferente cada vez que se conecta o se reinicia el router.

Si la intención es configurar un servidor http, ftp, etc, se necesita tener localizado el router en Internet para poder tener acceso. Esto se consigue con la función DDNS.

Dicha función permite configurar el router para asociarlo, mediante un nombre de dominio, a una dirección IP. Esto lo lleva a cabo un servidor que proporciona soporte para DNS con IP dinámica

Hay varios proveedores que ofrecen gratuitamente servicio DDNS, por ejemplo DNS-dynamic, no-ip, DynDNS, etc.

Para configurar un DDNS con el router seguiremos estos pasos:

1. Activar la opción DDNS en el router.

La forma de acceso al router suele ser a través del navegador Web y la IP interna del mismo. Hay que validarse como usuario administrador en la interfaz del router e ir a las opciones de Setup, pestaña DDNS (Ilustración 38: Activar DDNS router.). La ubicación del servicio puede cambiar en cada modelo de router, se recomienda leer las instrucciones del mismo.

UD 03 Servidor DNS

DDNS

Proveedor del servicio	Conexión WAN	Habilitar	Protocolo	Dominio	Nombre de usuario	Contraseña	Eliminar
http	nas_8_35	Habilitar	GNUDip.http	manuela-pc.aulasmr2.no-ip.biz	aulasmr2	*****	

Configuración

Proveedor del servicio: Otros Conexión WAN: nas_8_35

Equipo: Dominio: aulasmr2.no-ip.biz

Nombre de usuario: aulasmr2 Contraseña: *****

Dirección del servidor: Puerto del servidor: 80

Protocolo: GNUDip.http Nombre del servicio: http

Enviar

Ilustración 38: Activar DDNS router.

También se tendrá que abrir el puerto del router que de acceso a la máquina dónde está el servidor http, en este ejemplo.

ALG DMZ Asignación de puertos Puertos dinámicos

Asignación de puertos

Nombre Asignado	Protocolo	Equipo remoto	Puerto externo inicial	Puerto externo final	Puerto Interno	Equipo interno	Habilitar	Eliminar
WebServer(HTTP)	TCP		80	80	80	192.168.1.35	Habilitar	

Configuración

Tipo: ☐ Personalización ☒ Aplicación Elegir ...

Protocolo: TCP

Equipo remoto:

Puerto externo inicial: 80

Puerto externo final: 80

Equipo interno: 192.168.1.35

Puerto interno: 80

Nombre Asignado: WebServer(HTTP)

Enviar

Ilustración 39: Abrir puertos.

no-ip Managed DNS Services

Create Your No-IP Account

aulasmr2 prof.manuelagordillo@esalixar.org

aulasmr2 .no-ip.biz

☐ Create my hostname later

That address is also available with these Enhanced DNS domains for only \$14.95 a year:

- aulasmr2.ddns.me
- aulasmr2.noip.me
- aulasmr2.noip.us
- aulasmr2.ddns.net
- aulasmr2.hopto.me
- aulasmr2.no-ip.ca

1 line above to Enhanced DNS now will save

Ilustración 40: Crear cuenta en no-ip

2. Crear una cuenta en no-ip
 - a. Crear una cuenta en el servidor DDNS (www.no-ip.com), como muestra la Ilustración 40: Crear cuenta en no-ip.

- b. Descargar el programa cliente no-ip, para instalarlo en el ordenador que actuará como servidor.

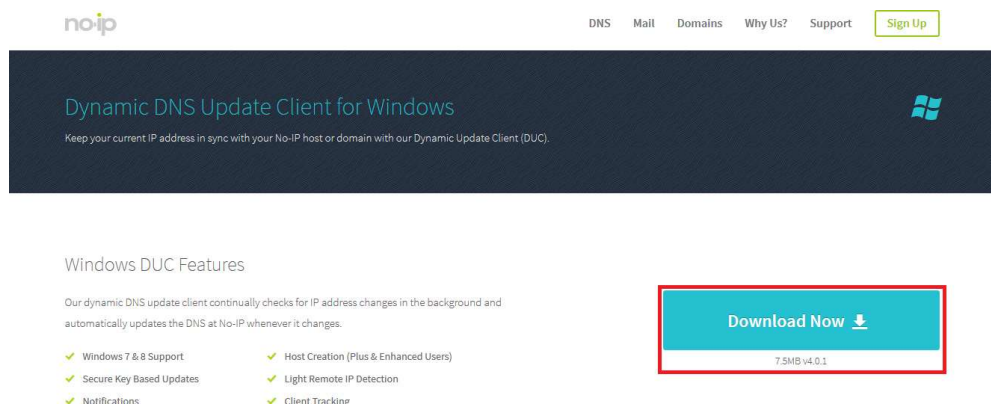


Ilustración 41: Descargar cliente no-ip

En la Ilustración 42: Programa cliente no-ip en ejecución. se observa el programa ejecutándose.

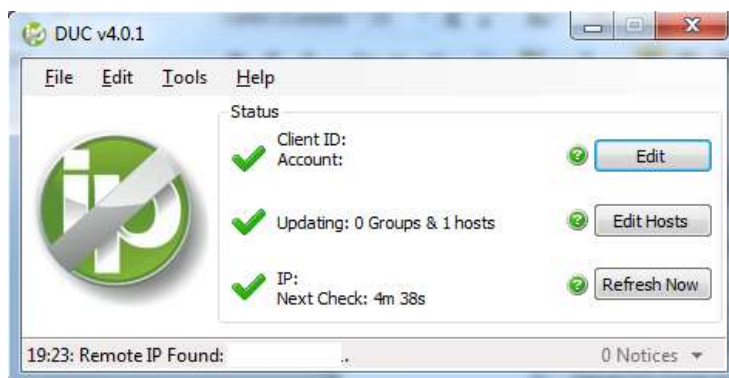


Ilustración 42: Programa cliente no-ip en ejecución.

- c. Al conectarse el router a Internet, éste obtiene una dirección IP.
d. Envía su IP y nombre del dominio al servidor `www.no-ip.com` a través de la cuenta creada.
e. El nombre de dominio que en este caso es `aulasmr2.no-ip.biz`, queda asociado a la IP.
f. Si se quiere comprobar la IP pública del router, hay que ejecutar la orden `ping` sobre el nombre del dominio, en este caso `aulasmr2.no-ip.biz`.

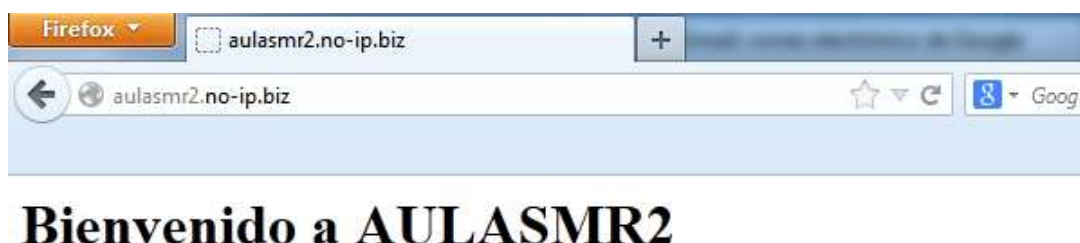


Ilustración 43: Acceso al servidor Web