

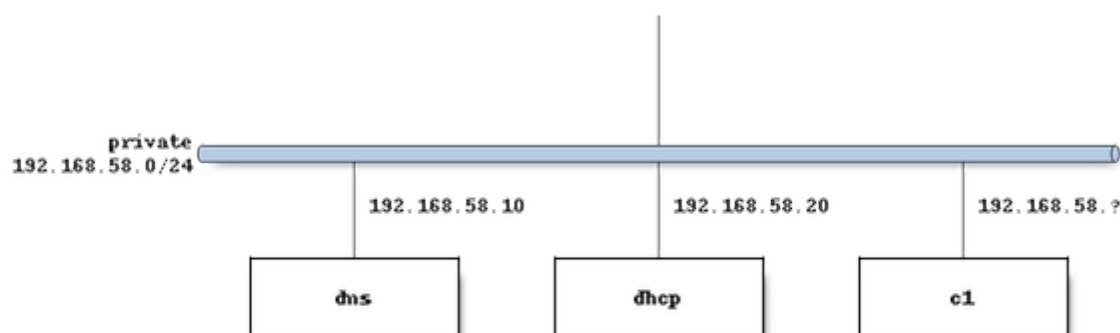
# Dynamic DNS (DDNS)

## Tabla de Contenido

1. Escenario .....	1
2. Práctica .....	2
2.1. Generar la Clave de Seguridad (en el servidor DNS) .....	2
2.2. Configurar ISC-DHCP-Server (en el servidor DHCP) .....	3
3. Pruebas .....	5

El DNS Dinámico es un mecanismo que permite a los clientes (en este caso, tu servidor DHCP en nombre del ordenador cliente) actualizar automáticamente los registros de un servidor DNS (BIND9) cuando cambia la información de una dirección IP.

## 1. Escenario



En este escenario tenemos:

### Servidor DHCP (ISC-DHCP-Server)

Cuando un cliente obtiene una nueva dirección IP dinámica, el servidor DHCP no solo le asigna la IP, sino que también inicia una transacción de actualización con el servidor DNS.

### Servidor DNS (BIND9)

Recibe la solicitud del DHCP, la autentica usando una clave TSIG (*Transaction Signature*), y actualiza los registros A (nombre a IP) y PTR (IP a nombre) de la zona correspondiente.

Esto es crucial en entornos con direcciones IP dinámicas, ya que garantiza que el nombre del host del cliente se resuelva consistentemente a la dirección IP correcta en todo momento, sin necesidad

de intervención manual.

## 2. Práctica

Para lograr que el servidor DHCP registre automáticamente los clientes que obtienen una dirección IP en el servidor DNS (DDNS), necesitas configurar la clave de seguridad que permitirá a ISC-DHCP-Server enviar actualizaciones a BIND9.

Dado que los servicios están en máquinas virtuales separadas, debes asegurarte que la comunicación de red entre ellas sea correcta (la máquina DHCP debe poder contactar con el servidor DNS).

### 2.1. Generar la Clave de Seguridad (en el servidor DNS)

#### 2.1.1. Genera la clave

El servidor DHCP necesita autenticarse para realizar cambios en las zonas DNS. Usaremos `tsig-keygen` para generar una clave secreta en el servidor DNS.

```
sudo tsig-keygen -a hmac-sha256 ddns-key > /etc/bind/ddns.key
```

Esto crea un archivo `ddns.key` con una clave HMAC-SHA256. El nombre `ddns-key` es un ejemplo y puede ser otro.



Copia la clave secreta generada. La necesitarás en el servidor DHCP.

#### 2.1.2. Define la clave en BIND9

Edita el archivo de configuración principal de BIND9, generalmente `/etc/bind/named.conf.options` (estilo Debian) o incluido en `/etc/bind/named.conf` (estilo Red Hat).

```
sudo nano /etc/bind/named.conf.options
```

Añade la definición de la clave (copiando la información del archivo `ddns.key`):

`/etc/bind/named.conf.options`

```
...  
  
key "ddns-key" {  
    algorithm hmac-sha256;  
    secret "TU_CLAVE_SECRETA_LARGA_AQUI"; ①  
};
```

...

① Sustituye con el valor de 'secret'

*/etc/bind/named.conf.local*

```
zone "example.test" IN { ①
    type master;
    file "/etc/bind/db.example.test";
    allow-update { key "ddns-key"; }; ②
};

zone "58.168.192.in-addr.arpa" IN { ③
    type master;
    file "/etc/bind/db.192";
    allow-update { key "ddns-key"; }; ④
};
```

① Reemplaza con tu dominio

② Permite actualizaciones con la clave

③ Asumiendo subred 192.168.58.0/24

④ Permite actualizaciones con la clave

### 2.1.3. Ajusta los Archivos de Zona:

Asegúrate de que el *Serial Number* (Número de Serie) en tus archivos de zona (e.g., */etc/bind/db.example.test* y */etc/bind/db.192*) sea un número y que se incrementará automáticamente con cada actualización dinámica.

### 2.1.4. Verifica y Reinicia BIND9:

```
sudo named-checkconf /etc/bind/named.conf.options
sudo named-checkconf /etc/bind/named.conf.local
sudo named-checkzone example.test. /var/lib/bind/db.example.test
sudo named-checkzone 58.168.192.in-addr.arpa. /var/lib/bind/db.192
sudo systemctl restart bind9
```

## 2.2. Configurar ISC-DHCP-Server (en el servidor DHCP)

El servidor DHCP necesita saber los detalles de la clave de seguridad y la configuración DDNS que debe usar.

### 2.2.1. Define la Clave de Seguridad:

Crea un archivo de clave en el servidor DHCP (*/etc/dhcp/ddns.key*) y pega la misma clave secreta que generaste en el servidor DNS (Paso anterior).

```
sudo nano /etc/dhcp/ddns.key
```

El contenido debe ser exactamente el mismo que el bloque **key** en el **named.conf.options** del DNS:

#### Zona DNS

```
key "ddns-key" {  
    algorithm hmac-sha256;  
    secret "TU_CLAVE_SECRETA_LARGA_AQUI"; ①  
};
```

① Pega la misma clave secreta

### 2.2.2. Configura **/etc/dhcp/dhcpd.conf**

Incluye la clave que acabas de crear:

#### */etc/dhcp/dhcpd.conf*

```
include "/etc/dhcp/ddns.key";  
  
# option definitions common to all supported networks...  
option domain-name "example.test";  
option domain-name-servers 192.168.58.10, 8.8.8.8;  
  
default-lease-time 86400; # 60s * 60m * 24h  
max-lease-time 691200;    # 8 dias  
  
option routers 192.168.58.1;
```

Añade las directivas de DDNS globales y las configuraciones de las zonas dentro de la declaración de subred (subnet):

```
ddns-update-style interim;  
ddns-domainname "example.test."; ①  
ddns-rev-domainname "58.168.192.in-addr.arpa.";  
  
subnet 192.168.58.0 netmask 255.255.255.0 {  
    range 192.168.58.100 192.168.58.200;  
    option routers 192.168.58.1;  
    option domain-name-servers IP_DEL_DNS_SERVER;  
    option domain-name "example.test";  
  
    # Configuración de la zona directa  
    zone example.test. {  
        primary IP_DEL_DNS_SERVER; ②  
        key "ddns-key";  
    }  
}
```

```
# Configuración de la zona inversa
zone 58.168.192.in-addr.arpa. {
    primary IP_DEL_DNS_SERVER; ③
    key "ddns-key";
}
}
```

- ① Asegúrate del punto final
- ② Reemplaza IP\_DEL\_DNS\_SERVER con la dirección IP de tu servidor DNS.
- ③ Reemplaza IP\_DEL\_DNS\_SERVER con la dirección IP de tu servidor DNS.

Reinicia el servidor DHCP:

```
sudo systemctl restart isc-dhcp-server
```

## 3. Pruebas

Fuerza a un cliente (otra máquina virtual) a renovar su concesión DHCP.

Verifica los logs del servidor DHCP y del servidor DNS para confirmar que la actualización dinámica se realizó correctamente.

Usa `nslookup` o `dig` desde el cliente o el servidor para resolver el nombre de host del cliente (ej: `nombre-cliente.example.test`) y la búsqueda inversa (PTR).



Asegúrate de que las zonas DNS estén correctamente configuradas en BIND9 antes de intentar la actualización dinámica.