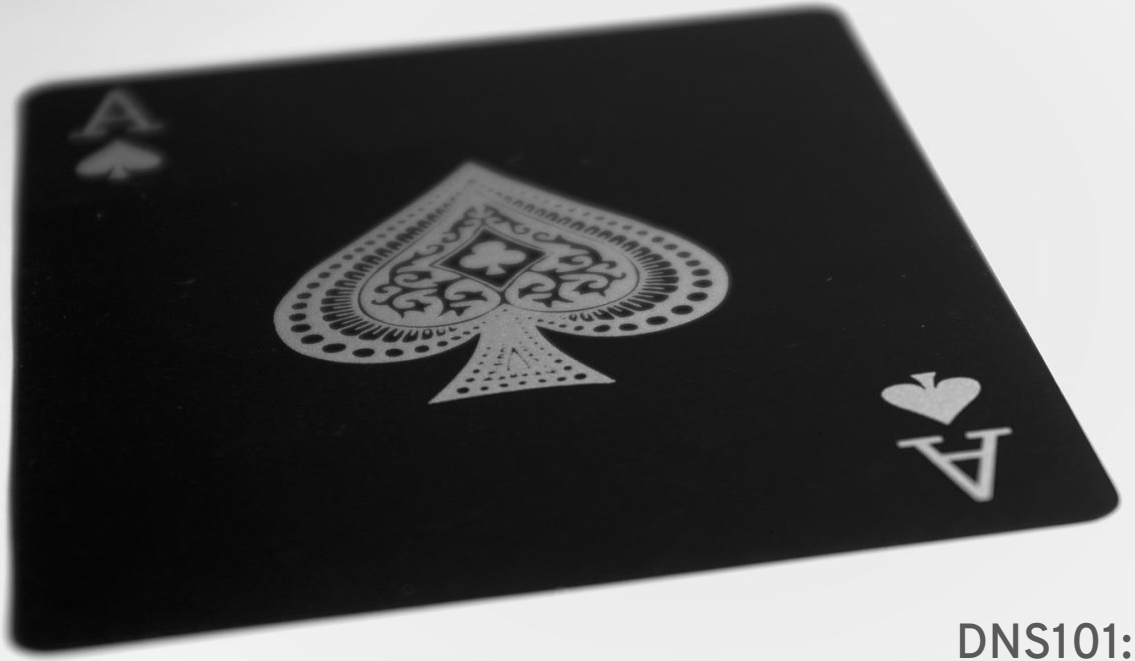


DNS101: Nada es lo que parece

Alex Callejas | Red Hat

Alex Callejas

Services Content Architect @Red Hat

@dark_axl

/rootzilopochtli

www.rootzilopochtli.com

darkaxl017.fedorapeople.org/slides/

Geek by nature, Linux by choice, Fedora of course!

sysarmy @ /home
@sysarmy

Si, internet anda para atrás. Lo único que observamos es algún tipo de degradación de conectividad internacional en ciertos proveedores locales.

9:40 · 06/07/20 · Twitter Web App

24 Retweets y comentarios **61** Me gusta

siggy🧡💚🏳️‍🌈 @th3siggy · 1h
En respuesta a @sysarmy
esto de alguna forma va a ser el DNS.
no tengo pruebas pero tampoco dudas.

Pablo Fredrikson @pablokbs · 1h
ponele un titulo a esto

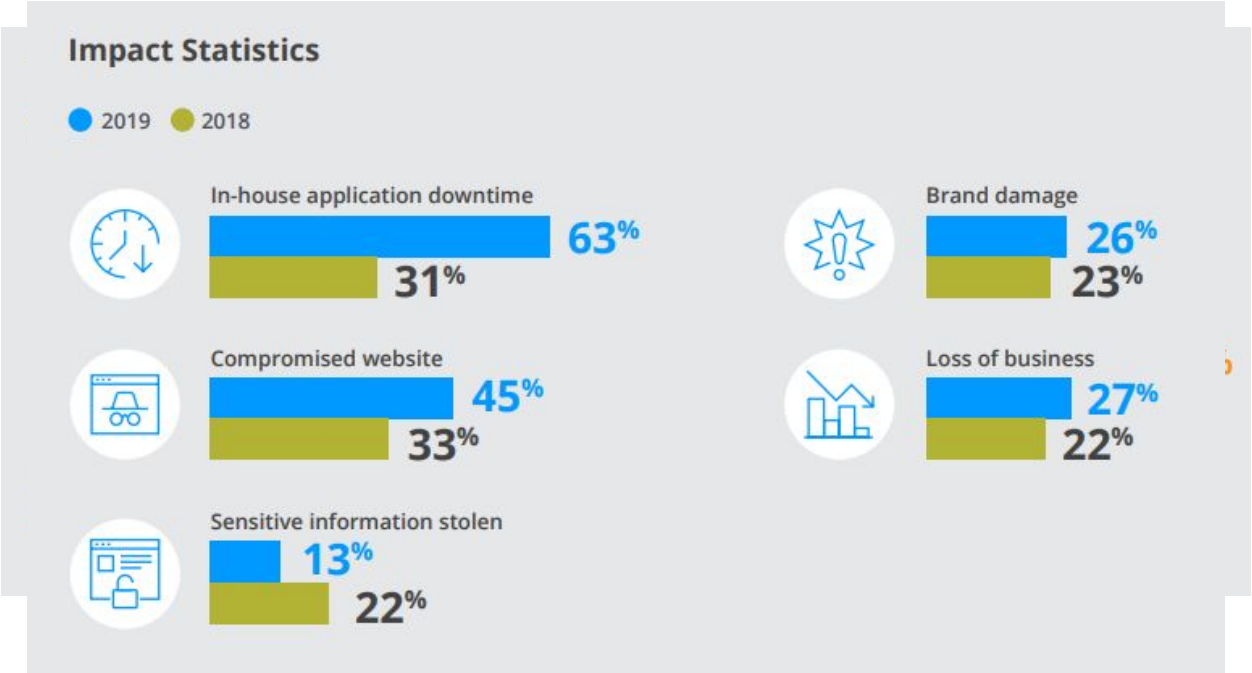
32 5 16

siggy🧡💚🏳️‍🌈
@th3siggy

Replying to @pablokbs

"Era el DNS. SIEMPRE ES EL DNS!"

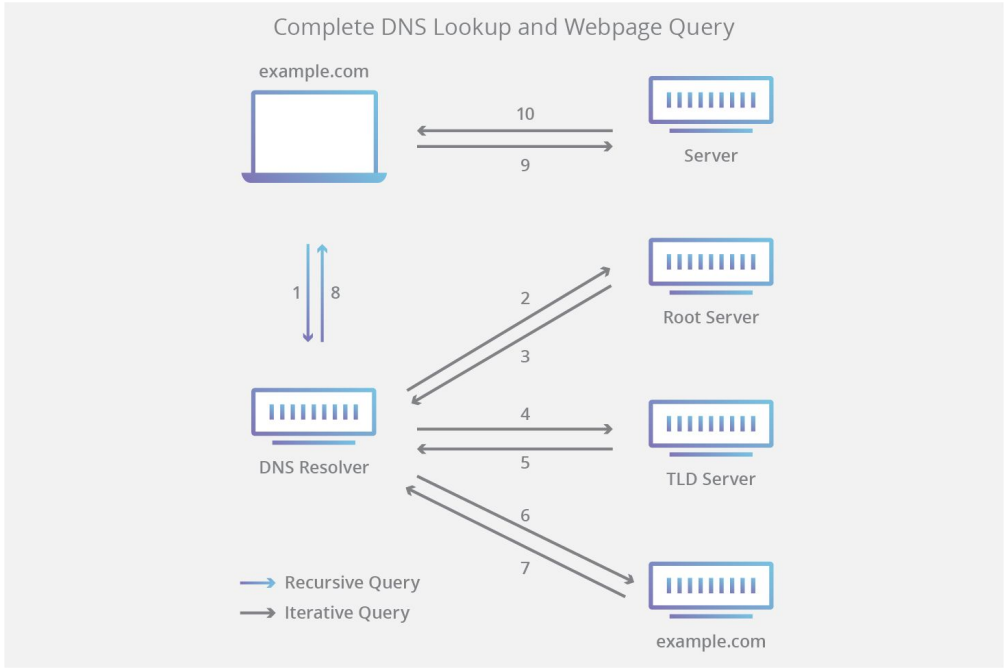
Around 82% of the organizations have faced a DNS (Domain Name System) attack in 2019, up 5% from 2018, according to IDC's 2019 Global DNS Threat Report.



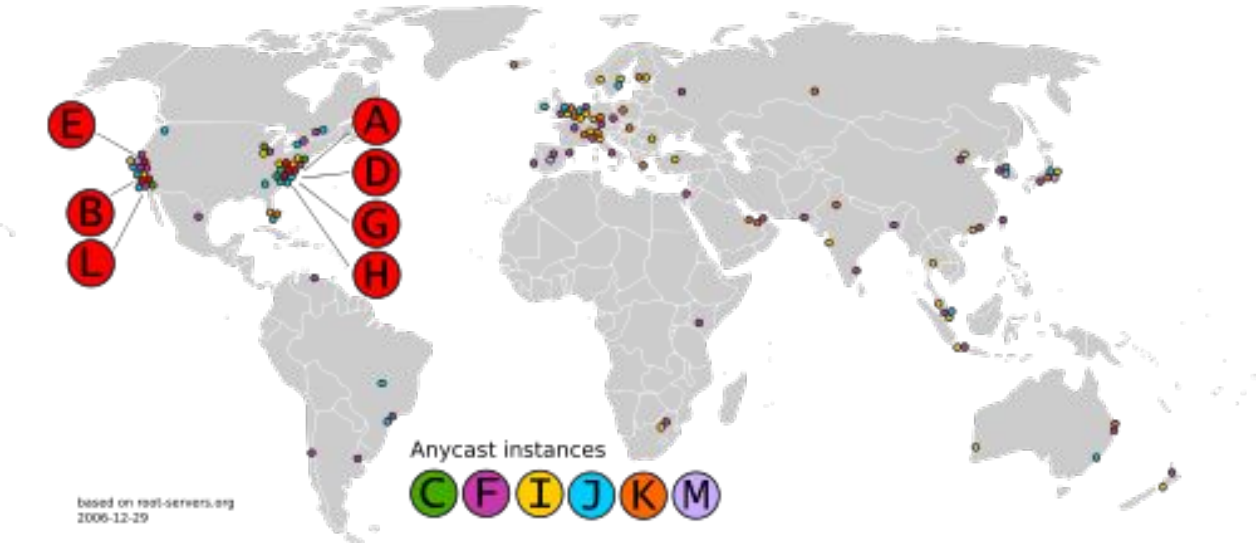
DNS?

Fuente: https://www.dailyhostnews.com/average-cost-per-dns-attack-is-1-07-million

Entendiendo el DNS



Entendiendo el DNS

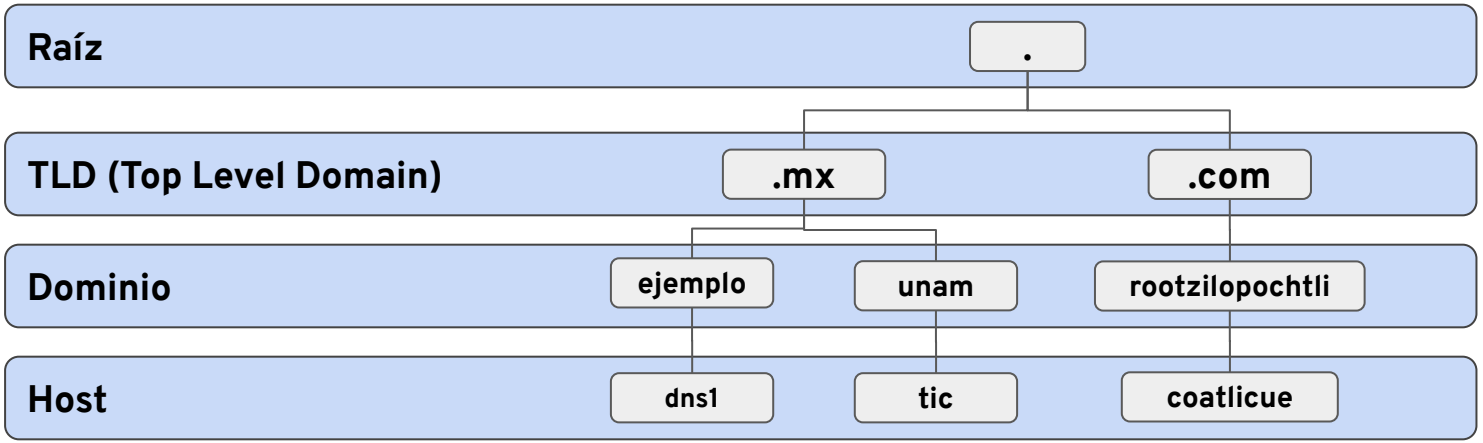


Fuente: [root-servers.org]

Entendiendo el DNS

Sistema de Nombre de Dominio → DNS

- El DNS es una **base de datos distribuida de forma global, redundante y jerárquica.**



Entendiendo el DNS

Dominio → Dirección IP → Resolución Tipo **A** (**Address**)

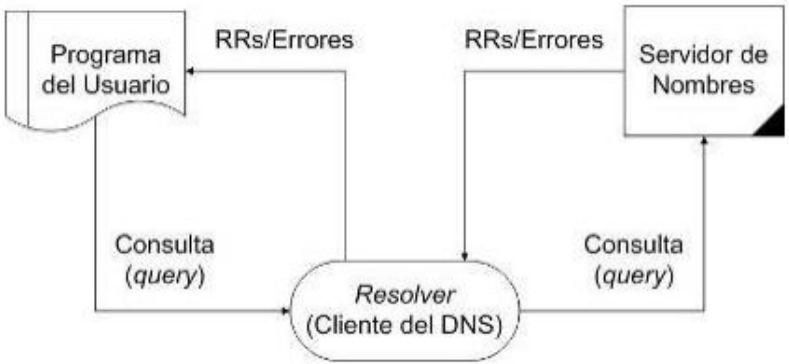
ejemplo.lab → **192.168.0.1**

Dirección IP → Dominio → Resolución Tipo **PTR** (**Pointer**)

192.168.0.4 → **mail.ejemplo.lab**

Entendiendo el DNS

- Generalmente un dominio es segmentado en zonas para facilitar su administración.
- Dentro de cada zona, uno o más servidores son considerados **autoritativos** (*authoritative*) para resolver nombres a direcciones y viceversa.
- Las **consultas** (*queries*) se hacen a través de librerías llamadas **resolvers.**



Configuración básica bind: named.conf

```
options {
 directory "/var/named/zones";
 pid-file "/var/run/named.pid";
};

zone "." {
 type hint;
 file "named.root";
};

zone "0.0.127.in-addr.arpa" {
 type master;
 file "127.0.0.zone";
};
```

Work directory & pid

IP's de *name servers* autoritativos para la *root zone*
https://www.iana.org/domains/root/files

Archivo de zona *loopback*

Configuración básica bind: named.conf

```
zone "ejemplo.lab" {
 type master;
 file "ejemplo.lab.zone";
};
```

Archivo de zona

```
zone "0.168.192.in-addr.arpa" {
 type master;
 file "192.168.0.zone";
};
```

Archivo de zona *reversa*

Archivo de zona: ejemplo.lab.zone

```
$ORIGIN .
$TTL 1d
ejemplo.lab      IN      SOA     dns1.ejemplo.lab. root.dns1.ejemplo.lab. (
                                 2020070301 ; numero de serie
                                 1200       ; refresh (20 minutos)
                                 3600       ; retry (1 hora)
                                 1209600    ; expire (2 semanas)
                                 3600       ; minimum (1 hora)
                                 )
```

origen

Time-to-Live

Start Of Authority

Archivo de zona: ejemplo.lab.zone

```
                              A   192.168.0.1
                              NS  dns1.ejemplo.lab.
                              NS  dns2.ejemplo.lab.
                              MX  10 mail.ejemplo.lab.
$ORIGIN ejemplo.lab.
dns1                          A         192.168.0.2
dns2                          A         192.168.0.3
mail                          A         192.168.0.4
www                           CNAME     ejemplo.lab.
portal                        CNAME     ejemplo.lab.
```

IP del dominio

name servers del dominio

Mail Exchanger del dominio

Canonical Name (alias)

Archivo de zona: 192.168.0.zone

```
$ORIGIN .
$TTL 1d
0.168.192.in-addr.arpa IN SOA  dns1.ejemplo.lab. root.dns1.ejemplo.lab. (
                               2020070301 ; numero de serie
                               1200       ; refresh (20 minutos)
                               3600       ; retry (1 hora)
                               1209600    ; expire (2 semanas)
                               3600       ; minimum (1 hora)
                               )
```

origen

Time-to-Live

Start Of Authority

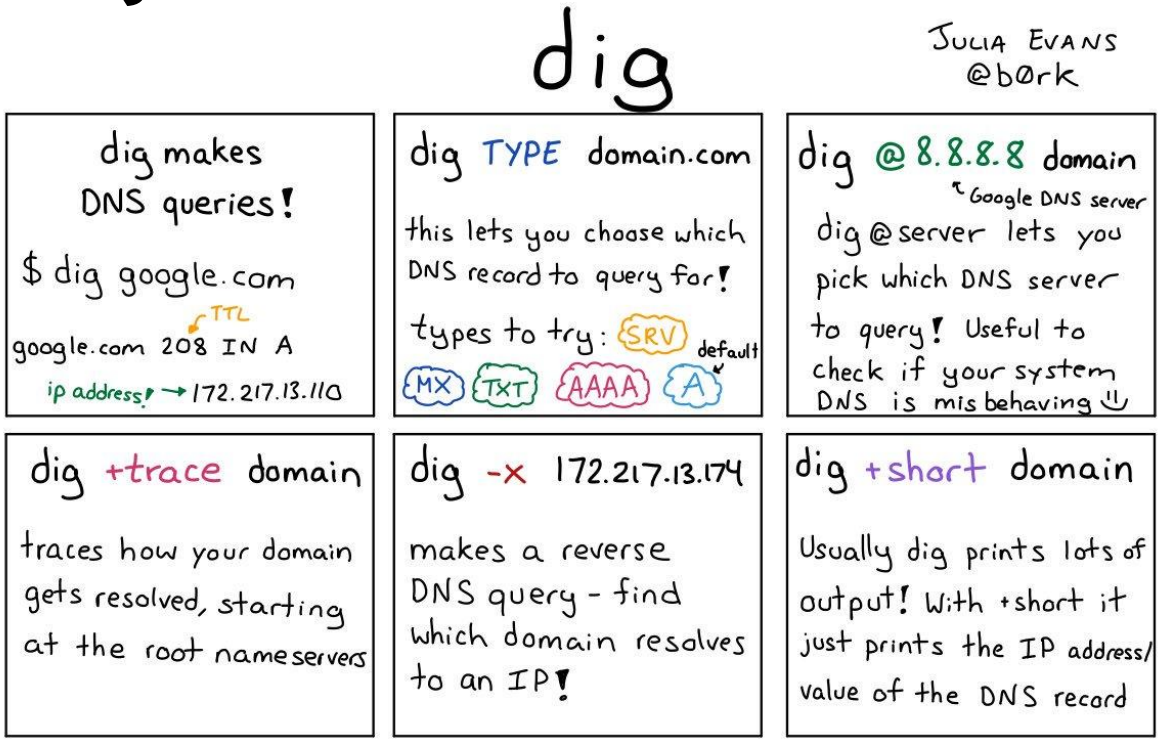
Archivo de zona: 192.168.0.zone

```
                        NS dns1.ejemplo.lab.
                        NS dns2.ejemplo.lab.
$ORIGIN 0.168.192.in-addr.arpa.
1                       PTR     ejemplo.lab.
2                       PTR     dns1.ejemplo.lab.
3                       PTR     dns2.ejemplo.lab.
4                       PTR     mail.ejemplo.lab.
```

Resource Records Opcionales

Tipo	Nombre	Función
HINFO	Host Information	Informa del Hardware y el SO
TXT	Text	Texto ASCII no interpretado
SRV	Service Record	Define la ubicación, es decir, el host y el puerto, para servicios específicos.
DMARC	Domain based Message Authentication Reporting and Conformance	Las políticas de la DMARC se publican en el DNS como registros de texto (TXT) y anuncian lo que un receptor de correo electrónico debe hacer con el correo *no alineado* que recibe.
DKIM	DomainKeys Identified Mail	Proporciona un método para validar la identidad de un dominio asociado a un mensaje mediante autenticación criptográfica
SPF	Sender Policy Framework	Identifica, a través de los registros de DNS, a los servidores de correo SMTP autorizados para el transporte de los mensajes.

DNS Tools: dig



DNS Hardening

Lista de Control de Acceso

- Listas de elementos que especifican direcciones IP's
- Cada elemento puede ser una dirección IP, un prefijo de IP o una lista de nombres
- Un prefijo de IP tiene el formato *red_en_formato_octal/bits_en_la_mascara*
  - 172.18/16 (red 172.18.0.0 con máscara de red 255.255.0.0)
- Formato:
  - **acl nombre_acl { lista_ips; };**
  - acl "red_cliente" { 172.18/16; };
- 4 sentencias reservadas:
  - **none** ("*ninguna dirección IP*")
  - **any** ("*cualquier dirección IP*")
  - **localhost** ("*cualquier dirección IP de localhost*")
  - **localnets** ("*cualquier red configurada en localhost*")

DNS Hardening: named.conf

```
acl "red_interna" { 192.168.122.0/24; };

options {
 directory "/var/named/zones";
 pid-file "/var/run/named.pid";
 allow-transfer { none; };
 allow-query { localnets; };
 version "Oculta deliberadamente";
 allow-recursion { "red_interna"; };
 recursive-clients 200;
};
```

DNS Hardening: logging

Canal

- El canal especifica a donde van los datos de log (a syslog, a un archivo, a la salida de error estándar de named, etc.)

Categoría

- La categoría especifica qué datos son los que se registran
- Cada categoría puede ser enviada a uno o a varios canales
- Los canales permiten filtrar la severidad del mensaje (*critical*, *error*, *warning*, *notice*, *info* (**default**), *debug* y *dynamic*)

DNS Hardening: logging

named.conf

```
logging {
  channel archivo {
     file "named.log" versions 9 size 10M;
     print-time yes;
     print-category yes;
     print-severity yes;
  };
  category default{ archivo; default_syslog; };
};
```

Administrative Tools

- **`named-checkconf`** checa la sintaxis del archivo named.conf
- **`named-checkzone`** checa un archivo maestro de zona en su sintaxis y composición
- **`rndc`** (*remote name daemon control*) permite el control remoto de las operaciones del *name server*
  - Se debe crear una llave con el comando:

    ```
    # rndc-confgen -a -b 512 -c /etc/bind/rndc.key
    ```

  - Con esta llave se crea el archivo de configuración **`rndc.conf`**

Administrative Tools: rndc

rndc.conf

```
options {
     default-server localhost;
     default-key "rndc-key";
};

key "rndc-key" {
     algorithm hmac-md5;
     secret "90aQ6gP9LrNwPIlG50h7HaarVRlfeV...";
};
```

Llave creada anteriormente

Administrative Tools: rndc

named.conf

```
controls {
  inet 127.0.0.1 port 953 allow  { localhost; } keys { "rndc-key"; };
};

key "rndc-key" {
     algorithm hmac-md5;
     secret "90aQ6gP9LrNwPIlG50YDErBk8TnCg...";
};
```

Llave creada anteriormente

Administrative Tools: rndc

Opción	Efecto
`halt`	Inmediatamente detiene el daemon *named*
`querylog`	Activa el registro de las consultas
`reload`	Indica al *name server* que cargue nuevamente los archivos de zona
`stats`	Guarda las estadísticas del servicio named en el archivo *named.stats*
`dumpdb`	Guarda el caché del DNS en el archivo *named_dump.db*
`flush`	Limpia la memoria caché
`status`	Muestra el estado del servicio *named*
`stop`	Detiene limpiamente al daemon *named*

DNS Domain Tools online

- tools.dnsstuff.com
- www.kloth.net/services/dig
- mxtoolbox.com/DNSLookup

DNS Design: DNS Slave

- Estos DNS están diseñados para proporcionar redundancia inherente y alta disponibilidad.
- El DNS secundario (*slave*) es un servidor autoritativo que obtiene información sobre una zona del servidor primario (*master*) a través de transferencia de zona.
- Periódicamente, el dns *slave* debe enviar una consulta de actualización para determinar si el contenido de la zona ha sido actualizado.

DNS Design: DNS Slave config

named.conf en DNS Master

```
options {
 ...
 allow-transfer { dns2.ejemplo.lab.; };
...
};
```

DNS Design: DNS Slave config

named.conf en DNS Slave

```
options {
 directory "/var/named/zones/slave";
 version "Oculta deliberadamente";
 allow-transfer { none; };
 allow-query { localnets; };
 allow-recursion { "red_interna"; };
 recursive-clients 200;
};
```

DNS Design: DNS Slave config

named.conf en DNS Slave

```
zone "ejemplo.lab" {
 type slave;
 file "ejemplo.lab.zone.slave";
 masters { 192.168.122.208; };
};

zone "0.168.192.in-addr.arpa" {
 type slave;
 file "192.168.0.zone.slave";
 masters { 192.168.122.208; };
};
```

IP Address de dns1.example.lab

DNS Zone Transfer: dig

```
$ dig axfr ejemplo.lab @dns1

; <<>> DiG 9.11.14-RedHat-9.11.14-2.fc30 <<>> axfr ejemplo.lab @dns1
;; global options: +cmd
; Transfer failed.
```

DNS Zone Transfer: dns slave

```
[root@dns2 ~]# rm -rf /var/named/zones/slave/*.slave

[root@dns2 ~]# systemctl restart named

[root@dns2 ~]# ls -l /var/named/zones/slave/*.slave
-rw-r--r--. 1 named named 454 Jul  9 00:27 /var/named/zones/slave/192.168.0.zone.slave
-rw-r--r--. 1 named named 526 Jul  9 00:27 /var/named/zones/slave/ejemplo.lab.zone.slave
```

Secure DNS Zone Transfer: tsig

- **TSIG** (*Transaction Signatures*) es el protocolo de autenticación de transacciones con llave cifrada para el DNS (*Secret Key Transaction Authentication for DNS*).

  Nota: TSIG *no es la solución adecuada para autenticar la comunicación entre varios servidores, ya que la administración de llaves se dificulta, ya que el número de llaves compartidas se incrementa de forma cuadrática por cada servidor adicional.*

- Es necesario que se configure una llave en cada entidad

DNS Zone Transfer: tsig

DNS Master

1. **Crear la llave tsig**

```
# dnssec-keygen -a HMAC-MD5 -b 512 -n HOST dns1-dns2.ejemplo.lab.
```

2. **Este comando crea un par de archivos que contienen las llaves generadas:**

```
# ls -l

-rw------- 1 root root 130 Jun 30 00:53 Kdns1-dns2.ejemplo.lab.+157+11948.key

-rw------- 1 root root 229 Jun 30 00:53 Kdns1-dns2.ejemplo.lab.+157+11948.private
```

DNS Zone Transfer: tsig

named.conf en DNS Master

```
options {
...
 allow-transfer { key dns1-dns2.ejemplo.lab.; };
 ...
};
key dns1-dns2.ejemplo.lab. {
        algorithm hmac-md5;
        secret "KtEvyFMM9vf5djEPTA3VFK1TNUz3k+2xOK1g...";
};
```

DNS Zone Transfer: tsig

named.conf en DNS Slave

```
key dns1-dns2.ejemplo.lab. {
        algorithm hmac-md5;
        secret "KtEvyFMM9vf5djEPTA3VFK1TNUz3k+2xOK1g...";
};

server 192.168.122.208 {
      keys { dns1-dns2.ejemplo.lab.; };
};
```

Referencias

- Administración de DNS
  - https://darkaxl017.fedorapeople.org/slides/Administracion_DNS.pdf
- BIND 9 Administrator Reference Manual
  - https://downloads.isc.org/isc/bind9/cur/9.16/doc/arm/Bv9ARM.pdf
- DNS 101: An introduction to Domain Name Servers
  - https://www.redhat.com/sysadmin/dns-domain-name-servers
- How to: Múltiples instancias de bind en un mismo server
  - http://www.rootzilopochtli.com/2015/07/how-to-multiples-instancias-de-bind-en-un-mismo-server/

Material

- rootzilopochtli/dns101
  - https://github.com/rootzilopochtli/dns101

Comunidades: Únete!

- **SysArmy México**
  - https://www.meetup.com/es/Sysarmy-Mexico/
  - https://t.me/sysarmymx
- **Fedora México**
  - https://www.meetup.com/es-ES/Fedora-Mexico/
  - https://t.me/fedoramexico
  - https://fedoramx.fedorapeople.org/


Gracias!