Manual de Zimbra parte I, Instalación de Bind 9 en CentOS 7, DNS Público, Registro de Dominio.

Iniciamos esta serie de Manuales de Zimbra, que se dicta en el curso de Zimbra de Aula Útil, asumiendo primero que ya instalamos previamente un firewall UTM, donde tenemos la Ip pública nateando hacia un servidor CentOS 7 en zona DMZ para instalar y configurar nuestro servidor Zimbra. Primero debemos registrar un dominio público y configurar un DNS público.

Tabla de Contenidos

1.- Conceptos Básicos de Resolución de Nombres

Los nombres de host se pueden resolver por 2 métodos - De forma local, poniendo nombre al equipo con **hostnamectl** y editando el archivo **/etc/hosts** - En red, con el uso de un **servidor DNS** y configurando el cliente en **/etc/resolv.conf**

1.1- Nombre de Host del equipo local

La resolución local de host del equipo, se hace con el nombre de host y se asigna con el comando hostnamectl

```
hostnamectl set-hostname mail.aulautil.tk
exit

#Abrir un nuevo terminal y comprobar el nuevo nombre con
hostnamectl
```

1.2.- Resolución Local de Hostnames y dominios

La resolución local de nombres de hosts y dominios se hace con el archivo /etc/hosts Ej.

```
vim /etc/hosts
127.0.0.1 localhost localhost.localdomain
192.168.3.201 mail.aulautil.tk mail
190.81.56.202 www.cualquierdominio.com www.quesemeocurra.com

ping mail.aulautil.tk
```

1.3.- Resolución de hosts y dominios en red

Para resolver nombres de hosts y dominios en red, usamos un servidor DNS. Los servidores DNS puede estar desplegados en diferentes zonas

1.3.1.- DNS WAN:

Es el servidor DNS que resuelve con Ips públicas los nombres de nuestros dominios Ej:

```
mail.aulautil.tk  --> 149.56.218.201
```

1.3.2.- DNS DMZ:

Es el servidor DNS que resuelve con Ips privadas los nombres de los servidores de la DMZ solo se usa en DMZ, no debe ser usado en la LAN

Ej:

```
mail.aulautil.tk  --> 192.168.3.201
```

1.3.3.- DNS LAN:

Es el servidor DNS que resuelve con Ips privadas los nombres de los pcs y servidores de la LAN; así como de los servidores DMZ con sus ips privadas; el DNS de LAN no debe ser usado en la DMZ

Ej:

```
mail.aulautil.tk  --> 192.168.3.201
pc1.aulautil.tk  --> 192.168.100.20
```

2.- Registros de DNS y Cliente DNS

2.1.- Cliente de DNS

El cliente DNS se configura en el archivo /etc/resolv.conf

```
vim /etc/resolv.conf
nameserver 8.8.8.8
```

En CentOS 7 el archivo resolv.conf es generado por la utilidad de red, por eso hay que editar el archivo de configuración de red y agregar el parámetro **DNS1**

Ej: Tenemos una tarjeta de red llamada **ens18** (esto se sabe con el comando **ip addr show**)

```
vim /etc/sysconfig/network-scripts/ifcfg-ens18
...
DNS1=8.8.8.8
....

systemctl restart network
cat /etc/resolv.conf
```

2.2.- Registros de DNS

Registro	Valor
A	Zona de dominio (ej: mail.dominio.com --> 149.56.218.3)
NS	Name Server (Servidores DNS del dominio)
SOA	Servidor DNS principal (Server of Authorization)
MX	Servidores de correo (Mail Exchange)
TXT	Información adicional del dominio (ej: SPF para hotmail)
CNAME	Alias de una zona de dominio (ej: web --> www.dominio.com)
PTR	Resolución Inversa (ej: 149.56.218.3 --> mail.dominio.com)

2.3.- Comprobación de registros DNS con dig

Instalar dig

```
yum -y install bind-utils
```

Dig tiene las siguientes Secciones

QUESTION SECTION consulta que se está realizando **ANSWER SECTION** respuesta (si la hubiera de la consulta) **AUTHORITY SECTION** detalle de los servidores de autorización (SOA) **ADDITIONAL SECTION** información adicional de zonas y otros

Ejercicios:

2.4.- Registro A

Verificar la zona de dominio www.dominio.com

```
dig www.dominio.com
;; QUESTION SECTION:
;www.dominio.com.               IN      A       ------> consulta

;; ANSWER SECTION:
www.dominio.com.        5       IN      A       190.102.150.200   -----> respuesta
```

2.5.- Registro NS

Verificar los DNS Server de dominio.com

```
dig NS dominio.com
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
```

```
;dominio.com.                  IN      NS

;; ANSWER SECTION:
dominio.com.           2257    IN      NS      ns2.telmex.net.pe.
dominio.com.           2257    IN      NS      ns1.telmex.net.pe.
```

2.6.- Registro MX

Verificar los servidores de correo de dominio.com

```
dig MX dominio.com
;; QUESTION SECTION:
;dominio.com.                  IN      MX

;; ANSWER SECTION:
dominio.com.           6245    IN      MX      10 mx1.dominio.com.
dominio.com.           6245    IN      MX      10 mx2.dominio.com.
dominio.com.           6245    IN      MX      10 mx4.dominio.com.
dominio.com.           6245    IN      MX      10 mx5.dominio.com.
dominio.com.           6245    IN      MX      20 mx3.dominio.com.
dominio.com.           6245    IN      MX      20 mx6.dominio.com.
```

Ejemplo de Configuración de los Registros MX

Balanceo de Carga

dominio.com. IN MX 10 ns.dominio.com. dominio.com. IN MX 10 ns1.dominio.com.

Alta Disponibilidad

dominio.com. IN MX 10 ns.dominio.com. dominio.com. IN MX 20 ns1.dominio.com.

2.7.- Registro PTR

El PTR verifica que una IP tenga un nombre de hosts, normalmente se aplica a los servidores de correo

Primero verificamos cuales son los servidores de correo de un dominio

```
dig MX dominio.com
dominio.com.        6245    IN  MX  10 mx1.dominio.com.
```

Ahora preguntamos por el registro A de uno de los servidores de correo

```
dig mx1.dominio.com
;; QUESTION SECTION:
;mx1.dominio.com.              IN      A
```

```
;; ANSWER SECTION:
mx1.dominio.com.       1310    IN      A       181.65.173.25
```

Vemos que la IP de mx1.dominio.com es 181.65.173.25 pasamos ahora a preguntar por el PTR de ese IP

```
dig -x 181.65.173.25
;; QUESTION SECTION:
;25.173.65.181.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
25.173.65.181.in-addr.arpa. 3596 IN     PTR     mx1.dominio.com.
```

2.8.- Registro TXT (SPF)

Verificar si hay registro SPF en el dominio dominio.com

```
dig TXT dominio.com
;; QUESTION SECTION:
;dominio.com.                   IN      TXT

;; ANSWER SECTION:
dominio.com.           7199    IN      TXT     "v=spf1 mx
include:spf.masterbase.com ~all"
```

Para crear un registro SPF ir a www.spfwizard.com

Verificar TODOS los registros de DNS del dominio dominio.com

```
dig ANY dominio.com

;; QUESTION SECTION:
;dominio.com.           IN  ANY

;; QUESTION SECTION:
;dominio.com.                   IN      ANY

;; ANSWER SECTION:
dominio.com.           6926    IN      TXT     "v=spf1 mx
include:spf.masterbase.com ~all"
dominio.com.           5362    IN      MX      20 mx6.dominio.com.
dominio.com.           5362    IN      MX      10 mx1.dominio.com.
dominio.com.           5362    IN      MX      10 mx2.dominio.com.
dominio.com.           5362    IN      MX      10 mx4.dominio.com.
dominio.com.           5362    IN      MX      10 mx5.dominio.com.
dominio.com.           5362    IN      MX      20 mx3.dominio.com.
dominio.com.           1088    IN      NS      ns1.telmex.net.pe.
dominio.com.           1088    IN      NS      ns2.telmex.net.pe.
```

Verificar si hay zona de dominio configurado para el dominio raiz dominio.com

```
dig dominio.com
;; QUESTION SECTION:
;dominio.com.                   IN      A

;; AUTHORITY SECTION:
dominio.com.            1734    IN      SOA     ns1.telmex.net.pe.
dnsmaster.telmex.net.pe. 2014101302 5400 600 90000 7200
```

Vemos que no está configurado el dominio raíz como zona A (mala práctica)

2.9.- Verificación de todos los registros mediante transferencias de zonas

```
dig axfr @DNSSERVER DOMINIO
dig axfr @ns1.telmex.net.pe dominio.com
```

3.- Configuración del dominio público de Internet, selección de la Ip pública

Los dominios públicos se adquieren en un proveedor de Dominios (register) Godaddy : com, org, net, cloud, etc ... RCP : pe, com.pe, org.pe ... Freenom : tk, ml ... (dominios gratuitos por 1 año)

3.1.- Seleccionar una Ip pública

Las Ip pública para el servidor de correo Zimbra deben estar limpia, usaremos como ejemplo la IP 149.56.218.201

Adicionalmente para verificar si la Ip está en listas negras ir a: MultiRBL http://multirbl.valli.org/

También debemos configurar en el Firewall perimetral: - Un Nat de entrada (DNAT) desde la Ip pública hacia la Ip privada del servidor zimbra (Ej: 192.168.3.201). Ej con iptables:

```
# DNS público
iptables -t nat -I PREROUTING -p udp -d 149.56.218.201 --dport 53 -j DNAT --to
192.168.3.201:53
# SMTP
iptables -t nat -I PREROUTING -p tcp -d 149.56.218.201 --dport 25 -j DNAT --to
192.168.3.201:25
# Https
```

```
iptables -t nat -I PREROUTING -p tcp -d 149.56.218.201 --dport 443 -j DNAT --to
192.168.3.201:443
```

Un Nat de salida (SNAT) desde la Ip privada del servidor Zimbra para que salga a la WAN con la IP pública asignada. Ej con iptables:

```
iptables -t nat -I POSTROUTING -s 192.168.3.201 -j SNAT --to 149.56.218.201
```

3.2.- Registrar un dominio público gratuito en freenom

Crear una cuenta en Freenom (usar la cuenta google) Ir a la derecha superior, click en registrarse Loguearse con cuenta google, facebook, o ms

3.2.1.- Registrar un nuevo dominio

Service --> Register a New Domain ej: aulautil.tk Selected y luego checkout Period: 12 Months Free ---> Continue LLENAR DATOS del Formulario Dar checkc en: I have read and agree to the Terms & Conditions Finalizar con Complete Order Click here to go to client area

3.3.2.- Comprobar Registro

Services --> My Domains

3.3.3.- Configurar los registros pegamento o nombres de host de los DNS server

Se deben registrar primero los nombres de hosts de los servidores DNS asociados a la IP pública del VPS Ej:

```
ns1.aulautil.tk ---> 149.56.218.201
ns2.aulautil.tk ---> 149.56.218.201
```

Ir a Freenom Services --> My Domains click en la fila del dominio en el botón "Manage Domain" Management Tools --> Register Glue Records Register a NameServer Name Namserver: NS1 IP: 149.56.218.201 Save Changes

Register a NameServer Name Namserver: NS2 IP: 149.56.218.201 Save Changes

Click en Back

3.3.4.- Configurar los DNS Server del dominio

Click en Management Tools --> Nameservers Use custom Nameserver: Nameserver 1: ns1.aulautil.tk Nameserver 2: ns2.aulautil.tk

Click Change Nameservers

3.3.5.- Nat de Puerto desde firewall

Una vez que hemos adquirido nuestro dominio púbico y asociado los DNS a nuestro Ip público, lo que debemos hacer es un NAT de destino desde la IP pública, puerto 53/udp hacia la Ip interna de nuestro servidor Zimbra, que se le configurará también como servidor de DNS público. Esto se configura en el firewall perimetral de la empresa

4.- Configuración del Servidor DNS Público en modo enjaulado chroot

Instalar los paquetes de servidor de DNS, bind 9

```
yum -y install bind bind-chroot bind-utils
```

Para configurar el DNS público seguimos los siguientes procedimientos: - Copiar los archivos de dns al entorno chroot - Generar la firma digital - Copiar la firma digital al entorno chroot - Configurar los parámetros de DNS y el dominio en el archivo principal de configuración de bind /var/named/chroot/etc/named.conf - Configurar los registros de dns en el archivo /var/named/chroot/var/named/dominio.com.zone - Reiniciar el servidor DNS - Configurar el dns cliente el archivo /etc/resolv.conf apuntado a nuestra propia ip - Configurar la resolución inversa en el proveedor de Internet (ISP) o en el panel del hosting de VPS contratado - Hacer consultas de nuestro dominio con dig

4.1.- Copiar los archivos del DNS al entorno chroot

```
cd /var/named
for f in named.* data dynamic slaves; do mv $f chroot/var/named/; ln -s
/var/named/chroot/var/named/$f /var/named/; done
```

4.2.- Generar la Firma Digital

```
rndc-confgen -a -c /etc/rndc.key
chown named:named /etc/rndc.key
```

4.3.- Copiar la firma digital al entorno chroot

```
cd /etc
for f in named.* rndc.key; do mv $f /var/named/chroot/etc/; ln -s
/var/named/chroot/etc/$f /etc/; done
```

Nota

Si se falla en algùn procedimiento en la instalación desinstalar y volver a instalar

ejecutar solo si hubo error al instalar $> yum erase bind bind-chroot bind-utils $> rm -fR /var/named $> rm -fR /etc/named* $> rm -f /etc/rndc.key $> yum -y install bind bind-chroot bind-utils

4.4.- Configurar los parámetros de DNS y el dominio en el archivo principal de configuración de bind

```
vim /var/named/chroot/etc/named.conf
```

```
//
// 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 {
// Ips en la que el demonio named escuchará las peticiones
// 149.56.218.201 es la Ip pública del dominio para zimbra
        listen-on port 53 { 149.56.218.201;};
        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";
// este parametro permite establecer quienes pueden usar el servidor DNS
        allow-query     { localhost; any; };
// este parametro permite reenviar las consultar hacia el servidor DNS publico;
// para aquellos dominios que no se resuelven en este servidor
        forwarders   { 8.8.8.8; };
        forward first;
        allow-transfer      {"none";};
        recursion           no;

        dnssec-enable no;
        dnssec-validation no;
        dnssec-lookaside auto;

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

```
};

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

// Zona raiz por defecto
zone "." IN {
        type hint;
        file "named.ca";
};

// Zona para nuestro dominio
zone "aulautil.tk" {
    type master;
    file "/var/named/chroot/var/named/aulautil.tk.zone";
    allow-update { none; };
};



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

4.5.- Creando los archivo zone por los dominios configurados

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

```
vim  aulautil.tk.zone
```

```
$TTL    86400
; @ representa este servidor
@                   IN SOA  @ root (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

; registro              IN      Tipo  Valor secundario  Valor principal
; ----------------     ------   ----  ----------------  ------------------
; cuando no hay nada en primera columna es igual a aulautil.tk.
aulautil.tk.        IN      NS                      ns1.aulautil.tk.
aulautil.tk.        IN      NS                      ns2.aulautil.tk.
; www es formato SQDN (Short Qualify Domain Name)
ns1                     IN      A                       149.56.218.201
ns2                     IN      A                       149.56.218.201
www                     IN      A                       149.56.218.201
; mail.aulautil.tk. es formato FQDN (Full Qualify Domain Name)
```

```
mail.aulautil.tk.       IN      A                       149.56.218.201
; el dominio raiz como zona A
aulautil.tk.            IN      A                       149.56.218.201
aulautil.tk.            IN      MX              10      mail.aulautil.tk.
```

4.6.- Configuración de PTR

El PTR debe configurarse; solicitando al Proveedor de Internet que ponga un nombre de host a la IP pública. Es probable que si contratamos servidores cloud, tengamos una opción para poner el PTR a las Ips públicas.

Reiniciar los servicios

```
systemctl start named
systemctl enable named
systemctl status named
```

Si salen errores en el servicio; verificar los logs

```
tail -f /var/log/messages
less /var/log/messages
G
```

Nota si sale errores de permisos o selinux

```
chgrp -R named /var/named/chroot/var/named
restorecon -FRvv /var/named/chroot/var/named
```

4.7.- Reglas de Firewall para habilitar el puerto 53 UDP del servidor DNS

Instalar firewalld

```
yum -y install firewalld
systemctl enable firewalld
systemctl start firewalld
```

Habililitar el servicio DNS

```
firewall-cmd --add-service dns --permanent
firewall-cmd --reload
```

Verificar el firewall con

```
iptables -S | grep 53
```

Natear en el Firewall UTM, ej: Endian el puerto 53 UDP hacia la IP interna de Zimbra

4.8.- Comprobación del DNS público (Ejecutar en su máquina local laptop)

Comprobación del DNS

```
dig NS aulautil.tk
dig MX aulautil.tk
ping mail.aulautil.tk
```

4.9.- Crear un registro SPF para el dominio

Entrar a spfwizard.com y poner nuestro dominio Domain: aulautil.tk Current MX handlers: mail.aulautil.tk (pref 10) : YES Current IP Address: 149.56.218.201 YES Enter any IP addresses in CIDR format for netblocks that originate or relay mail for this domain 149.56.218.201 How stringent should SPF-aware MTAs treat this? Soft fail:

EL valor generado: **aulautil.tk. IN TXT "v=spf1 mx a ip4:149.56.218.201 ~all"** Lo copiamos en nuestro archivo de DNS

```
vim /var/named/chroot/var/named/aulautil.tk.zone  (agregar al final)
; registro SPF para el correo
aulautil.tk.      IN TXT     "v=spf1 mx a ip4:149.56.218.201 ~all"
```

```
systemctl restart named
```

Comprobación desde nuestra laptop

```
dig TXT aulautil.tk
```