Pràctica 3
Sessió 3 - Implementar un servei DNS

Alumnes:
Mariona Farré Tapias,
Marc Pérez Guerrero

CARPETA VMS ENTREGA 3:
https://drive.google.com/drive/folders/1PVCHIntB0E07nq8ZiVUU3XHrIFrSaQmU?usp=sharing

---

ÍNDEX:

Enunciat

1- Configurar un servei de DNS.

- El servei estarà mantingut per dos servidors "dns1" i "dns2" que compartiran les següents caractarístiques:
  + Resoldran les peticions utilitzant forwarders.
  + Acceptaran peticions recursives només per les xarxes internes.
  + Disposen d'un servidor de SSH.

- Es defineixen dos dominis: "seax.edu" (màquines xarxes internes) i "public.seax.edu" (serveis al cloud de la UPC).
- Cada domini té un servidor màster i un slave diferents.
- El domini "seax.edu" te una zona directa i una inversa

  + Inclourà totes les adreces IP de totes les màquines de l'escenari llevat els routers (ie. servidors DNS, monitors i servidor nagios).
  + Als servidors "dns1" i "dns2" se'ls crearà uns àlias anomenats "ssh1" i "ssh2", respectívament.

+ Al servidor "nagios" se li crearà un àlias anomenat "monitor".
+ Estarà mantingut per dos servidors: "dns1" com a màster i "dns2" com esclau.

- El domini "seax.public.edu" només té zona directa
+ "dns2" en serà el màster i "dns1" l'esclau.
+ Contindrà les màquines de la DMZ "dns1" i "dns2" amb els mateixos àlies que abans, ie. "ssh1" i "ssh2".
+ Les màquines "dns1" i "dns2" compartiran la mateixa IP, la de la interfície que dóna a la xarxa troncal del router d'accés. (Nota: si no podeu fixar aquesta IP, us la inventeu, per ex. 192.168.1.1).
+ També els següents serveis situats al cloud de la UPC: la web "www.public.seax.edu", amb IPs 147.83.2.135 i 2001:40b0:7500:1::21

- Cal verificar que les zones estan ben escrites.
- Cal verificar el funcionament del servei resolent consultes dels dominis propis i d'altres.
- (opcional) Investigueu i comenteu si hi ha algun mecanisme que permeti implementar una coordinació del DNS i el DHCP, en un mateix servidor.

3- Protecció dels servidors de DNS
- Apliqueu les directrius de seguretat específiques pels servidors definides a la sessió 1 i 2
- Expliqueu com podríeu fer que només fossin accessibles els serveis de de DNS i SSH i, en el cas del servei SSH només des de les adreces IP 10.1.10.11 i 10.1.20.11.
- (Opcional) Implementeu i el punt anterior i verifiqueu el seu funcionament.

4- Lliurar els resultats.

Mitjançant Atenea (2 fitxers).
- Redactar l'informe de la pràctica p3_s3_cognom1_nom.txt.
- Realitzar les proves necessàries per justificar els resultats i encapsular els fitxers necessaris en el fitxer p3_s3_cognom1_nom.zip.

Mitjançant Google Drive (màquines virtuals)
- Compartir amb rafael.vidal@upc.edu una carpeta a Google Drive (UPC) amb les VMs dels 2 DNSs.

Important:
- L'informe de la pràctica ha de contenir l'enllaç a la carpeta amb les VMs.
- Les VMs han de contenir una còpia de l'informe al directori /root.

5- A títol orientatiu el resultat de la pràctica cal que doni resposta a les següents qüestions:

- Quines màquines i adreces IP formen el domini? (treballeu amb adreces privades)
- Cal instal·lar algun paquet de programari?
- Com es configura un servidor per ser màster (o esclau) d'un domini?

- Com es delega una part d'una domini?
- Com es pot verificar que un servidor fa d'esclau d'un altre?
- Com es configura una zona en un servidor (directa i inversa)?
- Com es controla l'acceptació de peticions recursives?
- Com es comprova la sintaxi d'un fitxer de zona?
- Com es comprova que un servidor funciona correctament?
- Relacionat amb l'anterior, quines eines de consola hi ha per fer aquest comprovació? Com s'han d'utilitzar?
- Com es verifica que el domini funciona correctament?
- Com fer que un servidor de DNS resolgui peticions de dominis pels que no és màster/esclau?
- Com es limiten els accessos als serveis d'una màquina?
- Com es comprova que aquests accesos han estat correctament limitats?
- (opcional) Com es pot coordinar en un mateix servidor el DNS i el DHCP?

Informe pràctica 2 sessió 3:

***** Introducció de l'escenari:**

L'escenari que estem configurant implica la implementació de dos servidors DNS, "dns1" i "dns2", que juguen un paper crucial en la gestió de la resolució de noms dins d'una infraestructura de xarxa més àmplia. Aquestes màquines són noves i han estat configurades per operar dins d'una zona desmilitaritzada (DMZ), la qual actua com un pont entre la nostra xarxa interna segura i l'Internet públic.

La DMZ és especialment dissenyada per a allotjar serveis que necessiten estar accessibles des de l'exterior, però al mateix temps, mantenint aïllada la resta de la xarxa interna de possibles amenaces externes. Això fa que la ubicació dels nostres servidors DNS en aquesta zona sigui estratègica, ja que permeten processar peticions de resolució de noms tant per als usuaris dins de l'organització com per als que es troben fora d'ella, sense comprometre la seguretat dels sistemes intern.

Els servidors DNS estan configurats per utilitzar "forwarders" per resoldre les peticions que ells mateixos no poden processar directament, millorant l'eficiència de la resolució de noms i reduint la càrrega sobre els propis servidors. També estan configurats per acceptar peticions recursives exclusivament de les xarxes internes, protegint així contra possibles atacs de denegació de servei distribuït (DDoS) o altres amenaces que podrien ser llançades des de l'Internet.

La configuració d'aquests servidors DNS no només implica l'aspecte tècnic de la instal·lació i configuració del programari DNS com BIND, sinó també la planificació detallada de la seguretat, incloent la gestió de l'accés a través de SSH només des d'adreces IP específiques, i la implementació de regles de tallafocs que limiten el tràfic a la DMZ.

Amb aquests servidors DNS, l'organització pot gestionar eficientment els dominis "seax.edu" per a les màquines en xarxes internes i "public.seax.edu" per a serveis allotjats al núvol, amb cada domini gestionat per un servidor màster i un esclau diferents, assegurant així redundància i disponibilitat del servei.

***** Configuració inicial de les màquines:**

Per configurar els servidors dns1 i dns2 hem de configurar inicialment una nova màquina virtual.

Pels diferents dominis podem veure que:
Domini seax.edu

- dns1.seax.edu
  IP: 10.1.10.3: Aquesta és l'adreça IP assignada al servidor DNS primari, que actua com a màster per a la zona.
- dns2.seax.edu

IP: 10.1.10.4: Aquesta és l'adreça IP assignada al servidor DNS secundari, que actua com a esclau per a la zona.

- monitor.seax.edu
  IP: 10.1.10.11: Aquesta és l'adreça IP assignada al servidor Nagios, que probablement s'utilitza per a la monitorització de la xarxa i els serveis.

ssh1.seax.edu - Alias que apunta a dns1.seax.edu.
ssh2.seax.edu - Alias que apunta a dns2.seax.edu.

Zona inversa per a 10.1.10.0/28
Seran les mateixes ips, ja que estan en una xarxa local:

- dns1.seax.edu:
  IP: 10.1.10.3 Resolució inversa per a l'adreça IP del servidor DNS primari.
- dns2.seax.edu:
  IP: 10.1.10.4 - Resolució inversa per a l'adreça IP del servidor DNS secundari.
- monitor.seax.edu
  IP: 10.1.10.11 - monitor.seax.edu: Resolució inversa per a l'adreça IP del servidor Nagios.

Primer de tot, lo més inicial és canviar els noms de les màquines per establir quina és el DNS1 i el DNS2:
Obre el fitxer amb un editor de textos el fitxer de hostnames: nano /etc/hostname
Esborrar el nom actual i escriure dns1 per al primer servidor o dns2 per al segon.

Després editar el fitxer /etc/hosts:
Configurar línia per al nou nom del host que apunti a la teva adreça IP local del servidor:
    10.1.10.3 dns1

Canvia 10.1.10.3 o 10.1.10.4 el corresponent segons si estàs configurant dns1 o dns2.

Al fer un reboot el nom de la màquina s'haurà canviat sortint a la terminal: root@dns1 o root@dns2

Configurar les ips de les màquines sota els nous noms i pels nous noms de les interfícies, així que en el fitxer /etc/network/interfaces configurar:

Pel dns1:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth-dmz
```

```
iface eth-dmz inet static
        address 10.1.10.3
        netmask 255.255.255.240
        gateway 10.1.10.1
```

Pel dns2:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth-dmz
iface eth-dmz inet static
        address 10.1.10.4
        netmask 255.255.255.240
        gateway 10.1.10.1
```

També canviar el nom de les interfícies per continuar amb l'escenari actual, posant el nom de la interfície eth-dmz per la connexió amb la xarxa DMZ dins dels diferents servidors.
Per fer això crear el fitxer de cat /etc/systemd/network/10-enp0s3-net.link
Segons la interfície que es connecti en la xarxa DMZ, en el nostre cas el enp0s3.
I modificar el fitxer posant:
/etc/systemd/network/10-enp0s3-net.link

```
[Match]
OriginalName=enp0s3

[Link]
Name=eth-dmz
```

Això actualitzar-ho en els dos servidors i fer un reboot per guardar i aplicar els canvis.

Una vegada ja hem configurat tots els noms de l'escenari, s'han d'instalar alguns paquets importants per ajudar amb la configuració dels servidorss, per això executar:

```
apt install bind9 bind9utils bind9-doc dnsutils -y
```

On els paquets instal·lats son per:

bind9: És el paquet bàsic que conté el servidor DNS, essencial per resoldre i gestionar noms de domini.
bind9utils: Aporta utilitats addicionals per administrar el servidor DNS, com ara controlar el servidor a distància.

bind9-doc: Proporciona la documentació necessària per entendre i configurar correctament les funcionalitats de BIND.
dnsutils: Inclou eines de diagnòstic com dig i nslookup, que són fonamentals per verificar la configuració del DNS i solucionar problemes de resolució de noms.

***** Configuració dels servidors:**

Una vegada tenint aquesta configuració inicial, podem anar configurant els diferents serveis del dns, per això necessitarem modificar el fitxer : /etc/bind/named.conf.options
Es important per poder establir forwarders, que permet al servidor DNS reenviar consultes que no pot resoldre localment a uns servidors DNS específics, usualment proporcionats per l'ISP o triats per fiabilitat i velocitat. Això pot millorar l'eficiència de la resolució de noms.
i també permetre Consultes i Recursions, determina quins clients poden fer consultes recursives al servidor. Això és important per limitar el servei DNS a usuaris autoritzats i evitar abús del servidor, com ara atacs de denegació de servei (DDoS).

Ara la configuració dels servidors dns1:
/etc/bind/named.conf.options

```
…
        forwarders {
                212.166.132.192;
                212.166.132.96;
                1.1.1.1;
                8.8.8.8;
                8.8.4.4;
        };

        allow-query { any; };
        allow-recursion { 10.1.0.0/16; };

//========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys

//========================================================================

        listen-on { 10.1.10.3; };
        listen-on { 10.1.10.4; };
        listen-on-v6 { none; };

        dnssec-validation auto;
        auth-nxdomain no;
};
```

Ara la configuració dels servidors dns2:

```
..
forwarders {
                212.166.132.192;
```

```
                212.166.132.96;
                1.1.1.1;
                8.8.8.8;
        };


//========================================================================
===
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys

//========================================================================
===

        allow-query { any; };
        allow-recursion { 10.1.0.0/16; };

        listen-on { 10.1.10.3; };
        listen-on { 10.1.10.4; };
        listen-on-v6 { none; };

        dnssec-validation no;

        auth-nxdomain no;
};
```

Les diferents línies noves signifiquen:
forwarders { 212.166.132.192, 212.166.132.96,1.1.1.1; 8.8.8.8; 8.8.4.4; } : Aquesta configuració especifica que les consultes DNS que no es poden resoldre localment han de ser reenviades a aquests servidors DNS externs (1.1.1.1 de Cloudflare, 8.8.8.8 i 8.8.4.4 de Google i 212.166.132.192, 212.166.132.96 són els dns de virutalbox). Això pot ajudar a millorar la velocitat i fiabilitat de la resolució de DNS fent ús de la infraestructura d'altres proveïdors

allow-query { any; }; Permet que qualsevol client pugui fer consultes a aquest servidor DNS. Això significa que no hi ha restriccions sobre qui pot utilitzar aquest servidor per a la resolució de noms.

allow-recursion { 10.1.0.0/16; }; Restringeix les peticions recursives només als clients dins de la xarxa 10.1.0.0/16. Aquesta mesura de seguretat prevé que el servidor DNS sigui utilitzat per atacs de reflexió o amplificació per part de usuaris malintencionats fora d'aquest rang d'IPs.

listen-on { 10.1.10.3; 10.1.10.4; }; Especifica les adreces IP locals en les quals el servidor BIND escoltarà les peticions de DNS. Això limita la recepció de peticions només a aquestes interfícies de xarxa.

listen-on-v6 { none; }; Desactiva l'escolta per a les adreces IPv6, indicant que el servidor només respondrà a peticions sobre IPv4.

dnssec-validation auto; Habilita la validació automàtica de DNSSEC, que és una capa de seguretat que verifica la autenticitat de les respostes a les consultes DNS per prevenir atacs de 'man-in-the-middle'.

auth-nxdomain no; Indica que el servidor no hauria de respondre afirmativament amb respostes NXDOMAIN que no vinguin autoritativament dels servidors DNS que gestionen aquestes zones. Això pot ajudar a evitar el 'DNS poisoning'.

***** Configuració de les zones:**

Ara s'han de configurar totes les zones directes i inverses en un servidor DNS com BIND és un procés clau per gestionar la resolució de noms de domini i les respostes a consultes sobre adreces IP.
La configuració de la zona directa és la responsable de la traducció de noms de domini a adreces IP.
I la configuració de zona inversa és la utilitzada per traduir adreces IP a noms de domini.

**** La zona Inversa**

Després s´han de configurar localment les zones dels dos servidors:

Pel dns1:
/etc/bind/named.conf.local

```
zone "seax.edu" {
        type master;
        file "/etc/bind/zones/db.seax.edu";
        allow-transfer { 10.1.10.4; };
};

zone "10.1.10.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/db.10.1.10";
        allow-transfer { 10.1.10.4; };
};

zone "10.1.20.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/db.10.1.20";
        allow-transfer { 10.1.10.4; };
};

zone "public.seax.edu" {
        type slave;
        file "/var/cache/bind/db.public.seax.edu";
        masters { 10.1.10.4; };
```

```
};
```

Pel dns2:

/etc/bind/named.conf.local

```
zone "seax.edu" {
        type slave;
        file "/var/cache/bind/db.seax.edu";
        masters { 10.1.10.3; };
};

zone "10.1.10.in-addr.arpa"  {
        type slave;
        file "/var/cache/bind/db.10.1.10";
        masters { 10.1.10.3; };
};

zone "10.1.20.in-addr.arpa"  {
        type slave;
        file "/var/cache/bind/db.10.1.20";
        masters { 10.1.10.3; };
};
zone "10.1.20.in-addr.arpa"  {
        type master;
        file "/var/cache/bind/db.10.1.20";
        allow-transfer { 10.1.10.3; };
};
zone "public.seax.edu" {
        type master;
        file "/etc/bind/zones/db.public.seax.edu";
        allow-transfer { 10.1.10.3; };
};
```

Configuració per a dns1

zone "seax.edu": Tipus: master Fitxer de zona: /etc/bind/zones/db.seax.edu
Permet transferències de zona a: 10.1.10.4 (direcció IP de dns2)
dns1 actua com a servidor principal (master) per la zona seax.edu, gestionant el fitxer de zona primari i permetent transferències de zona al servidor secundari.

zone "10.1.10.in-addr.arpa" Tipus: master Fitxer de zona: /etc/bind/zones/db.10.1.10
Permet transferències de zona a: 10.1.10.4
Similar a la zona anterior, dns1 és el master per a la zona inversa, gestionant el mapeig IP a noms de domini i permetent la sincronització amb dns2.

zone "10.1.20.in-addr.arpa" Tipus: master Fitxer de zona: /etc/bind/zones/db.10.1.20
Permet transferències de zona a: 10.1.10.4

Similar a la zona anterior, dns1 és el master per a la zona inversa, gestionant el mapeig IP a noms de domini i permetent la sincronització amb dns2.

zone "public.seax.edu" Tipus: slave Fitxer de zona:/var/cache/bind/db.public.seax.edu
Permet transferències de zona a: 10.1.10.4 (direcció IP de dns2)
Aquí, dns1 actua com a servidor esclau per la zona public.seax.edu, un cas únic on els rols s'inverteixen comparat amb les altres zones. dns1 permet transferències de zona cap a dns2.

Configuració per a dns2

zone "seax.edu" Tipus: slave Fitxer de zona: /var/cache/bind/db.seax.edu
Servidors master: { 10.1.10.3; } (direcció IP de dns1)
dns2 actua com a servidor secundari (slave) per la zona seax.edu, sincronitzant el seu contingut del fitxer de zona des del servidor master.

zone "10.1.10.in-addr.arpa" Tipus: slave Fitxer de zona: /var/cache/bind/db.10.1.10
Servidors master: { 10.1.10.3; }
De manera similar, per a la zona inversa, dns2 sincronitza les seves dades del master, dns1.

zone "10.1.20.in-addr.arpa" Tipus: master Fitxer de zona: /etc/bind/zones/db.10.1.20
Permet transferències de zona a: 10.1.10.4 Similar a la zona anterior, dns1 és el master per a la zona inversa, gestionant el mapeig IP a noms de domini i permetent la sincronització amb dns2.

zone "public.seax.edu" Tipus: master Fitxer de zona: /etc/bind/zones/db.public.seax.edu
Permet transferències de zona a: 10.1.10.3 (direcció IP de dns1)
Aquí, dns2 actua com a servidor master per la zona public.seax.edu, un cas únic on els rols s'inverteixen comparat amb les altres zones. dns2 permet transferències de zona cap a dns1.

Aquesta configuració demostra un entorn on dos servidors DNS es complementen entre si, amb un actuant com a master i l'altre com a slave per a la majoria de les zones, però poden intercanviar rols per a zones específiques per balancejar càrregues o per raons de política de gestió interna. Això assegura redundància i disponibilitat del servei DNS, claus per a la continuïtat del negoci i la resolució eficaç de noms de domini.

Per cada zona especificada, s'han de fer els fitxers nombrats, que haurien de ser els de la zona directa:

**** La zona directa:**

En els dos servidors crear la carpeta: mkdir -p /etc/bind/zones
És on crearem els fitxers de configuració de zona directa i zona inversa

Fitxer del dns1:
/etc/bind/zones/db.seax.edu

```
$TTL    604800
```

```
        @       IN      SOA     dns1.seax.edu. admin.seax.edu. (
                                2         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
        ;

        @       IN      NS      dns1.seax.edu.
        @       IN      NS      dns2.seax.edu.

        dns1    IN      A       10.1.10.3
        dns2    IN      A       10.1.10.4
        ssh1    IN      CNAME   dns1.seax.edu.
        ssh2    IN      CNAME   dns2.seax.edu.
        monitor IN      A       10.1.10.5      ; IP del servidor nagios

        ;

/etc/bind/zones/db.10.1.10
        $TTL    604800
        @       IN      SOA     dns1.seax.edu. admin.seax.edu. (
                                2         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
        ;

        @       IN      NS      dns1.seax.edu.
        @       IN      NS      dns2.seax.edu.

        3       IN      PTR     dns1.seax.edu.
        4       IN      PTR     dns2.seax.edu.
        5       IN      PTR     monitor.seax.edu.

/etc/bind/zones/db.10.1.20
        $TTL    604800
        @       IN      SOA     dns1.seax.edu. admin.seax.edu. (
                                2         ; Serial
                           604800         ; Refresh
                            86400         ; Retry
                          2419200         ; Expire
                           604800 )       ; Negative Cache TTL
        ;

        @       IN      NS      dns1.seax.edu.
        @       IN      NS      dns2.seax.edu.
```

```
3       IN      PTR     dns1.seax.edu.
4       IN      PTR     dns2.seax.edu.
5       IN      PTR     monitor.seax.edu.
```

Fitxer del dns2:
/etc/bind/zones/db.public.seax.edu

```
$TTL    604800
@       IN      SOA     dns2.public.seax.edu. admin.public.seax.edu. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

@       IN      NS      dns2.public.seax.edu.
@       IN      NS      dns1.public.seax.edu.

dns1    IN      A       192.168.1.1
dns2    IN      A       192.168.1.1
ssh1    IN      CNAME   dns1.public.seax.edu.
ssh2    IN      CNAME   dns2.public.seax.edu.
www     IN      A       147.83.2.135
www     IN      AAAA    2001:40b0:7500:1::21
```

Els fitxers /etc/bind/zones/db.10.1.10 i /etc/bind/zones/db.10.1.20 com que estaran creats en el dns1, i aquest es el master, el dns2 agafarà informació d'aquest per utilitzarla ja que té la funció de ser el seu esclau.

Finalment per acabar de configurar els servidors, hem de configurar el seu fitxer de resolució de dns per posar-se a ells mateixos i l'altre servidor, el fitxer de configuració pels dos dns hauria de quedar:

/etc/resolv.conf

```
nameserver 10.1.10.3
nameserver 10.1.10.4

#nameserver 212.166.132.192
#nameserver 212.166.132.96
```

Per guardar els canvis reiniciar el bind: systemctl restart bind9

***** Configuració dels routers**

La configuració dels routers en un entorn de xarxa que inclou servidors DNS com dns1 i dns2 és fonamental per a garantir la connectivitat i la correcta resolució de noms dins de la xarxa

Pels dos routers, router d'accés i router intern, quan un dispositiu com un router necessita resoldre un nom de domini a una adreça IP (per exemple, quan està redirigint tràfic o accedint a recursos de la xarxa), consulta el fitxer de resolució de dns per saber quins servidors DNS ha d'utilitzar, així que els hem de modificar per obligar a que usin els servidors dns que hem creat:

Pels routers d'accés, router intern i monitors utilitzats:
/etc/resolv.conf

```
nameserver 10.1.10.3
nameserver 10.1.10.4

#nameserver 212.166.132.192
#nameserver 212.166.132.96
```

***** Verificacions**

Per comprovar la sintaxi d'un fitxer de zona en un servidor DNS que utilitza BIND, pots fer servir l'eina named-checkzone. Aquesta eina és molt útil per verificar errors en els fitxers de configuració de zona abans de carregar-los al servidor DNS, evitant així possibles interrupcions del servei per configuracions incorrectes.
Per fer això s'ha d'executar:
Pel dns1:

```
named-checkzone seax.edu /etc/bind/zones/db.seax.edu
```

Pel dns2:

```
named-checkzone public.seax.edu /etc/bind/zones/db.public.seax.edu
```

Aixo es pot fer per tots els fitxers de configuració directa ,i si estan ben configurats la sortida d'aquesta comanda hauria de ser OK

Per verificar que un servidor funciona correctament es poden utilitzar diferents eines, les que nosaltres hem utilitzant son les següents:
Per verificar que el servei BIND està actiu dels dos servidors, podem executar la comanda

```
systemctl status bind9
```

On l'estat d'aquest ha de ser en actiu i en servei:

```
Active: active (running) since Tue 2024-05-14 18:59:47 CEST; 30min ago
```

Per verificar que un servidor fa d'esclau a un altre, la podem veure mirant els fitxers de servidor BIND que estan el la carpeta: /var/cache/bind/
Sinó podem mirar-ho amb l'eina rndc i amb digs utilitzant el SOA.

El SOA (Start of Authority) record de la zona proporciona informació sobre el servidor d'autoritat. Per verificar-ho, utilitza dig:
Des de dns1 a seax.edu:

```
dig @10.1.10.3 seax.edu SOA
```

Des del dns2 a seax.edu:

```
dig @10.1.10.4 seax.edu SOA
```

Els resultats els podem veure en la “ANSWER SECTION: ”

On dns1 ens diu que seax.edu el master és el servidor dns1.seax.edu:
seax.edu. 604800 IN SOA dns1.seax.edu. admin.seax.edu. 2 604800 86400 2419200 604800

On dns2 ens diu també que seax.edu el master és el servidor dns1.seax.edu:
seax.edu. 604800 IN SOA dns1.seax.edu. admin.seax.edu. 2 604800 86400 2419200 604800

Des de dns1 a public.seax.edu:

```
dig @10.1.10.3 public.seax.edu SOA
```

Des del dns2 a public.seax.edu:

```
dig @10.1.10.4 public.seax.edu SOA
```

On el dns1 ens diu que public.seax.edu el master és el servidor dns2.public.seax.edu:
public.seax.edu. 604800 IN SOA dns2.public.seax.edu. admin.public.seax.edu. 2 604800 86400 2419200 604800

On el dns2 ens diu també que public.seax.edu el master és el servidor dns2.public.seax.edu:
public.seax.edu. 604800 IN SOA dns2.public.seax.edu. admin.public.seax.edu. 2 604800 86400 2419200 604800

Podem també mirar-ho amb la RNDC per les diferents zones:

Des de dns1 a seax.edu:

```
rndc -b 10.1.10.3 zonestatus seax.edu
```

Des del dns2 a seax.edu:

```
rndc -b 10.1.10.4 zonestatus seax.edu
```

Els resultats surten que el dns1 : type:primary i el dns2: type: secondary

Des de dns1 a public.seax.edu:

```
rndc -b 10.1.10.3 zonestatus public.seax.edu
```

Des del dns2 a public.seax.edu:

```
rndc -b 10.1.10.4 zonestatus public.seax.edu
```

Els resultats surten el contrari que el dns1 : type:secondary i el dns2: type: primary

Després les proves més directes per provar la configuració del servidor dns, és utilitzar la eina dig:
Per el dns1 els digs utilitzats per provar que funciona han sigut:
- dig @10.1.10.3 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini google.com.

- dig @10.1.10.3 dns2.seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini dns2.seax.edu.

- dig @10.1.10.3 -x 10.1.10.3: Aquesta comanda envia una consulta inversa al servidor 10.1.10.3 per resoldre l'adreça IP 10.1.10.3 a un nom de domini.

- dig @10.1.10.4 -x 10.1.10.4: Aquesta comanda envia una consulta inversa al servidor 10.1.10.4 per resoldre l'adreça IP 10.1.10.4 a un nom de domini.

Per el dns2 els digs utilitzats per provar que funciona han sigut:
- dig @10.1.10.4 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini google.com.

- dig @10.1.10.4 dns1.seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini dns1.seax.edu.

- dig @10.1.10.3 -x 10.1.10.3: Aquesta comanda envia una consulta inversa al servidor 10.1.10.3 per resoldre l'adreça IP 10.1.10.3 a un nom de domini.

- dig @10.1.10.4 -x 10.1.10.4: Aquesta comanda envia una consulta inversa al servidor 10.1.10.4 per resoldre l'adreça IP 10.1.10.4 a un nom de domini.

També hem fet unes proves amb pings per assegurar-nos de la connexió del escenari:

Pel dns1 els pings utilitzats han sigut:
- ping -c 2 10.1.10.1: Aquesta comanda envia dues sol·licituds ICMP ping a la IP 10.1.10.1 per verificar la connectivitat.

- ping -c 2 google.com: Aquesta comanda envia dues sol·licituds ICMP ping al domini google.com per verificar la resolució de noms i la connectivitat.

- ping -c 2 10.1.10.4: Aquesta comanda envia dues sol·licituds ICMP ping a la IP 10.1.10.4 per verificar la connectivitat. (servidor dns2)

Pel dns2 els pings utilitzats han sigut:
- ping -c 2 10.1.10.1: Aquesta comanda envia dues sol·licituds ICMP ping a la IP 10.1.10.1 per verificar la connectivitat.

- ping -c 2 10.1.10.3: Aquesta comanda envia dues sol·licituds ICMP ping a la IP 10.1.10.3 per verificar la connectivitat. (servidor dns1)

- ping -c 2 google.com: Aquesta comanda envia dues sol·licituds ICMP ping al domini google.com per verificar la resolució de noms i la connectivitat.

Per verificar que un domini funciona correctament podem fer servir la eina dig per comprovar amb les diferents zones:

Pel dns1 els pings utilitzats han sigut:
- dig @10.1.10.3 www.public.seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini www.public.seax.edu.

- dig @10.1.10.3 seax.edu A: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre A del domini seax.edu, que retorna l'adreça IPv4 associada.

- dig @10.1.10.3 public.seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini public.seax.edu.

- dig @10.1.10.3 public.seax.edu A: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre A del domini public.seax.edu, que retorna l'adreça IPv4 associada.

- dig @10.1.10.3 public.seax.edu AAAA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre AAAA del domini public.seax.edu, que retorna l'adreça IPv6 associada.

- dig @10.1.10.3 ssh1.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh1.seax.edu, que retorna l'àlies associat.

- dig @10.1.10.3 ssh2.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh2.seax.edu, que retorna l'àlies associat.

- dig @10.1.10.3 ssh5.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh5.seax.edu, que retorna l'àlies associat. En aquest cas, el registre no existeix, i es verifica com gestiona el servidor DNS una consulta per un registre inexistent.

Pel dns2 els pings utilitzats han sigut:
- dig @10.1.10.4 www.public.seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini www.public.seax.edu.

- dig @10.1.10.4 seax.edu A: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre A del domini seax.edu, que retorna l'adreça IPv4 associada.

- dig @10.1.10.4 public.seax.edu A: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre A del domini public.seax.edu, que retorna l'adreça IPv4 associada.

- dig @10.1.10.4 public.seax.edu AAAA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre AAAA del domini public.seax.edu, que retorna l'adreça IPv6 associada.

- dig @10.1.10.4 ssh1.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh1.seax.edu, que retorna l'àlies associat.

- dig @10.1.10.4 ssh2.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh2.seax.edu, que retorna l'àlies associat.

- dig @10.1.10.4 ssh7.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh7.seax.edu, que retorna l'àlies associat. En aquest cas, el registre no existeix, i es verifica com gestiona el servidor DNS una consulta per un registre inexistent.

**** Verificacions amb monitors**

Hem comprovat la configuració del dns1 i dns2 amb un monitor dins la xarxa dmz amb la ip 10.1.10.11 per comprovar que els digs els feia utilitzant els dns creats, les comandes que hem provat per la verificació dels servidors són:

- dig @10.1.10.3 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el nom de domini google.com. El servidor respon correctament amb l'adreça IP de google.com.

- dig @10.1.10.4 google.com: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el nom de domini google.com. El servidor respon correctament amb l'adreça IP de google.com.

- ping -c 2 google.com: Aquesta comanda fa una prova de connectivitat (ping) a google.com enviant 2 paquets ICMP. La resposta indica que la connectivitat amb google.com és correcta.

- dig @10.1.10.4 seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el domini seax.edu. El servidor respon amb el registre SOA, confirmant que dns2 gestiona aquest domini.

- dig @10.1.10.4 public.seax.edu:Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el domini public.seax.edu. El servidor respon amb el registre SOA, confirmant que dns2 gestiona aquest domini.

- dig @10.1.10.3 seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el domini seax.edu. El servidor respon amb el registre SOA, confirmant que dns1 gestiona aquest domini.

- dig @10.1.10.3 public.seax.edu: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el domini public.seax.edu. El servidor respon amb el registre SOA, confirmant que dns1 gestiona aquest domini.

- dig @10.1.10.3 public.seax.edu SOA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per obtenir el registre SOA del domini public.seax.edu. El servidor respon correctament amb el registre SOA.

- dig @10.1.10.3 seax.edu SOA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per obtenir el registre SOA del domini seax.edu. El servidor respon correctament amb el registre SOA.

- dig @10.1.10.4 public.seax.edu SOA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per obtenir el registre SOA del domini public.seax.edu. El servidor respon correctament amb el registre SOA.

- dig @10.1.10.4 seax.edu SOA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per obtenir el registre SOA del domini seax.edu. El servidor respon correctament amb el registre SOA.

- dig @10.1.10.3 public.seax.edu AAAA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre AAAA del domini public.seax.edu. El servidor respon amb el registre AAAA.

- dig @10.1.10.4 public.seax.edu AAAA: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre AAAA del domini public.seax.edu. El servidor respon amb el registre AAAA.

- dig @10.1.10.3 ssh1.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh1.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.3 ssh2.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh2.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.3 ssh5.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh5.seax.edu. El servidor respon que el registre no existeix (NXDOMAIN).

- dig @10.1.10.4 ssh1.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh1.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.4 ssh2.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh2.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.4 ssh5.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh5.seax.edu. El servidor respon que el registre no existeix (NXDOMAIN).

- dig @10.1.10.3 ssh1.public.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh1.public.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.3 ssh2.public.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh2.public.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.3 ssh5.public.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.3 per resoldre el registre CNAME de ssh5.public.seax.edu. El servidor respon que el registre no existeix (NXDOMAIN).

- dig @10.1.10.4 ssh1.public.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh1.public.seax.edu. El servidor respon amb el registre CNAME.

- dig @10.1.10.4 ssh2.public.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh2.public.seax.edu. El servidor respon amb el registre CNAME.
Consulta del Registre CNAME per ssh5.public.seax.edu des de dns2

- dig @10.1.10.4 ssh5.public.seax.edu CNAME: Aquesta comanda envia una consulta DNS al servidor 10.1.10.4 per resoldre el registre CNAME de ssh5.public.seax.edu. El servidor respon que el registre no existeix (NXDOMAIN).

- dig @10.1.10.3 -x 10.1.10.3: Aquesta comanda envia una consulta inversa al servidor 10.1.10.3 per resoldre l'adreça IP 10.1.10.3 al seu nom de domini associat. El servidor respon correctament amb el nom de domini dns1.seax.edu.

- dig @10.1.10.4 -x 10.1.10.4: Aquesta comanda envia una consulta inversa al servidor 10.1.10.4 per resoldre l'adreça IP 10.1.10.4 al seu nom de domini associat. El servidor respon correctament amb el nom de domini dns2.seax.edu.

- cat /etc/resolv.conf: Aquesta comanda mostra la configuració actual de resolució de noms al fitxer resolv.conf. La configuració indica que les consultes DNS s'enviaran als servidors 10.1.10.3, 10.1.10.4, i 10.1.10.1.

Fitxers involucrats:

- /etc/hosts i /etc/hostnames

Per modificar els noms de les màquines virtuals
- /etc/network/interfaces
Per tota la configuració feta pels adaptadors de els diferents xarxes
- /etc/systemd/network/10-enp0s3-net.link
Per guardar els canvis dels noms de les interfícies
- /etc/bind/named.conf.options
Configuració del servidors dns
- /etc/bind/named.conf.local
Configuració local del servidor dns
- /etc/bind/zones/xx
Fitxers per la configuració de les zones
- /etc/resolv.conf
Configuració de resolució dels servidors dns per els servidors i els routers

Fitxers d'evidència:

configuració dns1: 1-1-dns1.txt
verificacions del servidor: 1-2-dns1-testing.txt
configuració dns2: 1-1-dns2.txt
verificacions del servidor: 1-2-dns2-testing.txt
configuració routers: 1-1-routers.txt
verificació monitor dmz: 1-3-dmz-testing.txt

Es poden veure els resultats de l'execució de les explicacions anteriors

Fonts d'informació:

Com configurar BIND com a servidor DNS de xarxa privada a Ubuntu 18.04:
https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04
Com configurar BIND com a servidor DNS només autoritatiu a Ubuntu 20.04:
https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-an-authoritative-only-dns-server-on-ubuntu-20-04
Manual 'administrador de BIND 9: https://bind9.readthedocs.io/en/latest/
Configuració de BIND 9: https://bind9.readthedocs.io/en/latest/reference.html
Configurar el servidor DNS (bind9):
https://ubuntu.com/server/docs/service-domain-name-service-dns
Configurar un servidor DNS BIND:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/networking_guide/setting_up_a_bind_dns_server
Com configurar BIND com a servidor DNS a Linux:
https://www.thegeekstuff.com/2014/03/bind9-dns-server/
Configuració de BIND9:
https://www.debian.org/doc/manuals/debian-reference/ch05.en.html#_the_domain_name_system