M3105 : DNS - LDAP

Guillaume Urvoy-Keller

July 18, 2018

1 Serveur DNS

On va analyser le répertoire qui contient les fichiers de configuration d'un serveur bind (serveur DNS populaire sous Linux).

1. On commence par regarder le fichier qui liste toutes les zones (named.conf) puis les zones par défaut - voir Figure 1. On s'intéresse aux zones par défaut.
   (a) Placez ces zones dans l'arbre global.
   (b) Est-ce que ce sont des zones directes ou inverses?
   (c) Soit le fichier de zone db.127 en Figure 2
      i. Combien y a-t-il d'enregistrements?
      ii. A quoi cette zone répond-elle (= à quoi le serveur va-il répondre)?
2. Les zones que vous créez doivent être dans le fichier named.conf.local. Ce fichier est décrit en Figure 3 ainsi que les zones correspond à la RFC 1918.
   (a) Expliquez
   (b) Comment devra être configuré un routeur d'un FAI?

2 Resolver DNS

Le resolver DNS est le proxy qui va récupérer la requête des machines de l'entreprise et la résoudre. Le resolver est ce qui est obtenu lors de la requête DHCP initiale du client. Par exemple, ci-desous, on voit les *lease* (locations) d'une machine client à l'intérieur du laboratoire I3S :

```
root@stretch:/etc/bind# tail -17 /var/lib/dhcp/dhclient.leases
}
lease {
  interface "eth1";
  fixed-address 134.59.129.225;
  option subnet-mask 255.255.255.0;
  option time-offset 3600;
  option routers 134.59.129.254;
  option dhcp-lease-time 14400;
  option dhcp-message-type 5;
  option domain-name-servers 134.59.130.1,134.59.1.7;
  option dhcp-server-identifier 134.59.131.13;
  option broadcast-address 134.59.129.255;
  option domain-name "i3s.unice.fr";
  renew 3 2018/07/18 14:40:33;
  rebind 3 2018/07/18 16:11:49;
  expire 3 2018/07/18 16:41:49;
}
```

Le schéma typique de résolution DNS est celui de la Figure 4.

(a) Quel(s) serveur(s) effectue(nt) des requêtes récursives (resp. itérative)?

```
root@stretch:/etc/bind# more named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
root@stretch:/etc/bind# more named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

Figure 1: Fichier de configuration des zones

```
root@stretch:/etc/bind# more db.127
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
```

Figure 2: Fichier de configuration des zones

```
root@stretch:/etc/bind# ls
bind.keys  db.127  db.empty  db.root     named.conf.default-zones  named.conf.options  zones.rfc1918
db.0       db.255  db.local  named.conf  named.conf.local          rndc.key
root@stretch:/etc/bind# more named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

root@stretch:/etc/bind# more zones.rfc1918
zone "10.in-addr.arpa"      { type master; file "/etc/bind/db.empty"; };

zone "16.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "17.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "18.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "19.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "20.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "21.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "22.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "23.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "24.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "25.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "26.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "27.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "28.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "29.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "30.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "31.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };

zone "168.192.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
root@stretch:/etc/bind# more db.empty
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
```

Figure 3: Fichier de configuration des zones

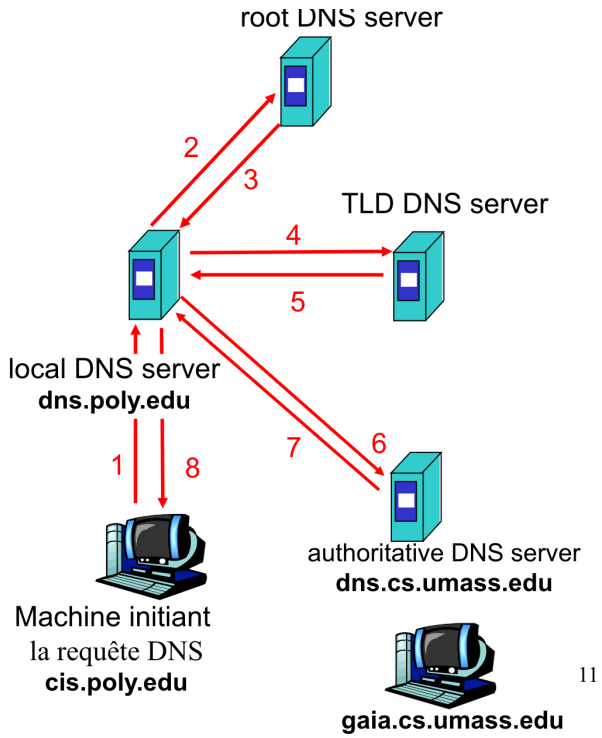

Figure 4: Trajet d'une requête DNS

(b) Pour transformer un serveur DNS en resolver, il suffit d'ajouter, dans le fichier la ligne *recursion* dans le fichier named.conf.options :

```
root@stretch:/etc/bind# cat named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // 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
        //========================================================================
        //dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        //listen-on-v6 { any; };

        recursion yes;
};
```

Quels serveurs DNS doit connaitre le resolver?

(c) Où se trouve cette information?

3. Soit une machine configurée en resolver. On effectue deux fois la même requêtes DNS. Expliquez le résultat en terme

de temps d'exécution.

```
root@stretch:/etc/bind# time nslookup www.mit.edu 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.101.176.36


real    0m0.788s
user    0m0.004s
sys     0m0.004s
root@stretch:/etc/bind# time nslookup www.mit.edu 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.101.176.36


real    0m0.010s
user    0m0.008s
sys     0m0.000s
```

4. En analysant le fichier named.conf.options, où se trouve d'après vous les données correspondant à la question précédente?

3 LDAP

1. Soit la requête suivante sur le serveur Active Directory de l'IUT.

```
urvoy@isis:~$ ldapsearch -h '134.59.136.23' -b "dc=iutnice,dc=unice,dc=fr" -D 'iutnice\urvoy' -W
    "sAMAccountName=urvoy"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=iutnice,dc=unice,dc=fr> with scope subtree
# filter: sAMAccountName=urvoy
# requesting: ALL
#

# urvoy, Enseignants, RT, Utilisateurs, iutnice.unice.fr
dn: CN=urvoy,OU=Enseignants,OU=RT,OU=Utilisateurs,DC=iutnice,DC=unice,DC=fr
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: urvoy
sn: URVOY-KELLER
description: Guillaume.URVOY-KELLER
givenName: Guillaume
distinguishedName: CN=urvoy,OU=Enseignants,OU=RT,OU=Utilisateurs,DC=iutnice,DC
 =unice,DC=fr
instanceType: 4
whenCreated: 20150713081154.0Z
whenChanged: 20180717095509.0Z
displayName: Guillaume URVOY-KELLER
uSNCreated: 225365
memberOf: CN=iut.sag.lecteurs.expanded,OU=Groupes NextCloud,OU=IUT_Global,OU=U
 tilisateurs,DC=iutnice,DC=unice,DC=fr
```

```
memberOf: CN=iut.sag.certec.membres.expanded,OU=Groupes NextCloud,OU=IUT_Globa
 l,OU=Utilisateurs,DC=iutnice,DC=unice,DC=fr
memberOf: CN=RT_Ens,OU=Enseignants,OU=RT,OU=Utilisateurs,DC=iutnice,DC=unice,D
 C=fr
memberOf: CN=iut.sag.certec.membres,OU=Groupes NextCloud,OU=IUT_Global,OU=Util
 isateurs,DC=iutnice,DC=unice,DC=fr
memberOf: CN=RTperma,OU=RT,OU=Utilisateurs,DC=iutnice,DC=unice,DC=fr
memberOf: CN=RTel,OU=RT,OU=Utilisateurs,DC=iutnice,DC=unice,DC=fr
memberOf: CN=RTp,OU=RT,OU=Utilisateurs,DC=iutnice,DC=unice,DC=fr
memberOf: CN=Utilisateurs du domaine,CN=Users,DC=iutnice,DC=unice,DC=fr
uSNChanged: 98507678
department: RT
name: urvoy
objectGUID:: 5XGPVrkddEK4The0a8PebQ==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
homeDirectory: \\rtsrv\urvoy
homeDrive: Z:
badPasswordTime: 131762948998254021
lastLogoff: 0
lastLogon: 131762949310887278
pwdLastSet: 131762318190664388
primaryGroupID: 3343
profilePath: \\rtsrv\urvoy\.win\Profile
objectSid:: AQUAAAAAAAUVAAAAOyNfQcTvYApwQVxwDg0AAA==
accountExpires: 132540523110975953
logonCount: 36
sAMAccountName: urvoy
sAMAccountType: 805306368
userPrincipalName: urvoy@iutnice.unice.fr
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=iutnice,DC=unice,DC=fr
dSCorePropagationData: 20180412095220.0Z
dSCorePropagationData: 20170901144925.0Z
dSCorePropagationData: 20170706121429.0Z
dSCorePropagationData: 16010101181633.0Z
lastLogonTimestamp: 131762949095242127
mail: Guillaume.URVOY-KELLER@unice.fr
msSFU30Name: urvoy
msSFU30NisDomain: iutnice
uidNumber: 26485
gidNumber: 1026485
gecos: Guillaume.URVOY-KELLER,DEPRT,,*
unixHomeDirectory: /home/rtel/pers/perma/urvoy
loginShell: /bin/bash

# search reference
ref: ldap://DomainDnsZones.iutnice.unice.fr/DC=DomainDnsZones,DC=iutnice,DC=un
 ice,DC=fr

# search reference
ref: ldap://ForestDnsZones.iutnice.unice.fr/DC=ForestDnsZones,DC=iutnice,DC=un
 ice,DC=fr

# search reference
ref: ldap://iutnice.unice.fr/CN=Configuration,DC=iutnice,DC=unice,DC=fr

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 1
# numReferences: 3
```

(a) Analyse de la commande :

i. Quelle est la partie de l'arbre sur laquelle s'effectue la recherche?

ii. Quelle est la chaine de caractères cherchée?

iii. Quel est l'identifiant utilisé pour s'identifier auprès du serveur LDAP?

(b) Analyse de la réponse :

i. Combien y a t-il d'objets retournés?

ii. Quelles sont les classes d'objet?

iii. Dessinez la partie de l'arbre que vous pouvez inférer à partir de la réponse

2. Comment trouver tous les objets de la base (quelle requête faire et comment la filtrer)?

3. Le fichier /etc/nsswitch.conf sur la machine isis est le suivant :

```
urvoy@isis:~$ more /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:         compat sss
group:          compat sss
shadow:         compat sss
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files sss
ethers:         db files
rpc:            db files

netgroup:       nis sss
sudoers:        files sss
```

Quels sont les moyens d'authentication possibles? Pourquoi laisser compat ?

4. SSSD est un service qui permet d'interfacer avec un Active Directory. Sa configuration sur isis est (version partielle) :

```
urvoy@isis:/etc/pam.d$ more /etc/sssd/sssd.conf.copy
[sssd]
config_file_version = 2
services = nss, pam
domains = iutnice.unice.fr
reconnection_retries = 3
sbus_timeout = 30

[domain/iutnice.unice.fr]
id_provider = ldap
auth_provider = krb5
chpass_provider = krb5

ldap_uri = ldap://dc-sirm-01.iutnice.unice.fr:389
ldap_backup_uri = ldap://dc-sirm-02.iutnice.unice.fr:389
ldap_search_base = OU=Utilisateurs,dc=iutnice,dc=unice,dc=fr
ldap_schema = rfc2307bis
ldap_sasl_mech = GSSAPI
ldap_user_object_class = user
ldap_group_object_class = group
ldap_user_home_directory = unixHomeDirectory
ldap_user_principal = userPrincipalName
ldap_access_order = expire
ldap_account_expire_policy = ad
ldap_force_upper_case_realm = true
ldap_search_timeout = 10

ldap_id_mapping = False
ldap_schema = ad
min_id = 8000
max_id = 4999999
```

```
entry_cache_timeout = 600
cache_credentials = False
enumerate = True
```

Que nous dit cette configuration?

5. Enfin, à partir du listing ci-dessous du common-auth du répertoire /etc/pam.d, faire un schéma montrant les relations entre nsswitch, pam, sssd?

```
urvoy@isis:/etc/pam.d$ grep -v "#" common-auth

auth    [success=2 default=ignore]      pam_unix.so nullok_secure try_first_pass
auth    [success=1 default=ignore]      pam_sss.so use_first_pass

auth    requisite                       pam_deny.so
auth    required                        pam_permit.so
auth    optional                        pam_cap.so
```