

Documentation

JOB 2: Installer FTP sur notre machine serveur

Pour installer FTP sur notre machine serveur, il faut entrer la commande:

sudo apt install proftpd-*

une fois le packet installé, on peut aller voir les fichier de configuration qui se trouve dans le chemin suivant:

cd /etc/proftpd/

```
raph@debian: /home/raph
# cd /etc/proftpd
raph@debian: /etc/proftpd
# ls
blacklist.dat  conf.d          geoip.conf      modules.conf    PROFTPD-MIB.txt  snmp.conf  ssl          virtuals.conf
cacerts.pem   dhparams.pem   ldap.conf       proftpd.conf    sftp.conf        sql.conf   tls.conf
```

Les commandes principal pour monitorer notre serveur ftp sont :

lancer: **sudo service proftpd start**

stop: **sudo service proftpd stop**

information: **sudo service proftpd status**

relancer: **sudo service proftpd restart**

recharger: **sudo service proftpd reload**

on peut aussi forcer le lancement, le stop ou le reload:

avec les commande :

sudo service proftpd force-start/reload/stop

```
raph@debian: /etc/proftpd
# sudo service proftpd _
force-reload force-start force-stop reload restart start status stop
```

job 3 : Création de deux user

pour créer un user on utilise la commande :

sudo useradd -m nom_utilisateur

sudo passwd nom_utilisateur

JOB 4 : Se connecter en anonyme sur FTP

pour se connecter en anonyme il faut se rendre dans les fichier de configuration FTP:

cd /etc/proftpd/

et modifier le fichier proftpd.conf

sudo nano proftpd.conf

```
raph@debian: /home/raph
[→ cd /etc/proftpd
raph@debian: /etc/proftpd
[→ ls
blacklist.dat  conf.d      geoip.conf  modules.conf  PROFTPD-MIB.txt  snmp.conf  ssl          virtuals.conf
cacerts.pem   dhparams.pem  ldap.conf   proftpd.conf  sftp.conf        sql.conf   tls.conf
raph@debian: /etc/proftpd
[→ sudo nano proftpd.conf
[[sudo] Mot de passe de raph :
```

on se retrouve donc dans le fichier de configuration proftpd et on décoche les lignes suivante :

```
<Anonymous ~ftp>
User anonymous
Group nogroup
# # We want clients to be able to login with "anonymous" as well as "ftp"
UserAlias anonymous ftp
# # Cosmetic changes, all files belongs to ftp user
#DirFakeUser on ftp
#DirFakeGroup on ftp
#
RequireValidShell off
#
# # Limit the maximum number of anonymous logins
MaxClients 10
#
# # We want 'welcome.msg' displayed at login, and '.message' displayed
# # in each newly chdir'd directory.
DisplayLogin welcome.msg
DisplayChdir .message
#
# # Limit WRITE everywhere in the anonymous chroot
#<Directory *>
#<Limit WRITE>
#DenyAll
#</Limit>
#</Directory>
#
# # Uncomment this if you're brave.
# # <Directory incoming>
# # # Umask 022 is a good standard umask to prevent new files and dirs
# # # (second parm) from being group and world writable.
# # Umask022 022
# # <Limit READ WRITE>
# # DenyAll
# # </Limit>
# # <Limit STOR>
# # AllowAll
# # </Limit>
# # </Directory>
#
</Anonymous>
```

JOB 6 : configuration SSL sur FTP

Pour configurer notre sur FTP sur le système de sécurité ssl, il faut dans un premier temps modifier le fichier de configuration TLS.conf:

sudo nano tls.conf

```
#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
# for more information.
#
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log
  TLSProtocol SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
# -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
# -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
  TLRSACertificateFile /etc/proftpd/ssl/proftpd.cert.pem
  TLRSACertificateKeyFile /etc/proftpd/ssl/proftpd.key.pem
#
# CA the server trusts...
  TLSCACertificateFile /etc/ssl/certs/CA.pem
# ...or avoid CA cert and be verbose
#TLSOptions NoCertRequest EnableDiags
# ... or the same with relaxed session use for some clients (e.g. FireFtp)
#TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired
#TLSOptions NoCertRequest AllowClientRenegotiations
#
# Per default drop connection if client tries to start a renegotiate
# This is a fix for CVE-2009-3555 but could break some clients.
#
#TLSOptions AllowClientRenegotiations
#
# Authenticate clients that want to use FTP over TLS?
#
  TLSVerifyClient off
#
# Are clients required to use FTP over TLS when talking to this server?
#
  TLSRequired off
#
# Allow SSL/TLS renegotiations when the client requests them, but
# do not force the renegotiations. Some clients do not support
# SSL/TLS renegotiations; when mod_tls forces a renegotiation, these
# clients will close the data connection, or there will be a timeout
# on an idle data connection.
#
#TLSRenegotiate required off
  TLSOptions NoSessionReuseRequired
  RequireValidShell no
</IfModule>
```

une fois les fichier de configuration `tls.conf` modifier, il faut ensuite créer nos clés ssl avec la commande:

```
sudo openssl req -new -x509 -keyout /etc/proftpd/ssl/proftpd.key.pem -days 365 -nodes -out /etc/proftpd/ssl/proftpd.cert.pem
```

Les clés doivent être créées dans le même fichier référence que dans le fichier `tls.conf`.

une fois ces étapes faites, il faut juste relancer le serveur avec la commande:
sudo service proftpd restart

JOB 7: Installation DNS sur le serveur

Pour l'installation du dns il faut installer le paquet `bind9`:

sudo apt install bind9

une fois le paquet installé on peut se rendre dans son fichier de configuration à l'emplacement suivant:

cd /etc/bind

une fois dans le dossier de configuration on copie les deux fichiers suivants `db.127` et `db.local`:

cp db.127 db.192

cp db.local db.dnsproject.prepa.com

```
raph@debian: /etc/bind
ls
bind.keys  db.127  db.255                db.empty  named.conf                named.conf.local  rndc.key
db.0       db.192  db.dnsproject.prepa.com db.local  named.conf.default-zones  named.conf.options zones.rfc1918
raph@debian: /etc/bind
```

maintenant les fichiers copiés on peut maintenant les modifier:

sudo nano db.192

```
GNU nano 5.4 db.192
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      dnsproject.prepa.com. root.dnsproject.prepa.com. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       dnsproject.prepa.com.
18        IN      PTR      dnsproject.prepa.com.
```

sudo nano db.dnsproject.prepa.com

```
GNU nano 5.4 db.dnsproject.prepa.com
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      dnsproject.prepa.com. root.dnsproject.prepa.com. (
                                2             ; Serial
                                604800         ; Refresh
                                86400          ; Retry
                                2419200        ; Expire
                                604800 )      ; Negative Cache TTL
;
@         IN      NS       dnsproject.prepa.com.
@         IN      A        192.168.65.18
@         IN      AAAA     ::1
```

maintenant on peut modifier les fichier named.conf

sudo nano named.conf.local

```
GNU nano 5.4 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";

zone "dnsproject.prepa.com" IN {
    type master;
    file "/etc/bind/db.dnsproject.prepa.com";
};

zone "65.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.192";
};
```

sudo nano named.conf.options

```
GNU nano 5.4 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";

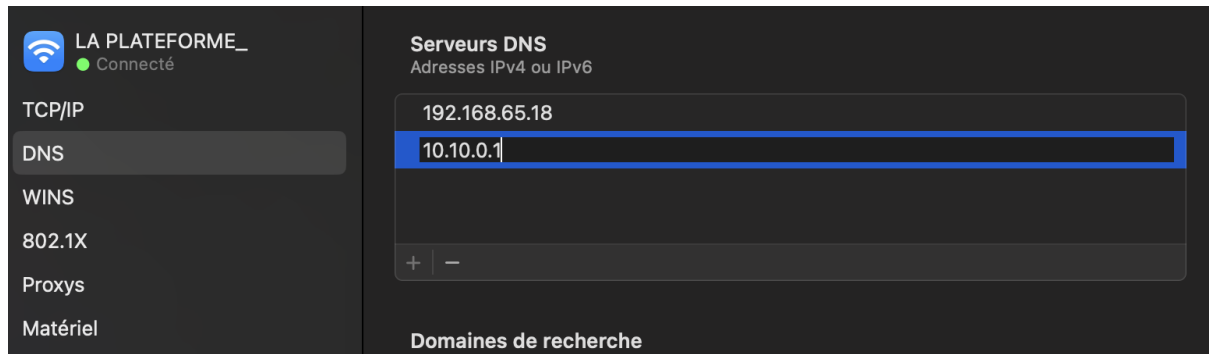
zone "dnsproject.prepa.com" IN {
    type master;
    file "/etc/bind/db.dnsproject.prepa.com";
};

zone "65.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.192";
};
```

une fois tous les fichiers bien configurés on peut maintenant redémarrer le serveur DNS:

sudo service bind9 restart

une fois le serveur redémarrer on peut indiquer sur notre machine hôte l'adresse de notre DNS (ip de notre machine serveur) pour que notre machine hôte puisse identifier le serveur dns



une fois cela fait on peut ping dnsproject.prepa.com depuis notre machine hôte

```
→ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.65.18): 56 data bytes
64 bytes from 192.168.65.18: icmp_seq=0 ttl=64 time=1.772 ms
64 bytes from 192.168.65.18: icmp_seq=1 ttl=64 time=1.134 ms
64 bytes from 192.168.65.18: icmp_seq=2 ttl=64 time=1.031 ms
64 bytes from 192.168.65.18: icmp_seq=3 ttl=64 time=1.031 ms
^C
--- dnsproject.prepa.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.031/1.242/1.772/0.309 ms
raphaelmalet@molet: /Users/raphaelmalet
→
```


JOB 8 : comment obtient-on un nom de domaine public ?

Pour déposer un nom de domaine, il faut s'adresser à l'un des nombreux prestataires agréés. Il est fréquent qu'ils proposent en complément des services comme de l'hébergement, des solutions de création de site, un service de messagerie. Exemples :

Amen, Gandi, Mail Club, Ovh, Ikoula, Ionos, etc.

Pour un .fr, le site de l'Association française pour le nommage internet en coopération - Afnic - l'organisme qui gère les noms de domaine en suffixe .fr - propose une liste de prestataires ayant adhéré à sa charte.

La plupart d'entre eux permet, en ligne, de vérifier la disponibilité du nom souhaité. Les différents types d'extension accessibles aux entreprises.

Les plus courants sont:

- .fr : peut être attribué à toute entité ou personne ayant une existence légale en France, sans autre condition. Le choix d'un suffixe .fr peut être rassurant pour les contacts commerciaux de l'entreprise. Il atteste d'une proximité de l'entreprise vis-à-vis du marché français ainsi que de sa réelle existence juridique. Les personnes physiques qui résident sur le territoire de l'un des Etats membres de l'Union européenne et les personnes morales qui y ont leur siège social ou leur établissement principal, peuvent demander l'enregistrement d'un nom de domaine en .fr.

- .com : plus "global" que le .fr. (à l'origine il était destiné aux entreprises commerciales), mais aussi moins "fiable" car aucune condition particulière n'est exigée pour son dépôt. Attention, cependant, à ne pas enregistrer, même involontairement, un nom correspondant à une marque appartenant à un tiers.

- .net : à l'origine destiné aux structures liées à Internet. Fonctionnant comme le .com, il peut aujourd'hui être déposé par toute personne.

- .org : à l'origine destiné aux structures à but non commercial. Il est aujourd'hui aussi "ouvert" que le .com.

- Et aussi : .biz, .info, .tv, .eu, .asia, .pro, etc. Hors de l'Europe, si, par exemple, votre entreprise travaille avec la Chine ou l'Inde, il est également recommandé de réserver le .cn ou le .in.

Le choix entre .fr, .com, .eu, .mobi : Ce choix relève de la stratégie de l'entreprise. Pour une entreprise française, le .fr s'impose. Si le .com est disponible, il ne faut pas hésiter à le réserver également. Le .eu quant à lui est très peu utilisé. Le .mobi permet d'identifier un site sur un téléphone mobile qui a été adapté à ce type de navigation mais avec l'évolution des sites qui s'adaptent automatiquement au support de consultation (responsive design), il est en voie de disparition progressive

JOB 9 : Se connecter en FTP grace au nom de domaine DNS

si votre dns est pingable depuis votre machine vous pouvez directement vous connecter grace au nom de domaine

Hôte :	<input type="text" value="dnsproject.prepa.cc"/>	Nom d'utilisateur :	<input type="text" value="raph"/>	Mot de passe :	<input type="password" value="..."/>	P
Statut :	Connexion interrompue par le serveur					
Statut :	Déconnecté du serveur					
Statut :	Résolution de l'adresse de dnsproject.prepa.com					
Statut :	Connexion à 192.168.65.18:21...					
Statut :	Connexion établie, attente du message d'accueil...					
Statut :	Initialisation de TLS...					
Statut :	Connexion TLS établie.					

Intermèdes BIS: C'est quoi un DHCP

DHCP : Dynamic Host Configuration Protocol, est un protocole client/serveur qui fournit automatiquement une adresse internet Protocol(IP) et d'autres informations de configuration pertinentes à un hôte IP (ex: masque de sous réseau)

si on veut mettre plusieurs machines sur le même on met donc en place un serveur DHCP pour distribuer automatiquement des adresses et l'on peut aussi associer des adresses IP fixe en fonction d'une adresse MAC d'une machine

JOB 10: Configuration serveur DHCP

il faut installer le packet dhcp:

sudo apt install isc-dhcp-server

une fois le packet installé on va dans /etc/default/isc-dhcp-server, et on va modifier le port d'écoute du serveur pour qu'il soit sur le port internet de notre machine ici enp0s1 sur l'interface ipV4, on ne va pas se servir de l'interface ipv6 dans notre cas.

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s1"
#INTERFACESv6=""
```

on peut maintenant aller dans les fichier de configuration dhcp:

cd /etc/dhcp

et on modifie le fichier dhcp.conf:

sudo nano dhcp.conf

```
GNU nano 5.4 dhcpd.conf *
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "dnsproject.prepa.com";
option domain-name-servers 192.168.65.18;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

subnet 192.168.65.0 netmask 255.255.255.0 {
option routers 192.168.65.1;
option domain-name-servers 192.168.65.18;
range 192.168.65.50 192.168.65.100;
}
```

on peut maintenant relancer notre service DHCP avec la commande:

sudo service isc-dhcp-server restart

et on regarde le statut avec

sudo service isc-dhcp-server status

```
raph@debian: /etc/dhcp
[+] sudo service isc-dhcp-server restart
raph@debian: /etc/dhcp
[+] sudo service isc-dhcp-server status
● isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: active (running) since Fri 2023-05-12 12:43:56 CEST; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 926 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS)
    Tasks: 4 (limit: 2263)
   Memory: 4.9M
      CPU: 36ms
    CGroup: /system.slice/isc-dhcp-server.service
            └─941 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf enp0s1

mai 12 12:43:54 debian systemd[1]: Starting LSB: DHCP server...
mai 12 12:43:54 debian isc-dhcp-server[926]: Launching IPv4 server only.
mai 12 12:43:54 debian dhcpd[941]: Wrote 0 leases to leases file.
mai 12 12:43:54 debian dhcpd[941]: Server starting service.
mai 12 12:43:56 debian isc-dhcp-server[926]: Starting ISC DHCPv4 server: dhcpd.
mai 12 12:43:56 debian systemd[1]: Started LSB: DHCP server.
raph@debian: /etc/dhcp
→
```

si vous n'avez pas de message d'erreur bravo vous venez de configurer votre serveur DHCP !!!!!

