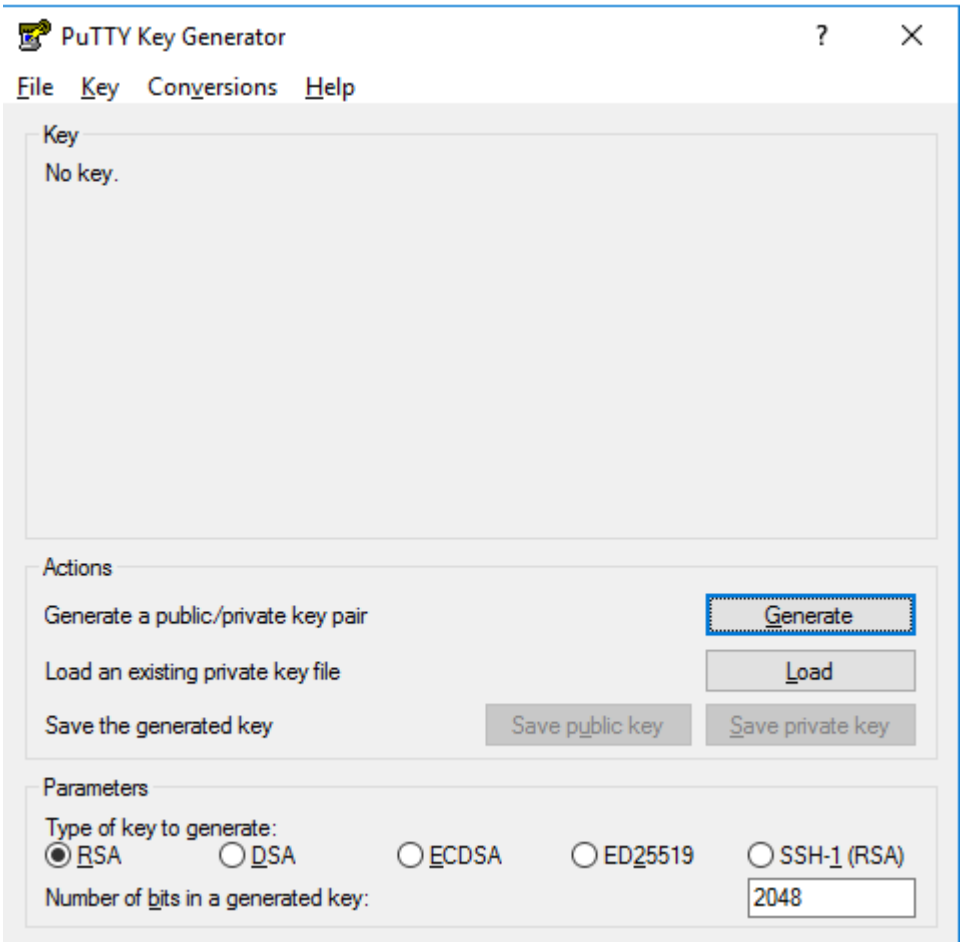
Document Technique: Configuration dns avec Bind9 sur debian 12

Date : 22/01/2025

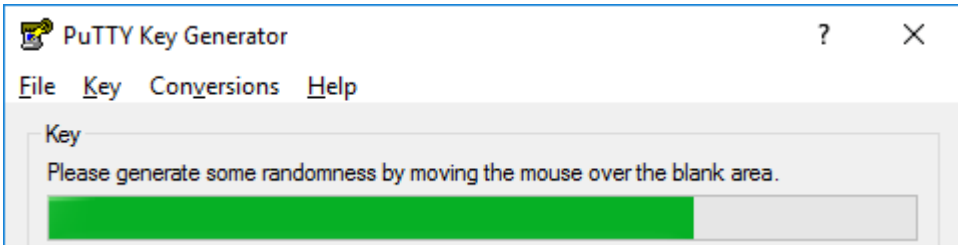
Pour cette partie de mission , mon maître de stage m'a expliqué la topologie. ce serveur dns et placer dans la dmz pour permettre au autre machine présent dans la dmz de pouvoir résoudre les nom de domaine qui sont present en local sur le domaine caib.fr souhaiter, sans etre dans le domaine.donc pouvoir résoudre que certaine nom de domaine dans le domaine caib.fr et sinon elle recherche sur internet avec le résolveur DNS public géré par Cloudflare 1.1.1.1 ou 1.0.0.1.

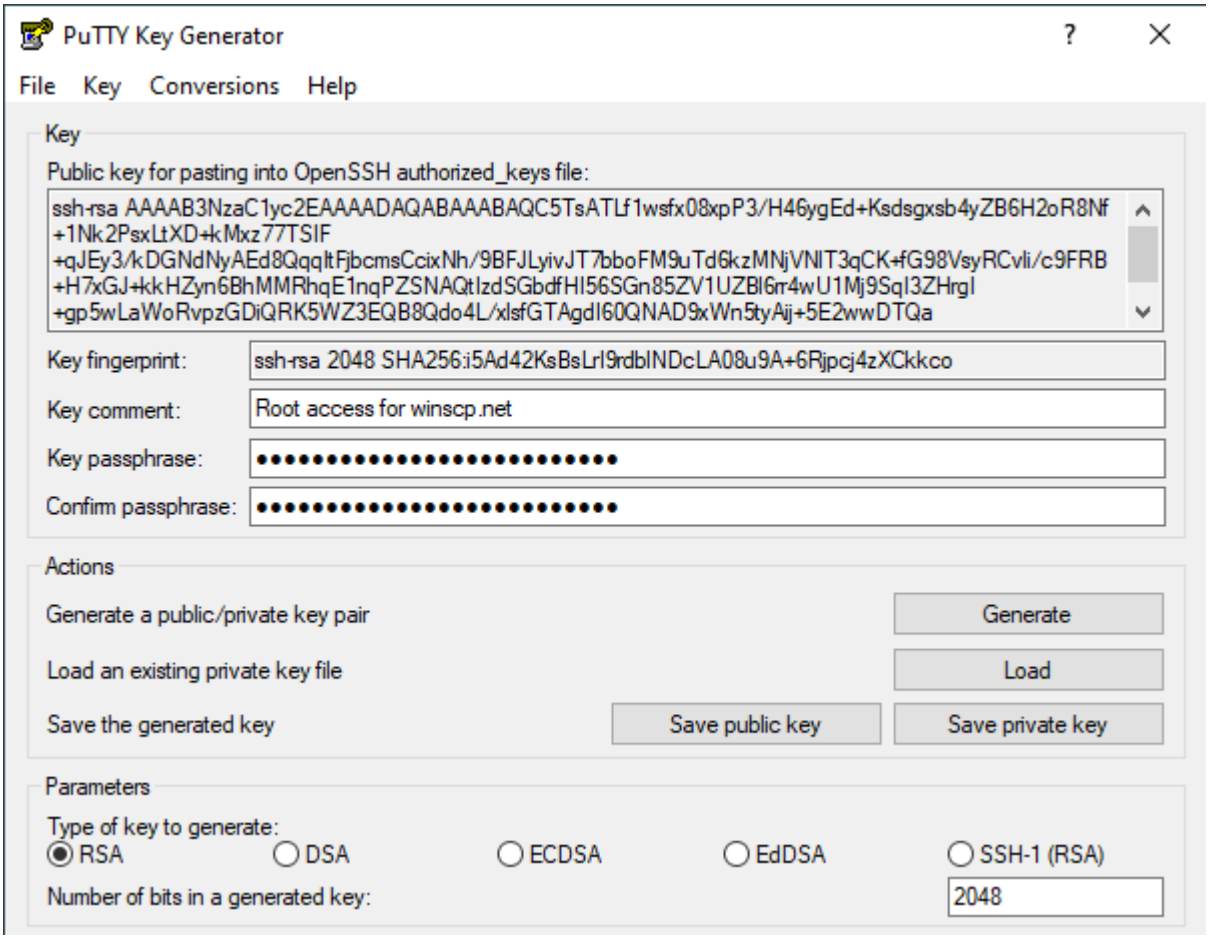
au préalable, avec mon maître de stage on a générer des paires de clés ssh avec puttygen

puttygen permet est un outil de génération de clés permettant de créer des clés SSH pour PuTTY



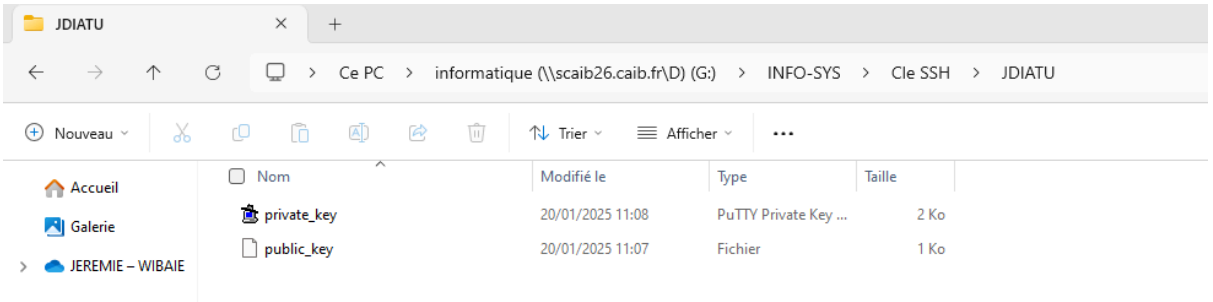
Une fois lancé on arrive sur cette page, en bas on peut choisir l'algorithme souhaité (nous c'est le RSA) et on choisit la en bits des clefs et on appuie sur Generate et on fait bouger la souris pour générer des chiffre aléatoire.



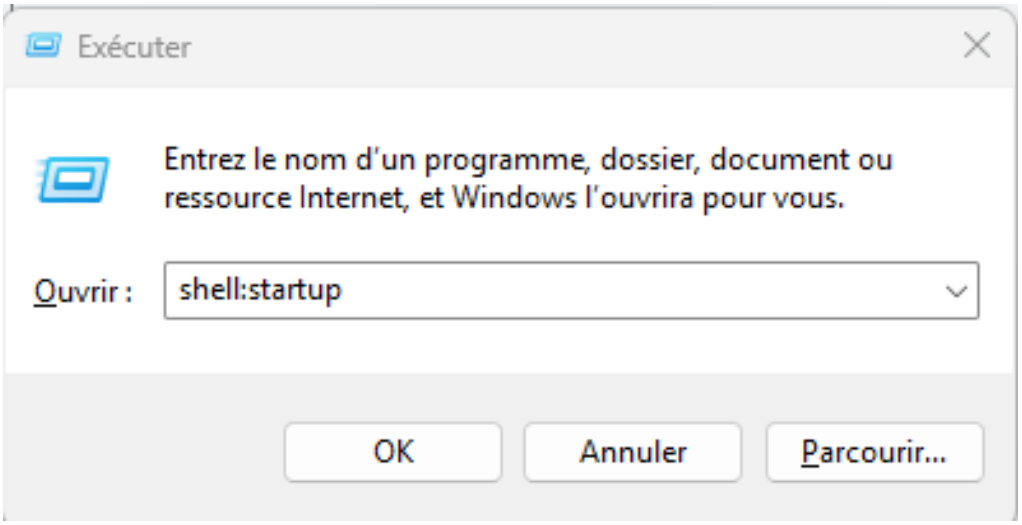


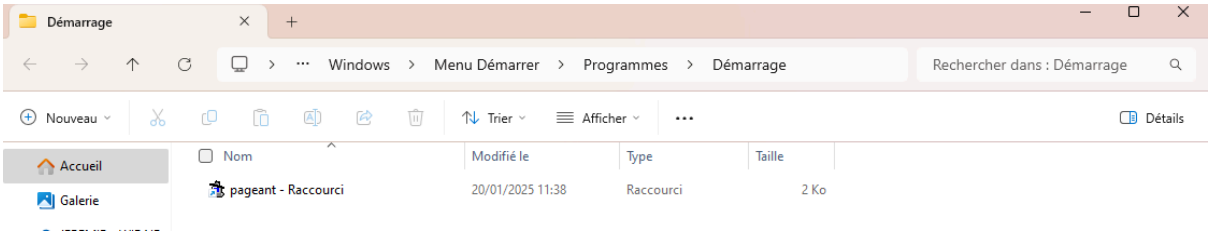
(cette image est pas la mienne, la mienne le key comment est “rsa-key-jdi”)

une fois fait il nous reste plus cas enregistrer la clé public et la clé privée dans l’emplacement voulu.

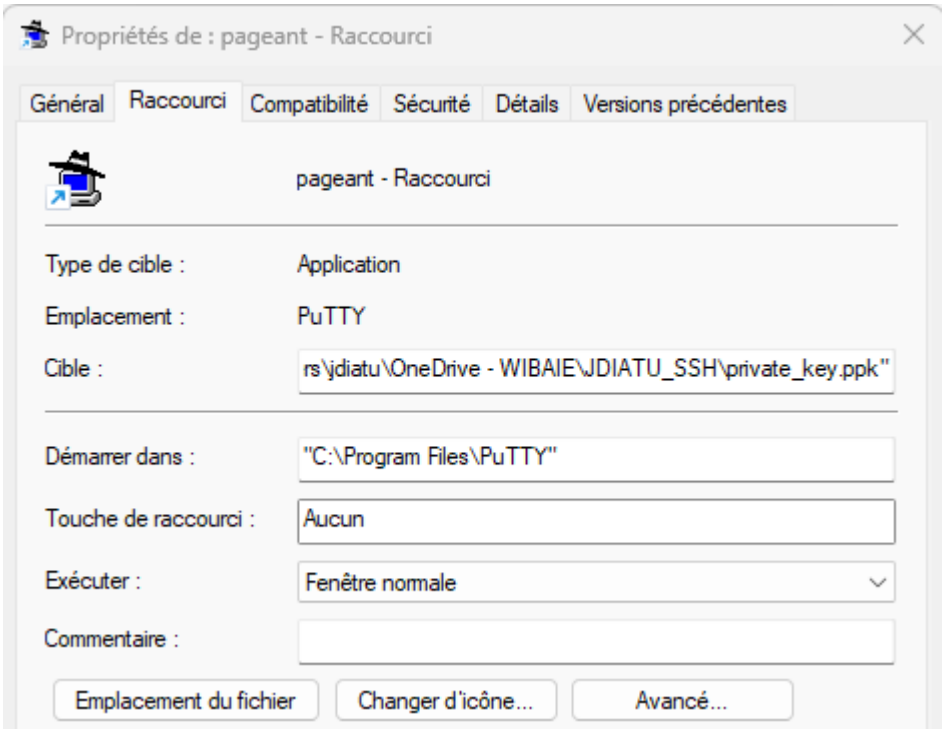


pour que cela se lance dès le démarrage de l'ordinateur je dois le préciser dans shell startup.



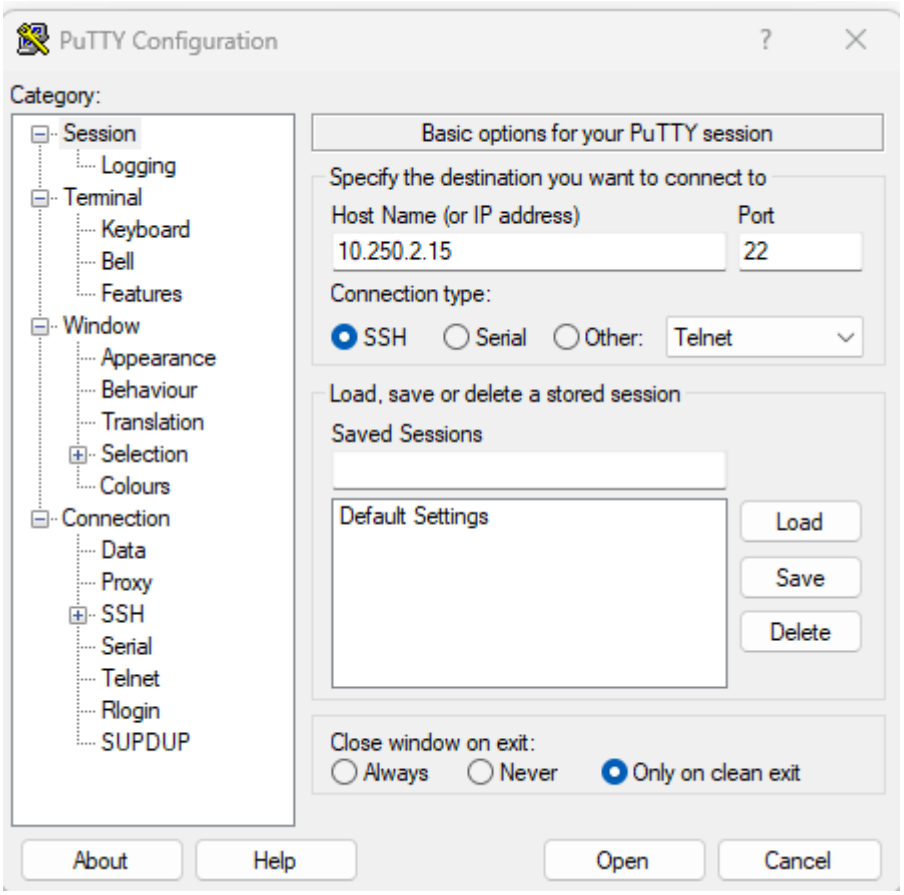


je me rend dans propriété

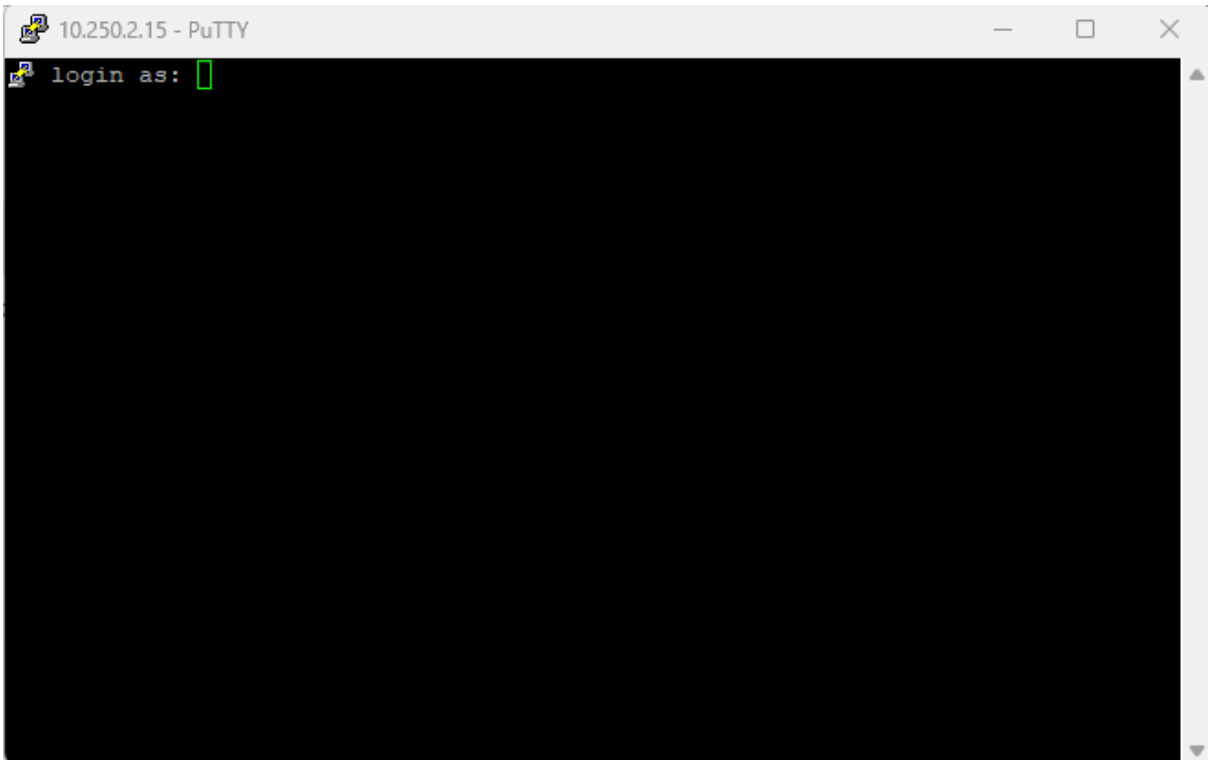


et je défini l'emplacement de ma clé. Après ses manipulations je peux me connecter sur la machine a present.

je me connecte sur ma machine serveur006 avec putty (avec l'adresse ip 10.250.2.15 et sur



le port 22 ssh) .



mon maître de stage a dû faire une manipulation sur puppet et ma aussi rajouter dans le groupe admin, et en plus des cle générer jai juste à indiquer mon nom d'utilisateur et ça se

connecte automatiquement .

```
jdi-admin@SERVEUR006: ~
login as: jdi-admin
Authenticating with public key "rsa-key-jdi" from agent
Linux SERVEUR006 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan 21 08:02:02 2025 from 192.168.102.48
jdi-admin@SERVEUR006:~$
```

on peut voir on ces authentifier avec la clé publique nomme “rsa-key-jdi”
après cela il ne me reste plus cas configurer les zones.

les indications de mon maître de stage sont celle ci:

- 192.168.100.22 helpdesk.caib.fr
- 192.168.100.4 elasticsearch.caib.fr
- 192.168.100.4 kibana.caib.fr

jai commencer par la configuration dans /etc/bind/named.conf.local:

```
jdi-admin@SERVEUR006:~$ cat /etc/bind/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 "caib.fr" {
        type master;
        file "/etc/bind/db.caib.fr";
};


zone "2.250.10.in-addr.arpa" {
        type master;
        file "/etc/bind/db.10.250.2";
};

jdi-admin@SERVEUR006:~$
```

puis je créer les fichiers de configuration de zones :

db.caib.fr db.10.250.2

et je les configure
db.caib.fr pour la zone directe:

jdi-admin@SERVEUR006: /etc/bind

```
  GNU nano 7.2
; 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     dns.caib.fr. root.caib.fr. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      dns.caib.fr.
dns     IN      A       10.250.2.15
serveur006      IN      A       10.250.2.15
helpdesk        IN      A       192.168.100.22
elasticsearch   IN      A       192.168.100.4
kibana  IN      A       192.168.100.4
```

db.10.250.2 pour la zone inverse:

jdi-admin@SERVEUR006: /etc/bind

```
  GNU nano 7.2
; 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     dns.caib.fr. root.caib.fr. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      dns.caib.fr.
15      IN      PTR     dns.caib.fr.
15      IN      PTR     serveur006.caib.fr.
22      IN      PTR     helpdesk.caib.fr.
4       IN      PTR     elasticsearch.caib.fr.
4       IN      PTR     kibana.caib.fr.
```

pour named.conf.options je garde les même informations:

```
acl "dmz" {
        10.250.2.0/24;
        10.250.1.0/24;
        localhost;
        localnets;
};



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 {
                1.1.1.1;
                1.0.0.1;
        };

        recursion yes;

        //========================================================================
        // 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 no;

        listen-on-v6 { none; };
        listen-on { any; };
        version none;

        allow-query { dmz; };
};
```

j’ai rajouter une acl pour autoriser que certaine machine a pouvoir interroger le dns et autoriser des requête que du dmz. (comme l’entreprise a 2 vlan pour le dmz)

201 VLAN DMZ	10.250.1.1	10.250.1.254	Non	Adresse Reseau = 10.250.1.0 Adresse Broadcast = 10.250.1.255 Masque de Sous-Reseau = 255.255.255.0 Masque Inverse (Wildcard)= 0.0.0.255 Nombre de Machines = 254 Premiere machine = 1 (...)
202 VLAN DMZ2	10.250.2.1	10.250.2.254	Non	Adresse Reseau = 10.250.2.0 Adresse Broadcast = 10.250.2.255 Masque de Sous-Reseau = 255.255.255.0 Masque Inverse (Wildcard)= 0.0.0.255 Nombre de Machines = 254 Premiere machine = 1 (...)

.
il nous reste à relancer le service bind9 et faire les teste.

serveur006:

```
jdi-admin@SERVEUR006:/etc/bind$ nslookup serveur006.caib.fr
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   serveur006.caib.fr
Address: 10.250.2.15
```

helpdesk(glpi):

```
jdi-admin@SERVEUR006:/etc/bind$ nslookup helpdesk.caib.fr
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   helpdesk.caib.fr
Address: 192.168.100.22
```

elasticsearch:

```
jdi-admin@SERVEUR006:/etc/bind$ nslookup elasticsearch.caib.fr
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   elasticsearch.caib.fr
Address: 192.168.100.4
```

kibana:

```
jdi-admin@SERVEUR006:/etc/bind$ nslookup kibana.caib.fr
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   kibana.caib.fr
Address: 192.168.100.4
```

on peut aussi tester notre resolver dns externe si elle fonctionne bien:

pour google:

```
jdi-admin@SERVEUR006:/etc/bind$ nslookup www.google.fr
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   www.google.fr
Address: 216.58.214.67
Name:   www.google.fr
Address: 2a00:1450:4007:810::2003

jdi-admin@SERVEUR006:/etc/bind$
```

et sainte-marie

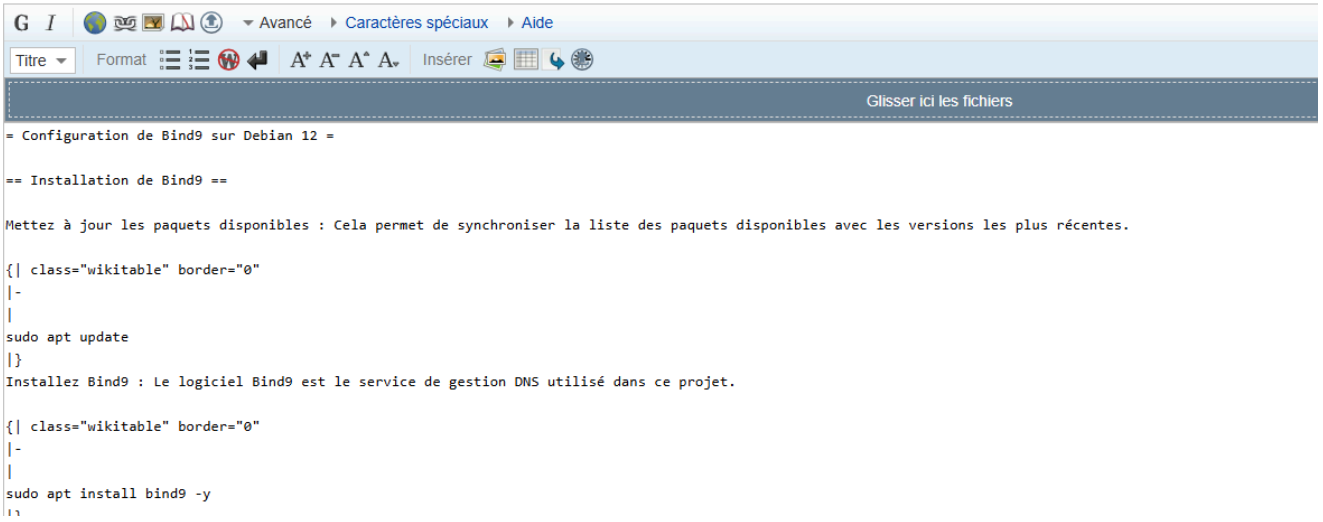
```
jdi-admin@SERVEUR006:/etc/bind$ nslookup www.saintemarie-cholet.eu
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
www.saintemarie-cholet.eu       canonical name = saintemarie-cholet.eu.
Name:   saintemarie-cholet.eu
Address: 178.33.198.3
```

Après cela, mon maître de stage m'a demandé de faire la documentation de tous les fichiers modifiés sur le serveur pour laisser des traces comme le serveur006 va continuer à vivre après mon départ. j'ai donc fait la documentation sur le mediawiki de l'entreprise .

la documentation je l'est fais en Wikitexte et html:

Modification de Bind9



voici la documentation :

JDIATU Discussion Préférences Liste de suivi Contributions Se déconnecter

CAIB FENÊTRES & PORTES

Page Discussion Lire Modifier Historique Plus Rechercher sur WIBAIE

Accueil
Modifications récentes
Page au hasard
Aide

Outils
Pages liées
Suivi des pages liées
Importer un fichier
Pages spéciales
Version imprimable
Adresse permanente
Information sur la page

Bind9

Sommaire [masquer]

Configuration de Bind9 sur Debian 12 [modifier]

Installation de Bind9 [modifier]

Installation avec Puppet (Récommandé) [modifier]

Il faut installer l'agent Puppet.
Puis configurer le tag 'bind9' sur le nom dans le fichier site.pp.

Instalation manuelle [modifier]

Mettez à jour les paquets disponibles : Cela permet de synchroniser la liste des paquets disponibles avec les versions les plus récentes.

```
# sudo apt update
```

Installez Bind9 : Le logiciel Bind9 est le service de gestion DNS utilisé dans ce projet.

```
# sudo apt install bind9 -y
```

Mettez à jour les paquets existants : Cela garantit la stabilité et la compatibilité des composants système.

```
# sudo apt update && sudo apt upgrade -y
```

Configuration des options DNS [modifier]

Le fichier named.conf.options définit les paramètres globaux du serveur DNS. Voici les principaux paramètres configurés :

- Forwarders : Spécifient les serveurs DNS publics (comme Cloudflare) pour résoudre les requêtes externes.
- Recursion : Active la recherche récursive, permettant au serveur de chercher des réponses pour les clients.
- ACL (Access Control List) : Limite l'accès au serveur DNS à une plage d'adresses IP spécifique (comme celles de la DMZ).

Ces options assurent la sécurité, la performance et la compatibilité du serveur DNS.

- /etc/bind/named.conf.options

```
acl "dmz" {
        10.250.2.0/24;
        10.250.1.0/24;
        localhost;
        localnets;
};
options {
        directory "/var/cache/bind";
        forwarders {
                1.1.1.1;
                1.0.0.1;
        };
        recursion yes;
        dnssec-validation no;
        listen-on-v6 { none; };
        listen-on { any; };
        version none;
        allow-query { dmz; };
};
```

Configuration des zones DNS [modifier]

Cette étape consiste à définir les zones DNS que le serveur va gérer. Les zones DNS configurées ici sont :

- Zone directe : Associe des noms de domaine à leurs adresses IP (exemple : serveur006.caib.fr à 10.250.2.15).
- Zone inversée : Permet de résoudre des adresses IP en noms de domaine (exemple : 10.250.2.15 vers serveur006.caib.fr).

Ces définitions permettent au serveur de répondre aux requêtes locales et de maintenir une cohérence dans la gestion

des noms de domaine internes.

- /etc/bind/named.conf.local

Ajouter les lignes ci-dessous pour gérer le domaine caib.fr.

```
zone "caib.fr" {
        type master;
        file "/etc/bind/db.caib.fr";
        allow-update { none; };
};
```

Configuration de la zone [modifier]

Le fichier de zone directe contient les enregistrements DNS pour le domaine caib.fr .
Contenu du fichier a éditer pour ajouter des entrées:

- /etc/bind.db.caib.fr

```
$TTL    86400
@       IN      SOA     dns.caib.fr. root.caib.fr. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@               IN      NS      dns.caib.fr.
dns             IN      A       10.250.2.15
helpdesk        IN      A       192.168.100.22
elasticsearch   IN      A       192.168.100.4
kibana          IN      A       192.168.100.4
```

- SOA (Start of Authority) : Définit le serveur DNS maître de la zone.
- Enregistrements NS : Indiquent le serveur DNS responsable de la zone.
- Enregistrements A : Associent les noms de domaine aux adresses IP correspondantes.

Ce fichier garantit que les services internes sont accessibles via leurs noms de domaine.

Zone DNS inversé [modifier]

--- PAS UTILISE ACTUELLEMENT ---
Création du fichier de zone inversée Le fichier de zone inversée est utilisé pour résoudre des adresses IP en noms de domaine. Cette configuration est essentielle pour certains services réseau, comme les journaux d'activité, qui nécessitent une résolution inversée. Voici les éléments inclus :

- /etc/bind/db.10.250.2

- /etc/bind/db.10.250.2

```
$TTL    86400
@       IN      SOA     dns.caib.fr. root.caib.fr. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      dns.caib.fr.
15      IN      PTR     dns.caib.fr.
22      IN      PTR     helpdesk.caib.fr.
4       IN      PTR     elasticsearch.caib.fr.
4       IN      PTR     kibana.caib.fr.
```

- SOA : Décrit la source d'autorité pour la zone.
- Enregistrements PTR (Pointer) : Mappent les adresses IP aux noms de domaine.

Ce fichier complète la configuration DNS pour assurer une résolution bidirectionnelle.

Configuration des paramètres de Bind9 [modifier]

Cette étape permet de configurer les paramètres supplémentaires pour Bind9, en particulier pour :

Désactiver resolvconf, afin que le fichier resolv.conf ne soit pas automatiquement écrasé. Ajouter des options de démarrage pour Bind9, comme forcer l'utilisation d'IPv4 uniquement avec -4. Ces paramètres garantissent que le service fonctionne de manière stable et adaptée à votre configuration réseau.

- /etc/default/named

```
# run resolvconf?
RESOLVCONF=no
# startup options for the server
OPTIONS="-u bind -4"
```

Test [modifier]

Relancez le service Bind9 : Après avoir configuré toutes les zones et options, le service doit être redémarré pour appliquer les modifications.

```
# sudo systemctl restart bind9
```

Vérifiez le statut de Bind9 : Cela permet de s'assurer que le service est actif et fonctionne sans erreur.

Test [modifier]

Relancez le service Bind9 : Après avoir configuré toutes les zones et options, le service doit être redémarré pour appliquer les modifications.

```
# sudo systemctl restart bind9
```

Vérifiez le statut de Bind9 : Cela permet de s'assurer que le service est actif et fonctionne sans erreur.

```
# sudo systemctl status bind9
```

Testez la résolution locale : Vérifiez que les noms de domaine internes configurés fonctionnent correctement :

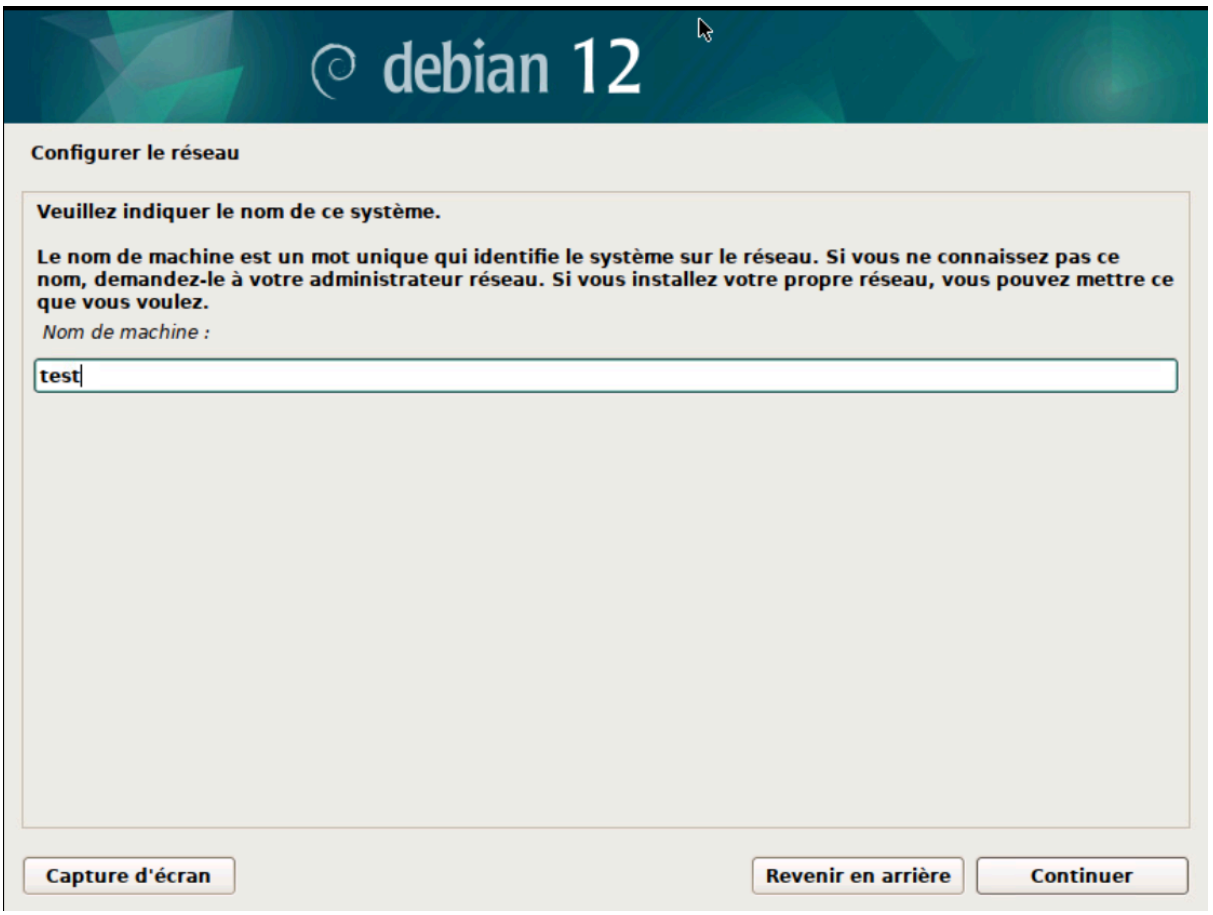
```
# dig helpdesk.caib.fr
```

```
# dig elasticsearch.caib.fr
```

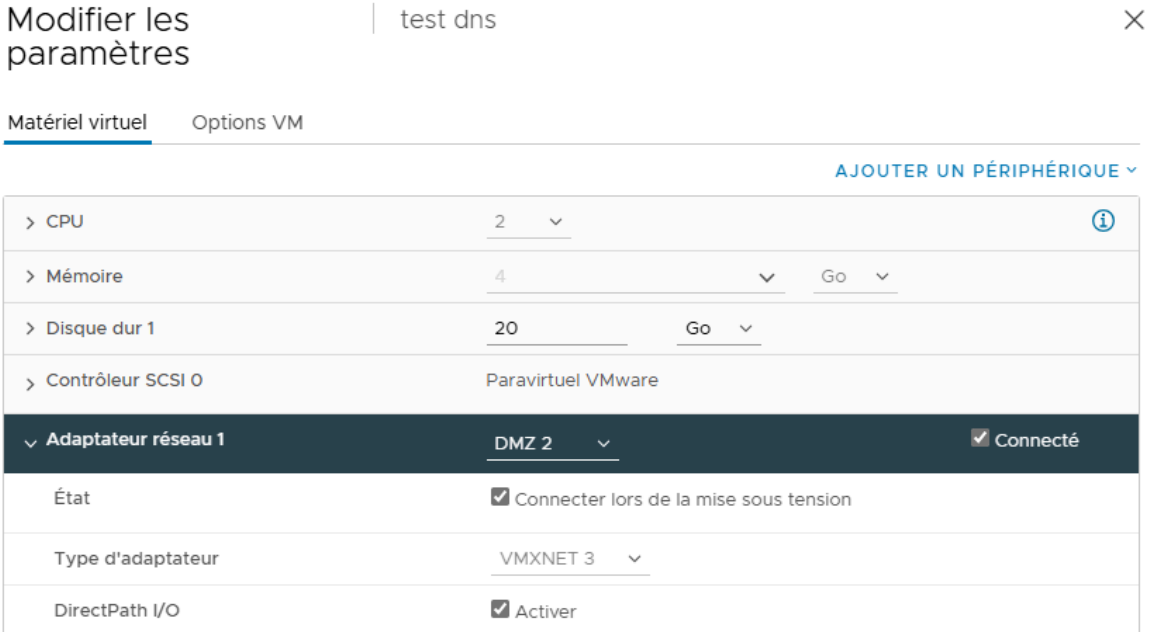
```
# dig kibana.caib.fr
```

Cette page a été modifiée pour la dernière fois le 23 janvier 2025 à 16:01.

après il me reste plus cas faire des teste pour voir si sa fonction, donc mon maître de stage ma demandé de créer une nouvel vm de tester pour faire les teste déçu avant de passer au serveur présent dans la dmz.



une fois fait, je défini une adresse ip statique du même réseau que le serveur dns dans la dmz



```
 GNU nano 7.2                                                /etc/network/interfaces
# 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 ens192
iface ens192 inet static
        address 10.250.2.16/24
        gateway 10.250.2.254
        # dns-* options are implemented by the resolvconf package, if installed
#       dns-nameservers 10.250.2.15
```

(on est pas obligé d'indiquer le serveur dns ici tant quil est indiqué dans le resolv.conf)
j'ai plus cas indiquer l'adresse ip du dns dans le resolv.conf et ensuite je pourrai faire des teste

test dns

```
 GNU nano 7.2
nameserver      10.250.2.15
```

Maintenant il me reste plus cas tester pour déterminer si mon serveur est prêt à être mis en prod.

pour le teste en local en va prendre une zones que j'avais créé et vérifier cela .
ex: helpdesk.caib.fr

test dns

```
root@test:~# dig helpdesk.caib.fr

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> helpdesk.caib.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52740
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0997ad88f57479f40100000067910edb96ab0a29e0f5c1ea (good)
;; QUESTION SECTION:
;helpdesk.caib.fr.              IN      A

;; ANSWER SECTION:
helpdesk.caib.fr.       86400   IN      A       192.168.100.22

;; Query time: 0 msec
;; SERVER: 10.250.2.15#53(10.250.2.15) (UDP)
;; WHEN: Wed Jan 22 16:29:36 CET 2025
;; MSG SIZE  rcvd: 89

root@test:~#
```

ça fonctionne bien car l’etat est en NOERROR et on vois bien en bas qu'il interroge un serveur dns qui a une adresse en 10.250.2.15

maintenant on va tester la resolution externe:
par exemple : www.saintemarie-cholet.eu

test dns

```
root@test:~# dig www.saintemarie-cholet.eu

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> www.saintemarie-cholet.eu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17091
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 884db91539d851f20100000067910ff08daef34b9d5c17be (good)
;; QUESTION SECTION:
;www.saintemarie-cholet.eu.     IN      A

;; ANSWER SECTION:
www.saintemarie-cholet.eu. 887  IN      CNAME   saintemarie-cholet.eu.
saintemarie-cholet.eu.  887     IN      A       178.33.198.3

;; Query time: 0 msec
;; SERVER: 10.250.2.15#53(10.250.2.15) (UDP)
;; WHEN: Wed Jan 22 16:34:12 CET 2025
;; MSG SIZE  rcvd: 112

root@test:~#
```

pareil sa fonction bien.