Table des matières

[1. Présentation du DNS 3](#_Toc98320061)

[1.1. Présentation des concepts 4](#_Toc98320062)

[1.1.1. Notion de domaine, de zone et de délégation 4](#_Toc98320063)

[1.1.2. Le domaine in-addr.arpa 5](#_Toc98320064)

[1.1.3. Service BIND 6](#_Toc98320065)

[1.1.4. Principaux types d'enregistrements 6](#_Toc98320066)

[1.1.5. Structure des enregistrements 7](#_Toc98320067)

[1.1.6. La délégation 8](#_Toc98320068)

[1.1.7. Serveur primaire et serveur secondaire 9](#_Toc98320069)

[1.1.8. Le cache 9](#_Toc98320070)

[2. Installation et configuration d'un serveur DNS 9](#_Toc98320071)

[2.1 Fichiers installés 9](#_Toc98320072)

[2.1.A Procédure de configuration du serveur 10](#_Toc98320073)

[2.1.B Configurer les fichiers 10](#_Toc98320074)

[2.1.C Configuration du DNS manuellement 11](#_Toc98320075)

[2.1.D Le fichier named.conf 11](#_Toc98320076)

[2.1.E Les fichiers ofppt.zone 12](#_Toc98320077)

[2.1.F Le fichier ofppt.rev 12](#_Toc98320078)

[2.1.G Comment se servir de l'utilitaire rndc 13](#_Toc98320079)

[2.2 Fonctionnalités avancées de BIND 14](#_Toc98320080)

[2.2.A Vues multiples 14](#_Toc98320081)

[2.2.B DNSSEC (DNS Security Extensions) 15](#_Toc98320082)

[2.2.C IPv6 (Internet Protocol version 6) 15](#_Toc98320083)

[2.2.D DNS maître esclave 15](#_Toc98320084)

[2.2.E DDNS (Dynamic DNS) 15](#_Toc98320085)

[2.3 Procédure de tests 17](#_Toc98320086)

[2.3.A Vérifier la résolution de noms : 17](#_Toc98320087)

[3. Remarques 20](#_Toc98320088)

[4. Annexes : extraits de fichiers de configuration 21](#_Toc98320089)

[5. Questions : 24](#_Toc98320090)

|  |
| --- |
| Présentation du DNSDNS (Domain Name System) est un système de base de données distribué utilisé pour associer les noms d'hôtes à leurs adresses IP respectives. Pour les utilisateurs, cela a l'avantage qu'ils peuvent faire référence à des machines du réseau par leur nom, ce qui est normalement plus facile à mémoriser que les adresses numériques de réseau. Pour les administrateurs de système, l'utilisation d'un serveur DNS (ou nameserver) permet de changer l'adresse IP pour un hôte sans affecter pour autant les recherches basées nom. L'utilisation des bases de données DNS sert non seulement à résoudre les adresses IP en noms de domaine, mais leur utilisation s'élargit de plus en plus au fur et à mesure que DNSSEC (Domain Name System Security Extensions) se déploie.Quelle est la structure d'un nom d'hôte? Nom\_d\_hôte ou bien Nom\_d\_hôte.NomDomaine**Exemple** : fedorasrv ou bien fedorasrv.ofppt.orgLe nom de domaine identifie une organisation dans l'Internet, comme, par exemple, google.com, ofppt.ma... Dans les exemples, nous utiliserons un domaine que l'on considère fictif : «  ofppt.org  ». Chaque organisation dispose d'un ou plusieurs réseaux. Ces réseaux sont composés de noeuds, ces noeuds (postes, serveurs, routeurs, imprimantes, téléphones IP) pouvant être adressés. Par exemple, la commande **ping *fedorasrv.ofppt.org***, permet d'adresser la machine qui porte le nom d'hôte fedorasrv, dans le domaine (organisation) ofppt.org. **Quelle différence entre la résolution de noms d'hôtes avec un serveur DNS et les fichiers hosts ?**Avec les fichiers hosts, chaque machine dispose de sa propre base de données de noms. Sur des réseaux importants, cette base de données dupliquée n'est pas simple à maintenir.Avec un service de résolution de noms, la base de données est localisée sur un serveur. Un client qui désire adresser un hôte cherche dans son cache local, s'il en connaît l'adresse. S'il ne la connaît pas il va interroger le serveur de noms.Tous les grands réseaux sous TCP/IP et Internet fonctionnent (schématiquement) sur ce principe.Avec un serveur DNS, un administrateur n'a plus qu'une seule base de données à maintenir. Il suffit qu'il indique sur chaque hôte, quelle est l'adresse de ce serveur. Ici il y a 2 cas de figures possibles :* Soit les hôtes (clients) sont des clients DHCP (Dynamic Host Configuration Protocol), cette solution est particulière et n'est pas abordée ici. Cette technique est l'objet d'un autre chapitre.
* Soit les clients disposent d'une adresse IP statique. La configuration des clients est détaillée dans ce document.

Normalement un service DNS nécessite au minimum deux serveurs afin d'assurer un minimum de redondance. Les bases de données des services sont synchronisées. La configuration d'un serveur de noms secondaire sera expliquée. Nous verrons également en TP le fonctionnement de la réplication des bases de données (bases d'enregistrements de ressources). On peut parler de bases de données réparties et synchronisées. Présentation des conceptsNotion de domaine, de zone et de délégationUn « domaine » est un sous-arbre de l'espace de nommage. Par exemple .com est un domaine, il contient toute la partie hiérarchique inférieure de l'arbre sous jacente au nœud .com.Un domaine peut être organisé en sous domaines. .facebook.com est un sous domaine du domaine .com. Un domaine peut être assimilé à une partie ou sous-partie de l'organisation de l'espace de nommage. Voir la diapositive sur les Domaines, zones et délégations.Une "zone" est une organisation logique (ou pour être plus précis, une organisation administrative) des domaines. Le rôle d'une zone est principalement de simplifier l'administration des domaines.Le domaine ".com" peut être découpé en plusieurs zones, z1.com, z2.com...zn.com. L'administration des zones sera déléguée afin de simplifier la gestion globale du domaine. La délégation consiste à déléguer l'administration d'une zone (ou une sous-zone) aux administrateurs de cette zone. Voir la diapositive sur la délégation.Attention à ces quelques remarques : * Un domaine est une organisation de l'espace de nommage. Il peut être attaché à un domaine parent, et/ou peut avoir un ou plusieurs sous-domaines enfants.
* Les zones correspondent à des organisations administratives des domaines. Un domaine peut être administré par plusieurs zones administratives, mais il est possible aussi qu'une zone serve à l'administration de plusieurs domaines. Prenons l'exemple d'un domaine "MonEntreprise.fr", membre de ".fr". Il peut être composé de trois sous-domaines France.MonEntreprise.fr, Italie.MonEntreprise.fr, Espagne.MonEntreprise.fr et de deux zones d'administration. Une en France pour les sous-domaines France.MonEntreprise.fr, Italie.MonEntreprise.fr (il n'y a pas de délégation), et une pour Espagne.MonEntreprise.fr, il y a délégation.
* L'adressage IP correspond à une organisation physique des noeuds sur un réseau IP.
* L'organisation de l'espace de nommage est complètement indépendante de l'implantation géographique d'un réseau ou de son organisation physique. L'organisation physique est gérée par des routes (tables de routage). L'espace de nommage indique pour un nom de domaine N, quels sont les serveurs de noms qui ont autorité sur cette zone. Elles ne donnent pas la façon d'arriver à ces machines.
* Les seules machines connues au niveau de l'espace de nommage, sont les serveurs de nom "déclarés". Ces informations sont accessibles par des bases de données "whois".
* La cohérence (le service de résolution de noms) entre l'organisation de l'espace de nommage global et les organisations internes des réseaux sur Internet est réalisée par les serveurs de noms.

Le domaine in-addr.arpaLe principe de la résolution de noms, consiste à affecter un nom d'hôte une adresse IP. On parle de résolution de noms directe. Le processus inverse doit pouvoir également être mis en oeuvre. On parle de résolution de noms inverse ou reverse. Le processus doit fournir, pour une adresse IP, le nom correspondant. Pour cela il y a une zone particulière, **in-addr.arpa**, qui permet la résolution inverse d'adresse IP. Par exemple, pour le réseau 192.168.1.0, on créera une zone inverse dans le domaine in-addr.arpa. La zone de recherche inverse dans le domaine deviendra : 1.168.192.in-addr.arpa. Cette zone devra répondre pour toutes les adresses déclarées dans la tranche 192.168.1.0 à 192.168.1.254. On inscrira dans cette zone tous les noeuds du réseau pour lesquels on désire que la résolution inverse fonctionne. Un serveur de noms peut, pratiquement, fonctionner sans la définition de cette zone tant que le réseau n'est pas relié à l'Internet. Si cela était le cas, il faudrait déclarer cette zone, sans quoi, des services comme la messagerie électronique, ne pourrait fonctionner correctement, notamment à causes des règles anti-spam. Service BINDBIND représente un ensemble de programmes liés au DNS. Il comprend un serveur de noms intitulé named, un utilitaire d'administration intitulé rndc, et un outil de déboggage intitulé DIG Quand le service named démarre, il lit la configuration à partir de fichier /etc/named.conf et les fichiers /etc/named/Principaux types d'enregistrementsLes types d'enregistrements, qui enrichissent une base de données DNS, sont de plusieurs types, dont voici les principaux : * Enregistrement de type **SOA** (Start Of Authority) : indique l'autorité sur la zone. Ces enregistrements contiennent toutes les informations sur le domaine. Par exemple le délai de mise à jour des bases de données entre serveurs de noms primaires et secondaires, le nom du responsable du site
* Enregistrements de type **NS** (Name Server) : ces enregistrements donnent les adresses des serveurs de noms pour le domaine.
* Enregistrement de type **A** (Adresse) : ces enregistrements permettent de définir les noeuds fixes du réseau (ceux qui ont des adresses IP statiques). Serveurs, routeurs, switchs ...
* Enregistrements de type **MX** (Mail eXchanger) : ils servent pour déclarer les serveurs de messagerie.
* Enregistrements de type **CNAME** (Canonical Name) : ils permettent de définir des alias sur des noeuds existants. Par exemple www.ofppt.org peut être la même machine que web.foo.org. Dans ce cas, «  www  » est un alias (CNAME) de «  web  ». Cela permet de différencier le nommage des machines des standards de nommages des services (www, ftp, news, smtp, mail, pop...).
* Enregistrement de type **PTR** (Pointeur) : ils permettent la résolution de noms inverse dans le domaine in-addr.arpa.

Ces enregistrements caractérisent des informations de type IN - INternet. Exemple d’enregistrements :* **fedorasrv IN A 192.168.1.226**
* **www IN CNAME fedorasrv**
* **ofppt.org. IN MX 10 mail.ofppt.org.**
* **227 IN PTR test.ofppt.org.**

Structure des enregistrementsStructure d'un enregistrement *SOA* : chaque fichier de ressource de zone commence par un enregistrement de type SOA. Voici un exemple d'enregistrement SOA :$ORIGIN ofppt.org.$TTL 3H@ IN SOA ofppt.org. root.ofppt.org. ( 0 ; serial 1D ; refresh 1H ; retry 1W ; expire 3H ) ; minimumSOA Start Of Authority, enregistrement qui contient les informations de synchronisation des différents serveurs de nom. @ peut être remplacé par ofppt.org (nom de la zone)Root.ofppt.org : la personne qui est responsable de la zone. Le premier point sera remplacé par l'arobase (@) pour envoyer un courrier électronique. Cela deviendra root.ofppt.org. 1. Numéro de série sert à identifier la dernière modification sur le serveur de noms maître. Ce numéro sera utilisé par les serveurs de nom secondaires pour synchroniser leurs bases. Si le numéro de série du serveur de noms primaire est supérieur à celui des serveurs de noms secondaires, alors le processus de synchronisation suppose que l'administrateur a apporté une modification sur le serveur maître et les bases seront synchronisées.
2. Rafraîchissement : Intervalle de temps donné en seconde pour indiquer au serveur la périodicité de la synchronisation.
3. Retry : intervalle de temps avant réitération si l'essai précédent n'a pas fonctionné.
4. Expire : temps au bout duquel le serveur ne remplit plus sa mission s'il n'a pu contacter le serveur maître pour mettre à jour ses données.
5. TTL : Time To Live, durée de vie des enregistrements. Plus la durée de vie est courte, plus l'administrateur est susceptible de considérer que ses bases sont à jour, par contre cela augmente le trafic sur le réseau.

Enregistrement de type *NS* pour le domaine ofppt.org :ofppt.org. IN NS srv1.ofppt.org. ; noter le point final "." IN NS srv2.ofppt.org. ; Le « **.** » final signifie que le nom est pleinement qualifié. On aurait pu mettre :@ IN NS srv1  IN NS srv2"@" signifie "ofppt.org" et pour le serveur de nom, comme "srv1" n'est pas pleinement qualifié, cela équivaut à " srv1.ofppt.org ". Enregistrements de type *A* : nous devons décrire la correspondance Nom / Adressesrv1.ofppt.org. IN A 192.168.1.254srv2.ofppt.org. IN A 192.168.0.253localhost.ofppt.org. IN A 127.0.0.1S'il y avait d'autres hôtes sur la zone, il faudrait les définir ici. *Enregistrements de type* CNAME*:* Ce sont les alias (Canonical Name). Une requête du type http://www.foo.org sera adressée à ns1.foo.org, puisque www est un alias de ns1.www IN CNAME srv1.ofppt.org.ftp IN CNAME srv1.ofppt.org.*Enregistrement de type* PTR*:* ils serviront à la résolution de noms inverse.254 IN PTR srv1.ofppt.org.253 IN PTR srv2.ofppt.org.La délégationLa délégation consiste à donner l'administration d'une partie du domaine à une autre organisation. Il y a transfert de responsabilité pour l'administration d'une zone. Les serveurs de la zone auront autorité sur la zone et auront en charge la responsabilité de la résolution de noms sur la zone. Les serveurs ayant autorité sur le domaine auront des pointeurs vers les serveurs de noms ayant autorité sur chaque zone du domaine. Serveur primaire et serveur secondaireLe serveur maître (primaire) dispose d'un fichier d'information sur la zone. Le ou les serveurs esclaves (secondaires) obtiennent les informations à partir d'un serveur primaire ou d'un autre serveur esclave. Il y a " transfert de zone". Les serveurs maîtres et esclaves ont autorité sur la zone. Le cacheL'organisation d'Internet est assez hiérarchique. Chaque domaine dispose de ses propres serveurs de noms. Les serveurs peuvent être sur le réseau physique dont ils assurent la résolution de nom ou sur un autre réseau. Chaque zone de niveau supérieur (edu, org, fr...) dispose également de serveurs de nom de niveau supérieur. L'installation du service DNS, installe une liste de serveurs de noms de niveaux supérieurs. Cette liste permet au serveur de résoudre les noms qui sont extérieurs à sa zone. Le serveur enrichit son cache avec tous les noms résolus. Si votre réseau n'est pas relié à Internet, vous n'avez pas besoin d'activer cette liste. Ce fichier est un peu particulier. Il est fourni avec les distributions. Il est utilisé par le serveur de noms à l'initialisation de sa mémoire cache. Si vos serveurs sont raccordés à Internet, vous pourrez utiliser une liste officielle des serveurs de la racine. Installation et configuration d'un serveur DNSL'application est installée via la commande **dnf -y install bind\***. Pour mettre en place le service de résolution de noms sur un serveur GNU/Linux, on va procéder successivement aux opérations suivantes : 1. Vérifier les fichiers déjà installés,
2. Configurer le fichier principal ;
3. Configurer les fichiers des zones administrées ;
4. Configurer les fichiers de transaction sécurisée pour rndc;
5. Démarrer et tester le service serveur.

Fichiers installés Le fichier de configuration consiste en un ensemble d'arguments comprenant des options imbriquées entourées par des crochets courbes ({ et }). Veuillez noter que si vous modifiez le fichier, le service **named** ne démarrera pas.Si vous avez installé le paquet **bind-chroot**, le service de liaison exécutera dans l'environnement **chroot**. Dans ce cas, le script d'initialisation procédera au montage des fichiers de configuration ci-dessus à l'aide de la commande **mount--bind**, afin que vous puissiez contrôler la configuration en dehors de cet environnement. Il n'y a pas besoin de copier quoi que ce soit dans le répertoire **/var/named/chroot/** parce qu'elle est montée automatiquement. Cela simplifie la maintenance puisque vous n'avez pas besoin de prendre un soin particulier des fichiers de configuration **BIND** si la commande est exécutée dans un environnement **chroot**. Vous pouvez tout organiser comme vous le feriez avec BIND si vous n'étiez pas dans un environnement **chroot**.Les répertoires suivants sont montés automatiquement sur **/var/named/chroot/** si les répertoires de point de montage correspondants qui se trouvent sous **/var/named/chroot/** sont vides :* **/etc/named**
* **/etc/pki/dnssec-keys**
* **/run/named**
* **/var/named**
* **/usr/lib/bind**
* **/etc/named.conf**
* **/etc/rndc.conf**
* **/etc/rndc.key**
* **/etc/named.rfc1912.zones**
* **/etc/named.dnssec.keys**
* **/etc/named.iscdlv.key**
* **/etc/named.root.key**

Le contenu de tous ces fichiers et commentaires se trouve en annexe.Procédure de configuration du serveurAprès avoir installé les services **bind**, via la commande **sudo dnf -y install bind\***, Il n'est pas nécessaire de copier les exemples de fichiers dans **/var/named/chroot/etc/** lors de l'utilisation de la version **chroot** car elle est montée automatiquement (mount --bind) avec /etc/. Ensuite on procède à l’enchainement des commandes suivantes :**#systemctl stop named.service****#systemctl disable named.service****#systemctl start named-chroot.service****#systemctl enable named-chroot.service**Configurer les fichiersVous pouvez configurer le serveur manuellement, c'est à dire créer les fichiers à l'aide d'un éditeur de texte ou à l'aide d'un outil de configuration graphique. En général on n'installe jamais d'interface graphique sur un serveur pour des questions de sécurité. Nous allons donc créer les fichiers complètement. La configuration est réalisable également à distance avec des requêtes HTTP grâce à des outils comme **webmin**. Configuration du DNS manuellementLe fichier racine pour la configuration du serveur de noms est le fichier /etc/named.conf. Ce fichier est lu au démarrage du service et donne la liste des fichiers qui définissent la base de données pour la zone.Le fichier named.confoptions { listen-on port 53 { 127.0.0.1; 192.168.1.226; }; listen-on-v6 port 53 { ::1; }; directory "/var/named"; dump-file "/var/named/data/cache\_dump.db"; statistics-file "/var/named/data/named\_stats.txt"; memstatistics-file "/var/named/data/named\_mem\_stats.txt"; secroots-file "/var/named/data/named.secroots"; recursing-file "/var/named/data/named.recursing"; allow-query { localhost; any;192.168.1/24; }; allow-query-cache { localhost; any; }; recursion no; managed-keys-directory "/var/named/dynamic"; geoip-directory "/usr/share/GeoIP"; pid-file "/run/named/named.pid"; session-keyfile "/run/named/session.key"; include "/etc/crypto-policies/back-ends/bind.config";};logging { channel default\_debug { file "data/named.run"; severity dynamic; };};zone "." IN { type hint; file "named.ca";};#zone directe et inversezone "ofppt.org" IN { type master; file "ofppt.zone"; allow-update { none; };};zone "1.168.192.in-addr.arpa" IN { type master; file "ofppt.rev"; allow-update { none; };};include "/etc/named.rfc1912.zones";include "/etc/named.root.key";key rndc-key { algorithm hmac-md5; secret "grYXJrtUhXnDK1GeS4eLh08e7oWOdLSR5EVAGoiAm+k="; };controls { inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { rndc-key; }; Les fichiers ofppt.zone $ORIGIN ofppt.org.$TTL 3H@ IN SOA ofppt.org. root.ofppt.org. ( 1 1D 1H 1W 3H ) IN NS fedorasrv.fedorasrv IN A 192.168.1.226test IN A 192.168.1.227www IN CNAME fedorasrvtest2.ofppt.org. IN A 192.168.1.228Le paramètre @, signifie qu'il s'agit du domaine "ofppt.org" (le nom tapé après le mot " zone " dans le fichier de configuration named.conf). Le paramètre "IN", signifie qu'il s'agit d'un enregistrement de type internet. Notez la présence d'un point (.) après le nom des machines pleinement qualifiés. Sans celui-ci, le nom serait " étendu ". Par exemple, fedorasrv (sans point) serait compris comme fedorasrv.ofppt.org (on rajoute le nom de domaine en l'absence du point terminal). Le point (.) terminal permet de signifier que le nom est pleinement qualifié.  Le fichier ofppt.rev$ORIGIN 1.168.192.in-addr.arpa.$TTL 3H@ IN SOA ofppt.org. root.ofppt.org. ( 1 1D 1H 1W 3H ) IN NS fedorasrvg.226 IN PTR fedorasrv.ofppt.org.227 IN PTR test.ofppt.org.228 IN PTR test2.ofppt.org. Comment se servir de l'utilitaire rndcL'utilitaire **rndc** est un outil de ligne de commandes qui vous permet d'administrer le service**named**, à la fois localement et à partir d'une machine éloignée.Pour éviter l'accès non autorisé au service, **named** doit être configuré pour écouter le port sélectionné (9 5 3 par défaut), et une clé identique doit être utilisée par le service et l'utilitaire **rndc** à la fois.[root@fedorasrv etc]# cat rndc.conf# Start of rndc.confkey "rndc-key" { algorithm hmac-sha256; secret "grYXJrtUhXnDK1GeS4eLh08e7oWOdLSR5EVAGoiAm+k=";};options { default-key "rndc-key"; default-server 127.0.0.1; default-port 953;};# End of rndc.conf# Use with the following in named.conf, adjusting the allow list as needed:# key "rndc-key" {# algorithm hmac-sha256;# secret "grYXJrtUhXnDK1GeS4eLh08e7oWOdLSR5EVAGoiAm+k=";# };## controls {# inet 127.0.0.1 port 953# allow { 127.0.0.1; } keys { "rndc-key"; };# };# End of named.confLe service **named** est configuré à l'aide de l'argument **controls** qui se trouve dans le fichier de configuration **/etc/named.conf**. À moins que cet argument soit présent, seules les connexions de l'adresse de loopback (127.0.0.1) seront autorisées, et la clé qui se trouve dans **/etc/rndc.key** sera utilisée.[root@fedorasrv etc]# cat rndc.keykey "rndc-key" { algorithm hmac-sha256; secret "ZbKNhAfMH/gZZ8jO5EjeojOxkDyPvIv0GwjJNJXnkBM=";};Pour une configuration en ligne de commande vous utilisez les commandes suivantes :Pour télécharger à nouveau les zones[root@fedorasrv ~]#rndc reload pour charger à nouveau le fichier de configuration et les zones nouvellement ajoutées[root@fedorasrv ~]#rndc reconfigSi vous souhaitez modifier une zone qui utilise un **DNS** Dynamique (DDNS), veillez à exécuter la commande[root@fedorasrv ~]#rndc freeze localhostQuand vous aurez terminé, exécuter la commande **thaw** pour autoriser **DDNS** à nouveau, et charger la zone à nouveau.[root@fedorasrv ~]#rndc thaw localhostPour activer (ou désactiver si elle est déjà activée) la journalisation des requêtes, veuillez exécuter la commande suivante en tant qu'utilisateur **root**:[root@fedorasrv ~]#rndc querylogFonctionnalités avancées de BINDVues multiplesÉventuellement, des informations différentes peuvent être présentées à un client selon le réseau de provenance de la demande. Ceci est principalement utilisé pour refuser l'accès à des données sensibles **DNS** de la part de clients se trouvant à l'extérieur du réseau local, tout en permettant aux requêtes des clients à l'intérieur du réseau local.Pour configurer plusieurs affichages, ajoutez l'argument **view** dans le fichier de configuration **/etc/named.conf**. Utilisez l'option de **match-clients** pour faire correspondre les adresses **IP** ou des réseaux dans leur ensemble et leur donner des options spéciales et les données de zone.[root@fedorasrv ~]#cat /etc/named.confacl acl\_intranet\_A { 192.168.0.0/24; };acl acl\_intranet\_B { 192.168.1.0/24; };acl acl\_internet { !acl\_intranet\_A; !acl\_intranet\_B; any; };options { listen-on port 53 { 127.0.0.1; any; }; listen-on-v6 port 53 { ::1; }; directory "/var/named"; dump-file "/var/named/data/cache\_dump.db"; statistics-file "/var/named/data/named\_stats.txt"; memstatistics-file "/var/named/data/named\_mem\_stats.txt"; allow-query { localhost; any; }; allow-query-cache { localhost; any; };};logging { channel default\_debug { file "data/named.run"; severity dynamic; };};view intranet\_A { match-clients { localhost; acl\_intranet\_A; }; recursion yes; include "/etc/named.intraA.zones";};view intranet\_B { match-clients { acl\_intranet\_B; }; recursion yes; include "/etc/named.intraB.zones";};view internet { match-clients { acl\_internet; }; recursion yes; include "/etc/named.internet.zones";};DNSSEC (DNS Security Extensions)Les extensions de sécurité du système des noms de domaine (DNSSEC) permettent aux titulaires de noms de domaine de signer numériquement l’information qu’ils envoient à travers le système des noms de domaine (DNS). Il s’agit d’un moyen de protéger les consommateurs en évitant qu’ils reçoivent des données DNS ayant été corrompues de manière accidentelle ou illicite.Les DNSSEC renforcent l'authentification du DNS en utilisant des signatures numériques basées sur la cryptographie à clé publique. Avec les DNSSEC, les requêtes DNS et les réponses ne sont pas elles-mêmes signées cryptographiquement, ce sont les données DNS qui sont signées par le propriétaire des données.IPv6 (Internet Protocol version 6)Internet Protocol version 6 (IPv6) est pris en charge par l'utilisation des enregistrements de ressources **AAAA**, et la directive **listen-on-v6** (Indique l'interface de réseau **IPv6** sur lequel écouter pour les requêtes. Sur un serveur **DNS** qui agit aussi en tant que passerelle, vous pouvez utiliser cette option pour répondre à des requêtes provenant d'un seul réseau. Toutes les interfaces **IPv6** sont utilisées par défaut).DNS maître esclaveLa plupart des changements au fichier **/etc/named.conf** d'un serveur de noms primaire ou secondaire consistent à ajouter, modifier ou supprimer des arguments de **zone**, et seul un petit nombre d'options d'arguments de **zone** est normalement utile pour qu'un serveur de noms puisse fonctionner efficacement.L'argument de **zone** d'un serveur secondaire est légèrement différent. Le type est défini sur **l'esclave**, et la directive du **master** indique au service **named** l'adresse **IP** du serveur maître.#zone du serveur principalzone "ofppt.org" IN { type master; file "ofppt.zone"; allow-update { none; }; allow-transfer {192.168.2.266;};};#zone du serveur secondairezone "ofppt.org" { type slave ; file "slaves/ofppt.zone"; master {192.168.1.226;}};Dans l’exemple ci-dessus, le service **named** est configuré pour interroger le serveur principal à l'adresse **IP 192.168.1.226** pour obtenir des informations sur la zone **ofppt.org**. L'information reçue est alors enregistrée dans le fichier **/var/named/slaves/ofppt.zone**. Notez que vous devez mettre toutes les zones esclave dans le répertoire **/var/named/slaves/**, sinon le service ne pourra pas transférer la zone.DDNS (Dynamic DNS)Le DNS dynamique (DDNS ou DynDNS) est une méthode de mise à jour automatique d'un serveur de noms dans le système de noms de domaine (DNS), souvent en temps réel, avec la configuration DDNS active de ses noms d'hôte, adresses ou autres informations configurés.Le terme est utilisé pour décrire deux concepts différents. Le premier est la "mise à jour DNS dynamique" qui fait référence aux systèmes utilisés pour mettre à jour les enregistrements DNS traditionnels sans modification manuelle. Ces mécanismes sont expliqués dans la RFC 2136 et utilisent le mécanisme TSIG pour assurer la sécurité. Le deuxième type de DNS dynamique permet des mises à jour légères et immédiates souvent à l'aide d'un client de mise à jour, qui n'utilise pas la norme RFC2136 pour la mise à jour des enregistrements DNS. Ces clients fournissent une méthode d'adressage persistante pour les appareils qui changent fréquemment d'emplacement, de configuration ou d'adresse IP.Pour activer le DDNS on procède de la manière suivante :Dans les fichiers de zoneszone "ofppt.org" IN { type master; file "ofppt.zone"; allow-update { 192.168.1.226; }; #l’adresse du serveur DHCP};zone "1.168.192.in-addr.arpa" IN { type master; file "ofppt.rev"; allow-update { 192.168.1.226; };}Après au niveau du DHCP on modifie le fichier **dhcpd.conf** :ddns-update-style interim;ddns-updates on;ddns-domainname = "ofppt.org"ddns-rev-domain = "1.168.192.in-addr.arpa"authoritative;allow client-updates;subnet 192.168.1.0 netmask 255.255.255.0 { range 192.168.1.100 192.168.1.200; option routers 192.168.1.254; option subnet-mask 255.255.255.0; option domain-name "ofppt.org"; option domain-name-servers 192.168.1.226; default-lease-time 21600; max-lease-time 43200; zone ofppt.org { primaire 192.168.1.226 ; } zone 1.168.192.in-addr.arpa { primaire 192.168.1.226 ; }   option server.ddns-hostname = concat("dhcp-", substring( binary-to-ascii(10, 8, "-", leased-address) , 8, 7)); option server.ddns-domainname = config-option domain-name ; option host-name = concat(config-option server.ddns-hostname, ".", config-option server.ddns-domainname);  }Procédure de testsAttention au fichier hosts et au fichier host.conf. Prenez le temps de regarder ce qu'il y a dedans. Faites une copie de sauvegarde de ces fichiers et renommez-les. Vérifiez au besoin leur utilité avec les commandes **man** host.conf et **man** hosts. Vous pouvez tester votre configuration avant même d'avoir configuré un client. Sur la même machine vous allez utiliser un service client du serveur (commande **ping**) qui utilisera un service serveur (DNS). *Test sur le serveur de noms :* Tapez la commande **ping** www.ofppt.org. Si la commande répond, le serveur fonctionne. En effet www est un alias de fedorasrv dans la zone ofppt.org. *Test sur le client :* Avant de lancer une commande, vous devez vérifier que vous n'avez pas de fichier hosts local, sinon vous devez le supprimer.*Pourquoi ?* L'utilisation de fichiers hosts et d'un serveur de noms n'est pas exclusive. Dans bien des environnements, le fichier hosts est consulté avant le serveur de noms (notamment windows, GNU/Linux à moins que ce ne soit précisé). Si vous avez un fichier hosts sur la machine, vous pouvez avoir des résultats qui ne sont pas ceux attendus. Vérifier la résolution de noms :Pensez à bien vérifier le nom d'hôte de votre machine avec la commande **hostname**, au besoin, sous root, modifiez ce nom, toujours avec cette commande. Fermez les sessions et rouvrez les, vous aurez le bon nom d'hôte qui s'affichera sur votre console.Pour vérifier le fonctionnement de la résolution de noms à partir d’un client, vous pouvez utiliser les commandes suivantes : ping mail.ofppt.orgping www.ofppt.orgping fedorasrv.ofppt.orgping test1.ofppt.orgSi vous voulez vérifier que c'est bien le serveur de noms qui réalise la résolution, il existe plusieurs solutions. La plus simple est d'arrêter le service serveur avec la commande **systemctl stop named**, puis de refaire les manipulations. Aucune machine n'est atteignable en utilisant son nom, mais cela est toujours possible en utilisant l'adresse IP. Il existe des commandes de vérification de la résolution notamment **nslookup**, **dig** et **host.**Ces commandes sont très largement utilisées par les administrateurs de réseau pour résoudre les problèmes liés aux services de résolution de noms. Tests avec dig :# Test sur une zone[root@fedorasrv named]# dig any ofppt.org; <<>> DiG 9.16.24-RH <<>> any ofppt.org;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59032;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 1232; COOKIE: c4b50d4d8a999d0f01000000622f4c8c3a40322d4fe5f7f2 (good);; QUESTION SECTION:;ofppt.org. IN ANY;; ANSWER SECTION:ofppt.org. 10800 IN SOA ofppt.org. root.ofppt.org. 0 86400 3600 604800 10800ofppt.org. 10800 IN NS fedorasrv.;; Query time: 0 msec;; SERVER: 192.168.1.226#53(192.168.1.226);; WHEN: Mon Mar 14 15:09:16 +01 2022;; MSG SIZE rcvd: 130# Récupération de l'enregistrement SOA d'une zone[root@fedorasrv named]# dig soa ofppt.org; <<>> DiG 9.16.24-RH <<>> soa ofppt.org;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35331;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1;; WARNING: recursion requested but not available;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 1232; COOKIE: b8b2c823894f733001000000622f4cc2d900cbce318cc832 (good);; QUESTION SECTION:;ofppt.org. IN SOA;; ANSWER SECTION:ofppt.org. 10800 IN SOA ofppt.org. root.ofppt.org. 1 86400 3600 604800 10800;; Query time: 0 msec;; SERVER: 192.168.1.226#53(192.168.1.226);; WHEN: Mon Mar 14 15:10:10 +01 2022;; MSG SIZE rcvd: 107#Vérification de la résolution de nom sur www.ofppt.org**[root@fedorasrv named]# dig www.ofppt.org**; <<>> DiG 9.16.24-RH <<>> www.ofppt.org;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28792;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1;; WARNING: recursion requested but not available;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 1232; COOKIE: fee7f3080562ec0601000000622f4d0da24a6f4416860d97 (good);; QUESTION SECTION:;www.ofppt.org. IN A;; ANSWER SECTION:www.ofppt.org. 10800 IN CNAME fedorasrv.ofppt.org.fedorasrv.ofppt.org. 10800 IN A 192.168.1.226;; Query time: 0 msec;; SERVER: 192.168.1.226#53(192.168.1.226);; WHEN: Mon Mar 14 15:11:25 +01 2022;; MSG SIZE rcvd: 110**[root@fedorasrv named]# nslookup www.ofppt.org**Server: 192.168.1.226Address: 192.168.1.226#53www.ofppt.org canonical name = fedorasrv.ofppt.org.Name: fedorasrv.ofppt.orgAddress: 192.168.1.226# Vérification de la résolution de nom inverse.**[root@fedorasrv named]# dig ptr 227.1.168.192.in-addr.arpa**; <<>> DiG 9.16.24-RH <<>> ptr 227.1.168.192.in-addr.arpa;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11298;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1;; WARNING: recursion requested but not available;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 1232; COOKIE: 5ac3309c59ec9f5801000000622f4de8fa00c26c6f43e310 (good);; QUESTION SECTION:;227.1.168.192.in-addr.arpa. IN PTR;; ANSWER SECTION:227.1.168.192.in-addr.arpa. 10800 IN PTR test.ofppt.org.;; Query time: 0 msec;; SERVER: 192.168.1.226#53(192.168.1.226);; WHEN: Mon Mar 14 15:15:04 +01 2022;; MSG SIZE rcvd: 111**[root@fedorasrv named]# nslookup 192.168.1.227**227.1.168.192.in-addr.arpa name = test.ofppt.org.Dans le cas où le serveur n’arrive pas à résoudre le nom ou l’adresse IP on aura la réponse suivante :**[root@fedorasrv named]# dig ptr 230.1.168.192.in-addr.arpa**; <<>> DiG 9.16.24-RH <<>> ptr 230.1.168.192.in-addr.arpa;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 11817;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 1232; COOKIE: 47db44854664e25b01000000622f4e8daadf755f17967643 (good);; QUESTION SECTION:;230.1.168.192.in-addr.arpa. IN PTR;; AUTHORITY SECTION:1.168.192.in-addr.arpa. 10800 IN SOA ofppt.org. root.ofppt.org. 0 86400 3600 604800 10800;; Query time: 0 msec;; SERVER: 192.168.1.226#53(192.168.1.226);; WHEN: Mon Mar 14 15:17:49 +01 2022;; MSG SIZE rcvd: 133**[root@fedorasrv named]# nslookup 192.168.1.230**\*\* server can't find 230.1.168.192.in-addr.arpa: NXDOMAINRemarquesSi vous désirez mettre en place la résolution de noms sur un réseau local, il n'y a pas grand chose de plus à réaliser. Il faut rajouter les enregistrements de type MX pour la messagerie, cette opération sera réalisée pendant la configuration du service de messagerie. Il faut également mettre en place un service de synchronisation des bases de données avec un serveur secondaire pour assurer le service d'un serveur de noms de backup.Si vous désirez vous relier sur internet, le processus est plus complexe. Il faudra approfondir la description des enregistrements et la structure des fichiers. Par convention, on considère que chaque domaine dispose d'au moins 1 serveur de noms primaire et un serveur de noms secondaire afin d'assurer une redondance en cas de panne d'un serveur. Les clients réseau seront configurés pour utiliser indifféremment le serveur de noms primaire ou les serveurs de nom secondaires. Il en résulte une duplication de la base de données du DNS primaire sur les serveurs secondaires. La base de données est rafraîchie en fonction des paramètres de l'enregistrement SOA. Ce procédé met en oeuvre un principe de base de données répartie. Vous trouverez quelques éléments dans les annexes qui suivent. Annexes : extraits de fichiers de configuration[root@fedorasrv etc]# cat /etc/named.conf//// named.conf//// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS// server as a caching only nameserver (as a localhost DNS resolver only).//// See /usr/share/doc/bind\*/sample/ for example named configuration files.//options { listen-on port 53 { 127.0.0.1; 192.168.1.226; }; listen-on-v6 port 53 { ::1; }; directory "/var/named"; dump-file "/var/named/data/cache\_dump.db"; statistics-file "/var/named/data/named\_stats.txt"; memstatistics-file "/var/named/data/named\_mem\_stats.txt"; secroots-file "/var/named/data/named.secroots"; recursing-file "/var/named/data/named.recursing"; allow-query {localhost; any; 192.168.1/24; }; allow-query-cache { localhost; any; }; /\* - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion. - If you are building a RECURSIVE (caching) DNS server, you need to enable recursion. - If your recursive DNS server has a public IP address, you MUST enable access control to limit queries to your legitimate users. Failing to do so will cause your server to become part of large scale DNS amplification attacks. Implementing BCP38 within your network would greatly reduce such attack surface \*/ recursion no; managed-keys-directory "/var/named/dynamic"; geoip-directory "/usr/share/GeoIP"; pid-file "/run/named/named.pid"; session-keyfile "/run/named/session.key"; /\* https://fedoraproject.org/wiki/Changes/CryptoPolicy \*/ include "/etc/crypto-policies/back-ends/bind.config"; check-names master ignore; check-names slave ignore; check-names response ignore;};logging { channel default\_debug { file "data/named.run"; severity dynamic; };};zone "." IN { type hint; file "named.ca";};#zone directe et inversezone "ofppt.org" IN { type master; file "ofppt.zone"; allow-update { none; };};zone "1.168.192.in-addr.arpa" IN { type master; file "ofppt.rev"; allow-update { none; };};include "/etc/named.rfc1912.zones";include "/etc/named.root.key";key rndc-key { algorithm hmac-md5; secret "grYXJrtUhXnDK1GeS4eLh08e7oWOdLSR5EVAGoiAm+k="; };controls { inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { rndc-key; }; }; // named.rfc1912.zones://// Provided by Red Hat caching-nameserver package//// ISC BIND named zone configuration for zones recommended by// RFC 1912 section 4.1 : localhost TLDs and address zones// and https://tools.ietf.org/html/rfc6303// (c)2007 R W Franks//// See /usr/share/doc/bind\*/sample/ for example named configuration files.//// Note: empty-zones-enable yes; option is default.// If private ranges should be forwarded, add// disable-empty-zone "."; into options//zone "localhost.localdomain" IN { type master; file "named.localhost"; allow-update { none; };};zone "localhost" IN { type master; file "named.localhost"; allow-update { none; };};zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN { type master; file "named.loopback"; allow-update { none; };};zone "1.0.0.127.in-addr.arpa" IN { type master; file "named.loopback"; allow-update { none; };};zone "0.in-addr.arpa" IN { type master; file "named.empty"; allow-update { none; };};zone "ofppt.org" IN { type master; file "ofppt.zone"; allow-update { none; };};zone "1.168.192.in-addr.arpa" IN { type master; file "ofppt.rev"; allow-update { none; };}; [root@fedorasrv etc]# cat /etc/rndc.conf# Start of rndc.confkey "rndc-key" { algorithm hmac-sha256; secret "grYXJrtUhXnDK1GeS4eLh08e7oWOdLSR5EVAGoiAm+k=";};options { default-key "rndc-key"; default-server 127.0.0.1; default-port 953;};# End of rndc.conf# Use with the following in named.conf, adjusting the allow list as needed:# key "rndc-key" {# algorithm hmac-sha256;# secret "grYXJrtUhXnDK1GeS4eLh08e7oWOdLSR5EVAGoiAm+k=";# };## controls {# inet 127.0.0.1 port 953# allow { 127.0.0.1; } keys { "rndc-key"; };# };# End of named.conf [root@fedorasrv etc]# cat /etc/rndc.keykey "rndc-key" { algorithm hmac-sha256; secret "ZbKNhAfMH/gZZ8jO5EjeojOxkDyPvIv0GwjJNJXnkBM=";};[root@fedorasrv etc]# cat /etc/named.root.keytrust-anchors { # ROOT KEYS: See https://data.iana.org/root-anchors/root-anchors.xml # for current trust anchor information. # # This key (20326) was published in the root zone in 2017. # Servers which were already using the old key (19036) should # roll seamlessly to this new one via RFC 5011 rollover. Servers # being set up for the first time can use the contents of this # file as initializing keys; thereafter, the keys in the # managed key database will be trusted and maintained # automatically. . initial-ds 20326 8 2 "E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D";}; |