



Serveur DNS

DNS Domain Name System. C'est un système hiérarchique distribué permettant la résolution des noms de machines en adresses IP et inversement, utilise le **port 53**.

Il existe deux types de

- Requêtes : **requêtes récursives** et **requêtes itératives**.
- Serveur DNS **Principal (Master)** et DNS **secondaire (Slave)**.
- Zone : Zones de **recherche directe**, et zones de **recherche inversée**

Installation	#yum install -y bind bind-utils
Vérification d'installation	# rpm -qa bind
Démarrage du service	#systemctl start named.service
Activation au démarrage du service	#systemctl enable named.service
Nom et chemin du fichier de configuration	/etc/named.conf
Configuration globale	listen-on port 53 { localhost; }; // Autoriser les requêtes récursives que depuis lui-même ou any (tous le monde) ou Adresse IP forwarders { 212.27.40.240; 212.27.40.241; }; //Envoyer les requête vers d'autre serveurs DNS allow-query // Définit une liste d'adresses IP autorisées à effectuer des requêtes des DNS classiques, c'est-à-dire itératives allow-query-cache // Définit les adresses IP autorisées à accéder au cache local des requêtes récursives du serveur. allow-recursion // Définit une liste d'adresses IP autorisées à effectuer des requêtes récursives sur le serveur.
Configuration d'un serveur DNS primaire (maître)	Zone directe : zone "votredomaine.com" IN { type master; file "votredomaine.com.zone"; allow-update { none; }; //ne pas autoriser la mise à jour }; Zone inverse IPV4 : zone "Adresse réseau inverse.in-addr.arpa" IN { type master; file "votredomaine.com.inverse"; allow-update { none; }; }; Zone inverse IPV6 : (mettre un point entre chaque élément d'adresse IP) zone "Adresse réseau inverse.ip6.arpa" IN { type master; file "votredomaine.com.inverse";

	<pre>allow-update { none; }; };</pre> <p>Autres options :</p> <pre>allow-transfer { adresse ip ; }; //Autoriser le transfert notify yes/no; //Activer ou non la notification allow-notify { adresse ip ; }; //Autoriser les serveur à notifier en cas de modification</pre>
Configuration de la zone DNS directe	<pre>\$TTL 86400 @ IN SOA ns.votredomaine.com. dnsmaster.votredomaine.com. (2019 //Numéro de série 2H // La période de rafraîchissement des données 1D // La période de nouvelle essaie 1W // La période d'expiration 38400) // la durée de validité des données communiquée par le serveur pour toute requête . @ IN NS ns.votredomaine.com. @ IN NS ns2.votredomaine.com. @ IN MX 10 mail.votredomaine.com. @ IN MX 20 mail2.votredomaine.com. _lldap_tcp.ntic.ma 86400 IN SRV 20 100 389 AD.ntic.ma. ns IN A votreip ns2 IN A votreip mail IN A votreip mail2 IN A votreip www IN A votreip www IN AAAA votreipV6 ftp IN CNAME www.votredomaine.com.</pre>
Configuration de la zone DNS inversé	<pre>\$TTL 86400 @ IN SOA ns.votredomaine.com. dnsmaster.votredomaine.com. (2019 //Numéro de série 2H // La période de rafraîchissement des données 1D // La période de nouvelle essaie 1W // La période d'expiration 38400) // la durée de validité des données communiquée par le serveur pour toute requête . @ IN NS ns.votredomaine.com. Votreip (partie hote) IN PTR ns Votreip (partie hote) IN PTR mail Votreip (partie hote) IN PTR ns2</pre>
Modification des droits des fichiers de configuration de zone	<pre>#chown root.named votredomaine.com.zone #chown root.named votredomaine.com.inverse</pre>
Vérification de la configuration	<ul style="list-style-type: none"> ▪ Fichier de configuration : #named-checkconf ▪ Fichiers zone : <pre>#named-checkzone -d nomdomaine.com /var/named/nomdomaine.zone #named-checkzone -d adresse inverse reseau.in-addr.arpa /var/named/nomdomaine.inverse</pre>
Redémarrage du service	<pre>#systemctl restart named.service</pre>
Test Client	<ol style="list-style-type: none"> 1. Modifier resolv.conf en ajoutant l'adresse du serveur DNS 2. #nslookup Nom de domaine du hôte ou adresse IP Il est possible de modifier le mode d'interrogation de la commande nslookup grâce à l'option type : type=mx ,type=ns, type=aaaa, type=soa et type=cname 3. #dig nom du domaine

Configuration serveur secondaire	<ol style="list-style-type: none"> 1. Configuration global : Modifier la ligne allow-query { Adresse serveur secondaire; }; 2. Configuration de la zone primaire : zone "ntic.ma" { type master; file "ntic.ma.direct"; allow-transfer{AdresseIPserveurSlave;}; notify yes; }; 3. Configuration de la zone secondaire : zone "ntic.ma" { type slave; file "ntic.ma.directe" masters {AdresseIPprimaire;}; allow-notify { AdresseIPprimaire; }; };
Configuration DDNS	<ol style="list-style-type: none"> 1. Au niveau du serveur DNS : Dans named.conf indiquer l'adresse IP du serveur DHCP dans l'option allow-update 2. Au niveau du serveur DHCP : ajouter les lignes suivantes dans dhcpd.conf ddns-updates on; //Autoriser les mises à jour des zones DNS ddns-update-style interim; //Précise qu'il s'agit d'une mise à jour vers un serveur DNS local. deny client-updates; // Empêcher les clients de s'enregistrer eux-mêmes auprès du serveur DNS. ddns-domainname "Nom de la zone directe"; ddns-rev-domainname "nom de la zone inverse"; authoritative; //Serveur DHCP prioritaire sur le réseau local. zone Nom de zone directe. { primary 192.168.2.1; } zone Nom de zone inverse. { primary 192.168.2.1; }
Délégation DNS	<ol style="list-style-type: none"> 1- Dans le fichier de zone ajouter les informations du serveur DNS qui sera délégué tri.ntic.local. IN NS SRV2.tri.ntic.local. SRV2.tri.ntic.local. IN A Adresse IP SRV2 2- Au niveau du fichier named.conf modifier les lignes suivante : dnssec-enable no ; dnssec-validation no ;