

# BIND et DNS - Agenda

- À propos de moi
- À propos de BIND et des serveurs DNS
- Régistres
- Outils (pas de graphique ou de menu, SVP !)
- Fichiers de zones et types d'enregistrements
  - Fichier(s) de configuration

# BIND et DNS – Agenda (suite)

- À propos de DNS dynamique et DHCP
- Secret partagé pour mise à jour
- Domaines gratuits et hébergement
- Implantation d'un DNS de cache
  - Bons et mauvais côtés
  - Suggestions

# À propos de BIND et DNS

- BIND signifie *Berkeley Internet Name Domain*
- Ce service est aussi connu sous le nom de DNS et constitue les pages jaunes de l'internet, mais sur un modèle distribué et redondant.
- BIND est [une des] implantation majeure du service DNS sur le net.
- BIND fonctionne avec Ipv4 et IPv6. Cette présentation couvre seulement IPv4.
- BIND utilise des fichiers textes simples pour l'information statique. On appelle ça des ZONES.

# Registres

- Un régistres est une autorité qui peut enregistrer un domaine en votre nom.
- Il peut enregistrer sous de multiples noms de domaines principaux, tels .com, .net, etc... selon les autorités qui lui sont déléguées.
- Il ne peut que vous enregistrer comme détenteur. Ce que vous en faites ne le regarde pas.
- Un régistres fournira l'information WHOIS de votre domaine.
- Les serveurs DNS d'autorité pour un domaine résident chez le régistres.

# Registraires (suite)

- Différents domaines ont différentes conditions.
  - Pour enregistrer un domaine .ca, vous devez être citoyen canadien. Les domaines .ca sont gérés par la **Canadian Internet Registration Authority (CIRA)**. [www.cira.ca](http://www.cira.ca).
  - Pour enregistrer un domaine .mobi, vous devez fournir un contenu web adapté aux dispositifs mobiles (cellulaires, agenda, etc)
- Les domaines .TV appartiennent au Tuvalu.
- Les enregistrements de domaines sont renouvelables annuellement.

# BIND et DNS – Les outils

- En soi, BIND n'est qu'un service. Pour l'utiliser, on a besoin d'outils:
  - NSLOOKUP et DIG
    - Démo
  - WHOIS
    - Démo
  - PING ( NON !!! )
- Ces outils fonctionnent avec les adresses IP et les noms de domaines.

# BIND – Fichiers de ZONE

- Une zone peut couvrir un ensemble d'adresses IP, classe A, B ou C
- Une zone peut aussi être un [sous-]domaine (tel `home.messier.ca`)
- Les noms (sans point) peut avoir jusqu'à 32 caractères de long
  - `www.cenomdeserveurestvraimentlong.cenomdedomainestextremementlong.com`
- À propos de l'autorité et de la délégation

# BIND – Types d'info

- Il existe plusieurs types d'enregistrements et instructions, encore plus avec IPv6.
- SOA définit le domaine, ou les IP pour lequel le serveur a autorité.
- `messier.ca. SOA ns5.secureserver.net(`
  - `2008030401 ; Serial (yyyymmddxx)`
  - `10800 ; Raffraichir apres 3 hours`
  - `900 ; Resserer apres 15 minutes`
  - `900 ; Expire apres 15 minutes`
  - `900 ) ; duree maximale (TTL): 15 minutes`

# BIND – Types d'info (suite)

- Un enregistrement NS indique qui peut servir des requêtes pour la zone, de façon officielle.

- IN       NS       ns5.secureserver.net.

- IN       NS       ns6.secureserver.net.

- Un enregistrement MX indique un plusieurs serveurs où les courriels sont livrés avec un "poid" associé à chacun.

- IN       MX       0   smtp.secureserver.net.

- IN       MX       10 mailstore1.secureserver.net.

- home   IN       MX       0   home.messier.ca.

# BIND – Types d'info (suite)

- Un enregistrement A(adresse) indique une adresse IP pour un nom de serveur.

pop                    IN     A     207.164.234.129

serveur.home        IN     A     76.71.141.59

serveur.home.messier.ca.    IN A   76.71.141.59 ; equivalent

- Le serveur pop.messier.ca affichera l'adresse IP 207.164.234.129
- Le serveur serveur.home.messier.ca affichera l'adresse IP 76.71.141.59

# BIND – Types d'info (suite)

- Les noms canoniques (CNAME) permettent à un serveur d'avoir plusieurs noms. Aussi, il suffit d'un changement, et tous les noms sont mis à jour.

www        IN A            192.168.25.60

web        IN CNAME        www ; retournera aussi 192.168.25.60

serveur   IN A            192.168.25.50

ftp        IN CNAME        serveur ; retournera aussi 192.168.25.50

- Aussi :

www.clo.messier.ca. IN CNAME www.linux-gatineau.org ; Voir le point

# BIND – Types d'info (La fin)

- Les enregistrements PTR permettent une recherche inverse. Ils indiquent le nom de base (s'il en est un) pour une adresse IP.
- Les enregistrements PTR ont un point à la fin du nom complet du serveur.

```
50 IN PTR serveur.messier.ca.
```

# BIND – À propos du TTL

- TTL signifie *Time To Live*.
- Un TTL peut s'appliquer à une zone, ou un enregistrement en particulier. Il indique en secondes la durée de validité d'un enregistrement.
- Une fois échue, l'information devrait être effacé de la cache et demandé à nouveau depuis un serveur.

# BIND – Plus d'info sur TTL

- Le TTL pour une zone apparaît au début du fichier ou pour des items individuels

; données officielles pour messier.ca

;

\$TTL 86400 ; default de 24 heures.

imprimante        IN        A        192.168.25.60

serveur 300        IN        A        192.168.25.50

; valide pour 5 minutes

# BIND – Configuration principale

- Une configuration de BIND comporte de nombreuses options. Les plus importantes sont les répertoires des fichiers de zone, et les ports utilisés pour la gestion et l'utilisation du serveur.

```
options {  
    directory "/var/named";  
    query-source address * port 53;  
};
```

# BIND – Configuration principale

- La section "logging" indique la quantité d'information à accumuler par catégorie:

```
logging {  
    category lame-servers { null; };  
    category client { null; };  
    category queries { null; };  
};
```

- Il y en a encore bien plus...

# BIND – Configuration principale

- Le plus intéressant est pour les zones.
- On peut avoir autant de zones qu'on veut.
- les zones ".", "localhost" et "0.0.127-in-addr.arpa" doivent exister en tout temps.
- Chaque zone soit est maître ou esclave.
- De multiples items aussi !
- On ne peut pas y mettre de commentaires.

# BIND – Configuration (la fin)

```
zone "." IN {  
type hint;  
file "named.ca";  
};
```

```
zone "localhost" IN {  
type master;  
file "localhost.zone";  
allow-update { none; };  
};
```

```
zone "0.0.127-in-addr.arpa" IN {  
type master;  
file "named.local";  
allow-update { none; };  
};
```

```
zone "messier.ca" {  
type master;  
file "master/messier.ca";  
allow-query { any; };  
allow-update { none; };  
allow-transfer {192.168.25.10;};  
notify yes;  
};
```

# BIND – Autres fichiers

- named.ca est un fichier qui désigne les serveurs racine.
  - Ceux-ci sont nommés "a.root-servers.net" jusqu'à "m.root-servers.net".
- Les fichiers de zones d'adresses IP sont nommés dans la direction inverse de la section réseau de la zone.
- Exemple: 25.168.192.in-addr.arpa désigne le segment 192.168.25.0 / 24

# BIND – Échange et mise à jour

- De façon régulière ou si requis, un serveur d'autorité mettra des serveurs esclaves à jour.
- Ceci peut être protégé par un secret partagé.
- Un serveur esclave peut aussi demander une mise à jour du serveur maître.
- Ces processus sont aussi basés sur le TTL des zones.

# DNS dynamique et DHCP

- Quand un ordinateur demande une adresse automatique, par DHCP, il diffuse une requête à l'adresse 255.255.255.255.
- Le serveur DHCP alloue une adresse IP et la retourne avec d'autres informations, telles les serveurs DNS.
- Finalement, certains serveurs DHCP ajouteront le nouveau membre dans le DNS dynamique avec le nom pour recherche normale et inversée.

# Domaines gratuits/hébergement

- Plusieurs détenteurs de domaines permettent à des usagers d'utiliser un sous-domaine. Des services tels DynDNS.ORG vous donnent plein contrôle sur votre sous-domaine.
- La plupart ont aussi un logiciel client qui fait la mise à jour automatique lorsqu'une adresse IP change. Utile pour les usagers de connexion haute-vitesse.

# Un serveur DNS cache

- Il effectue les demandes DNS et conserve les résultats en cache, basé sur le TTL. La prochaine demande sera servie immédiatement.
- La plupart des distributions Linux ont un ensemble disponible, prêt à installer.
- Il suffit de pointer les autres ordinateurs à ce serveur, et il effectuera toutes les requêtes.

# Un serveur DNS cache (La suite)

## Le bon

- On peut le mettre dans la configuration DHCP.
- Il consultera le net une seule fois, pas pour chaque ordinateur.

## Le moins bon

- Un point faible.
- Retournera toujours la même adresse pour la durée du TTL.

# Serveur DNS cache – suggestion

- Avoir deux serveurs, pas un seul.
- Configurer chaque serveur cache pour envoyer les requêtes à des serveurs différents.
- Ce peut être aussi être des serveurs publics, autres que ceux de votre fournisseur.
- Publier les adresses des deux serveurs cache dans votre configuration DHCP.

# Références

- <http://www.messier.ca/wordpress>
- <http://www.bind9.net/>
- <http://www.oreilly.com/catalog/dns5/index.html>
- <http://www.zytrax.com/books/dns/>
- <http://www.cira.ca>

**BIND**

**Questions ???**