



ICT-123-Activer les services d'un serveur

DNS

Février 2021 – JBL / LG Version 1.0



1. Présentation du DNS

- Aujourd'hui l'ensemble des communications informatiques se font avec le protocole TCP/IP et les adresses IP
- Pour communiquer avec une machine, il n'est pas pratique de devoir utiliser son adresse IP
- Afin de pouvoir utiliser des noms de machines, un mécanisme a été mis en place permettant de résoudre (transformer) le nom d'une machine en son adresse IP
- Ce mécanisme est le DNS (domaine name system)
- Les machines s'occupant de résoudre ces noms sont des serveurs DNS



2. Noms DNS

- Un nom DNS entièrement qualifié est appelé FQDN (full qualified domain name)
- Sa syntaxe est:

srvdc00.ict00.lan.

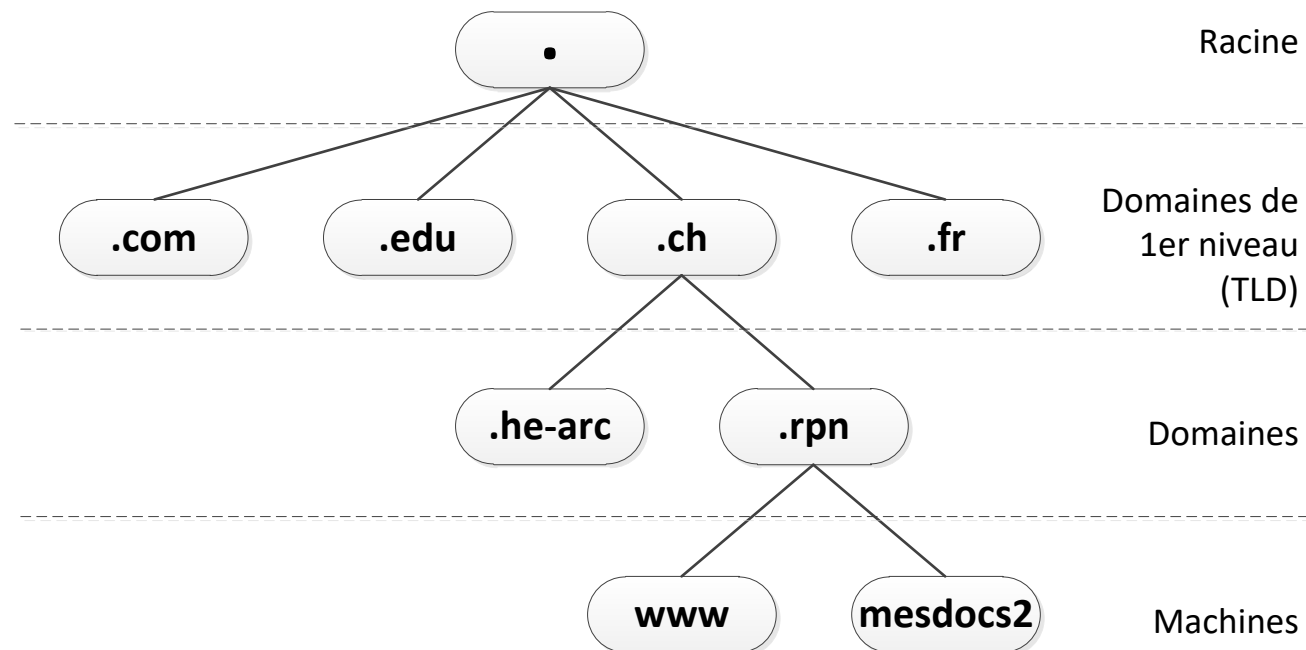
Nom de la machine Domaine Domaine de premier niveau

- Le domaine de premier niveau est appelé TLD (top level domain)
- Le «[.](#)» à la fin indique la racine



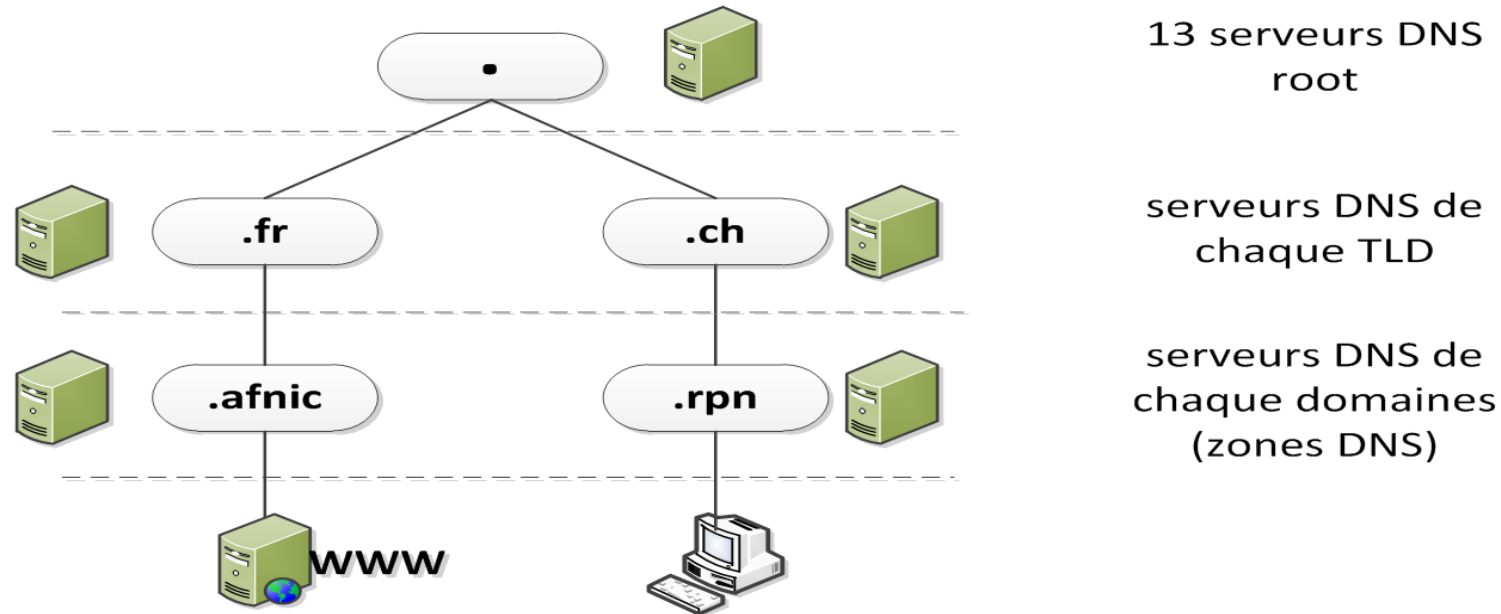
3. Résolution DNS

- Vu le nombre de domaine et noms existants sur internet, le système est arborescent.





3. Résolution DNS

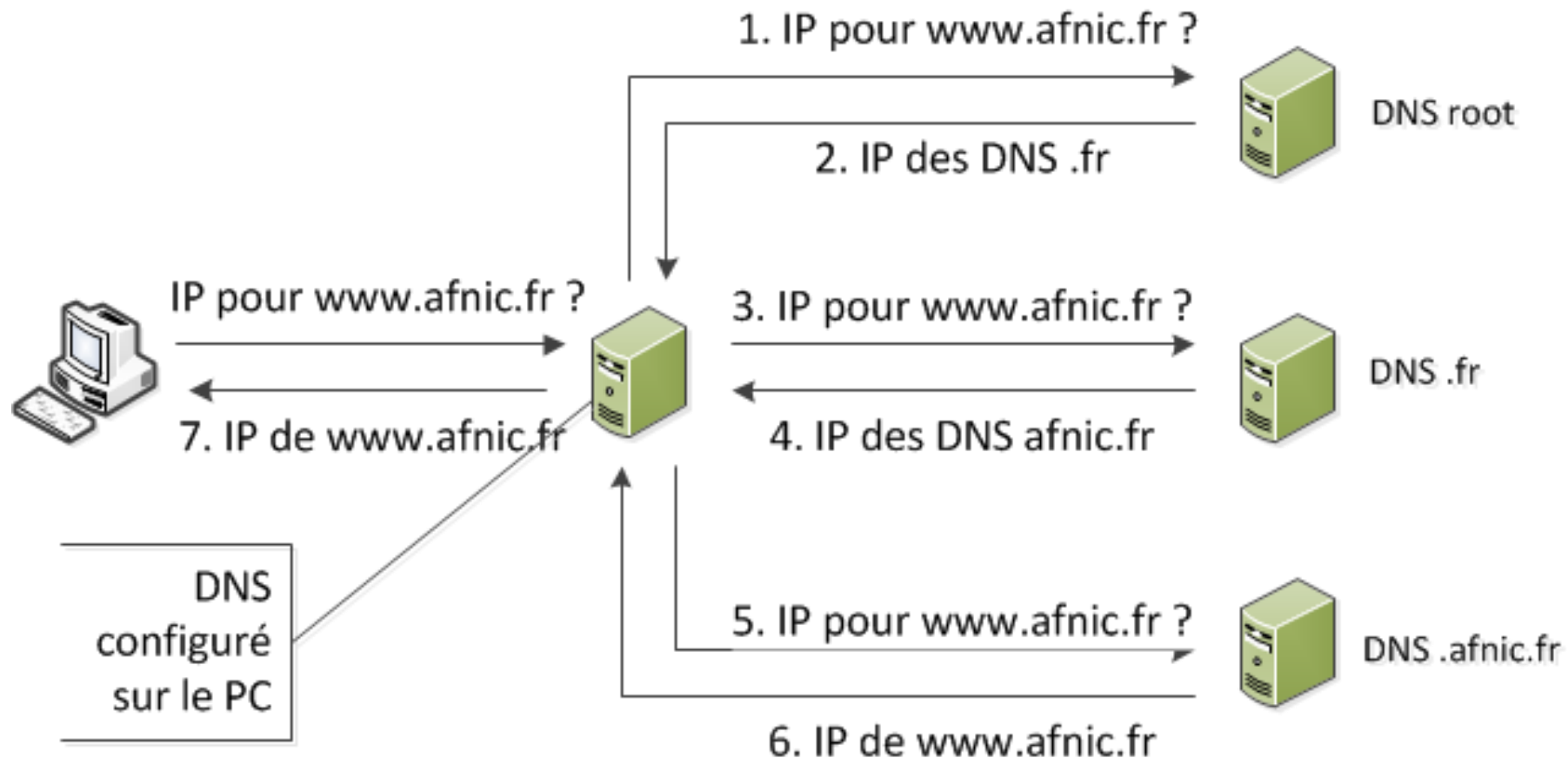


- Les serveurs root répertorient les serveurs DNS de chaque TLD
- Les serveurs DNS de chaque TLD répertorient les serveurs DNS des domaines inscrits sous leur TLD
- Les serveurs DNS des domaines répertorient l'ensemble des machines du domaine



3. Résolution DNS

- Résolution de `www.afnic.fr` depuis un ordinateur





3. Résolution DNS

- Les résolutions DNS effectuées sont stockées en cache à 2 endroits:
 - Dans le cache du serveur DNS
 - Dans le cache de l'ordinateur client
- Par conséquent, l'ordre de recherche lors d'une résolution est le suivant:
 1. cache du client
 2. zones hébergées sur le serveur DNS local
 3. Cache du serveur DNS local
 4. Résolution par l'arborescence DNS



4. Serveur DNS

- Le serveur DNS est la machine sur laquelle tourne le service DNS
- Il héberge une ou plusieurs zones DNS
- Une zone DNS contient l'ensemble relations «noms de machines» ↔ «adresses IP» d'un domaine.
- Une zone de recherche directe permet de trouver l'IP en fonction du nom de la machine
- Une zone de recherche inverse permet de trouver un nom de machine en fonction de l'adresse IP
- Il y aura un ou plusieurs serveurs DNS par domaine



5. Types de zones DNS

- Les choix de zones sur un serveur Windows

Assistant Nouvelle zone

Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.

Sélectionnez le type de zone que vous voulez créer :

☒ Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

☐ Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.

☐ Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.

☐ Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)

< Précédent Suivant > Annuler



5. Types de zones DNS

- Zone principale
 - On créer une zone principale lorsque que c'est le premier serveur qui héberge cette zone
- Zone secondaire
 - On créer une zone secondaire quand on héberge une copie d'une zone déjà présente sur un autre serveur.
Ceci permet d'avoir de la redondance en cas de panne d'un serveur
- Zone stub
 - Permet de stocker uniquement les infos des serveurs de noms s'occupant de cette zone



5. Types de zones DNS

- Par défaut une zone DNS est un fichier texte *nom_zone.dns*. Il se trouve dans le dossier *%windir%\System32\Dns* sur le serveur
- L'option «enregistrer la zone dans active directory» est présente uniquement si le serveur est un contrôleur de domaine
- Cette option permet d'intégrer la zone dans la base AD
- Elle est **répliquée automatiquement** sur tous les contrôleurs du domaine. Il suffit d'ajouter le rôle DNS pour avoir de la redondance



6. Enregistrements des ressources

- Dans un environnement Microsoft, les mappages nom d'hôte / adresse IP et adresse IP / nom d'hôte sont appelés **enregistrements de ressources**.
- Voici la liste des principaux types d'enregistrements de ressources
 - **A** : Les enregistrements de ressources A (pour Adresse d'hôte) sont des mappages entre un nom d'hôte et une adresse IPv4 (adresse IP d'une longueur de 32 bits). Ils représentent généralement la majorité des enregistrements de ressources des zones de recherches directes.
 - **CNAME** : les enregistrements de ressources de type CNAME (Canonical NAME ou nom canonique) sont des mappages entre un nom d'hôte et un autre nom d'hôte. Ils permettent de créer des alias pour un nom d'hôte donné (c'est-à-dire d'associer plusieurs noms d'hôte à une même machine).



6. Enregistrements des ressources

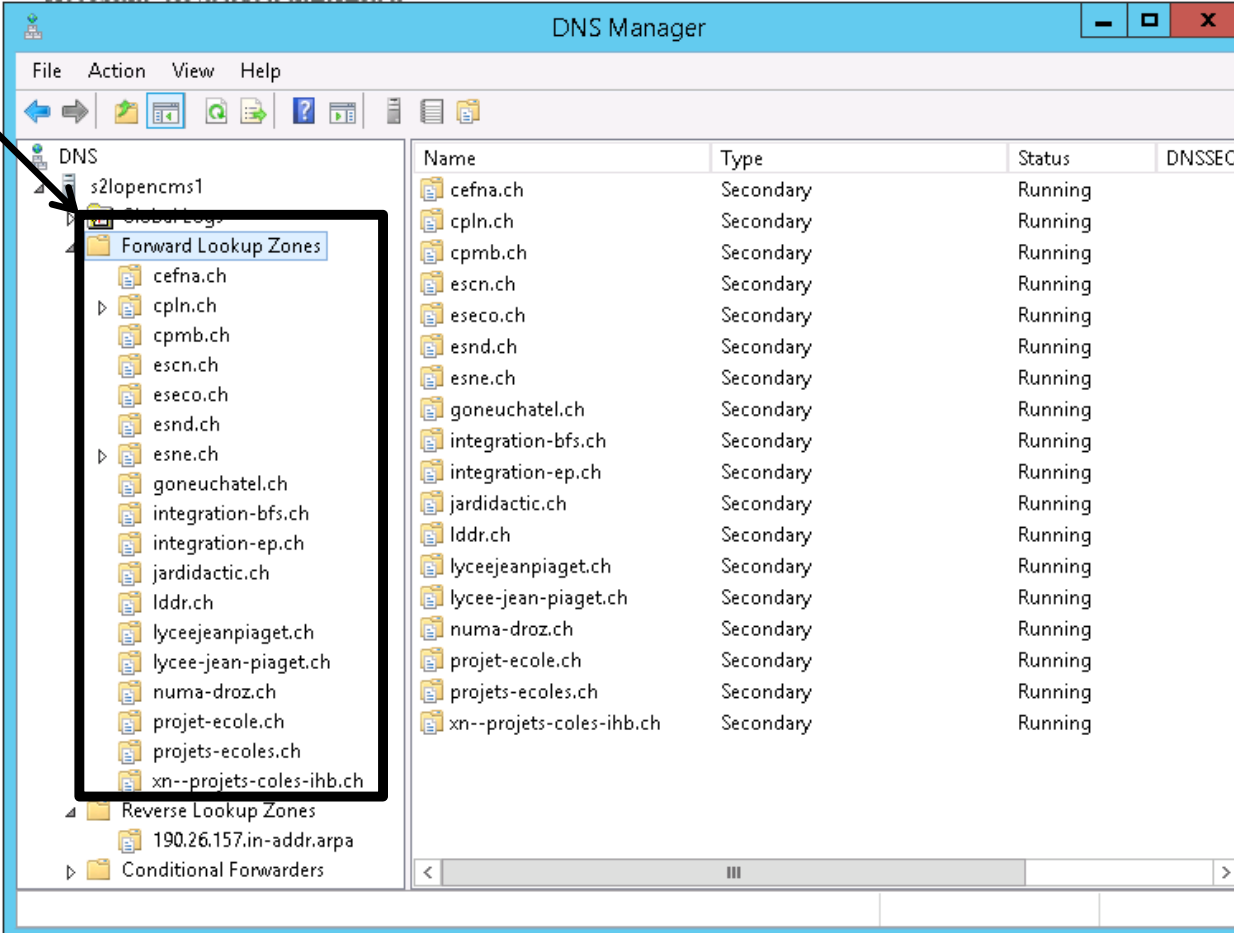
- **MX** : les enregistrements de ressources de type MX (Mail eXchanger) identifient les serveurs de messageries. Chaque serveur de messagerie doit aussi disposer d'un enregistrement de ressource A. Il est possible de donner une priorité différente à chaque enregistrement MX.
- **NS** : les enregistrements de ressources de type NS (Name Server ou serveur de nom) identifient les serveurs DNS de la zone DNS. Ils sont utilisés dans le cadre de la délégation DNS.
- **PTR** : les enregistrements de ressources de type PTR (PoinTeR ou pointeur) sont des mappages entre une adresse IP et un nom d'hôte. Ils représentent la majorité des enregistrements des zones de recherches inversées.
- **SOA** : les enregistrements de ressources de type SOA (Start Of Authority) contiennent le nom d'hôte et l'adresse IP du serveur DNS qui héberge actuellement la zone DNS principale. Il y a un seul enregistrement SOA par zone DNS. C'est le premier enregistrement créé dans une zone DNS.
- **SRV** : les enregistrements de type SRV (service) permettent de mapper un nom d'hôte à un type de service donné. Ainsi les enregistrements SRV peuvent permettre de retrouver la liste des serveurs HTTP ou bien encore des contrôleurs de domaines. Il est possible de donner une priorité différente à chaque enregistrement SRV.



7. Serveur DNS Windows

- Exemple d'un serveur DNS hébergeant plusieurs zones

Zones

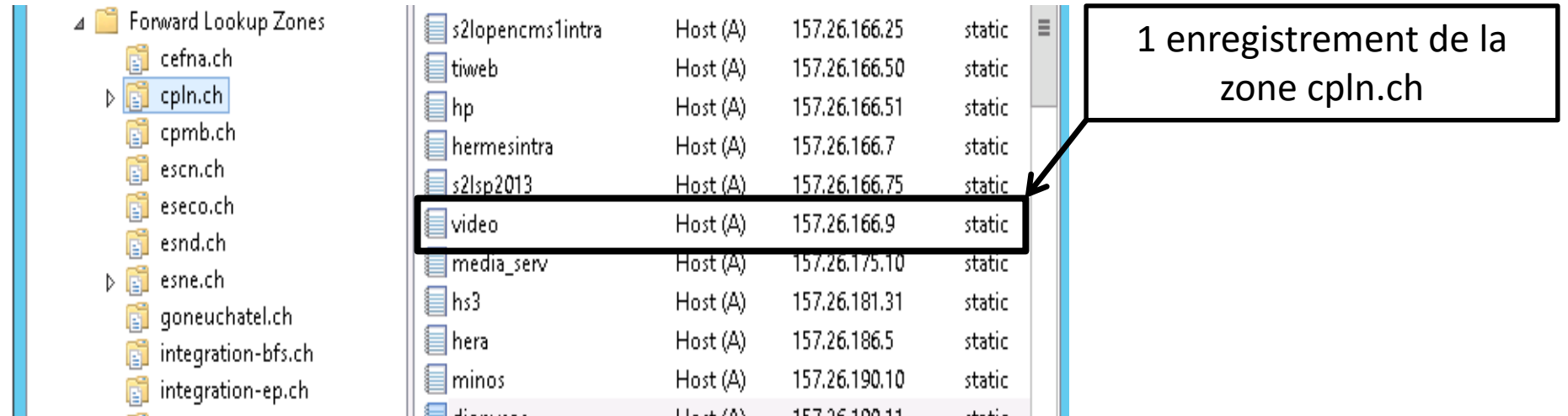


The screenshot displays the DNS Manager interface. The left pane shows the hierarchy: DNS > s2lopecms1 > Forward Lookup Zones. The right pane lists the zones with their names, types, and statuses.

Name	Type	Status	DNSSEC
cefna.ch	Secondary	Running	
cpln.ch	Secondary	Running	
cpmb.ch	Secondary	Running	
escn.ch	Secondary	Running	
eseco.ch	Secondary	Running	
esnd.ch	Secondary	Running	
esne.ch	Secondary	Running	
goneuchatel.ch	Secondary	Running	
integration-bfs.ch	Secondary	Running	
integration-ep.ch	Secondary	Running	
jardidactic.ch	Secondary	Running	
lddr.ch	Secondary	Running	
lyceejeanpiaget.ch	Secondary	Running	
lycee-jean-piaget.ch	Secondary	Running	
numa-droz.ch	Secondary	Running	
projet-ecole.ch	Secondary	Running	
projets-ecoles.ch	Secondary	Running	
xn--projets-coles-ihb.ch	Secondary	Running	



7. Serveur DNS Windows



Forward Lookup Zones

- cefna.ch
- cpln.ch
- cpmb.ch
- escn.ch
- eseco.ch
- esnd.ch
- esne.ch
- goneuchatel.ch
- integration-bfs.ch
- integration-ep.ch

s2lopecms1intra	Host (A)	157.26.166.25	static
tiweb	Host (A)	157.26.166.50	static
hp	Host (A)	157.26.166.51	static
hermesintra	Host (A)	157.26.166.7	static
s2lsp2013	Host (A)	157.26.166.75	static
video	Host (A)	157.26.166.9	static
media_serv	Host (A)	157.26.175.10	static
hs3	Host (A)	157.26.181.31	static
hera	Host (A)	157.26.186.5	static
minos	Host (A)	157.26.190.10	static
...

1 enregistrement de la zone cpln.ch