DNS

Le serveur DNS (Domain Name Service) sert à translater les Hostname ou services en IP. Avant, cela se faisait avec le fichier Host mais comme tout le monde devait avoir le fichier, cela devenait trop gros. De plus, il était local et statique.

Domain Name Space

Le Domain Name Space est la structure de définition des noms d'hôtes que l'on peut utiliser en résolution de noms.

Il est structuré de manière hiérarchisée.



Il démarre à « • » viennent ensuite les **FIRST LEVEL DOMAIN** (COM, EDU, BE, FR,...), viennent ensuite les **SECOND LEVEL DOMAIN** (skynet.be, google.com,...) et les **SUB DOMAIN** suivent (mail.skynet.be, <u>www.skynet.be</u>,...).

A partir du second level domain, on peut définir des Hosts. Les hosts sont définis par leur **FQDN** (Fully Qualified Domain Name) : 256 caractères max. et 64 max. par niveau. Le Hostname le plus répandu sur Internet est « www ». Exemple : « toto.brol.bazar.be. » . : Root be : First level domain bazar : Second level domain brol : Sub level domain toto : Hostname

toto : Hostname

Mécanisme de résolution de nom en partant du client

- Chaque workstation connaît une liste de serveurs DNS qu'elle peut interroger. Lorsqu'elle cherche à résoudre un nom en IP, elle contacte les serveurs DNS dans l'ordre de préférence. Si le 1^{er} ne répond pas, elle essaye le 2^{ème},...
- 2) Elle envoie au DNS qu'elle connaît le FQDN de l'hôte qu'elle cherche.
- Lorsqu'il reçoit une demande de résolution de la workstation, le serveur DNS commence par vérifier si le Host recherché appartient à un domaine appartenant à une zone qu'il gère :
 - a. Le domaine appartient à une zone qu'il gère : il parcourt le fichier de zone et cherche l'enregistrement de l'host recherché. S'il le trouve, il communique l'adresse IP au client, s'il ne le trouve pas, il peut indiquer au client que la machine recherchée n'existe pas
 - b. Le domaine n'appartient pas à une zone qu'il gère : il va procéder à une succession de requêtes vers d'autres DNS pour résoudre le nom (voir schéma).



Name Server (ou serveur DNS)

C'est une machine responsable de la gestion de un ou plusieurs fichiers de zone. → Qui peut traduire <u>www.microsoft.com</u> ? tous les DNS qui gèrent la zone microsoft.com → tous les DNS qui contiennent le domaine dans lequel se trouve le host www.

Installation

Pour installer le serveur DNS en interface graphique sous 2008, il faut aller dans les rôles.



Pour l'installer en ligne de commande, on tapera :

- Dism /online /enable-feature /featurename:DNS-Server-Full-Role (en mode GUI)
- Dism /online /enable-feature /featurename:DNS-Server-Core-Role (en mode Core)

Zones

Sous-ensemble du Domain Name Space constitué de domaine contigu (avec lien entre eux). C'est un ou plusieurs domaines.

Pour chaque zone, il y a un fichier de zone qui contient les traductions Nom ou service \rightarrow IP pour les Hosts appartenant à un des domaines faisant partie de la zone \rightarrow au lieu d'avoir un seul gros fichier Host, on a des milliers de plus petits fichiers de zone. Il y a deux zones possibles dans le DNS :

- Forward Lookup Zones : pour résoudre le nom ou le service en IP
- Reverse Lookup Zones : pour résoudre l'IP en nom ou service.

Pour créer une **Forward Lookup Zones**, il faut faire un clic droit sur Forward Lookup Zones, New Zone



Il existe 3 types de zones :

• Primary Zone : cette zone sera accessible en lecture et en écriture sur ce serveur

New Zone Wizard
Zone Type The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone Creates a copy of a zone that can be updated directly on this server.
Secondary zone Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
New Zone Wizard
Zone Name What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name: startrektng.be

Si la zone n'est pas intégrée à l'AD, il vous demande en plus le nom du fichier de zone. Ce fichier est stocké dans %systemroot%\system32\dns

New Zone W	izard	
Zone File You c	e an create a new zone file or use a file copied from another D	DNS server.
Do yo from a	u want to create a new zone file or use an existing file that another DNS server? reate a new file with this file name:	you have copied
s O Us	tartrektng.be.dns	
Г		

L'écran suivant demande quel type de mise à jour est possible pour le DNS :

New Zone Wizard	×
Dynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.	
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.	
Select the type of dynamic updates you want to allow:	
C Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones.	
 Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be accepted from untrusted sources. 	
O Do not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must update these records manually.	

- **Secure Only** (uniquement disponible si la zone est dans l'AD) : quand un enregistrement a été créé dans le DNS, une sécurité est mise en place pour que cet enregistrement ne soit pas modifiable par n'importe qui (il n'y a que le créateur de l'enregistrement et certains groupes qui pourront le modifier)
- Non-secure and secure : moins de sécurité mais seule solution si la zone n'est pas dans l'AD. Cela permet au client Windows Legacy (Windows 98&Cie) et non Windows (Mac, Linux) de s'enregistrer dans le DNS (ce qui n'est pas nécessaire si c'est le DHCP qui fait les enregistrements).
- **Not allow** : il faut faire les enregistrements à la main. Ca n'est utilisé que pour des zones statiques (une zone pour le serveur Web par exemple).

• Secondary Zone : cette zone sera accessible en lecture seule sur ce serveur et sera copiée depuis un autre serveur.

New Zone Wizard			×
Zone Name What is the name of t	he new zone?		and the second
The zone name specifi authoritative. It might or a portion of the dor not the name of the D	es the portion of the D be your organization's nain name (for example NS server.	NS namespace for which domain name (for exan e, newzone.microsoft.co	h this server is nple, microsoft.com) om). The zone name is
Zone name:			_
New Zone Wizard			×
Master DNS Servers The secondary zone is	copied from one or ma	ore DNS servers.	
Specify the DNS serve contacted in the order	rs from which you wan shown.	t to copy the zone. Ser	vers are
Master Servers:			
IP Address	Server FQDN	Validated	Delete
Click here to 192.168.87.1	srv01.startrek.ent	OK	Цр

ATTENTION : pour qu'un DNS B puisse récupérer une zone depuis un DNS A, il faut que le DNS A autorise le transfert de zone pour cette zone (ce qui n'est pas autorisé par défaut).

• Stub Zone : pour mettre dans une DMZ. N'affiche que 2 infos : le SOA (Start Of Authority) et les NS (Name Server).

Ces 3 zones peuvent être intégrées à l'Active Directory si le serveur DNS est sur un DC.

ATTENTION : Un serveur DNS n'est pas MASTER ou SLAVE : c'est pour chaque zone qu'il l'est (il peut être master pour l'une et slave pour d'autres).

De base dans une zone, il crée deux enregistrements :

 le SOA (Start Of Authority) : chaque fois que l'on change quelque chose dans le DNS, il incrémente le numéro de série. Dans le SOA, le serveur voit s'il est primaire ou secondaire pour la zone (si c'est son nom qui apparaît, il sait qu'il est primaire et si c'est un autre, il sait qui est primaire). Il y a moyen d'incrémenter le numéro de série manuellement. C'est utilisé, par exemple, lorsque l'on a restauré un backup du DNS pour forcer la synchronisation depuis le serveur restauré.

startrek.ent Prop	erties	<u>? ×</u>
WINS General	Zone Transfers Start of Authority (SOA)	Security Name Servers
Serial number: 36		Increment
Primary server: srv01.startrek.er	nt.	Browse
Responsible pers hostmaster.startr	son: rek.ent.	Browse
Refresh interval: Retry interval:	15 minutes	-
Expires after:	1 days	
Minimum (default) TTL: 1 hours	
TTL for this reco	rd: 0 :1 :0 :0	(DDDDD:HH.MM.SS)
	OK Cancel	Apply Help

La synchronisation des zones se fait à l'initiative des serveurs qui vont contacter le master tous les **Refresh Interval**. Ils demandent au master son numéro de série et s'il est plus grand que le leur, ils se mettent à jour et demande un transfert de zone. S'il n'arrive pas à contacter le master, le slave va réessayer tous les **Retry Interval** \rightarrow Refresh Interval doit être plus grand que Retry Interval. Au bout de **Expire Time** (s'il n'y arrive pas), le slave se dit que ses enregistrements sont trop vieux et donc il ne répond plus aux requêtes \rightarrow si le master est mort, plus aucun slave ne répondra \rightarrow plus de résolution.

2) le Name Server: donne la liste des serveurs connue du primaire gérant cette zone.

Le transfert de zone

Par défaut, un serveur DNS ne communique pas les données de ses zones aux autres serveurs DNS sauf si elles sont intégrées à l'AD. Cependant, il peut être pratique d'avoir un serveur DNS sur un serveur qui n'est pas DC (et donc ne sait pas mettre ses zones dans l'AD), comme « backup » par exemple. Dans ce cas, il faut autoriser le transfert de zone.

startrek.ent Prop	erties		? ×	
General	Start of Authority (SC	DA)	Name Servers	
WINS	Zone Transfer	s	Security	
A zone transfer sends a copy of the zone to the servers that request a copy. Allow zone transfers:				
○ <u>T</u> o any server				
Only to servers listed on the Name Servers tab				
Only to the following servers				
IP Addr	ess	Server FQ	DN	

3 possibilités s'offrent à nous :

- Vers n'importe quel serveur : ce qui veut dire que si n'importe qui installe un serveur DNS et configure une zone secondaire pointant vers votre zone, il pourra répondre aux demandes de ses clients par rapport à cette zone
- Uniquement vers les serveurs qui sont dans les Names Servers : la solution la plus simple.
- Uniquement vers les serveurs suivant : vous devez mettre la liste des serveurs autorisés à la main

Les Forwarders

Dans la configuration des DNS, on va définir des Forwarders (FWD) vers lequel le DNS va renvoyer toutes les requêtes auxquelles il ne sait répondre. Il y a deux types de forwarders :

• Les conditionnels

Pour une certaine zone, on transfère vers un certain serveur

 DNS SRV01 Forward Lookup Zones msdcs.startrek.ent startrek.ent startrek.ent Conditional Forwarders Global Logs 	Name New Conditional Forwa	arder		
New Conditional Forwarder]
DNS Domain:				
startrektng.be				
IP addresses of the master <u>s</u> ervers:				
IP Address Server	FQDN	Validated	Delet	е
<click a<br="" add="" here="" to="">(2) 192.168.87.2 srv02.s</click>	tartrek.ent	The server with th	nis IP Up	
			D <u>o</u> wi	1
✓ Store this conditional forwarder in	Active Directory, and	replicate it as foll	ows:	1
All DNS servers in this forest				
This will not replicate to DNS S Domain Controllers Number of seconds before forward qu	ervers that are pre-W eries time out: 5	Vindows Server 20	003	
The server FQDN will not be available configured.	if the appropriate reve	erse lookup zones	and entries are not	

Le Forwarder peut être stocké dans l'AD pour qu'il se réplique automatiquement avec les autres DNS au niveau de la forêt, du domaine ou des DC (selon l'option choisie).

• Les inconditionnels

Quand on ne sait pas résoudre un nom et que cette zone n'est pas dans nos Forwarders conditionnel.

SRV01 Properties	;		? ×	
Debug Logging Interfaces Forwarders are D	Event Logging Forwarders DNS servers that this	Trust Anchors Mo Advanced server can use to re	nitoring Security Root Hints solve DNS	
IP Address 8.8.8.8	ds that this server ca	Innot resolve.	olve>	
s atompting to recorre				
Use root hint	s if no forwarders are	e available	<u>E</u> dit	
Note: If condition used instead of s forwarders, navig	nal forwarders are de server-level forwarde gate to the Condition	fined for a given don rs. To create or view al Forwarders node ir	nain, they will be v conditional n the scope tree.	

Tout ce que le serveur DNS ne sait pas résoudre sera renvoyé vers ce ou ces serveurs-là (ici c'est un DNS open de Google). On mettra souvent ici les IP des DNS du provider.

Les délégations

Dans la hiérarchie des noms de domaine, la plupart du temps, on aura un simple nom de domaine (startrek.ent par exemple). Dans les sociétés plus importantes ou plus complexes, on va avoir des sous-zones dans notre domaine (capitaine.startrek.ent). Plusieurs solutions s'offrent à nous quant à la gestion de ces sous-zones :

• On gère cela sur le même serveur

Dans ce cas, on fera un nouveau domaine sur le domaine existant



On devra juste entrer le nom du sous-domaine (sans le nom du domaine parent).

• On délègue la gestion de la zone

C'est un autre serveur qui va s'occuper de la sous-zone

ew Delegation Wizard
Delegated Domain Name Authority for the DNS domain you supply will be delegated to a different zone.
Specify the name of the DNS domain you want to delegate. Delegated domain:
capitaine
Fully qualified domain name (FQDN):
capitaine.startrek.ent

Après avoir mis le nom de la délégation, on doit lui dire vers quel serveur on va déléguer.

New Delegation Wizard			×	
Name Servers You can select one or more name servers to host the delegated zone.				Da
Specify the names and IP addresses delegated zone.	of the DNS servers you	want to have host the		
Name servers:				
Server Fully Qualified Domain Name	(FQDN)	IP Address]	
Add Edit	Remove			13
New Name Server Record				×
Enter the name of a DNS server that is auth	noritative for this zone.			
Server fully qualified domain name (FQDN):				
srv02.startrek.ent			Resolve	
IP Addresses of this NS record:				
IP Address	Validated		Delete	
<click add="" address="" an="" here="" ip="" to=""></click>				
X 192.168.87.2	The server with this I	P address is not	Up	

Ensuite, on devra créer une zone primaire capitaine.startrek.ent sur ce serveur

Les différents types d'enregistrement

Différents types d'enregistrement sont possibles dans une zone

New Host (A or AAAA)... New Alias (CNAME)... New Mail Exchanger (MX)... New Domain... New Delegation... Other New Records...

• Host(A)

Pour associer une IP à un nom de machine (normalement ça se fait automatiquement). Cela sert par exemple quand on a une machine statique (site web ou autre).

• Alias (CNAME)

Quand une machine doit avoir plusieurs noms pour les autres, il est plus aisé de créer un alias (un pointeur) vers un Host existant que de créer un nouvel Host pointant vers la même IP. En effet, en cas de changement d'IP du Host, on ne doit pas modifier plusieurs enregistrements, mais uniquement le principal.

New Resource Record	×
Alias (CNAME)	
Alias name (uses parent domain if left blank):	
www	
Fully qualified domain name (FQDN):	
www.startrek.ent.	
Eully qualified domain name (FQDN) for target host:	
srv02.startrek.ent	Browse

Dans ce cas-ci, on crée un Alias www (attention qu'on ne doit pas mettre le FQDN) pointant vers la machine qui va héberger le serveur Web.

• Mail Exchanger (MX)

Pour indiquer au client, qui veut envoyer un mail à votre domaine, le nom du serveur de mail. Ainsi, le client va envoyer un mail à <u>toto@startrek.ent</u> sans connaître l'adresse du serveur mail. C'est le DNS qui va donner l'adresse.

New Resource Record			
Mail Exchanger (MX)			
Host or child domain:			
By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.			
Fully qualified domain name	e (FQDN):		
startrek.ent.			
Fully qualified domain name (FQDN) of mail server: srv03.startrek.ent Browse			
Mail server priority:			
10			

On n'est pas obligé de donner un nom au MX, il faut juste le faire pointer vers le bon serveur. Si on a plusieurs serveurs mails, on va pouvoir donner des priorités. Selon la disponibilité, il va les prendre dans l'ordre. Plus le chiffre est élevé, moins la priorité est importante. C'est utilisé par certaines sociétés comme Skynet pour servir de backup aux sociétés qui sont chez eux. Si le serveur mail de la société est indisponible, c'est Skynet qui stocke les mails et qui les transfère quand le serveur est de nouveau accessible.

• Other

Pour créer d'autres types d'enregistrement

Propriétés d'une zone

Quand vous allez sur les propriétés d'une zone, plusieurs onglets s'offrent à vous.

• General

startrek.ent Properties							
WINS	Zone Transfers	Security					
General	Start of Authority (SOA)	Name Servers					
Status: Run	ning	Pause					
Type: Activ	ve Directory-Integrated	Change					
Replication: All D)NS servers in this domain	C <u>h</u> ange					
Data is stored in	Active Directory.						
Dynamic updates	s: Secure only	•					
Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.							
To set aging/scavenging properties, click Aging. Aging							

Cet onglet vous permet de

- Mettre la zone en pause
- Changer le type de zone (AD-Integrated, Primary, Secondary, Stub)
- Changer le scpope de replication

Change Zone Replication Scope	×
Choose how you want zone data to be replicated.	
○ To all DNS servers running on domain controllers in this forest: startrek.ent	
To all DNS servers running on domain controllers in this domain: startrek.ent	
O To all domain controllers in this domain (for Windows 2000 compatibility): startrek.ent	
C To all domain controllers in the scope of this directory partition:	
-]
OK Cancel	

• Start of Authority

Voir plus haut.

Name Servers

Donne la liste des serveurs de noms

• WINS

startrek.ent Prope	rties	?×				
General Start of Authority (SOA) Name Servers						
WINS	Zone Transfers	Security				
You can use WINS to resolve names not found by querying the DNS namespace. WINS only supports IPv4 addresses.						
IP address 192 .168	: .87 .1 Add					

Si le serveur DNS ne possède pas un enregistrement, parce qu'une machine ne s'enregistre pas automatiquement par exemple (NT4, Linux,...), on peut demander au DNS de transférer la requête au WINS. La case « Do not replicate this record » est à cocher si on a des serveurs DNS autres que Microsoft. En effet, cette option est purement Microsoft et les autres serveurs ne comprendraient pas cet enregistrement.

Ne pas oublier de cliquer sur la case ADD.

• Zone Transfers

Voir plus haut.

• Security

C'est ici que l'on peut mettre les différentes permissions aux utilisateurs sur la zone pour qu'ils puissent faire certaines actions.

Propriétés du serveur

Quand vous allez sur les propriétés du serveur, plusieurs onglets s'offrent à vous.

• Interfaces

Si le serveur DNS a plusieurs interfaces réseaux, on va pouvoir lui dire ici sur laquelle il doit écouter. On peut aussi désactiver l'écoute sur l'IPv6.

SR	V01 Properties				? ×			
ſ	Debug Logging	Event Logging	Trust Anchors	Monitoring	Security			
	Interfaces	Forwarders	Advanced	Roo	t Hints			
	Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses.							
	Listen on:							
	All IP address	ses						
	C Only the follo	wing IP addresses:						
	IP address:							
	 ✓ fe80::99d0:9e4a:40aa:8828 ✓ 192.168.87.1 							

• Forwarders

Voir plus haut.

- Advanced
 - <u>Recursion</u> : regarde d'abord sur soi puis à l'extérieur (contrairement à Itération où il donne la meilleure réponse qu'il peut sans regarder ailleurs).
 - <u>BIND Secondaries</u>: Microsoft, par défaut, compresse la zone avant de la transférer → il n'y a que Microsoft qui sache lire le fichier. BIND (Berclay Internet Name Domain) est un autre type de serveur DNS, produit Linux (le plus connu après Microsoft). Si on coche la case BIND Secondaries, il ne compresse pas le fichier pour être compatible avec les autres serveurs DNS.
 - <u>Fail on load if bad zone data</u> : si une des données dans la zone est incompréhensible, il ne charge pas du tout la zone (si la case est cochée).
 - <u>Enable round Robin</u> : quand on a plusieurs mêmes noms de machine avec des IP différentes, il répond au ping avec les IP les unes après les autres.
 - <u>Enable Netmask ordering</u> : va avec la case précédente : il répondra plutôt avec l'IP qui est dans le même réseau que l'IP demanderesse.
 - <u>Secure cache against pollution</u> : par défaut lorsque la réponse à une résolution de nom vient d'un autre serveur que celui qui est censé la donner, il ne met pas en

cache cette réponse (si c'est le serveur skynet.be qui répond à une requête pour <u>www.google.be</u> par exemple).

5RV01 Properties				? ×			
Debug Logging	Event Logging Forwarders	Trust Anchors Advance	Monitoring	Security			
Server version n	Server version number:						
6.1 7601 (0x1db	1)						
Disable recursion (also disables forwarders) BIND secondaries Fail on load if bad zone data Penable round robin Enable netmask ordering Secure cache against pollution							
Name checking:	[Multibyte (UTF8))	•			
Load zone data	Load zone data on startup: From Active Directory and registry						
Enable autor	natic scavenging o	of stale records					
Scavenging	period:	0	days	7			

• Root Hints

Donne la liste des 13 serveurs racines DNS (la zone point).

• Debug Logging

Permet d'avoir des logs plus détaillés en cas de problème (ceux-ci ne sont pas activés par défaut).

SRV01 Properties			? ×
Interfaces Debug Logging	Forwarders Event Logging	Advanced Trust Anchors	Root Hints
To assist with de the DNS server t	bugging, you can re o a log file. Debug l	ecord the packets se ogging is disabled b	ent and received by y default.
Log packets	for debugging		
Packet direction: Outgoing Incoming	} select a least on	Transport proto t I III UDP e IIII TCP	select at least one
Packet contents © Queries/Tran © Updates Notifications	: Isfers } select a least on	Packet type: Request t PResponse	<pre>} select at least one</pre>
Other options: Log unmatch Details	ed incoming respor	nse packets	
Filter packets	s by IP address	Filter	1
Log file File path and r Maximum size	ame: (bytes): 5000000	00	

• Event Logging

Défini ce qui est surveillé (Tout est surveillé par défaut).

s	RV01 Properties					
	Interfaces Debug Logging	Forwarders Event Logging	Advanced Trust Anchors	Monitoring	ot Hints	
The DNS event log maintains a record of errors, warnings, and other events encountered by the DNS server. You can use this information to analyze server performance.						
	Log the following events:					
	O No events					
	C Errors only					
	 Errors and ware All events 	amings				

• Trust Anchors (Nouveauté 2008)

s	RV01 Properties				? ×
I	Interfaces	Forwarders	Advanced	Roo	ot Hints
	Debug Logging	Event Logging	Trust Anchors	Monitoring	Security
Trust Anchors are used to validate secure DNS (DNSSEC) responses from remote DNS servers. Configure Trust Anchors in the form of public keys in the DNSKEY format to validate signed DNS responses. <u>T</u> rust Anchors:					ses from keys in
	Name	Attributes			
		A <u>d</u> d	<u>E</u> dit	<u>B</u> e	move

• DNS Query blocklist(Nouveauté 2008)

Nouvelle fonctionnalité dans Windows 2008, il y a une liste d'URL qui est bloquée par défaut. Pour afficher cette liste : « dnscmd /info /globalqueryblocklist ». Par défaut, 2 adresses sont bloquées : WPAD et ISATAP http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8219

A FAIRE

• Monitoring

5RV01 Prope	erties						? ×
Interface	s	Forwarders		Advance	ed	Roo	t Hints
Debug Logg	jing	Event Logging	Tn	ust Anchors	Mor	Security	
To verify th automatic t	To verify the configuration of the server, you can perform manual or automatic testing.						r
Select a te	st type	:					
A simple query against this DNS server							
A recur	rsive qu	uery to other DNS	sen	rers			
To perform	the te	st immediately, cli	ck T	est Now.		Ies	t Now
Eerforn	n autor	natic testing at th	e foll	owing interv	al:		
Test interval: 1 minutes							
Te <u>s</u> t results:							
Date		Time	Sim	ple Query	Recu	ursive Q.	

Permet de vérifier la configuration de votre DNS

• Security

Comme pour une zone, permet de mettre des permissions aux utilisateurs de faire certaines choses sur le DNS

Commandes intéressantes pour tester et configurer un DNS

- ipconfig
 - /registerdns : permet de forcer l'enregistrement d'une machine dans le DNS (valable uniquement si elle appartient à une des zones de son DNS)
 - o /displaydns : permet d'afficher la cache DNS
 - o /flushdns : permet de vider la cache DNS
- nslookup

permet de vérifier les enregistrements d'un DNS. Si vous obtenez une erreur au lancement de la commande (Default Server : Unknown), c'est que vous avez oublié de créer la zone reverse sur votre serveur.

Set type= : permet de modifier le mode d'interrogation de la commande.

- set type=mx permet de recueillir les informations concernant le ou les serveurs de messagerie d'un domaine.
- set type=ns permet de recueillir les informations concernant le serveur de noms associé au domaine
- set type=a permet de recueillir les informations concernant un hôte du réseau. Il s'agit du mode d'interrogation par défaut.
- set type=soa permet d'afficher les informations du champ SOA (Start Of Authority).
- o set type=cname permet d'afficher les informations concernant les alias.
- set type=hinfo permet, lorsque ces données sont renseignées, d'afficher les informations concernant le matériel et le système d'exploitation de l'hôte.
- o set type=ALLou ANY donne toutes les informations
- ο...
- dnscmd

permet de configurer le serveur DNS en ligne de commande.

- dnscmd /ZoneAdd startrektng.be /DsForwarder 10.0.0.7 pour ajouter un forwarder
- <u>dnscmd /ZoneAdd startrekent.be /Primary /file startrekent.be.dns</u> pour ajouter une zone startrekent.be avec un fichier de zone startrekent.be.dns
- o dnscmd /config startrekent.be /AllowUpdate 1 pour mettre cette zone en mise à jour dynamique secure ET non secure (mettre 2 si la zone est AD Integrated pour les mises à jour secure only)
- o <u>dnscmd /ZoneResetType startrekent.be /DsPrimary</u> pour intégrer la zone à l'AD.
- o dnscmd /info /globalqueryblocklist : pour voir quels sont les URL bloquées.

Dépannage simple DNS

Pour savoir si notre DNS fonctionne bien, il faut faire des tests soit avec nslookup, soit, plus simplement avec un ping.

- 1) ping 192.168.87.1 pour être sûr que la machine répond au ping
- 2) ping srv01.startrek.ent pour voir si on a une résolution DNS

Si on fait l'essai depuis un client, il faut faire attention aux différentes caches (en cas d'erreur).

- 1) ipconfig /flushdns sur le client
- 2) ipconfig /flushdns sur le serveur
- 3) faire un « clear cache » sur le serveur (dans la console DNS, clic droit sur le serveur, Clear Cache)



En effet, le serveur a une double cache (une serveur et une cliente).

- 4) Il faudra faire attention que si on passe par d'autres serveurs pour atteindre le serveur qui doit nous donner la réponse, il faut faire ces manipulations serveur/client sur tous.
- 5) Ne pas oublier bien entendu de vérifier qu'il n'y a pas d'entrées erronées dans le fichier Host des différentes machines (dans c:\windows\system32\drivers\etc)

Exercices :



NS1 :

- 1) zone primaire : techni.be
 - a. Sous-domaine (SD) : sales+ Délégation d'autorité (DA) : NS2
 - b. SD: IT + DA: NS3

NS2 :

2) Zone primaire : sales.techni.be

NS3 :

3) Zone primaire : it.techni.be

NS4 :

4) Zone primaire : supinfo.coma. SD : training + DA NS5

NS5 :

5) Zone primaire : training.supinfo.com

NS2 :

- 6) Forwarder (FW) : NS1
- NS3 :
 - 7) Forwarder (FW) : NS1

NS5 :

8) Forwarder (FW) : NS4

NS1 :

9) Conditional Forwarder (CFW) : NS4 (pour supinfo.com) + FW vers ISP

NS4 :

10) FW : NS1

Si un domaine, on peut faire le DNS pendant le DCPromo, cela évite les erreurs. Si on a plusieurs domaines, il faut d'abord faire toute l'architecture DNS.

→DNS^A

→ 1 zone primaire (Attention à bien mettre dynamic update, qui ne se fait pas par défaut).

 \rightarrow \rightarrow Sous domaine \rightarrow délégation d'authorité \rightarrow NS correspondant

+ forwarder

+ Conditionnal FW

→DNS B

→Zone secondaire (Dynamic update)

Attention, si on n'est pas en domaine, il faut penser à mettre le suffixe DNS au niveau de la machine (dans les propriétés système, Computer Name, Change, More)

Une fois que les zones sont configurées, on peut mettre l'AD

ATTENTION à ne pas oublier de mettre les zones primaires en AD Integrated et les secondaires en Primaires ADI.



- 1) NS1:
 - a. ZP : supinfo.com
 - i. SD : linux + DA NS2
 - b. ZP:techni.be
 - i. SD : windows + DA : NS2
 - ii. SD : linux + DA : NS
- 2) NS3:
 - a. ZP: linux.techni.be
 - b. ZP: training.windows.techni.be
 - c. ZP:it.techni.fr
 - d. ZP: w2003.training.techni.fr
- 3) NS2:
 - a. ZP: linux.supinfo.com
 - b. ZP: windows.techni.be
 - i. SD : sales
 - ii. SD : HR
 - iii. SD : training + DA NS3
- 4) NS4 :
 - a. ZP:techni.fr
 - i. SD : training
 - 1. SD : w2008
 - 2. SD : w2003 + DA NS3
 - ii. SD : IT + DA NS3
- 5) NS2 : FW : NS1
- 6) NS1 : FWC : NS4
- 7) NS3 : FW : NS1
- 8) NS4 : FW : NS1

Pour le backup de tout, on refait les ZP en ZS (pas les SD) et on autorise le transfert de zone.

Sur chaque serveur, on fera une reverse locale et sur le serveur principal, on fera des reverses de tout.