DNS SINGLE POINTS OF FAILURE DETECTION USING TRANSITIVE AVAILABILITY DEPENDENCY ANALYSIS

Florian Maury

15 juin 2018

CONTEXTE ET REMERCIEMENTS

Travaux initiés à l'ANSSI

- observatoire de la résilience de l'Internet français
- `https://github.com/X-Cli/transdep/`

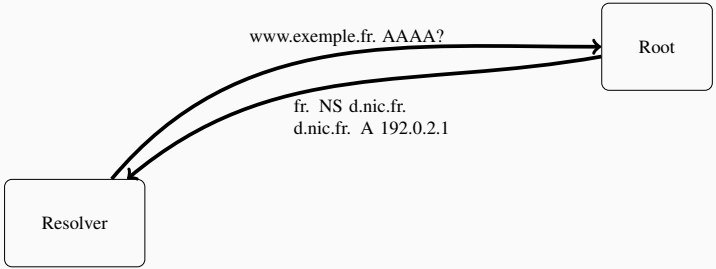
Merci à l'équipe, et notamment à Guillaume Valadon et Nicolas Vivet

Continuation des travaux chez Gandi

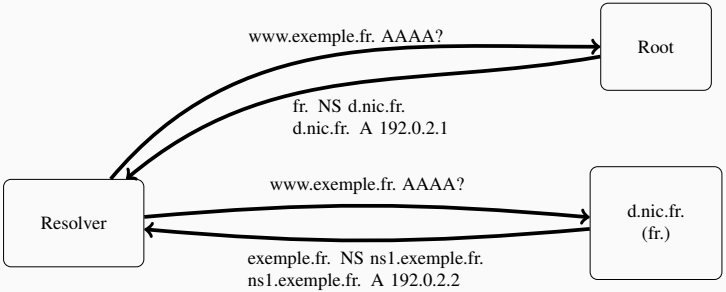
- implémentation en cours des recommandations

Rappels sur le DNS

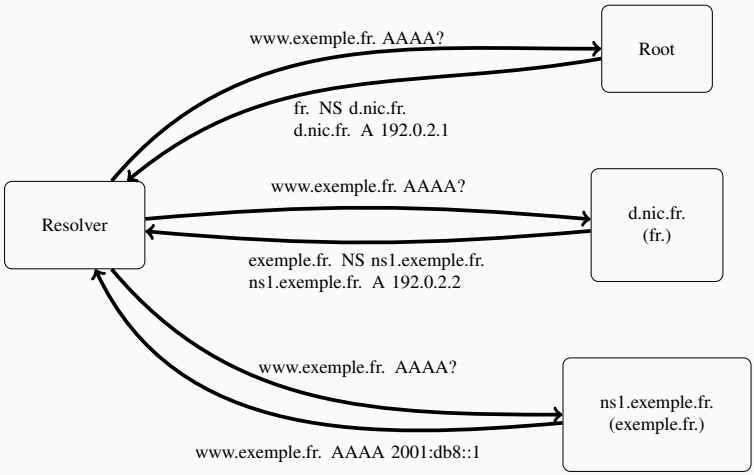
RÉSOLUTION DNS : LE CAS SIMPLE



RÉSOLUTION DNS : LE CAS SIMPLE



RÉSOLUTION DNS : LE CAS SIMPLE



À PROPOS DES DÉLÉGATIONS ET DES ENREGISTREMENTS GLUE

Délégation vers des noms dans le sous-domaine délégué :

exemple.fr. IN NS ns1.exemple.fr.

À PROPOS DES DÉLÉGATIONS ET DES ENREGISTREMENTS GLUE

Délégation vers des noms dans le sous-domaine délégué :

exemple.fr.	IN NS	ns1.exemple.fr.
ns1.exemple.fr.	IN A	192.0.2.2

À PROPOS DES DÉLÉGATIONS ET DES ENREGISTREMENTS GLUE

Délégation vers des noms dans le sous-domaine délégué :

À PROPOS DES DÉLÉGATIONS ET DES ENREGISTREMENTS GLUE

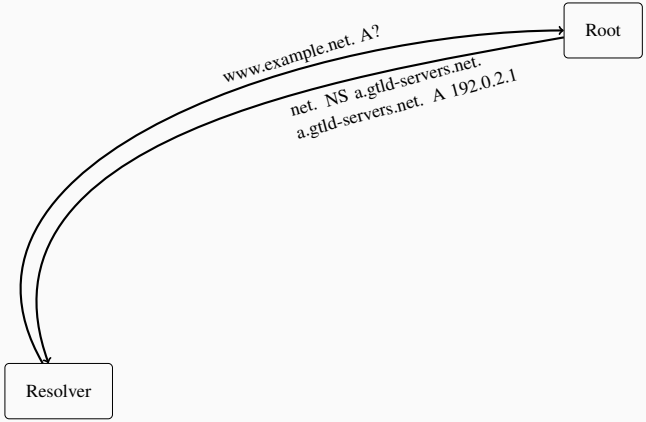
Délégation vers des noms dans le sous-domaine délégué :

exemple.fr.	IN NS	ns1.exemple.fr.
ns1.exemple.fr.	IN A	192.0.2.2

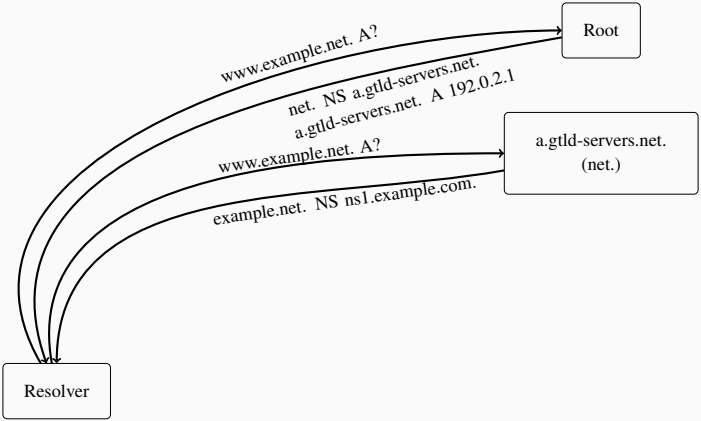
Pas de glue nécessaire :

example.net.	IN NS	ns1.example.com.

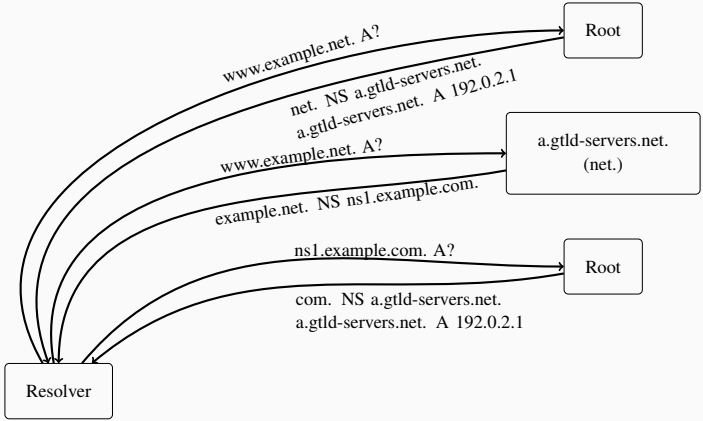
RÉSOLUTION DNS : LE CAS DES DÉLÉGATIONS SANS GLUE



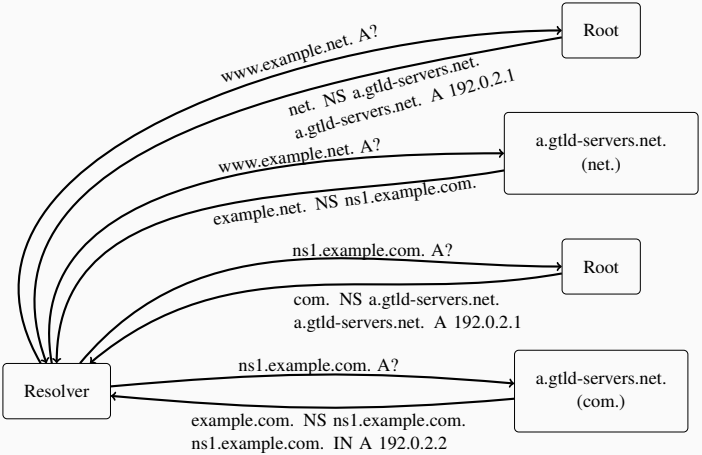
RÉSOLUTION DNS : LE CAS DES DÉLÉGATIONS SANS GLUE



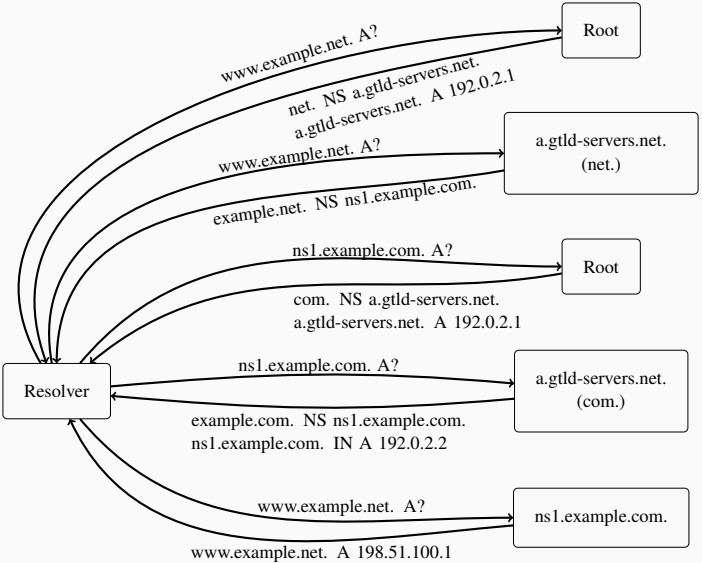
RÉSOLUTION DNS : LE CAS DES DÉLÉGATIONS SANS GLUE



RÉSOLUTION DNS : LE CAS DES DÉLÉGATIONS SANS GLUE



RÉSOLUTION DNS : LE CAS DES DÉLÉGATIONS SANS GLUE



RÉPARTITION DES TYPES DE DÉLÉGATION POUR LA ZONE .FR

Rapport 2016 de l'observatoire de la résilience de l'Internet français :

- seulement des glues : $< 1\,\%$
- aucune glue : $99\,\%$

Raison de cette quasi unanimité :

- forte concentration des domaines sur des plateformes d'hébergement
  - bureau d'enregistrements
  - CDN

« Donc, il n'y a pas de débat.
(Presque) aucun professionnel
du DNS n'utilise de glue.
Ça doit bien marcher. »

Avantages d'utiliser des délégations sans glue

Avantages de l'absence de glue :

- facilité d'administration
  - centralisation
  - pas d'infos dans la zone parente
- résilience

Avantages d'utiliser des délégations sans glue

Avantages de l'absence de glue :

- facilité d'administration
  - centralisation
  - pas d'infos dans la zone parente
- résilience ?

Conséquences de l'usage de délégations sans glue

Études précédentes :

- problème d'intégrité
- problème de performance au niveau des résolveurs

Cette étude :

- problèmes de résilience ?

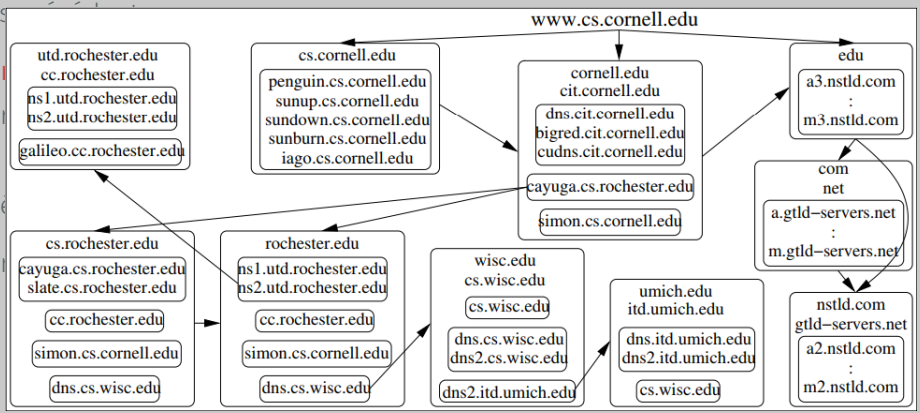
CONSÉQUENCES DE L'USAGE DE DÉLÉGATIONS SANS GLUE

Études

- pr
- pr

Cette é

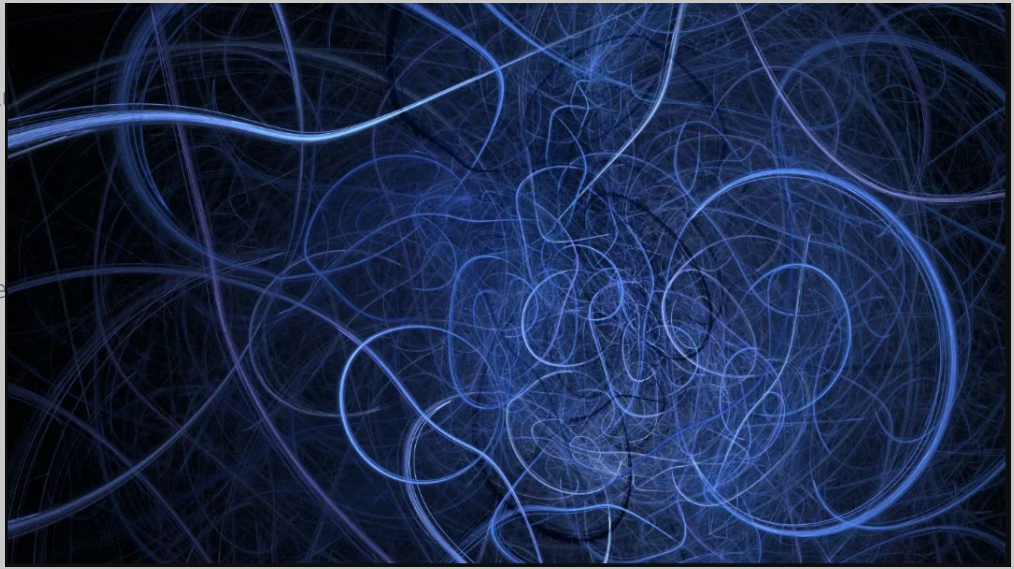
- pr



CONSÉQUENCES DE L'USAGE DE DÉLÉGATIONS SANS GLUE

Ét

Ce



Conséquences de l'usage de délégations sans glue

Études précédentes :

- problème d'intégrité
- problème de performance au niveau des résolveurs

Cette étude :

- problèmes de résilience ?

Conséquences de l'usage de délégations sans glue

Études précédentes :

- problème d'intégrité
- problème de performance au niveau des résolveurs

Cette étude :

- problèmes de résilience ?

Conséquences de l'usage de délégations sans glue

Études précédentes :

- p
- p

Cette

- p

Exemple de www.amazon.com :

- Graph de dépendance dessiné : `https://github.com/X-Cli/transdep/releases/download/v0.1/amazon.pdf`
- 284 éléments uniques pouvant causer une indisponibilité
- analyse manuelle quasi impossible

Quels éléments peuvent causer une indisponibilité du DNS?

ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponibilité :

- une adresse IP
- un préfixe réseau
- un AS
- la connectivité à une version des réseaux IP
- un nom de domaine

ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponibilité :

- une adresse IP
- un préfixe réseau
- un AS
- la connectivité à une version des réseaux IP
- un nom de domaine

ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Cause

- u
- u
- u
- la
- u

Comment un nom peut-il être indisponible ?
Quelques exemples :

- DDoS
- zone tronquée
- incident opérationnel avec DNSSEC
- interruption administrative
- dangling names

ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

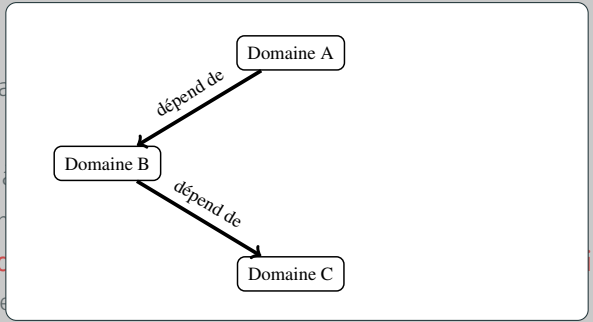
Causes d'indisponibilité :

- une adresse IP
- un préfixe réseau
- un AS
- la connectivité à une version des réseaux IP
- un nom de domaine
- une dépendance (causée par une délégation sans glue ou un alias DNS)
  - transivité (i.e. problème des dépendances des dépendances)

ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponibilité :

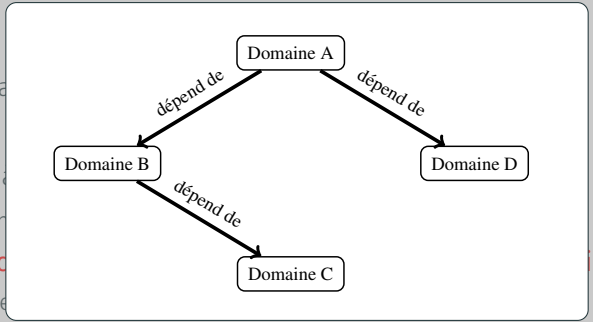
- une adresse IP
- un préfixe réseau
- un AS
- la connectivité
- un nom de dom
- une dépendanc (cas DNS)
  - transivité (i.e



ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponibilité :

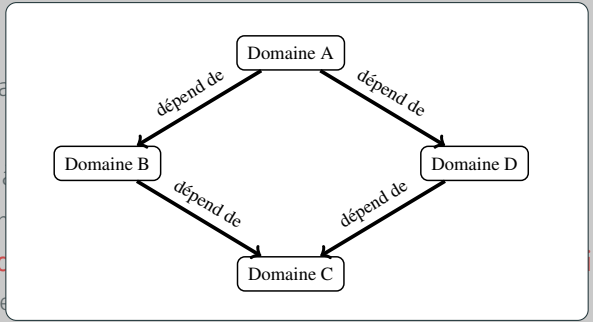
- une adresse IP
- un préfixe réseau
- un AS
- la connectivité
- un nom de dom
- une dépendanc ias DNS)
  - transivité (i.e



ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponibilité :

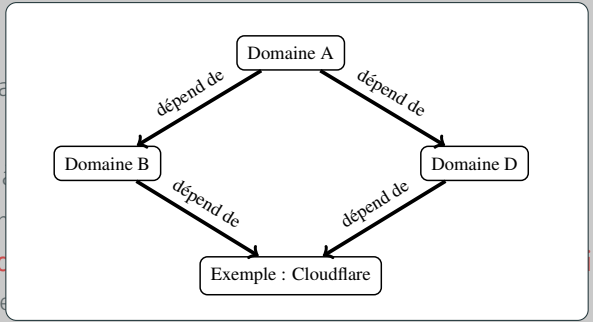
- une adresse IP
- un préfixe réseau
- un AS
- la connectivité
- un nom de dom
- une dépendanc (cas DNS)
  - transivité (i.e



ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponibilité :

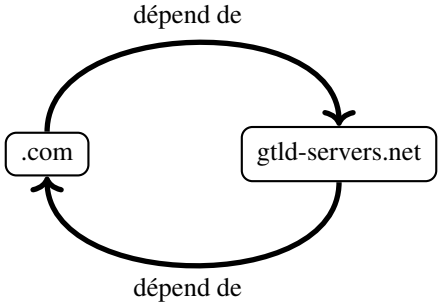
- une adresse IP
- un préfixe réseau
- un AS
- la connectivité
- un nom de dom
- une dépendanc ias DNS)
  - transivité (i.e



Causes d'indis

- une adres
- un préfixe
- un AS
- la connect
- un nom de
- une déper
  - transiv

Relation de dépendance circulaire

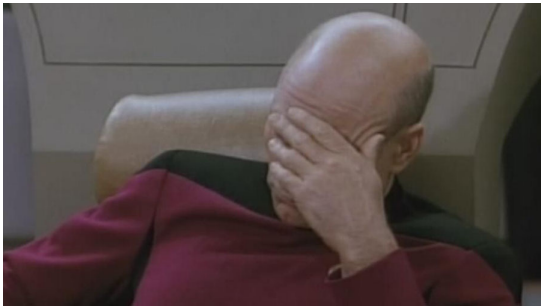


NS)

ÉLÉMENTS ANALYSÉS DANS CETTE ÉTUDE

Causes d'indisponi

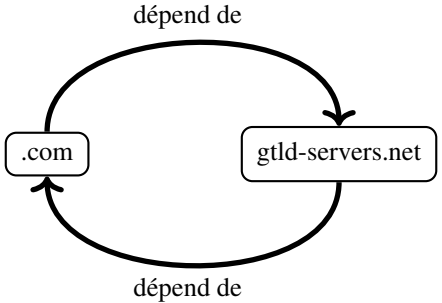
- une adresse IP
- un préfixe rése
- un AS
- la connectivité
- un nom de do
- une dépendar s DNS)
  - transivité (



Causes d'indis

- une adres
- un préfixe
- un AS
- la connect
- un nom de
- une déper
  - transiv

Relation de dépendance circulaire



NS)

Développement de l'outil

Transdep

TRANSDEP : COLLECTEUR ET ANALYSEUR DE DÉPENDANCES DNS

Caractéristiques :

- est développé en Go
- est publié sous licence BSD 2-Clause
- est utilisable en CLI ou avec un service web en REST/JSON auto-hébergeable
- agit comme un pseudo-résolveur DNS
- traque les alias et les noms des serveurs DNS
- construit à la volée un graph/arbre de dépendances
- détecte les points de défaillance uniques (SPOF)

https://github.com/X-Cli/transdep

Création d'une expression booléenne

Intuitivement, pour **www.example.com**, l'arbre de dépendance contient :

- la racine du DNS **ET**
- la zone .com **ET**
- les dépendances de .com pour sa délégation depuis la racine (e.g. .net) **ET**
  - l'adresse IP de a.gtld-servers.net **OU**
  - l'adresse IP de b.gtld-servers.net **OU**
  - l'adresse IP de...
- la zone example.com **ET**
- les dépendances de example.com (e.g. son CDN qui reçoit la délégation du nom depuis .com) **ET**
- ...

Création d'une expression booléenne

Intuitivement, pour **www.example.com**, l'arbre de dépendance contient :

- la racine du DNS **ET**
- la zone .com **ET**
- les dépendances de .com pour sa délégation depuis la racine (e.g. .net) **ET**
  - l'adresse IP de a.gtld-servers.net **OU**
  - l'adresse IP de b.gtld-servers.net **OU**
  - l'adresse IP de...
- la zone example.com **ET**
- les dépendances de example.com (e.g. son CDN qui reçoit la délégation du nom depuis .com) **ET**
- ...

Création d'une expression booléenne

Intuitivement, pour **www.example.com**, l'arbre de dépendance contient :

- la racine du DNS ET
- la zone .com ET
- les dépendances de .com pour sa délégation depuis la racine (e.g. .net) ET
  - l'adresse IP de a.gtld-servers.net OU
  - l'adresse IP de b.gtld-servers.net OU
  - l'adresse IP de...
- la zone example.com ET
- les dépendances de example.com (e.g. son CDN qui reçoit la délégation du nom depuis .com) ET
- ...

SOURCE DES DOMAINES ANALYSÉS

Quatre millions de domaines analysés :

- OpenData de l'Afnic (zone .fr) ($\approx$ 3M)
- Top 1 million Alexa (monde)

Tous les noms de domaine ont été préfixés par "www."

.VOCABULAIRE

Ceci n'est pas (encore !) un TLD

Dépendance == SPOF

Dépendance == SPOF

Le DNS est arborescent

⇒ un nom est nécessairement **dépendant** de ses parents

www.gandi.net.

Toute autre dépendance est **évitable** (nom, IP, AS, préfixe…)

Dépendance == SPOF

Le DNS est arborescent

⇒ un nom est nécessairement **dépendant** de ses parents

www.**gandi.net.**

Toute autre dépendance est **évitable** (nom, IP, AS, préfixe…)

Dépendance == SPOF

Le DNS est arborescent

⇒ un nom est nécessairement **dépendant** de ses parents

www.gandi.**net.**

Toute autre dépendance est **évitable** (nom, IP, AS, préfixe...)

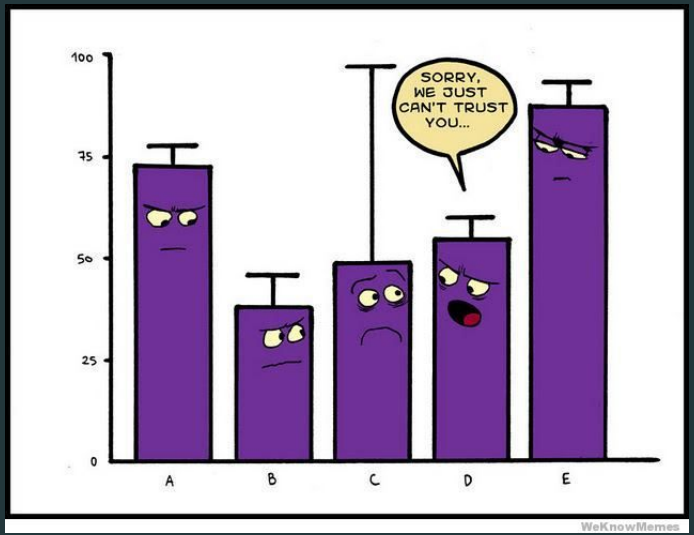
Dépendance == SPOF

Le DNS est arborescent

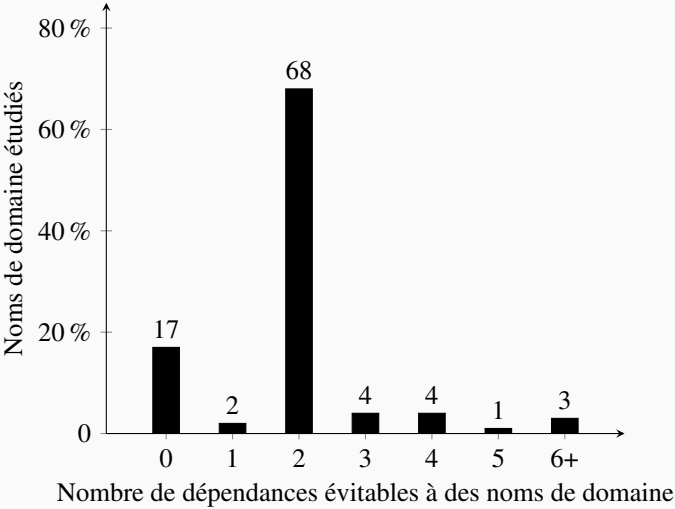
⇒ un nom est nécessairement **dépendant** de ses parents

www.gandi.net.

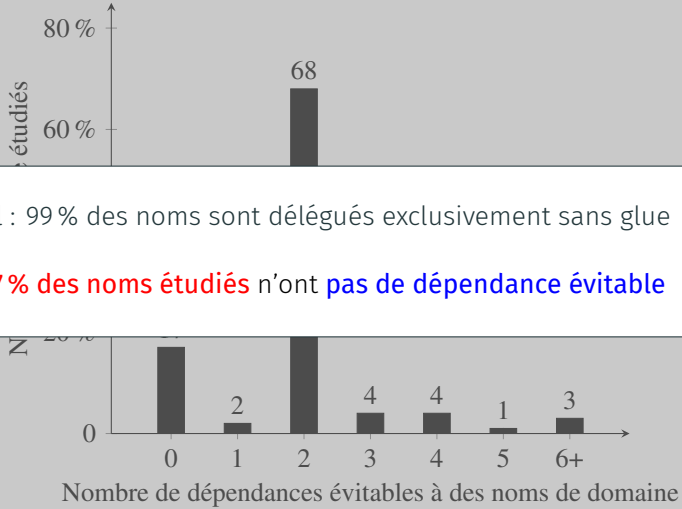
Toute autre dépendance est **évitable** (nom, IP, AS, préfixe...)


100
75
50
25
0
A
B
C
D
E
SORRY, WE JUST CAN'T TRUST YOU...
WeKnowMemes

DÉPENDANCE À DES NOMS DE DOMAINE (.FR)



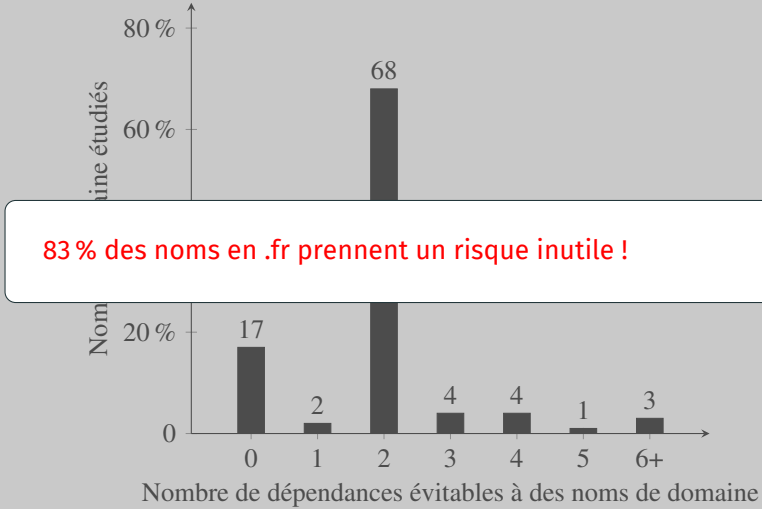
Dépendance à des noms de domaine (.fr)



Rappel : 99 % des noms sont délégués exclusivement sans glue

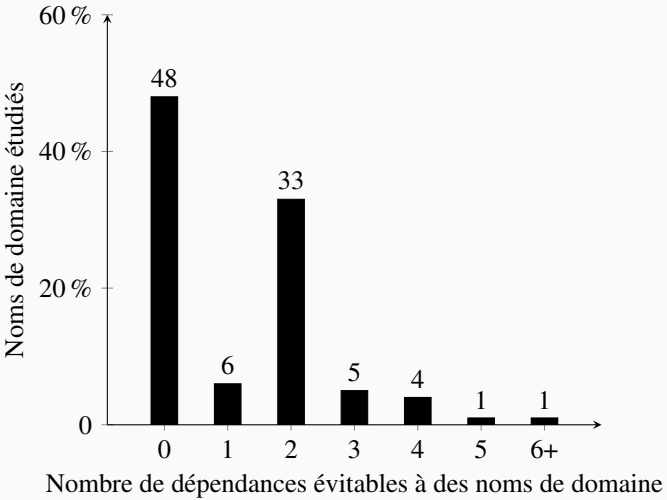
Seul 17 % des noms étudiés n'ont pas de dépendance évitable

DÉPENDANCE À DES NOMS DE DOMAINE (.FR)



83 % des noms en .fr prennent un risque inutile !

Dépendance à des noms de domaine (top 1M Alexa)



Dépendance sous l'angle d'IP

Type de dépendance	.fr	Alexa
Adresse IP	0,3 %	5,0 %
Réseau IPv4	33,7 %	58,5 %
Réseau IPv6	0,1 %	0,1 %
AS	88,1 %	75,9 %
Préfixe	8,4 %	14,6 %


What am I gonna do? What am I gonna do?

Source de recommandations :

- `https://www.ssi.gouv.fr/guide-dns`
- `https://www.ssi.gouv.fr/observatoire`

Bonnes pratiques de résilience :

- diversifier sa topologie réseau
- adopter une stratégie de nommage n'introduisant pas de SPOF
  - utiliser des glues
  - répartir/diversifier les délégations (TLD différents, SLD différents…)
- vérifier son graph de dépendances à intervalle

`https://github.com/X-Cli/transdep`


I CAN HAZ
QUESTIONS?
memegenerator.net

DIFFICULTÉS POUR LA CONCEPTION DE L'OUTIL

Constat triste de l'état de l'écosystème DNS :

- CDN violant la nature arborescente du DNS
- implémentations ou mises en œuvre médiocres
  - répartiteurs de charge faisant du GSLB
  - BIND8
- boucles ou assimilées

Dépendance à des noms de domaine (.fr)

Rang	ccTLD .fr	#domaines
1	net.	1 574 938
2	ovh.net.	851 505
3	com.	547 328
4	gandi.net.	347 512
5	me.	119 528
6	anycast.me.	119 101
7	it.	47 902
8	register.it.	46 318
9	nordnet.fr.	46 176
10	amazonaws.com.	45 082

Dépendance à des noms de domaine (Top 1M Alexa)

Rang	Top 1M Alexa	#domaines
1	com.	192 003
2	net.	150 681
3	cloudflare.com.	59 767
4	jp.	16 155
5	domaincontrol.com.	15 716
6	google.com.	14 062
7	dynect.net.	11 085
8	amazonaws.com.	10 351
9	ovh.net.	10 109
10	dnsv2.com.	9 420

PRÉFIXES ÉTANT DES DÉPENDANCES

	Préfixe	Opérateur	#domaines
`.fr` ccTLD	81.88.63.0/24	RegisterIT	65,381
	194.206.126.0/24	Nordnet	46,138
	194.2.0.0/24	Oleane	13,900
	193.252.243.0/24	Pages Jaunes	11,590
	93.88.255.0/24	Infomaniak	5,742
Alexa	162.251.82.0/24	Public Domain Registry	4,602
	46.242.149.0/24	Loopia	2,125
	93.188.0.0/24	Loopia	716
	129.232.248.0/24	Hetzner	639
	192.185.5.0/24	Hostgator	621

DÉPENDANCE À DES AS

	ASN	Opérateur	#domaines
`.fr` ccTLD	16276	OVH	1,034,859
	29169	Gandi	351,325
	8560	1&1	349,300
	16509	Amazon	133,085
	39729	RegisterIT	65,849
Alexa	13335	Cloudflare	152,458
	16509	Amazon	63,233
	26496	GoDaddy	59,082
	15169	Google	23,999
	16276	OVH	23,529