Switch

The DNS as national critical infrastructure in an era of geopolitical tensions

Michael Hausding, Competence Lead DNS & Domain Abuse
Version 1.2, October 28, 2025

About me and Switch

Michael Hausding, Competence Lead DNS & Domain Abuse

Resilience in a mad, mad world

GESCHÄFT ABONNIEREN

22.4411   POSTULAT

Strategie Digitale Souveränität der Schweiz

Eingereicht von:

Z'GRAGGEN HEIDI

Die Mitte-Fraktion. Die Mitte. EVP.
Die Mitte

Einreichungsdatum: 14.12.2022

Eingereicht im: Ständerat

Stand der Beratungen: Überwiesen an den Bundesrat

WEITERFÜHRENDE UNTERLAGEN

AMTLICHES BULLETIN

INFORMATIONEN ZUM VERFAHREN BEI POSTULATEN

⊖ ALLES ZUKLAPPEN

⊖ **EINGEREICHTER TEXT**

Der Bundesrat wird beauftragt, Bericht zu erstatten, wie er "Digitale Souveränität" für die Schweiz definiert; wie er den Stand der digitalen Souveränität unseres Landes beurteilt; welche übergeordnete, umfassende Strategie zur Stärkung der staatspolitisch, wirtschaftlich und gesellschaftlich als von höchster Bedeutung einzuordnende digitale Souveränität unseres Landes er zu ergreifen gedenkt.

Der Bericht definiert gestützt auf diese übergeordnete Strategie allenfalls gesetzgeberischen Handlungsbedarf, Prioritäten, einen Zeitplan für die Umsetzung der notwendigen Massnahmen und macht Aussagen zur Bereitstellung der notwendigen Mittel, um die dringendsten und erfolgversprechendsten Projekte zur Stärkung/Erreichung der digitalen Souveränität rasch umzusetzen.

Digital sovereignty

The ability of a state or entity to have authoritative control over its critical infrastructure, data, and communications, free from unauthorized foreign influence or exposure to vulnerabilities through data routing beyond jurisdictional boundaries.

Switch

Criminal Court: Microsoft's email block a wake-up call for digital sovereignty

Microsoft blocked the email account of Chief Prosecutor of the International Court of Justice after Trump's sanctions. Critics: "We urgently need alternatives."

The International Criminal Court in The Hague. (Image: ICC)

The DNS as Critical Infrastructure

Summary of the Amazon DynamoDB Service Disruption in the Northern Virginia (US-EAST-1) Region

We wanted to provide you with some additional information about the service disruption that occurred in the N. Virginia (us-east-1) Region on October 19 and 20, 2025. While the event started at 11:48 PM PDT on October 19 and ended at 2:20 PM PDT on October 20, there were three distinct periods of impact to customer applications. First, between 11:48 PM on October 19 and 2:40 AM on October 20, Amazon DynamoDB experienced increased API error rates in the N. Virginia (us-east-1) Region. Second, between 5:30 AM and 2:09 PM on October 20, Network Load Balancer (NLB) experienced increased connection errors for some load balancers in the N. Virginia (us-east-1) Region. This was caused by health check failures in the NLB fleet, which resulted in increased connection errors on some NLBs. Third, between 2:25 AM and 10:36 AM on October 20, new EC2 instance launches failed and, while instance launches began to succeed from 10:37 AM, some newly launched instances experienced connectivity issues which were resolved by 1:50 PM.
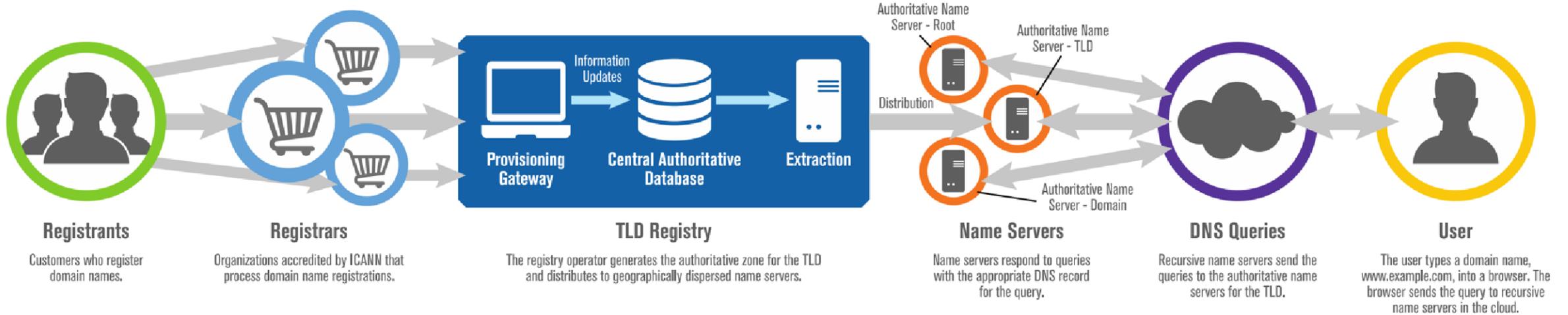
DynamoDB

Between 11:48 PM PDT on October 19 and 2:40 AM PDT on October 20, customers experienced increased Amazon DynamoDB API error rates in the N. Virginia (us-east-1) Region. During this period, customers and other AWS services with dependencies on DynamoDB were unable to establish new connections to the service. The incident was triggered by a latent defect within the service's automated DNS management system that caused endpoint resolution failures for DynamoDB.

Many of the largest AWS services rely extensively on DNS to provide seamless scale, fault isolation and recovery, low latency, and locality. Services like DynamoDB maintain hundreds of thousands of DNS records to operate a very large heterogeneous fleet of load balancers in each Region. Automation is crucial to ensuring that these DNS records are updated frequently to add additional capacity as it becomes available, to correctly handle hardware failures, and to efficiently distribute traffic to optimize customers' experience. This automation has been designed for resilience, allowing the service to recover from a wide variety of operational issues. In addition to providing a public regional endpoint, this automation maintains additional DNS endpoints for several dynamic DynamoDB variants including a FIPS compliant endpoint, an IPv6 endpoint, and account-specific endpoints. The root cause of this issue was a latent race condition in the DynamoDB DNS management system that resulted in an incorrect empty DNS record for the service's regional endpoint (**dynamodb.us-east-1**.amazonaws.com) that the automation failed to repair. To explain this event, we need to share some details about the DynamoDB DNS management architecture. The system is split across two independent components for availability reasons. The first component, the DNS Planner, monitors the health and capacity of the load balancers and periodically creates a new DNS plan for each of the service's endpoints consisting of a set of load balancers and weights. We produce a single regional DNS plan, as this greatly simplifies capacity management and failure mitigation when capacity is shared across multiple endpoints, as is the case with the recently launched IPv6 endpoint and the public regional endpoint. A second component, the DNS Enactor, which is designed to have minimal dependencies to allow for system recovery in any scenario, enacts DNS plans by applying the required changes in the Amazon Route53 service. For resiliency, the DNS Enactor operates redundantly and fully independently in three different Availability Zones (AZs). Each of these independent instances of the DNS Enactor looks for new plans and attempts to update Route53 by replacing the current plan with a new plan using a Route53 transaction, assuring that each endpoint is updated with a consistent plan even when multiple DNS Enactors attempt to update it concurrently. The race condition involves an unlikely interaction between two of the DNS Enactors. Under normal operations, a DNS Enactor picks up the latest plan and begins working through the service endpoints to apply this plan. This process typically completes rapidly and does an effective job of keeping DNS state freshly updated. Before it begins to apply a new plan, the DNS Enactor makes a one-time check that its plan is newer than the previously applied plan. As the DNS Enactor makes its way through the list of endpoints, it is possible to encounter delays as it attempts a transaction and is blocked by another DNS Enactor updating the same endpoint. In these cases, the DNS Enactor will retry each endpoint until the plan is successfully applied to all endpoints. Right before this event started, one DNS Enactor experienced unusually high delays needing to retry its update on several of the DNS endpoints. As it was slowly working through the endpoints, several other things were also happening. First, the DNS Planner continued to run and produced many newer generations of plans. Second, one of the other DNS Enactors then began applying one of the newer plans and rapidly progressed through all of the endpoints. The timing of these events

9

DNS a global resource for the Internet

The Relationship of Registries with the DNS Ecosystem

Registrants
Customers who register domain names.

Registrars
Organizations accredited by ICANN that process domain name registrations.

TLD Registry
The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.

Name Servers
Name servers respond to queries with the appropriate DNS record for the query.

DNS Queries
Recursive name servers send the queries to the authoritative name servers for the TLD.

User
The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.

Provisioning Gateway — Information Updates — Central Authoritative Database — Extraction

Authoritative Name Server - Root
Authoritative Name Server - TLD
Distribution
Authoritative Name Server - Domain

Switch

DNS a global resource for the Internet

e,d,k,j root servers in Switzerland

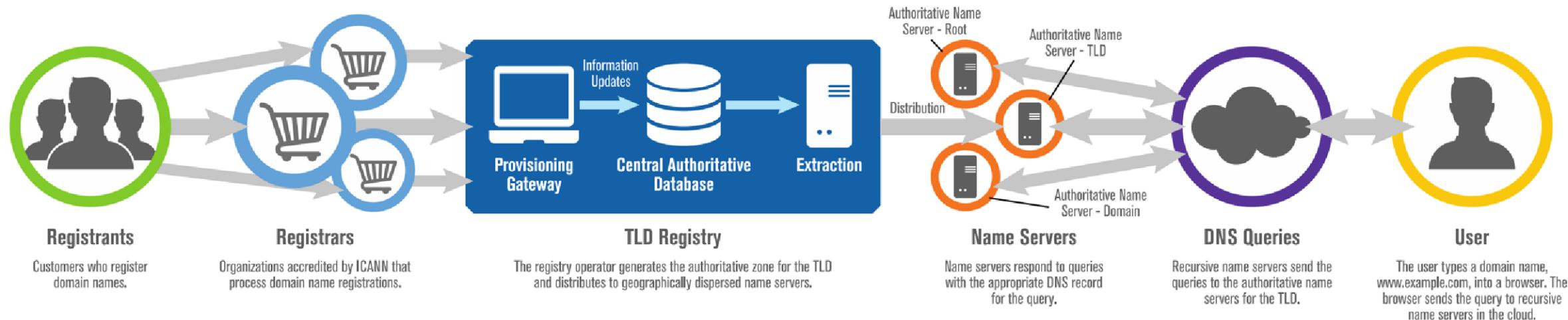The Relationship of Registries with the DNS Ecosystem
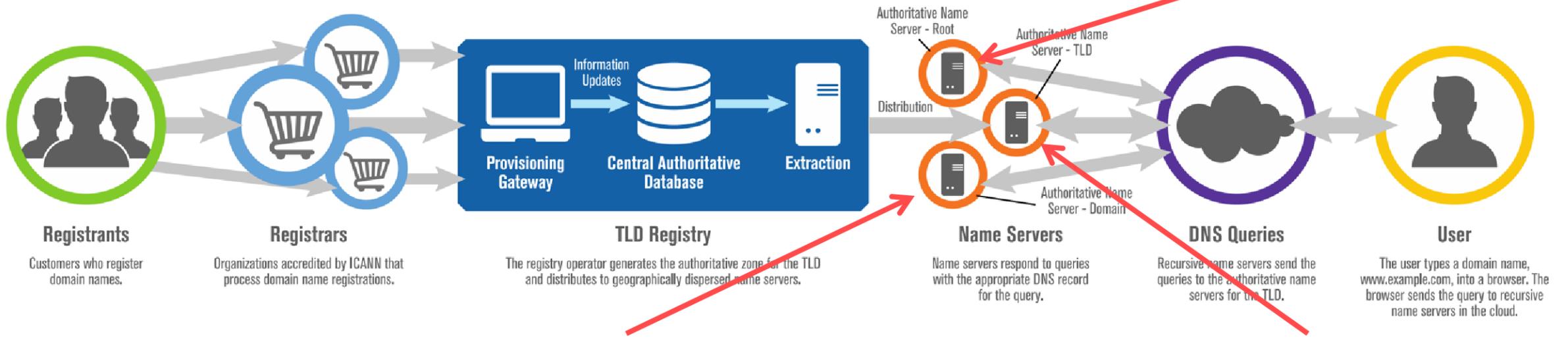
Authoritative name server for domain often run by the registrar, hoster or Cloudprovider

TLD name servers run by registry

swisscyberstorm.com

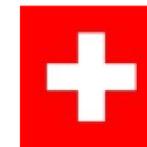
The Relationship of Registries with the DNS Ecosystem

Registrants
Customers who register domain names.

Registrars
Organizations accredited by ICANN that process domain name registrations.

TLD Registry
The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.

Name Servers
Name servers respond to queries with the appropriate DNS record for the query.

DNS Queries
Recursive name servers send the queries to the authoritative name servers for the TLD.

User
The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.

Cyberstorm

Swizzonic
Combell-Group

.com (Verisign)

nine

Swisscom

Cyberstorm
attendant

admin.ch

The Relationship of Registries with the DNS Ecosystem

Registrants	Registrars	TLD Registry	Name Servers	DNS Queries	User
Customers who register domain names.	Organizations accredited by ICANN that process domain name registrations.	The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.	Name servers respond to queries with the appropriate DNS record for the query.	Recursive name servers send the queries to the authoritative name servers for the TLD.	The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.
Swiss Confederation	cyon	.ch (Switch)	BIT	ISP operated Resolver	Residential Internet User

admin.ch

23 Oct 2025 10:45 UTC

Domain Name System

- ✔ DNS Zone ▪
- ✔ DNS Records ▪
- ✘ DNSSEC ▪
- ✔ CAA ▪

Email

- ✔ Mail servers ▪

SECURE TRANSPORT (SMTP)

- ✔ TLS ▪
- ✔ Certificates ▪
- ✘ MTA-STS ▪
- ✘ TLS-RPT ▪
- ✘ DANE ▪

AUTHENTICATION AND POLICY

- ✔ SPF ▪
- ✔ DMARC ▪

WWW

PROTOCOLS

- ✔ HTTP (80) ▪
- ✔ HTTPS (443) ▪

% dig ns admin.ch

;; ANSWER SECTION:

admin.ch. 2353 IN NS ins3.admin.ch.

admin.ch. 2353 IN NS ins4.admin.ch.

admin.ch. 2353 IN NS ins5.admin.ch.

admin.ch. 2353 IN NS ins2.admin.ch.

admin.ch. 2353 IN NS ins1.admin.ch.

;; ADDITIONAL SECTION:

ins3.admin.ch. 2353 IN AAAA 2a00:c38:2:28:0:ffff:d467:4855

ins1.admin.ch. 902 IN A 162.23.22.32

ins2.admin.ch. 902 IN A 162.23.23.32

ins3.admin.ch. 902 IN A 212.103.72.85

ins4.admin.ch. 2353 IN A 162.23.22.34

ins5.admin.ch. 2353 IN A 162.23.23.34

Nestlé (nestle.ch)

The Relationship of Registries with the DNS Ecosystem

Registrants
Customers who register domain names.

Registrars
Organizations accredited by ICANN that process domain name registrations.

TLD Registry
The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.

Name Servers
Name servers respond to queries with the appropriate DNS record for the query.

DNS Queries
Recursive name servers send the queries to the authoritative name servers for the TLD.

User
The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.

Cyberstorm   Com laude   .ch (Switch)   neustar   Swisscom   Cyberstorm attendant
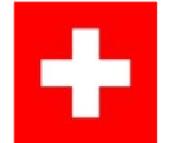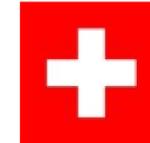
% dig nestle.ch ns

;; ANSWER SECTION:
nestle.ch. 3409 IN NS eurdns1.nestle.com.
nestle.ch. 3409 IN NS amsdns1.nestle.com.
nestle.ch. 3409 IN NS aoadns1.nestle.com.
nestle.ch. 3409 IN NS ctrdns1.nestle.com.

;; ADDITIONAL SECTION:
amsdns1.nestle.com. 58828 IN AAAA 2001:502:f3ff::29a
aoadns1.nestle.com. 58828 IN AAAA 2610:a1:1015::29a
ctrdns1.nestle.com. 58828 IN AAAA 2610:a1:1014::29a
eurdns1.nestle.com. 58828 IN AAAA 2001:502:4612::29a
amsdns1.nestle.com. 58828 IN A 204.74.66.154
aoadns1.nestle.com. 58828 IN A 204.74.67.154
ctrdns1.nestle.com. 58828 IN A 204.74.110.154
eurdns1.nestle.com. 58828 IN A 204.74.111.154

Nestlé (nestle.ch)

The Relationship of Registries with the DNS Ecosystem

Registrants
Customers who register domain names.

Registrars
Organizations accredited by ICANN that process domain name registrations.

TLD Registry
The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.

Name Servers
Name servers respond to queries with the appropriate DNS record for the query.

DNS Queries
Recursive name servers send the queries to the authoritative name servers for the TLD.

User
The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.

Cyberstorm

Com laude

.ch (Switch)

neustar
Verisign

Swisscom

Cyberstorm
attendant
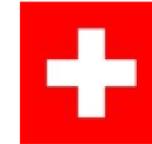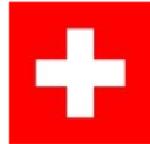
Geopolitical Considerations

Geopolitical Dependencies

Can geopolitical tensions force IANA (ICANN) to remove a TLD from the root zone file?

2 March 2022

Mykhailo Fedorov
Deputy Prime Minister, Minister of Digital Transformation
Ukraine

Dear Deputy Prime Minister,

I am writing in response to your letter received 28 February 2022. First, let me express my personal concern for the well-being of your citizens in the midst of this conflict. ICANN and its global community are aware of and concerned about the terrible toll being exacted against your country.

You have asked that ICANN target Russia's access to the Internet by revoking specific country-code top-level domains operated from within Russia, arranging the revocation of SSL certificates issued within those domains, and shutting down a subset of root servers located in Russia.

DESIGN DEVELOPMENT HOSTING CLOUD DOMAINS MARKETING WORDPRESS SERVERS TECH

Announcements

Changes to ResellerClub's Countries of Operation

BY SHRIDHAR LUTHRIA - NOVEMBER 10, 2013 - 2 MIN READ

At the end of **October 2013**, ResellerClub became a US based entity and this move resulted in a change in the legal jurisdiction applicable to us. As a result of this change, we are no longer able to support partners and clients from Cuba, Iran, North Korea, Sudan and Syria. These include Resellers, Sub Resellers and Customers. If any of the following actions are performed by users from OFAC Countries, the respective domain/hosting package will be suspended. Funds that are received from customers in OFAC Countries will not be refunded as per US Regulations.

1. Domain Registration
2. Domain Transfers
3. Purchase of Hosting Packages
4. Transfer or migration of Hosting Services from another provider

SUBSCRIBE TO OUR BLOG

Enter your email address   SUBMIT

WRITE

Switch   https://www.resellerclub.com/blog/important-changes-in-resellerclubs-countries-of-operation/

Sovereignty and Resilience for the DNS in Switzerland

Ordinance on Internet Domains: for .ch, .swiss, .zurich….

784.104.2

English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

Ordinance on Internet Domains

(OID)

of 5 November 2014 (Status as of 1 January 2024)

The Swiss Federal Council,

based on Articles 13a paragraph 3, 28 paragraphs 2, 3, 4 and 6, 28e, 48a paragraph 2, 59 paragraph 3, 62 and 64 paragraph 2, of the Telecommunications Act of 30 April 1997[1] (TCA),[2]

ordains:

[1] SR **784.10**

[2] Amended by No I of the O of 18 Nov. 2020, in force since 1 Jan. 2021 (AS **2020** 6251).

— Chapter 1 General Provisions

— Art. 1 Aim

[1] The aim of this Ordinance is to ensure that private individuals, businesses and public bodies in Switzerland are offered a sufficient, reasonably priced, high quality range of internet domain names that fulfils their requirements.

[2] It must in particular:

a. ensure the efficient, transparent and judicious use of the top-level domains that Switzerland is responsible for managing;

b. preserve the security and availability of the infrastructure and the services necessary for the operation of the domain name system (DNS);

c. ensure that Swiss law and the interests of Switzerland are respected during the management and use of the top-level domains that have an effect in Switzerland.

— Art. 2 Scope

[1] This Ordinance governs:

a. the country code Top-Level Domain [ccTLD]) ".ch" and its transpositions in other alphabets or graphic systems;

b. the generic Top-Level Domain [gTLD]) ".swiss";

c. the generic Top-Level Domains the management of which has been entrusted to Swiss public bodies other than the Confederation.
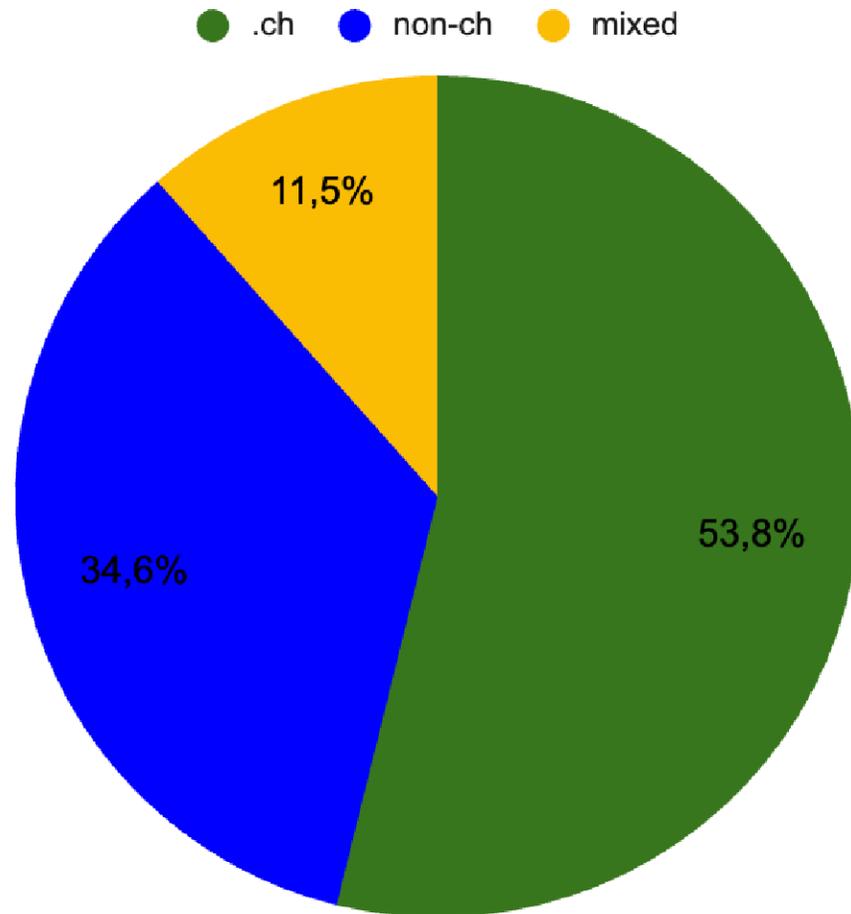
Market share of TLDs for Swiss Domain Holders

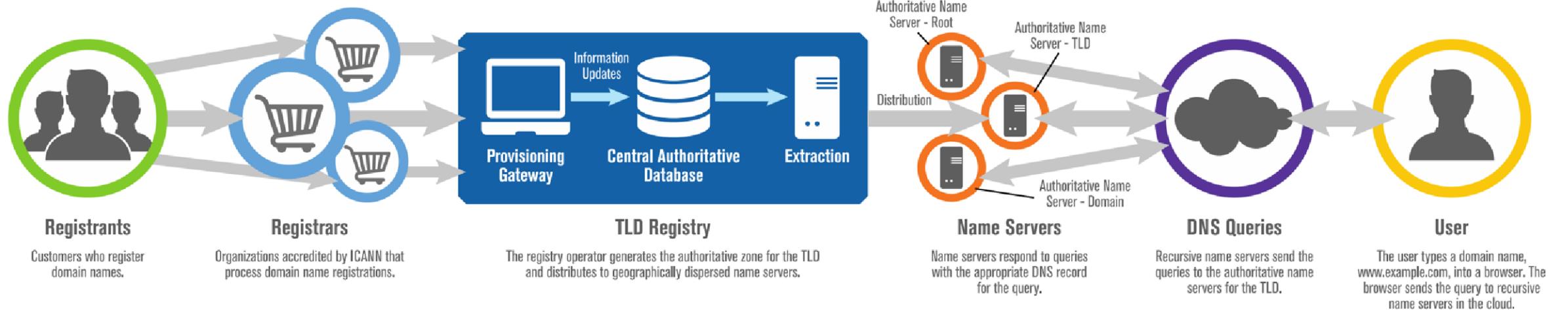Market share of various TLDs among Swiss holders
July 2025

other TLDs 5.2%
.it 0.4%
.uk 0.5%
.swiss 0.6%
.li 0.6%
.at 0.8%
.info 0.9%
.fr 1.5%
.org 2.5%
.de 2.7%
.net 2.8%
.com 23.0%
.ch 58.5%
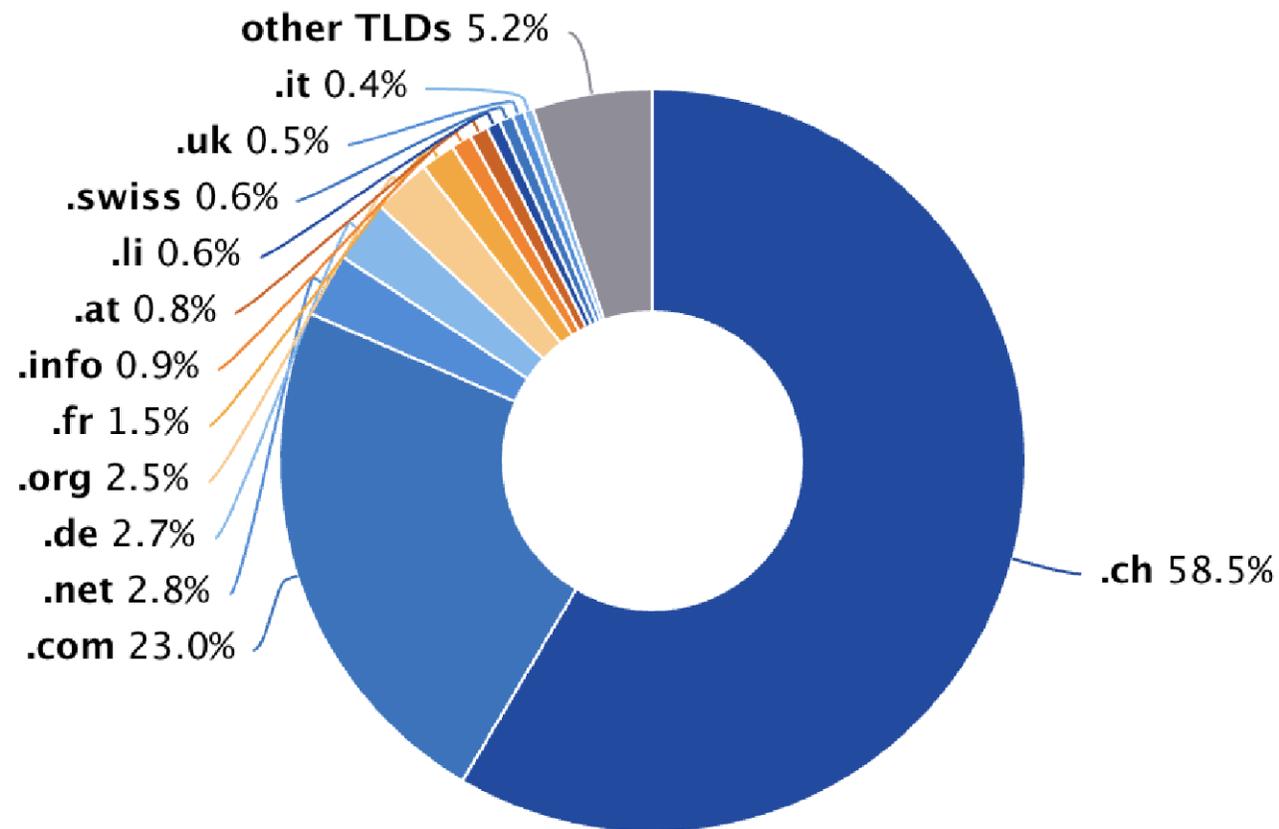
Source: centr.org

Cantons NS domains

Legend: ● .ch ● non-ch ● mixed

.ch	53,8%
non-ch	34,6%
mixed	11,5%

ag.ch	xdnsXX.ag.ch
ai.ch	Ip-plus.net
ar.ch	ns3-03.azure-dns.org. ns4-03.azure-dns.info. ns1-03.azure-dns.com. ns2-03.azure-dns.net.
be.ch	nsx.be.ch
bl.ch	nsa2.nts.ch.
bs.ch	ns1.bs.ch
fr.ch	pfrns01.fr.ch
ge.ch	nsc11.infomaniak.com, switch.ch
gl.ch	nsx.gl.ch
gr.ch	nsx.gr.ch
ju.ch	nsx.jura.ch.
lu.ch	ns1.sunrise.ch ns1.lu.ch
ne.ch	dns1.ne.ch, switch.ch
nw.ch	ns1.hoonix.com
ow.ch	ns1.hoonix.com
sg.ch	ns1.abxsec.com
sh.ch	dns1.ksd.ch, ns2.cablecom.net
so.ch	ns1.so.ch
sz.ch	ns-822.awsdns-38.net.
tg.ch	scsnms.switch.ch. ns1.ip-plus.net
ti.ch	ns1-01.ti.ch.
ur.ch	cns1.cloudpit.de, cns2.cloudpit.com, cns3.cloudpit.io
vd.ch	dnsx.vd.ch
vs.ch	nsx.vs.ch.
zg.ch	a.zg-ns.ch, a.zg-ns.net.
zh.ch	dnsx.swisscom.com

Switch

Appenzell Ausserrhoden (ar.ch)

The Relationship of Registries with the DNS Ecosystem

Registrants
Customers who register domain names.

Registrars
Organizations accredited by ICANN that process domain name registrations.

TLD Registry
The registry operator generates the authoritative zone for the TLD and distributes to geographically dispersed name servers.

Name Servers
Name servers respond to queries with the appropriate DNS record for the query.

DNS Queries
Recursive name servers send the queries to the authoritative name servers for the TLD.

User
The user types a domain name, www.example.com, into a browser. The browser sends the query to recursive name servers in the cloud.

Appenzell Ausserrhoden	Swizzonic Combell-Group	.ch (Switch)	Microsoft Verisign PIR Identity digital	Swisscom	Cyberstorm attendant
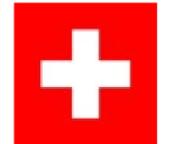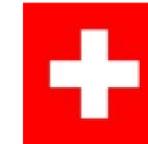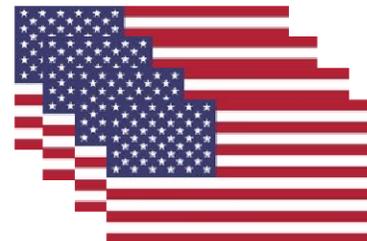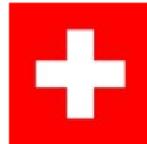
NS Dependence and DNSSEC

% dig ar.ch ns

;ar.ch. IN NS

;; ANSWER SECTION:
ar.ch. 273 IN NS ns3-03.azure-dns.org.
ar.ch. 273 IN NS ns4-03.azure-dns.info.
ar.ch. 273 IN NS ns1-03.azure-dns.com.
ar.ch. 273 IN NS ns2-03.azure-dns.net.

Multiple NS TLDs increase the attack surface
DNSSEC is a way to protect from DNS spoofing attacks

ar.ch
23 Oct 2025 11:13 UTC   ↻   Tweet

Domain Name System

✓ DNS Zone   ■
✓ DNS Records   ■
✓ DNSSEC   ■
✓ CAA   ■

52.4% of all .ch domains are singed with DNSSEC (Oct. 1)

Percentage of .ch domain names with DNSSEC

© Switch
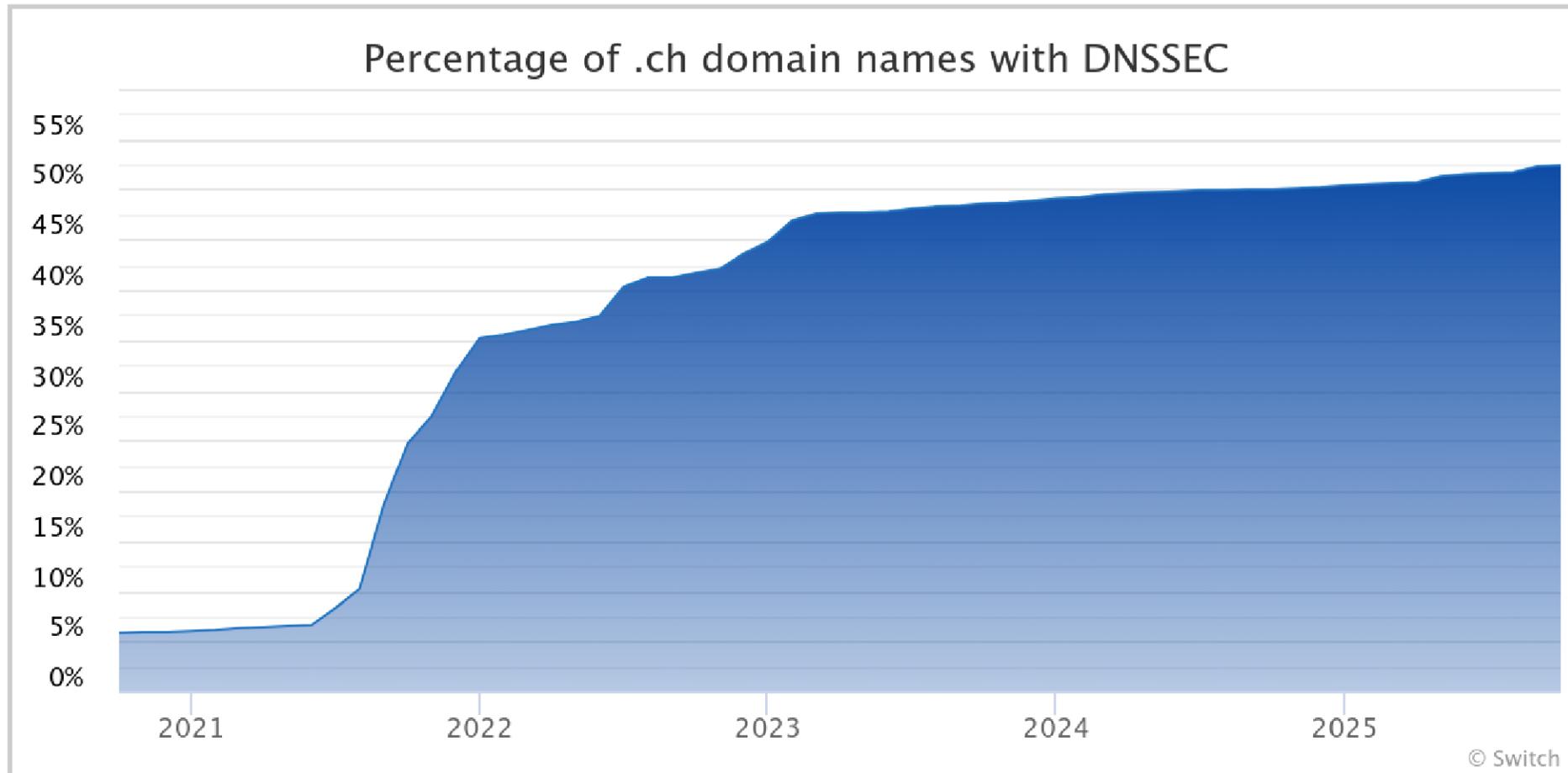
Industrial Dependencies

Switch

Authoritative DNS Service global market share

Rank	AS	Auth Srv Query Share	Cumulative	Name
1	AS16509	35.7%	35.7%	Amazon-O2, US
2	AS13335	9.3%	45.0%	Cloudflare, US
3	AS15169	8.3%	33.3%	Google, US
4	AS21342	4.0%	57.3%	Akamai, US
5	AS8068	3.9%	61.2%	Microsoft, US
6	AS397239	3.7%	64.9%	UltraDNS (Neustar), US
7	AS714	3.4%	68.3%	Apple, US
8	AS31898	3.1%	71.4%	Oracle, US
9	*	2.5%	73.9%	NXDOMAIN (Root Servers)
10	AS62597	2.5%	76.4%	NSone, US

Switch   Source: Apnic

Use of TLD & DNS Services by the 20 SMI Companies

TLD used

- .abb 5,0%
- .ch 30,0%
- .com 65,0%
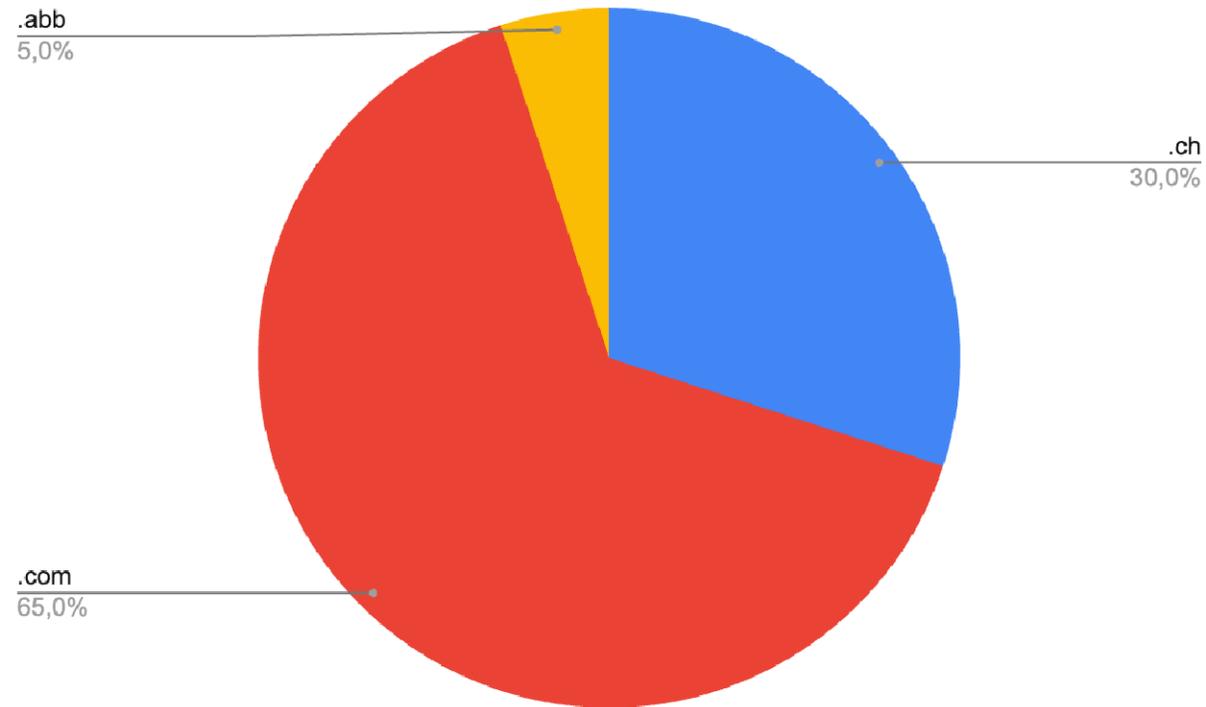
Authoritative Nameserver Operator

- UK 5,0%
- CH 15,0%
- US 80,0%

Switch

33

DNS Software

Recursive DNS in Switzerland

Recursive resolvers see all activities of the Internet users

Privacy & Security
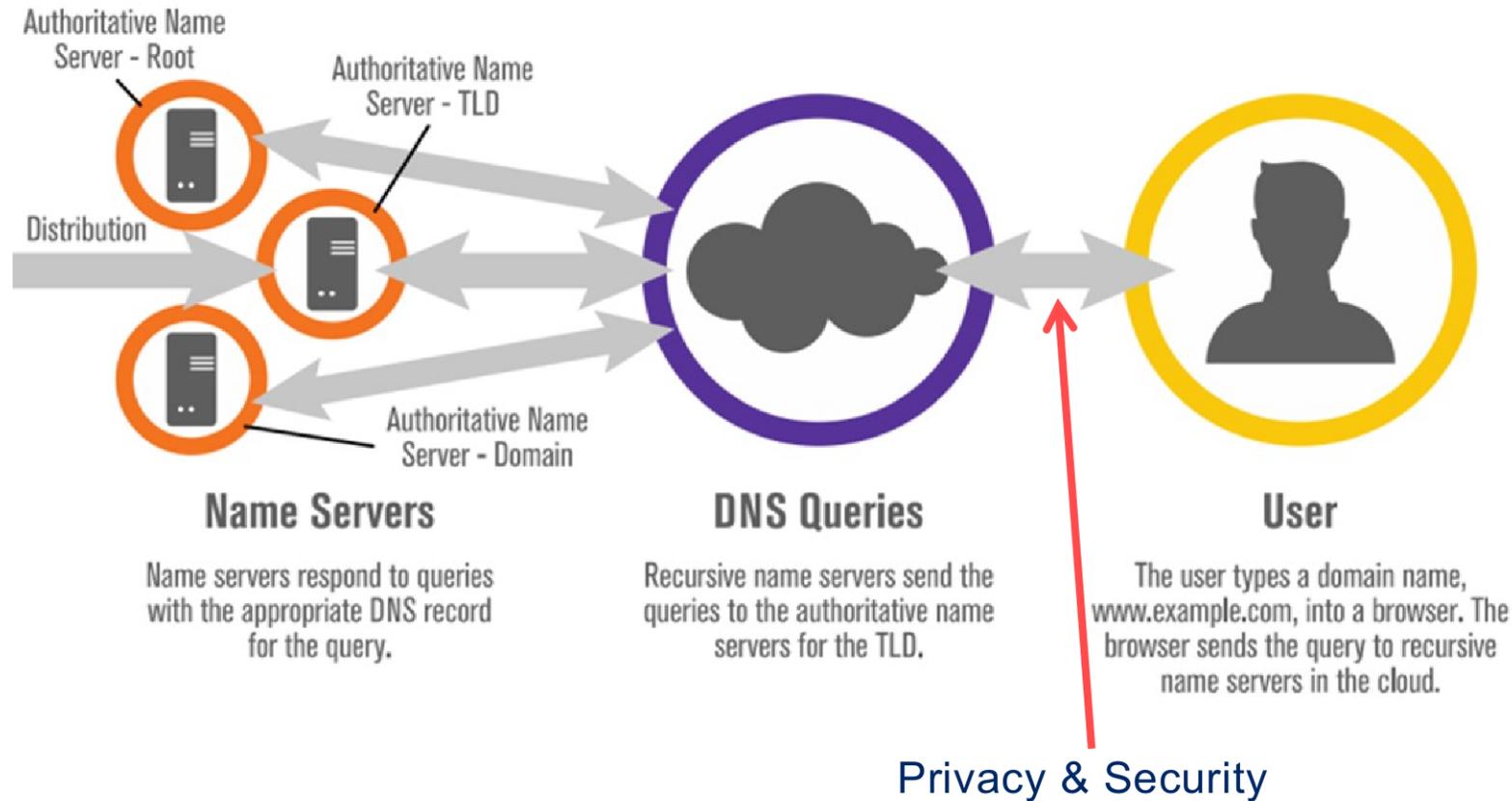
Where are the DNS Resolvers used in Switzerland?
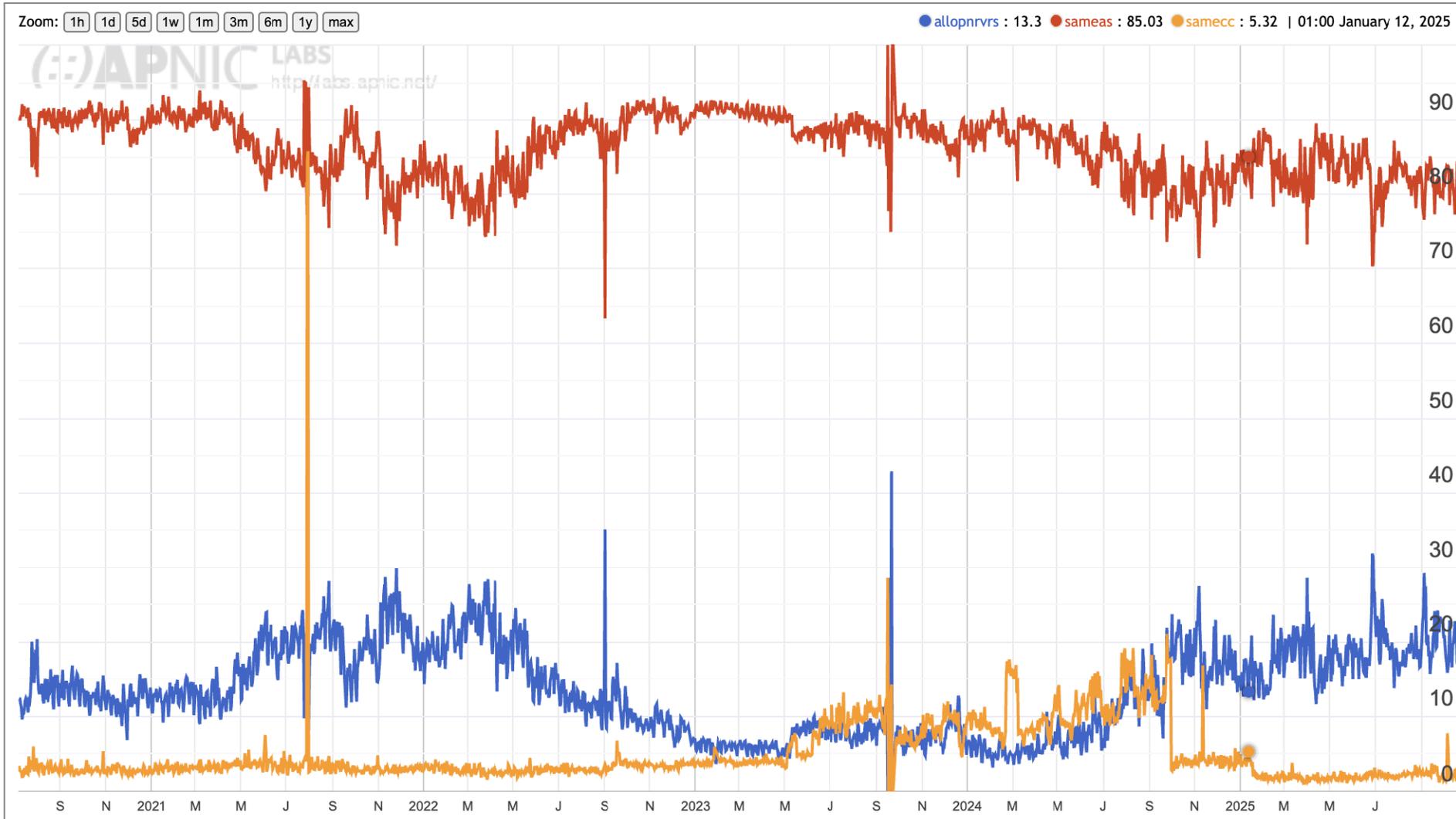
STOP!

[informations en français] [informazione in italiano]

Die von Ihnen aufgerufenen Internetseite enthält Geldspielangebote, die in der Schweiz nicht bewilligt sind. Es besteht keine Gewähr für eine sichere, transparente und sozialverträgliche Spielabwicklung. Der Zugang ist gemäss Art. 86 ff. des Bundesgesetzes über Geldspiele gesperrt.

Die folgenden Angebote sind von der Eidgenössischen Spielbankenkommission und von der interkantonalen Lotterie- und Wettkommission bewilligt. Die Erträge dieser Anbieter kommen ganz oder grösstenteils der Allgemeinheit (AHV, Kultur und Sport) zugute.

Bewilligte Angebote:

Lotterien und Sportwetten:
www.swisslos.ch
www.loro.ch

Spielbanken:
Es wurden Stand heute noch
keine Spielbewilligungen erteilt.

Weitere Auskünfte erhalten Sie auf den Internetseiten der beiden Aufsichtsbehörden:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Spielbankenkommission ESBK

comlot

Lotterie- und Wettkommission
Commission des loteries et paris
Commissione delle lotterie e delle scommesse
Swiss Lottery and Betting Board

www.esbk.admin.ch   www.comlot.ch

Switch

Protective DNS Resolvers – DNS Firewall

More security with the Switch DNS Firewall

https://www.switch.ch/en/dns-firewall
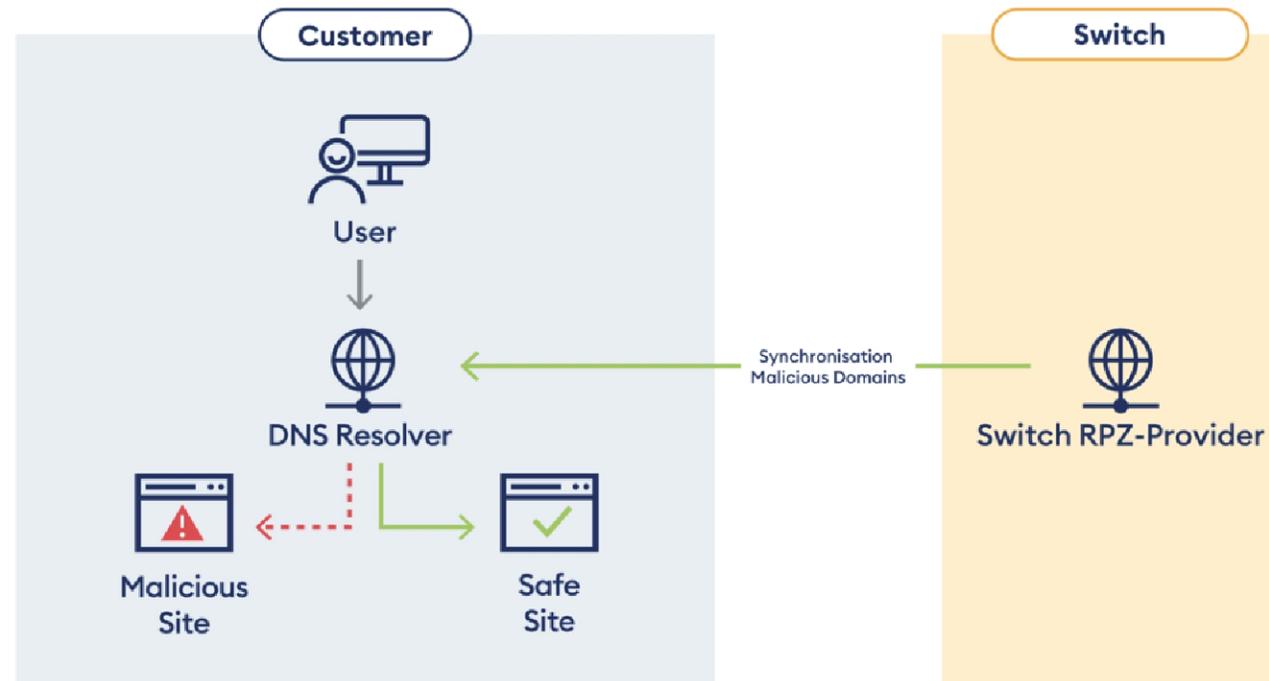
quad9

IPv4
9.9.9.9   **149.112.112.112**

IPv6
2620:fe::fe   **2620:fe::9**

More options ▶

An open DNS recursive service for free security and high privacy

Quad9 is a free service that replaces your default ISP or enterprise Domain Name Server (DNS) configuration. When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in addition to guaranteeing privacy. The Quad9 DNS service is operated by the Swiss-based Quad9 Foundation, whose mission is to provide a safer and more robust Internet for everyone.

Watch our short videos on how to set up Quad9 - Windows / MacOS ▶

670M+
Average Daily Blocks

230+
Resolver Clusters in over 110 countries

25+
Threat Intelligence Providers