Engineer

DNS

katalogen som gör ett namn till en adress

Vad det är

DNS, Domain Name System, är den distribuerade katalog som internet slår upp i innan nästan något annat händer. Ett program som har ett namn som `example.com` frågar den efter adressen att ansluta till, och samma system besvarar en handfull andra frågor om namnet: vilka servrar som tar emot dess e-post, vilken text ägaren har publicerat och vilka servrar som ansvarar för det.

Katalogen är ett träd som läses från höger till vänster. Överst sitter roten, under den toppdomäner som `.com` eller `.se`, under dem de domäner som människor registrerar, och under dem de underdomäner som ägarna skapar. Trädet är utspritt över många servrar. Varje nivå lämnar över ansvaret för nästa nivå nedåt till namngivna servrar, och den del av trädet som en uppsättning servrar svarar för kallas en zon. Den som styr en zon bestämmer vad dess namn pekar på.

Två slags servrar gör jobbet. Auktoritativa namnservrar håller en zon och svarar för den med sista ordet. Rekursiva resolvrar, som drivs av internetleverantörer, företag eller publika tjänster, går igenom trädet åt en klient: de frågar en rotserver var `.com` finns, frågar `.com` var `example.com` finns, frågar domänens egna servrar efter posten och lämnar tillbaka svaret. Ditt operativsystem kör bara en liten stubbresolver som skickar frågan vidare till en rekursiv resolver och väntar.

Svaren är poster av olika typer, och en zonfil är det klassiska sättet att skriva ned dem:

```
$ORIGIN example.com.
$TTL 3600
@     IN  SOA    ns1.example.net. hostmaster.example.com. (
                 2026101701 7200 900 1209600 300 )
```

```
@     IN  NS     ns1.example.net.
@     IN  A      192.0.2.10
@     IN  AAAA   2001:db8::10
www   IN  CNAME  example.com.
@     IN  MX     10 mail.example.net.
@     IN  TXT    "v=spf1 include:_spf.example.net -all"
```

`A` och `AAAA` anger IPv4- och IPv6-adresser. `CNAME` gör ett namn till ett alias för ett annat. `MX` pekar ut servern som tar emot e-post, och `TXT` bär fri text, vilket i praktiken betyder policyer för autentisering av e-post och bevis på att någon styr domänen. `NS` och `SOA` beskriver själva zonen.

Varje post har en livslängd, time to live eller TTL, här 3 600 sekunder, och det talet är nyckeln till hur DNS beter sig. En resolver som har hämtat ett svar får fortsätta återanvända det tills dess TTL har gått ut, utan att fråga igen. Resultatet är ett system som besvarar de flesta uppslag från en cache nära klienten och fortsätter svara när en auktoritativ server en kort stund är onåbar, till priset att ingen kan tvinga världen att glömma ett gammalt svar i förtid.

Använd begreppet i ett beslut

Använd ”Vad är DNS?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Wi-Fi, brandväggar och fjärråtkomst uppsatta så att personalen kan arbeta varifrån som helst och bara rätt personer kommer in.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Förvaltade 30 VPS-instanser med Ubuntu Linux — 30 förvaltade Linux-servrar, med en plan för återställning

Förvaltade 30 VPS-instanser med Ubuntu Linux Hör av er →

Varför det spelar roll

Varje anslutning till en namngiven tjänst börjar med ett uppslag. När DNS är fel kan servrarna vara helt friska och webbplatsen, API:t och e-posten ändå se nere ut, eftersom ingenting når fram till dem. När DNS är rätt märker ingen det, och därför brukar det vara den sämst dokumenterade delen av ett system.

DNS är också platsen där kontrollen över en domän utövas och bevisas. E-postleverantörer läser policyer för SPF, DKIM och DMARC ur `TXT` -poster för att avgöra om ett meddelande som påstår sig komma från din domän är äkta, så en felaktig eller saknad post skickar riktig e-post till skräpposten. Certifikatutfärdare och hostade tjänster ber om en post med ett visst värde som bevis på att du äger

namnet. Den som kan redigera zonen kan styra om webbplatsen, fånga upp e-posten och skaffa certifikat för domänen, vilket gör åtkomsten till DNS-kontot lika känslig som åtkomsten till servrarna.

Cachning formar varje ändring. Det som brukar kallas propagering är egentligen tusentals resolvrar som var och en väntar på att den egna kopian ska löpa ut. Sättet att flytta en webbplats med lite störning är att sänka TTL ungefär ett dygn i förväg, vänta tills den gamla TTL har passerat, göra ändringen och höja TTL igen när den har satt sig.

Klassisk DNS färdas i klartext, och både frågorna och svaren går att läsa längs vägen. DNSSEC låter en resolver kontrollera att ett svar verkligen kom från zonens ägare och inte har ändrats, och enligt sin egen specifikation tillför den ingen sekretess. Krypterade transporter som DNS over HTTPS döljer frågorna för nätverket på vägen, medan resolvern i andra änden fortfarande ser varje namn som efterfrågas. Att välja resolver är att välja vem som får den listan.

Så ser det ut i praktiken

Företagets egen zon visar den vanligaste utgångspunkten och en väg därifrån. Den höll ungefär tjugo poster i en leverantörs webbkonsol, som täckte webbnärvaron, en underdomän för git, två personliga omdirigeringar, e-post som gick via en leverantör av hostade e-postlådor, en avsändardomän för transaktionsmejl och autentiseringsposterna för båda. I en konsol är det nuvarande tillståndet det som den som senast klickade lämnade efter sig. Zonen är nu data i ett repo: aktiva poster, applikationsposter, poster för transportpolicy och en separat lista över poster som väntar på borttagning. En play stämmer av den deklarationen mot leverantörens API. Två ytterligare ingångar ligger bakom uttryckliga opt-in-taggar: en granskning som rapporterar skillnaden och lämnar zonen orörd, och en export som skriver ut zonen i det vanliga zonfilsformatet, så att något annat än repot kan läsa den. Granskningen är den del som används mest, eftersom det oftare är skillnaden man vill känna till än att stänga den.

Samma leverantör har ett medvetet smalt uppdrag. Webbplatsens kolofon förklarar att Cloudflare besvarar DNS för webbplatsen och bara DNS, utan någon proxy framför, och den skriver ut serverns adress rakt av, eftersom DNS redan lämnar ut den adressen till vem som helst som frågar.

Att läsa DNS hör också till den löpande beskrivningen av miljön. Bland sju rapportroller som bara läser och återger värddatorn i drift som Markdown finns en leverantörsinventering som läser DNS tillsammans med två moln-API:er och ett API för dedikerade servrar, under regeln att ingen rapport skriver ut ett tal som körningen inte har mätt.

Var det går fel

I DNS kommer felen ofta fördröjda, cachade eller delade, så att samma namn fungerar för en person och fallerar för en annan. Det här är de som återkommer.

En ändring tar tid på sig att slå igenom. Någon redigerar en post med en TTL på ett dygn och väntar sig att den nya adressen ska gälla direkt, men resolvrar som cachade det gamla svaret fortsätter lämna ut det tills deras kopia löper ut. En tystare variant drabbar nya namn: om ett namn slogs upp innan dess post fanns cachas även det negativa svaret, så länge som zonens `SOA` tillåter (RFC 2308). Sänk TTL före planerade ändringar, och skapa poster innan något frågar efter dem.

Ett alias står där det inte får stå. RFC 1034 säger att ett namn som har en `CNAME` inte får ha några andra data. Den nakna domänen, `example.com` själv, har alltid poster av typen `SOA` och `NS`, så en zon som följer standarden kan inte göra apex till ett alias, och en `CNAME` på en underdomän som också behöver poster av typen `MX` eller `TXT` bryter mot samma regel. Leverantörer erbjuder plattade poster eller `ALIAS`-poster som sin egen lösning; var och en beter sig lite olika, så läs vad din leverantör faktiskt levererar.

Autentiseringen av e-post välter. Varje `include` i en SPF-post ger upphov till uppslag i DNS, och RFC 7208 sätter taket för det totala antalet vid tio. Ytterligare en tjänst för nyhetsbrev eller ärendehantering kan trycka posten över gränsen, och mottagarna behandlar då policyn som ett permanent fel, så den e-post den skulle autentisera bedöms utan den. Räkna uppslagen varje gång en avsändare läggs till.

En post lever längre än sitt mål. En underdomän pekar med `CNAME` på en bucket i molnlagring eller en hostad app som sedan har tagits bort. Om leverantören låter vem som helst ta det resursnamnet kan en främling ta det och leverera eget innehåll under din underdomän, med din domäns rykte fastsatt. Ta bort posten i samma ändring som tar bort det den pekar på.

Zonen finns bara i en konsol. Historik, granskning och diff saknas då, så en oavsiktligt raderad `MX` -post upptäcks när e-posten slutar komma fram, och det tidigare värdet måste rekonstrueras ur minnet. Att exportera zonen regelbundet, eller ännu bättre deklarera den som kod, ger varje ändring ett spår och en väg tillbaka.

Läs mer

- RFC 1035: Domain Names, Implementation and Specification — postformaten, syntaxen för zonfiler och protokollet på tråden.
- RFC 1034: Domain Names, Concepts and Facilities — trädet, zonerna, delegeringen och hur resolvrar går igenom dem.
- RFC 9499: DNS Terminology — noggranna definitioner av orden som den här sidan använder.
- RFC 2308: Negative Caching of DNS Queries — hur länge en resolver får minnas att ett namn saknas.
- RFC 4033: DNS Security Introduction and Requirements — vad DNSSEC skyddar, och vad det lämnar orört.
- RFC 8484: DNS Queries over HTTPS — uppslag som färdas inuti vanlig krypterad webbtrafik.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är DNS?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/dns/