Engineer

Vert

en datamaskin koblet til et nettverk

Hva det er

En vert er en datamaskin i enden av en nettverksvei: maskinen trafikken er adressert til og kommer fra, i motsetning til ruterne og svitsjene som bare sender den videre. Det engelske ordet er host, og det brukes mye også på norsk. Ingeniører sier også *vertsmaskin*, kaller navnet den svarer på, for *vertsnavnet*, og snakker innen virtualisering om den fysiske verten som bærer gjestemaskiner. Å være *vert* for noe, slik et webhotell er vert for nettsteder, er å kjøre det på en slik maskin.

Internettets egen definisjon er fra oktober 1989. RFC 1122, kravdokumentet for internettverter, kaller en vertsdatamaskin, eller bare en vert, den endelige forbrukeren av kommunikasjonstjenester, en maskin som som regel kjører applikasjonsprogrammer på vegne av brukerne sine. Den tilsvarer det OSI-modellen kalte et endesystem. Nettverkene mellom vertene er koblet sammen av gateways, som i dag kalles rutere. Det samme dokumentet dekker alt fra verter med ett enkelt formål til verter med full tjeneste, og kaller en vert med mer enn ett nettverksgrensesnitt multihomed.

Grensen mellom vert og ruter trekkes ut fra oppførsel, ikke ut fra maskinvare. RFC 1122 sier at enhver vert som videresender datagrammer som en annen vert har laget, opptrer som en gateway, krever en bryter som slår gateway-funksjonen av, og krever at den bryteren står av som standard. En vert med to nettverksgrensesnitt holder seg derfor til sin egen trafikk helt til noen slår videresendingen på. En bærbar PC, en telefon, en skriver, en leid virtuell maskin og en container med egen adresse er alle verter.

NIST-ordlisten har to definisjoner side om side. Den ene regner med enhver maskinvareenhet som har en vei inn på et nettverk. Den andre, fra veiledning om sikring av webservere, sier at en server er en vert for klientene sine, og at en

klientstasjon også er en vert, fordi den er en kilde til informasjon for nettverket, i motsetning til en ruter eller svitsj som dirigerer trafikk. Det er den nyttige kontrasten til ordet server. En server er en rolle et program spiller, nemlig å svare på forespørsler. En vert er maskinen, enten den svarer noen eller ikke. Én vert kan kjøre mange servere, og en bærbar PC som ikke kjører en eneste server, er fortsatt en vert.

En vert samler på navn. Søsterdokumentet, RFC 1123, satte reglene for vertsnavn: det første tegnet kan være en bokstav eller et siffer, vertsprogramvare må håndtere navn på opptil 63 tegn og bør håndtere navn på opptil 255, og overalt der en bruker kan skrive inn navnet til en vert, bør det også gå an å skrive inn adressen i desimal punktnotasjon. I tillegg kan DNS peke et hvilket som helst antall navn mot én adresse, og HTTP lar en klient si hvilket av dem den vil ha, i `Host` -feltet i hver forespørsel, så én vert kan svare for mange nettsteder.

Bruk begrepet i en beslutning

Bruk «Hva er en vert?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Servere dimensjonert etter det du faktisk bruker, flyttet inn i skyen eller ut av den igjen, med månedsregningen regnet ut på forhånd.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Driftet 20 Docker-apper på Google Cloud og AWS — 20 containeriserte applikasjoner produksjonssatt og overvåket

Driftet 20 Docker-apper på Google Cloud og AWS Ta kontakt →

Hvorfor det er viktig

Verten er enheten driften teller i. Inventarlister ramser opp verter, overvåkingen følger med på verter, brannmurregler og tilgangslister navngir dem, og skyleverandører fakturerer dem per time eller per måned. En plan som sier «legg til en vert», er konkret på en måte «legg til kapasitet» ikke er: den betyr én maskin til som skal opprettes, navngis, patches, sikkerhetskopieres og betales for.

Verten er også enheten et innbrudd måles i. Den som kontrollerer en vert, kontrollerer hvert serverprogram på den, hver nøkkel som ligger på disken, og hver forbindelse den kan åpne. Det en vert holder på, bestemmer hva det koster å miste den, og derfor avgjør nøye operatører per vert hvilke hemmeligheter, hvilke data og hvilke nettverksveier den får, og gir den ikke mer enn det.

Og verten er der navnene møtes. Den samme maskinen er kjent under navnet i inventaret, navnet den kaller seg selv, DNS-navnene som peker mot adressen, og navnene i forespørslene den tar imot. Når de stemmer overens, fører en logglinje, et driftsvarsel og en supportsak til den samme boksen. Når de glir fra hverandre, bruker den som blir tilkalt om natten, de første minuttene av driftshendelsen på å finne maskinen.

Slik ser det ut i praksis

Driftsarbeidet bak dette nettstedet behandler verten som det som skal bygges fra kode og få sine egne hemmeligheter. Da plattformen trengte en maskin nummer to hos en annen leverandør, ble svaret at vert nummer to opprettes, eller tas over på nytt, fra repoet. Den første maskinen var laget for hånd og hadde fått brannmuren sin etterpå, noe som etterlater et vindu der en fersk vert med en standard passordpolicy kan nås fra internett. Rollen som oppretter den andre, tar over en eksisterende maskin i stedet for å duplisere den, så det er trygt å kjøre den på nytt, og rollens egen fil oppgir instanstypen, regionen, spesifikasjonen og den månedlige kostnaden i euro, fordi det er den ene rollen i repoet som bruker penger.

Overgangen fra én vert til to avslørte deretter hver verdi som var skrevet ut fra antakelsen om at det aldri ville bli mer enn én. Hver driftshemmelighet ble en oppslagstabell med verten som nøkkel. Siden forklarer hvorfor deling var feil på to måter. En dødmannsknapp som deles av to verter, varsler mindre enn to knapper, ikke mer: så lenge én av vertene fortsatt melder seg, holder knappen seg grønn mens den andre er død. Og en felles passordfrase for sikkerhetskopier knytter vertenes eksponering sammen. Separate restic-repoer kan ha forskjellige hovednøkler selv om de bruker samme passfrase, men den som får tak i den og kan lese de krypterte dataene og nøkkelfilene i begge repoene, kan låse opp begge. Den eksisterende verten ble ført opp i alle fire tabellene med sikkerhetskopirepoet sitt og begge knappene stående tomme, og det kaller siden den sannferdige tilstanden.

Fra en besøkendes side betyr ordet noe mindre: et navn nettleseren kontakter. Sikkerhetssiden ber leseren om å åpne nettverkspanelet i nettleseren og telle vertene, og sier at det er én, og at den er nettstedets egen.

Hvor det går galt

En vert begynner å videresende trafikk den bare skulle ta imot. Containernettverk og VPN-programvare slår på IP-videresending, og fra da av ruter verten mellom grensesnittene sine. Dokumentasjonen til Docker, for å ta ett eksempel, sier at Docker slår på begge innstillingene nedenfor når den starter, og deretter forkaster videresendte pakker med mindre en regel godtar dem. Der videresending er slått på uten en slik regel, lar brannmurregler som er skrevet for trafikk adressert til verten, trafikken som passerer gjennom den, være i fred, og et nettverk bak verten blir nåbart via en vei ingen har tegnet. Les bryterne, og skriv regler for videresending med vilje der de står på `1`:

```
sysctl net.ipv4.ip_forward net.ipv6.conf.all.forwarding
```

Navnene er uenige. Inventaret sier én ting, maskinen kaller seg det leverandørens image valgte, DNS har et tredje navn og TLS-sertifikatet et fjerde. Hvert driftsvarsel bærer da navnet ingen bruker. Hent maskinens eget vertsnavn fra den samme kilden som inventaret og DNS-postene, og sett det når verten opprettes, i stedet for når noen legger merke til det.

En server svarer på hvilket som helst vertsnavn den får. `Host`-feltet kommer fra klienten, og en server som svarer på ukjente navn med et standardnettsted, bygger lenker, omdirigeringer og bufrede sider ut fra et navn en angriper har valgt. RFC 9110 advarer om at feltet er et hyppig mål for skadevare som prøver å forgifte en delt hurtigbuffer eller sende en forespørsel videre til en server den aldri var ment for. Svar bare på navnene verten faktisk betjener, avvis resten, og bygg absolutte lenker ut fra konfigurasjonen i stedet for ut fra forespørselen.

Klonede verter deler identitet. En maskin som er kopiert fra et image, bærer med seg det imaget inneholdt: SSH-vertsnøkler, tokener, noen ganger en passordfrase for sikkerhetskopier. Klientene kan da ikke lenger skille kopiene fra hverandre, og én lekkasje åpner hver eneste kopi. Generer vertsnøkler ved første oppstart, hold hemmeligheter utenfor imagene, og gi hver vert sin egen oppføring overalt der en hemmelighet konfigureres.

Les mer

- host — NIST CSRC Glossary — begge definisjonene, også den som stiller verter opp mot rutere og svitsjer.

- RFC 1122: Requirements for Internet Hosts, Communication Layers — definisjonen av en vert fra 1989, multihoming og videresending som er slått av som standard.
- RFC 1123: Requirements for Internet Hosts, Application and Support — reglene for vertsnavn og lengdene deres, i avsnitt 2.1.
- RFC 9110, HTTP Semantics: Host and :authority — hvordan én server skiller mange vertsnavn fra hverandre, og hvorfor feltet er et mål for angrep.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er en vert?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/host/