Engineer

Värddator

en dator som är ansluten till ett nätverk

Vad det är

En värddator är en dator i änden av en väg genom nätverket: den maskin som trafiken är adresserad till och kommer ifrån, till skillnad från de routrar och switchar som bara skickar den vidare. Ingenjörer säger också *värd* eller *värdmaskin*, kallar det namn som den svarar på för dess *värdnamn* och talar inom virtualisering om den fysiska värd som bär gästmaskinerna. Att vara värd för något, som när ett webbhotell driver en webbplats, är att köra det på en sådan maskin.

Internets egen definition är från oktober 1989. RFC 1122, kravdokumentet för internetvärdar, kallar en värddator, eller bara värd, för den slutliga konsumenten av kommunikationstjänster, en maskin som i allmänhet kör applikationsprogram åt sina användare. Den motsvarar det som OSI-modellen kallade ett slutsystem. Näten mellan värdarna är sammankopplade av gateways, som i dag kallas routrar. Samma dokument täcker allt från värdar med ett enda syfte till värdar som erbjuder full service, och kallar en värd med mer än ett nätverksgränssnitt för multihomed.

Den gränsen mellan värd och router dras utifrån beteende, inte utifrån hårdvara. RFC 1122 säger att varje värd som vidarebefordrar datagram som en annan värd har skapat agerar som gateway, kräver en brytare som stänger av gateway-funktionen och kräver att den brytaren som standard står i läget av. En värd med två nätverksgränssnitt börjar därför fortfarande inte vidarebefordra trafik på egen hand. En bärbar dator, en telefon, en skrivare, en hyrd virtuell maskin och en container med en egen adress är alla värdar.

NIST:s ordlista håller två definitioner sida vid sida. Den ena räknar in varje hårdvaruenhet som har en väg in i ett nätverk. Den andra, från vägledning om att säkra webbservrar, säger att en server är en värd för sina klienter och att en

klientstation också är en värd, eftersom den är en informationskälla för nätverket, till skillnad från en router eller switch som styr trafiken. Det är den användbara kontrasten till ordet server. En server är en roll som ett program spelar, nämligen att besvara förfrågningar. En värd är maskinen, oavsett om den svarar någon eller inte. En värd kan köra många servrar, och en bärbar dator som inte kör någon är fortfarande en värd.

En värd samlar på sig namn. Systerdokumentet, RFC 1123, satte reglerna för värdnamn: det första tecknet får vara en bokstav eller en siffra, mjukvara på en värd måste klara namn på upp till 63 tecken och bör klara namn på upp till 255, och varhelst en användare kan skriva in en värds namn bör det också fungera att skriva in dess adress i punktdecimal form. Ovanpå det kan DNS peka hur många namn som helst mot en och samma adress, och HTTP låter en klient säga vilket av dem den vill ha i fältet `Host` i varje förfrågan, så att en enda värd kan svara för många webbplatser.

Använd begreppet i ett beslut

Använd ”Vad är en värddator?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Servrar dimensionerade efter vad du faktiskt använder, flyttade till molnet eller tillbaka ut ur det, med månadskostnaden uträknad först.

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. Drev 20 Docker-appar på Google Cloud och AWS — 20 containerbaserade applikationer, driftsatta och övervakade

Drev 20 Docker-appar på Google Cloud och AWS Hör av er →

Varför det spelar roll

Värden är den enhet som driften räknar i. Inventarier listar värdar, övervakning bevakar värdar, regler i brandväggar och åtkomstlistor namnger dem, och molnleverantörer fakturerar dem per timme eller per månad. En plan som säger ”lägg till en värd” är konkret på ett sätt som ”lägg till kapacitet” inte är: den betyder ytterligare en maskin att skapa, namnge, patcha, säkerhetskopiera och betala för.

Den är också den enhet som intrång sker i. Den som kontrollerar en värd kontrollerar varje serverprogram på den, varje nyckel som ligger på dess disk och varje anslutning som den kan öppna. Det en värd bär på avgör vad det kostar att förlora den, och det är därför noggranna operatörer bestämmer för varje värd vilka hemligheter, vilka data och vilka vägar genom nätverket den får, och ger den inte mer än så.

Och det är där namnen möts. Samma maskin är känd under namnet i inventariet, det namn den kallar sig själv, de namn i DNS som pekar mot dess adress och namnen i de förfrågningar den tar emot. När de stämmer överens leder en loggrad, ett larm och ett supportärende till samma låda. När de glider isär ägnar den som blir väckt på natten de första minuterna av incidenten åt att leta upp maskinen.

Så ser det ut i praktiken

Webbplatsens driftarbete behandlar värden som det som ska byggas från kod och få sina egna hemligheter. När plattformen behövde en andra maskin hos en annan leverantör blev det så att den andra värden skapas, eller tas över på nytt, från repot. Den första maskinen hade skapats för hand och fått sin brandvägg i efterhand, vilket lämnar ett fönster där en ny värd med en standardpolicy för lösenord är nåbar från internet. Rollen som skapar den andra tar över en befintlig maskin i stället för att duplicera den, så att det är säkert att köra den igen, och dess egen fil anger instanstypen, regionen, specifikationen och månadskostnaden i euro, eftersom det är den enda rollen i repot som kostar pengar.

Att gå från en värd till två blottlade sedan varje värde som hade skrivits under antagandet att det bara skulle finnas en. Varje operativ hemlighet blev en mappning med värden som nyckel. Sidan beskriver varför delning var fel på två sätt. Ett dödmansgrepp som delas av två värdar larmar mindre än två grepp, inte mer: så länge någon av värdarna fortfarande hör av sig förblir det grönt medan den andra är död. Och en gemensam lösenfras för säkerhetskopior innebär en gemensam risk vid en läcka. Separata restic-repon kan ha olika huvudnycklar även om de använder samma lösenfras, men den som får tag på den och kan läsa båda reponas krypterade data och nyckelfiler kan låsa upp båda. Den befintliga värden namngavs i alla fyra mappningarna med sitt repo och båda greppen lämnade tomma, vilket sidan kallar det sanningsenliga tillståndet.

Från en besökares sida betyder ordet något mindre: ett namn som webbläsaren kontaktar. Säkerhetssidan uppmanar läsaren att öppna webbläsarens nätverkspanel och räkna värdarna, och säger att det finns en, och att den är webbplatsens egen.

Var det går fel

En värd börjar vidarebefordra trafik som den bara skulle ta emot. Nätverk för containrar och mjukvara för VPN slår på vidarebefordran av IP-paket, och från den stunden routar värden mellan sina gränssnitt. Dockers dokumentation, för att ta ett exempel, säger att Docker slår på båda inställningarna nedan när den startar och sedan kastar vidarebefordrade paket om inte en regel accepterar dem. Där vidarebefordran är påslagen utan en sådan regel lämnar brandväggsregler som skrivits för trafik adresserad till värden den trafik som passerar genom den orörd, och ett nätverk bakom den blir nåbart via en väg som ingen har ritat. Läs av brytarna, och skriv regler för vidarebefordran med avsikt varhelst de står på `1`:

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

Namnen stämmer inte överens. Inventariet säger en sak, maskinen kallar sig vad leverantörens avbild än valde, DNS har ett tredje namn och TLS-certifikatet ett fjärde. Varje larm bär då det namn som ingen använder. Hämta maskinens eget värdnamn från samma källa som inventariet och posterna i DNS, och sätt det när värden skapas i stället för när någon lägger märke till det.

En server svarar på vilket värdnamn den än får. Fältet `Host` kommer från klienten, och en server som besvarar okända namn med en standardwebbplats bygger länkar, omdirigeringar och cachade sidor från ett namn som en angripare har valt. RFC 9110 varnar för att fältet är ett vanligt mål för skadlig kod som försöker förgifta en delad cache eller omdirigera en förfrågan till en server den inte var avsedd för. Svara bara på de namn som värden faktiskt betjänar, avvisa resten och bygg absoluta länkar från konfigurationen i stället för från förfrågan.

Klonade värdar delar identitet. En maskin som kopieras från en avbild bär med sig allt som avbilden innehöll: värdnycklar för SSH, token, ibland en lösenfras för säkerhetskopior. Klienterna kan då inte längre skilja kopiorna åt, och en enda läcka öppnar varje kopia. Generera värdnycklar vid första uppstarten, håll hemligheter utanför avbilderna och ge varje värd en egen post överallt där en hemlighet konfigureras.

Läs mer

- host — NIST CSRC Glossary — båda definitionerna, inklusive den som ställer värdar mot routrar och switchar.
- RFC 1122: Requirements for Internet Hosts, Communication Layers — definitionen av en värd från 1989, multihoming och vidarebefordran som är avstängd som standard.
- RFC 1123: Requirements for Internet Hosts, Application and Support — reglerna för värdnamn och deras längd, i avsnitt 2.1.
- RFC 9110, HTTP Semantics: Host and :authority — hur en server skiljer många värdnamn åt, och varför fältet är ett mål.

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 en värddator?” 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/host/