Engineer

virtuel maskine

en hel computer, der kører i software på en fysisk vært

Hvad det er

En virtuel maskine stiller en hel computer til rådighed gennem software: processorer, hukommelse, diske og netværkskort, som leveres af et virtualiseringslag på en fysisk vært, og som et styresystem starter på, som om de var dedikeret hardware. Den forkortes ofte VM. Nogle enheder kan gives direkte videre fra værten i stedet for at blive emuleret. NIST's vejledning om fuld virtualisering, SP 800-125, definerer den på én linje som et simuleret miljø skabt ved virtualisering. I den form for virtualisering, vejledningen handler om, kører et eller flere styresystemer med deres programmer på virtuel hardware, hvert i sin egen VM, hvor det kaldes et gæstestyresystem.

To ord bærer det meste af arbejdet. Den rigtige maskine er værten, og hver virtuel maskine på den er en gæst. Programmet, der fordeler værten mellem gæsterne, er hypervisoren, også kaldet virtual machine monitor, som SP 800-125 beskriver som den komponent, der styrer gæsternes styresystemer på en vært og kontrollerer strømmen af instruktioner mellem dem og den fysiske hardware: processor, diske, hukommelse og netværkskort. Samme vejledning peger på de to ting, der gør ordningen nyttig. Hypervisoren kan dele værtens ressourcer op, så hver gæst får adgang til sine tildelte ressourcer og de ressourcer, der udtrykkeligt er delt, og en gæst kan pakkes helt ind, så den kan flyttes fra én vært til en anden.

En virtuel maskine adskiller sig fra en container ved, hvor grænsen går. En container er en proces på værtens kerne med et begrænset udsyn over systemet. En virtuel maskine starter sin egen kerne på hardware, som hypervisoren stiller til rådighed. Derfor kan en Linux-gæst køre på en vært med Windows eller macOS, og derfor har hver gæst også brug for sit eget styresystem, som skal installeres, opdateres og have hukommelse nok til at køre.

Brug begrebet i en beslutning

Brug »Hvad er en virtuel maskine?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Servere dimensioneret efter det, I rent faktisk bruger, flyttet op i skyen eller hjem igen, med den månedlige regning regnet ud først.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har drevet 20 Docker-apps på Google Cloud og AWS — 20 containeriserede applikationer udrullet og overvåget

Har drevet 20 Docker-apps på Google Cloud og AWS Kontakt os →

Hvorfor det betyder noget

En server, man lejer hos en cloududbyder, er typisk en virtuel maskine, og infrastructure as a service er bygget på dem. Udbyderen driver hypervisorerne og den fysiske maskinpark; kunden får maskiner, der kan oprettes, gøres større eller mindre og nedlægges gennem et API i stedet for at blive bestilt, leveret og monteret i et rack. Hardwaren forbliver en andens problem, mens styresystemet bliver kundens.

Den anden grund er isolation. KVM-projektets side siger, at hver virtuel maskine har sin egen private virtualiserede hardware: netværkskort, disk, grafikkort og så videre. Gæsterne deler ingen kerne, så et kernenedbrud eller en dårlig opdatering i én gæst bliver i den gæst, og det er hypervisoren, ikke gæsterne, der afgør, hvad der når den fysiske hardware. To kunder, eller to miljøer hos samme kunde, kan dele en fysisk maskine uden at dele styresystem.

For det tredje kan en maskine med imagebaseret lagring blive til en samling filer. En gæsts disk kan være en imagefil på værten, som kan kopieres, gemmes som skabelon eller bruges til at starte flere ens maskiner. QEMU's qcow2-format kan nøjes med at registrere forskellene fra et basisimage og kan gemme snapshots af disken i samme fil, så ét skabelonimage plus et tyndt lag pr. gæst er en naturlig opbygning.

For det fjerde lader emulering programmer, der er bygget til én processorfamilie, køre på en anden. QEMU's systememulering stiller en virtuel model af en maskine til rådighed, med processor, hukommelse og enheder, som et gæstestyresystem kan køre på. Med en accelerator, for eksempel KVM på Linux, Hypervisor Framework på macOS eller Windows Hypervisor Platform på Windows, klarer værtsprocessorens understøttelse af virtualisering det tunge

arbejde. Uden en accelerator oversætter QEMU's Tiny Code Generator gæstens instruktioner i software, og det er sådan, eksemplet i QEMU's egen introduktion starter en Arm64-maskine med `-accel tcg`.

Prisen er, at hver gæst er en hel computer, der skal passes. Hver har sit eget styresystem, der skal opdateres, sin egen reserverede hukommelse og sin egen opstart. Containere slipper for det ved at dele værtens kerne, hvilket gør hver enkelt lettere, men opgiver en separat kerne som væg mellem arbejdsbelastningerne. At vælge mellem de to er at vælge, hvor den væg skal stå.

Sådan ser det ud i praksis

På x86-Linux er det sædvanlige par KVM og QEMU. KVM er kernedelen: et indlæseligt modul, `kvm.ko`, med en processorspecifik makker, `kvm-intel.ko` eller `kvm-amd.ko`, og det har været med i den officielle Linux-kerne siden version 2.6.20. Det kræver processorens udvidelser til virtualisering, Intel VT eller AMD-V. KVM's FAQ leder efter deres flag, `vmx` og `svm`, i `/proc/cpuinfo`, og dens fejlsøgningsliste omfatter at bekræfte, at `/dev/kvm` findes, og at brugeren har rettigheder til at åbne den:

```
grep -E -c '^flags.*(vmx|svm)' /proc/cpuinfo
ls -l /dev/kvm
```

Et tal over nul betyder, at processoren melder udvidelserne. QEMU er brugerrumsdelen, som bygger maskinen op omkring KVM. Disken til en ny gæst kan være et tyndt lag oven på et fælles basisimage:

```
qemu-img create -f qcow2 -b debian-base.qcow2 -F qcow2 web1.qcow2
qemu-img info --backing-chain web1.qcow2
```

Manualen til qemu-img siger, at et image, der oprettes oven på et basisimage, kun registrerer forskellene fra det, og at basisimaget aldrig ændres, medmindre forskellene skrives tilbage i det med `qemu-img commit`. Den anden kommando viser hver fil i kæden, og den er værd at læse, før noget flyttes eller slettes. Selve opstarten af gæsten ser sådan ud:

```
qemu-system-x86_64 -accel kvm -m 2G -smp 2 \
    -drive file=web1.qcow2,if=virtio,format=qcow2 \
    -nographic
```

`-accel kvm` overlader processorarbejdet til KVM, som standard gennem `/dev/kvm`. `-m` sætter gæstens hukommelse og `-smp` dens antal processorer. På `-drive` kobler `if=virtio` disken på virtio-grænsefladen, en af de grænsefladetyper, manualen nævner, og `format=qcow2` angiver formatet i stedet for at lade QEMU finde frem til det. `-nographic` slår det grafiske vindue fra, så QEMU bliver et rent kommandolinjeprogram med gæstens serielle konsol i terminalen, delt med QEMU-monitoren; Ctrl-a h viser, hvordan man skifter mellem de to.

Mens gæsten er lukket ned, tager og gendanner det samme værktøj snapshots af disken. `-c` opretter et, `-l` viser dem, og `-a` sætter disken tilbage til en gemt tilstand:

```
qemu-img snapshot -c before-upgrade web1.qcow2
qemu-img snapshot -l web1.qcow2
qemu-img snapshot -a before-upgrade web1.qcow2
```

Dimensionering er en designbeslutning og ikke et felt i en formular. Porteføljeindlægget om at køre virksomhedens offentligt tilgængelige tjenester på én lille server dokumenterer en opsætning fra september 2026 med én processorkerne, en disk på 10 GB og 512 MB hukommelse, hvoraf programmerne kan bruge cirka 464 MB. Værten leverer syv domæner over TLS og kører desuden git-forgen, mens automatisering af sikkerhedskopiering er implementeret separat; hukommelsen er den grænse, som hvert designvalg dér retter sig efter. Om den også kunne klare en onion-tjeneste på Tor, blev afgjort ud fra et registreret døgns stikprøver, hvor den laveste aflæsning af tilgængelig hukommelse lå på cirka 310 MB. Hver gæsts `-m` -indstilling stiller det samme spørgsmål, og en måling besvarer det bedre end et større abonnement.

Indlægget om administration af tredive Ubuntu Linux-VPS-instanser viser den anden ende af skalaen. Instanserne var sat op lidt ad gangen gennem årene, uden nogen plan, og konfigurationerne var gledet fra hinanden. Siden blev de drevet som én samlet maskinpark: én hærdet netværkskonfiguration på hver instans og gendannelser, der blev afprøvet frem for at blive taget for givet.

Hvor det går galt

Det meste besvær med virtuelle maskiner kommer af at glemme, at hver enkelt er en rigtig computer, der skal passes, og at en imagebaseret disk også er en almindelig fil på en anden maskine.

KVM mangler, når gæsten starter. I x86-opsætningen ovenfor forhindrer manglende processorudvidelser eller udvidelser, der er slået fra i firmwaren, KVM-acceleration, og `/dev/kvm` kan mangle, så en gæst, der startes med `-accel kvm`, stopper med det samme. KVM's FAQ advarer om, at nogle producenter slår VT fra i BIOS på en måde, så det ikke kan slås til igen. Løsningen er at køre flagtjekket ovenfor, lede efter en indstilling i firmwaren, der slår virtualisering til, og bekræfte, at `/dev/kvm` findes og tilhører en gruppe, brugeren er med i; FAQ'en foreslår en gruppe ved navn `kvm`.

En gæst uden angivet hukommelse får 128 MiB. Det er QEMU's standard for `-m`, og den gælder, uanset hvor meget værten har ledigt, så en gæst kan starte og derefter fejle på måder, der ligner fejl i softwaren inde i den. Løsningen er altid at sætte `-m` og `-smp` og dimensionere dem ud fra målinger, sådan som indlægget om den lille server afgjorde spørgsmålet om onion-tjenesten med en dags målinger.

Et image, der ændres, mens gæsten kører, kan blive ødelagt. Manualen til qemu-img er ligefrem: brug den aldrig til at ændre et image, som en kørende virtuel maskine eller en anden proces bruger, for det kan ødelægge imaget. At tage et snapshot af en kørende gæsts disk med `qemu-img snapshot -c` er netop det. Løsningen er at lukke gæsten ned, før qemu-img rører dens disk, og at skrive det ind som et trin i hver driftsvejledning, der gør det.

Snapshots bruges som backup. Snapshots lavet med qemu-img ligger i den samme imagefil, hvilket `qemu-img info` viser ved at liste dem sammen med disken. Når filen går tabt eller bliver beskadiget, forsvinder alle snapshots med den. Løsningen er at kopiere sikkerhedskopier til lagring på en anden maskine og at teste gendannelsen, for en gendannelse, der aldrig er kørt, beviser ingenting.

Et basisimage ændres eller flyttes under sine overlays. Et tyndt image indeholder kun forskelle, så det er meningsløst uden præcis det basisimage, det blev lavet ud fra. Manualen advarer om, at hvis man skifter basisfil i usikker tilstand og vælger den forkerte fil, bliver det indhold, gæsten ser, ødelagt, og en relativ sti til basisimaget slås op fra overlayets egen mappe, så flytter man den

ene fil uden den anden, knækker kæden. Løsningen er at behandle basisimages som skrivebeskyttede og give hver ny version et nyt navn, at læse `qemu-img info --backing-chain`, før noget flyttes, og kun at køre `qemu-img commit` med vilje, da den skriver ind i basisimaget og tømmer overlayet.

Diskformatet gættes ud fra selve imaget. Uden `format=` udleder QEMU formatet af filens indhold, og manualen anbefaler `format=raw` for at undgå at fortolke en formatheader, man ikke kan stole på. Et image hentet et andet sted fra, eller et, som en gæst har skrevet i, er netop den slags. Løsningen er at angive formatet på hver `-drive` -linje.

Hver gæst glider over i at blive et kæledyr. Maskiner, der konfigureres i hånden, glider fra hinanden én ændring ad gangen, indtil der ikke er to, der er ens, og det var der, VPS-flåden ovenfor stod, før den kom under styring. Løsningen er at bygge hver gæst ud fra det samme image og den samme konfiguration, holde konfigurationen i versionsststyring og styre maskinerne som én flåde med én baseline.

Læs mere

- Guide to Security for Full Virtualization Technologies (NIST SP 800-125) — definitionen af en VM, hypervisorens opgave og adskillelsen af gæster.
- KVM — projektsiden: moduler, processorudvidelser og første kerneversion.
- KVM FAQ — tjekket for vmx og svm, rettigheder til `/dev/kvm` og BIOS-indstillingen.
- QEMU System Emulation introduction — acceleratorerne, Tiny Code Generator og et komplet eksempel.
- QEMU invocation — alle tilvalg brugt ovenfor: `-accel`, `-m`, `-smp`, `-drive`, `-nographic`.
- QEMU disk image utility — qcow2, basisimages, snapshots og advarslen om images i brug.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er en virtuel maskine?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/virtual-machine/