Engineer

Nettverksport

tallet som velger en tjeneste på en vert

Hva det er

En nettverksport er et 16-bits tall i headeren på hvert TCP- og UDP-segment, og tallet forteller maskinen som tar imot, hvilket av programmene dens dataene skal til. Adressen bringer pakken fram til riktig vert; porten bringer den videre til riktig prosess når den først er framme. Ingeniører sier portnummer når de vil være presise, og «portene» i flertall betyr som regel settet en server lytter på. Ordet har ingenting med den fysiske porten på en svitsj å gjøre, og heller ikke med å «portere» programvare til en annen plattform.

Fordi feltet er 16 bit bredt, finnes det 65 536 verdier, fra 0 til 65535, og TCP og UDP har hvert sitt sett. TCP-port 53 og UDP-port 53 er to forskjellige ting, og DNS bruker begge. TCP-spesifikasjonen, RFC 9293, definerer en socket som en internettadresse koblet til en port, og en tilkobling som et par sockets. Det gir fire verdier: klientadresse, klientport, serveradresse og serverport. Det forklarer også hvorfor én serverport kan bære tusenvis av samtaler samtidig. Hver samtale skiller seg fra de andre i minst én av de tre andre verdiene, som regel klientporten.

RFC 6335 deler tallområdet i tre. Portene 0–1023 er «System Ports», 1024–49151 er «User Ports», og 49152–65535 er «Dynamic Ports», som IANA aldri tildeler. IANA fører registeret som knytter et tjenestenavn til et nummer: 22 for SSH, 53 for DNS, 443 for HTTPS og 5432 for PostgreSQL. En registrering er en konvensjon som klientene stoler på. Ethvert program kan lytte på et hvilket som helst ledig nummer, og det er slik SSH havner på en port ingen ville ha gjettet.

Klientsiden av en tilkobling får som regel en port den aldri har valgt selv. Når et program kobler seg ut, plukker operativsystemet et nummer fra intervallet for midlertidige porter (på engelsk «ephemeral ports»), og Linux bruker 32768–

60999 som standard, ikke IANAs dynamiske område. Å be om å binde port 0 betyr det samme: gi meg en hvilken som helst ledig port.

Bruk begrepet i en beslutning

Bruk «Hva er en nettverksport?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Wi-Fi, brannmurer og fjerntilgang satt opp slik at de ansatte kan jobbe hvor som helst, og bare de rette personene slipper inn.

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. Administrerte 30 Ubuntu Linux-VPS-instanser — 30 Linux-servere administrert, med gjenoppretting planlagt på forhånd

Administrerte 30 Ubuntu Linux-VPS-instanser Ta kontakt →

Hvorfor det er viktig

Beslutningen bak hver nettverksport handler om eksponering: hvilke programmer som svarer utenfra, og på hvilken adresse. En port uten lytter gir et avslag. En port med lytter er et stykke programvare som alle som når adressen, kan snakke med, feil inkludert. Den billigste tjenesten å sikre er den som lytter på 127.0.0.1, fordi pakker fra andre maskiner aldri når loopback-adressen, uansett hva brannmuren sier.

Det første spørsmålet for hver tjeneste er derfor om den i det hele tatt må kunne nås utenfra. En database som bare applikasjonen på samme maskin snakker med, hører hjemme på loopback. Et verktøy som bare administratorer bruker, kan bli liggende på loopback og nås gjennom en hoppvert (jump host) eller et VPN. Det som blir igjen, typisk 80 og 443 for et nettsted og én port for SSH, er den offentlige flaten. Å holde den kort er like mye et kostnadsvalg som et sikkerhetsvalg, fordi hver offentlig lytter trenger oppdateringer, logging og en brannmurregel som stemmer med den.

Det andre spørsmålet er selve nummeret. Standardporter koster ingenting i konfigurasjon: nettleserne, klientene og strengt låste nettverk forventer 443 og slipper den gjennom. Å flytte SSH bort fra 22 kutter støyen fra skannere som bare prøver standardporten, og loggene blir lettere å lese. En skanning av hele tallområdet finner den likevel, og hvert verktøy som viser til porten, må lære det nye nummeret. Det siste er den delen team glemmer.

Det tredje spørsmålet gjelder privilegier og deling. På Linux trenger en prosess root eller CAP_NET_BIND_SERVICE-rettigheten for å binde en port under 1024, med mindre ip_unprivileged_port_start er senket fra standardverdien 1024. Og

normalt eier ett program en gitt kombinasjon av adresse og port, så to tjenester som begge vil ha 443, trenger noe foran seg som deler trafikken mellom dem. Som regel er det en omvendt proxy som leser vertsnavnet klienten ba om.

Slik ser det ut i praksis

Tre deler av selskapets infrastrukturarbeid dreier seg om portnumre: én om hvor en lytter sitter, én om en port som flyttet seg, og én om å finne ut hvilke porter som faktisk er åpne.

Da selskapet satte opp sin egen git-forge i juli 2026, ble SSH-lytteren til forgen bundet til loopback på port 23231, og den som er utenfor, når den via en hoppvert. Antallet offentlige porter ble dermed stående der det var. En multiplekser som ville ha servert HTTPS og git over SSH fra én offentlig port ved å se på de første bytene i hver tilkobling, er skrevet og slått av. En lytter uten brukere måtte likevel ha vært forsvart.

I august 2026 fant en herdingsgjennomgang ut at SSH var flyttet til port 1986 under den første herdingen av verten, mens jailen for utestenging av inntrengere fortsatt overvåket 22. Hver utestenging jailen skrev, blokkerte en port der ingenting lyttet, så vernet hadde aldri slått til en eneste gang. Rettelsen var liten. Det som ble igjen, var en regel: hver sikkerhetskontroll får en kontroll som setter den på prøve.

Verten har 464 MB minne og ikke noe dashbord, så spørsmålene om den besvares av sju rapporteringsroller som bare leser og gjengir maskinen i drift som Markdown. Faktarapporten lister de lyttende socketene, altså den portoversikten systemkjernen faktisk har, og ikke den som konfigurasjonen beskriver. Blant de virkelige funnene rapportene gjorde, var en lyttende port som ingen deklarasjon nevnte.

Hvor det går galt

En tjeneste som var ment for maskinen selv, svarer hele internett. Mange programmer lytter som standard på alle adresser, vist som `0.0.0.0`, `[::]` eller `*` i socketlisten. En database eller et administrasjonspanel som skulle være lokalt, er da én brannmurtabbe unna å ligge åpent. Sett bindingsadressen eksplisitt til `127.0.0.1` eller `::1`, og bekreft den i kolonnen for lokal adresse:

```
ss -tlnp
ss -ulnp
```

Et vern fortsetter å overvåke en port tjenesten har forlatt. Tjenesten har flyttet til et nytt nummer, mens brannmurregelen, utestengingsjailen, sonden i overvåkingen eller en klientkonfigurasjon fortsatt peker på det gamle. Hvert av disse verktøyene fortsetter å fungere korrekt mot en port der ingen daemon lytter. Hold nummeret i én variabel som alle forbrukerne leser, og legg til en sjekk som sammenligner den lyttende socketen med det hver kontroll overvåker.

Utgående tilkoblinger begynner å feile under last med «Cannot assign requested address». Hver utgående tilkobling tar en lokal port fra intervallet for midlertidige porter, og en lukket tilkobling holder de fire verdiene sine reservert i TIME_WAIT en stund etterpå. Med standardintervallet i Linux, 32768–60999, kan én klientadresse ha 28 232 tilkoblinger til samme serveradresse og port, åpne eller nylig lukkede. En proxy eller en arbeidsprosess som åpner en ny tilkobling per forespørsel mot én og samme backend, bruker dem opp. Gjenbruk tilkoblinger med keep-alive eller en tilkoblingspool først; et bredere intervall eller flere kildeadresser kjøper bare mer takhøyde.

En tjeneste som startes som vanlig bruker, stopper med «Permission denied» på port 80. Å binde under 1024 krever privilegier. Gi tjenesten CAP_NET_BIND_SERVICE gjennom unit-filen, legg den på en høy port bak en omvendt proxy, eller senk ip_unprivileged_port_start på en vert der alle lokale brukere er til å stole på. Å kjøre hele tjenesten som root for å få én port er den dårligste avveiningen av dem alle.

Oppstarten stopper med «Address already in use». En annen prosess holder porten, ofte en gammel kopi av den samme tjenesten som fortsatt holder på å avslutte, eller en annen tjeneste med samme standardport (8080 er en populær en). `ss -tlnp` viser hvem som eier den. Bestem hvilken tjeneste som skal eie nummeret, og gi hver tjeneste en eksplisitt port i konfigurasjonen i stedet for å stole på standardverdier.

Les mer

- RFC 9293, section 4: Glossary — TCP-spesifikasjonens egne definisjoner av port, socket og tilkobling.

- RFC 6335: IANA Procedures for the Management of the Service Name and Transport Protocol Port Number Registry — de tre tallområdene for porter, og hvordan numrene i dem tildeles.
- Service Name and Transport Protocol Port Number Registry — IANAs liste over hvilken tjeneste som er registrert på hvilket nummer.
- RFC 768: User Datagram Protocol — UDP-spesifikasjonen på tre sider, med kilde- og målport.
- RFC 6056: Recommendations for Transport-Protocol Port Randomization — hvordan en klient bør velge de midlertidige portene sine så de blir vanskelige å gjette.
- IP Sysctl — innstillinger i Linux-kjernen, blant dem ip_local_port_range og ip_unprivileged_port_start.

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 nettverksport?» 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/port/