**Engineer**

# Port

Numéro qui désigne un service sur un hôte

## Ce que c’est

Un port est un nombre de 16 bits dans l’en-tête de chaque segment TCP ou UDP, qui indique à la machine destinataire à quel programme les données sont destinées. L’adresse mène le paquet au bon hôte ; le port le dirige ensuite vers le bon processus. Pour être précis, on parle de numéro de port. Au pluriel, les ports désignent généralement ceux sur lesquels un serveur écoute. Le terme n’a pas de rapport avec un port physique de commutateur ni avec le portage d’un logiciel vers une autre plateforme.

Le champ de 16 bits admet 65 536 valeurs, de 0 à 65535. TCP et UDP possèdent chacun leur ensemble : le port TCP 53 et le port UDP 53 sont distincts, et DNS utilise les deux. La spécification TCP, la RFC 9293, définit un socket comme une adresse internet associée à un port, et une connexion comme une paire de sockets. Cela donne quatre valeurs : adresse du client, port du client, adresse du serveur, port du serveur. Un même port serveur peut ainsi porter des milliers de conversations simultanées. Chacune diffère par au moins une des trois autres valeurs, généralement le port du client.

La RFC 6335 divise la plage en trois. Les ports 0–1023 sont les ports système (System Ports), les 1024–49151 sont les ports utilisateur (User Ports) et les 49152–65535 sont les ports dynamiques (Dynamic Ports), que l’IANA n’attribue jamais. L’IANA tient le registre qui associe un nom de service à un numéro : 22 pour SSH, 53 pour DNS, 443 pour HTTPS, 5432 pour PostgreSQL. Un enregistrement est une convention sur laquelle les clients s’appuient. Tout programme peut écouter sur n’importe quel numéro libre, ce qui permet de placer SSH sur un port que personne ne devinerait.

Le côté client d'une connexion reçoit généralement un port qu'il n'a pas choisi. Lorsqu'un programme ouvre une connexion sortante, le système d'exploitation choisit un numéro dans sa plage éphémère. Dans sa configuration initiale, Linux utilise 32768–60999 plutôt que la plage dynamique de l'IANA. Demander à se lier au port 0 signifie la même chose : attribuez-moi n'importe quel port libre.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un port ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Du Wi-Fi, des pare-feu et des accès à distance configurés pour travailler de partout, en laissant entrer uniquement les personnes autorisées.

**Découvrir nos prestations** Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 30 instances VPS Ubuntu Linux administrées — 30 serveurs Linux gérés, avec récupération prévue

**30 instances VPS Ubuntu Linux administrées** Contactez-nous →

## Pourquoi c'est important

Derrière chaque port se pose la question de l'exposition : quels programmes répondent aux demandes venues de l'extérieur, et sur quelle adresse ? Sans processus à l'écoute, la connexion au port est refusée. Avec un processus à l'écoute, toute personne pouvant atteindre l'adresse peut communiquer avec ce logiciel, défauts compris. Le service le moins coûteux à sécuriser est celui qui écoute sur 127.0.0.1 : les paquets d'autres machines ne peuvent pas atteindre cette adresse de bouclage, quoi qu'en dise le pare-feu.

Pour chaque service, il faut donc d'abord se demander s'il doit être accessible de l'extérieur. Une base avec laquelle seule l'application de la même machine communique doit rester sur l'interface de bouclage. Un outil réservé aux administrateurs peut y rester lui aussi, avec un accès par un hôte de rebond ou un VPN. Ce qui reste, généralement 80 et 443 pour un site web et un port pour SSH, forme la surface publique. La réduire est une décision de coût autant que de sécurité : chaque service publiquement à l'écoute exige des correctifs, des journaux et une règle de pare-feu correspondante.

La deuxième question est le numéro. Les ports standards ne demandent aucune configuration particulière : navigateurs, clients et réseaux restrictifs s'attendent au 443 et le laissent passer. Déplacer SSH hors du 22 réduit le bruit des scanners qui n'essaient que le port par défaut et rend les journaux plus lisibles. Un scan de la plage entière le retrouvera pourtant, et chaque outil qui utilise ce port doit connaître le nouveau numéro. C'est ce dernier point que les équipes oublient.

La troisième question concerne les privilèges et le partage. Sous Linux, un processus doit être root ou posséder la capacité CAP_NET_BIND_SERVICE pour se lier à un port inférieur à 1024, sauf si ip_unprivileged_port_start a été abaissé par rapport à sa valeur par défaut de 1024. Normalement, un seul programme occupe une adresse et un port donnés. Deux services qui veulent tous deux le 443 ont donc besoin d'un intermédiaire pour répartir le trafic, généralement un proxy inverse qui lit le nom d'hôte demandé par le client.

## À quoi cela ressemble en pratique

Lorsque l'entreprise a installé sa forge Git en juillet 2026, le service SSH de la forge a été configuré pour écouter sur l'interface de bouclage au port 23231. Les accès extérieurs passent par un hôte de rebond : le nombre de ports publics est donc resté inchangé. Un multiplexeur capable de servir HTTPS et Git sur SSH depuis un même port public, en examinant les premiers octets de chaque connexion, est écrit mais désactivé. Un service à l'écoute sans utilisateurs aurait tout de même besoin d'être défendu.

En août 2026, une revue de durcissement a constaté que SSH était passé au port 1986 lors du durcissement initial de l'hôte, tandis que le jail de blocage des intrusions continuait à surveiller le 22. Chaque bannissement du jail bloquait un port sur lequel aucun processus n'écoutait : la protection n'avait donc jamais été effective. La correction était minime. Il en est resté une règle : chaque contrôle de sécurité est associé à une assertion qui le met à l'épreuve.

L'hôte dispose de 464 Mo de mémoire et n'a pas de tableau de bord. Pour répondre aux questions, sept rôles de rapport en lecture seule décrivent en Markdown la machine en fonctionnement. Le rapport d'informations système liste les sockets à l'écoute : c'est l'inventaire des ports réellement détenu par le noyau, et non celui décrit par la configuration. Parmi les faits découverts par ces rapports figurait un port à l'écoute qu'aucune déclaration ne mentionnait.

## Où les problèmes surviennent

**Un service réservé à la machine répond à tout internet.** Beaucoup de programmes écoutent par défaut sur toutes les adresses, indiquées par `0.0.0.0`, `[::]` ou `*` dans la liste des sockets. Une base ou une interface d'administration censée rester locale n'est alors qu'à une erreur de pare-feu de l'exposition publique. Définissez explicitement l'adresse d'écoute à `127.0.0.1` ou `::1` et vérifiez-la dans la colonne des adresses locales :

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

**Une protection surveille toujours un port que le service a quitté.** Le service a changé de numéro, mais la règle de pare-feu, le jail de bannissement, la sonde de supervision ou la configuration d'un client indique encore l'ancien. Chacun de ces outils continue de fonctionner correctement sur un port où aucun démon n'écoute. Conservez le numéro dans une variable lue par tous les consommateurs, et ajoutez un contrôle qui compare le socket à l'écoute à ce que chaque protection surveille.

**Les connexions sortantes commencent à échouer sous charge avec « Cannot assign requested address ».** Chaque connexion sortante prend un port local dans la plage éphémère. Après sa fermeture, elle conserve pendant un certain temps ses quatre valeurs réservées dans l'état TIME_WAIT. Avec la plage Linux par défaut, 32768–60999, une adresse cliente peut conserver 28 232 connexions vers la même adresse et le même port serveur, ouvertes ou récemment fermées. Un proxy ou un processus de travail qui ouvre une nouvelle connexion à chaque requête vers le même backend les épuise. Réutilisez d'abord les connexions avec keep-alive ou un pool ; élargir la plage ou ajouter des adresses sources ne fait qu'accroître la marge disponible.

**Un service lancé sous un compte utilisateur ordinaire s'arrête avec « Permission denied » sur le port 80.** Se lier à un port inférieur à 1024 exige des privilèges. Accordez au service la capacité CAP_NET_BIND_SERVICE dans son fichier d'unité, placez-le sur un port élevé derrière un proxy inverse ou, sur un hôte où tous les utilisateurs locaux sont de confiance, abaissez ip_unprivileged_port_start. Exécuter tout le service en root pour obtenir un seul port est le pire compromis.

**Le démarrage s'arrête avec « Address already in use ».** Un autre processus occupe le port : souvent une ancienne instance du même service encore en cours d'arrêt, ou un second service avec la même valeur par défaut, 8080 étant un choix fréquent. `ss -tlnp` indique qui l'occupe. Décidez quel service possède le numéro et attribuez à chacun un port explicite dans sa configuration, plutôt que de vous fier aux valeurs par défaut.

# Pour aller plus loin

- RFC 9293, section 4 : glossaire — Définitions du port, du socket et de la connexion dans la spécification TCP.
- RFC 6335 : procédures de l'IANA pour gérer le registre des noms de service et des numéros de port des protocoles de transport — Trois plages de ports et attribution des numéros.
- Registre des noms de service et des numéros de port des protocoles de transport — Liste de l'IANA des services enregistrés pour chaque numéro.
- RFC 768 : protocole de datagrammes utilisateur (UDP) — Spécification UDP en trois pages, avec les ports source et destination.
- RFC 6056 : recommandations pour la sélection aléatoire des ports des protocoles de transport — Choix des ports éphémères d'un client pour les rendre difficiles à deviner.
- IP Sysctl : paramètres IP du noyau — Réglages du noyau Linux, dont ip_local_port_range et ip_unprivileged_port_start.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

**Consulter les tarifs** Contactez-nous →

# Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un port ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

**Découvrir nos prestations**

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

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

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/port/