

05.01.23 | Configuration (<https://www.ionos.fr/digitalguide/serveur/configuration/>)

pour
le f
at l'i
w.ia
//w
u.ia

Produits associés

Ubuntu SSH : comment l'installer et l'activer ?

**Serveurs Cloud**

Si, au moment de l'installation, vous n'avez pas activé le serveur SSH d'Ubuntu par défaut (OpenSSH), il n'est pas trop tard pour cela. Après avoir installé le service de sécurité par l'intermédiaire du terminal, vous avez la possibilité de personnaliser librement la configuration du démon SSH d'Ubuntu.

Sommaire

1. Installer le serveur SSH d'Ubuntu : instructions étape par étape

Installer le serveur SSH d'Ubuntu : instructions étape par étape

Si vous souhaitez accéder à distance et en toute sécurité à votre propre ordinateur ou serveur, vous ne pouvez pas faire l'impasse sur le protocole SSH (<https://www.ionos.fr/digitalguide/serveur/outils/protocole-ssh/>) (Secure Shell). Grâce à trois principaux piliers, cette procédure de sécurité encadre n'importe quel accès à distance :

- L'authentification du poste à distance, de manière à ce que le mauvais interlocuteur (client comme serveur) ne soit jamais contacté ;
- Le chiffrement des transferts de données, pour que les informations ne soient jamais consultées par des personnes non autorisées ;
- La garantie de l'intégrité des données, afin de rendre inviolables toutes les données communiquées.

Les distributions Linux comme Ubuntu (<https://www.ionos.fr/digitalguide/serveur/know-how/ubuntu-le-systeme-linux-pour-tous/>) se reposent depuis plusieurs années déjà sur une suite logicielle open source, OpenSSH, pour profiter des avantages du SSH et transférer des fichiers en toute sécurité par SCP (<https://www.ionos.fr/digitalguide/serveur/know-how/scp-secure-copy/>) ou SFTP (<https://www.ionos.fr/digitalguide/serveur/know-how/sftp-ssh-file-transfer-protocol/>).

Les outils OpenSSH sont désactivés par défaut lorsque vous installez Ubuntu pour la première fois ; commencez donc par activer ce service. Découvrez avec nous son fonctionnement et les différentes options de configuration qui s'offrent à vous après l'activation du serveur SSH d'Ubuntu.

! Note

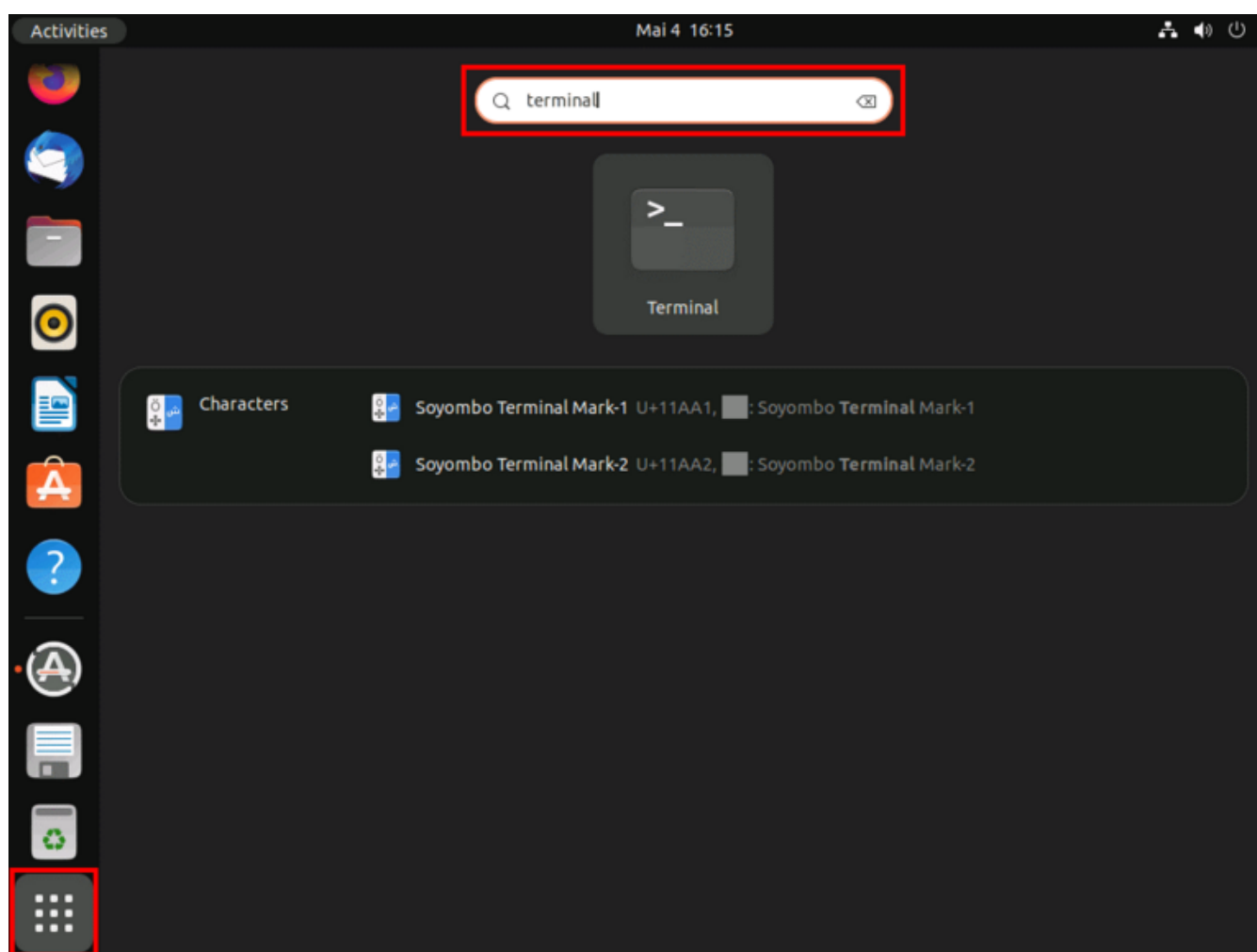
Si vous utilisez l'édition serveur d'Ubuntu pour configurer un serveur Ubuntu (<https://www.ionos.fr/digitalguide/serveur/configuration/serveur-ubuntu/>), vous pouvez activer le SSH au moment de l'installation.

Étape 1 : appeler le terminal

Vous devez utiliser le terminal, c'est-à-dire l'outil de ligne de commande de la distribution Linux pour installer ou activer SSH dans Ubuntu (à l'aide de la commande *install*). La première étape consiste donc à ouvrir cet outil d'administration. Pour ce faire, utilisez simplement la combinaison de touches [Ctrl] + [Alt] + [t].

[Voir les packs ►](#)

Il est également possible d'ouvrir le terminal depuis le menu « Afficher les applications » : cliquez sur le bouton du même nom et utilisez la fonction de recherche pour trouver le terminal.



(https://www.ionos.fr/digitalguide/fileadmin/DigitalGuide/Screenshots_2022/ubuntu-search-function-search-for-terminal.png)

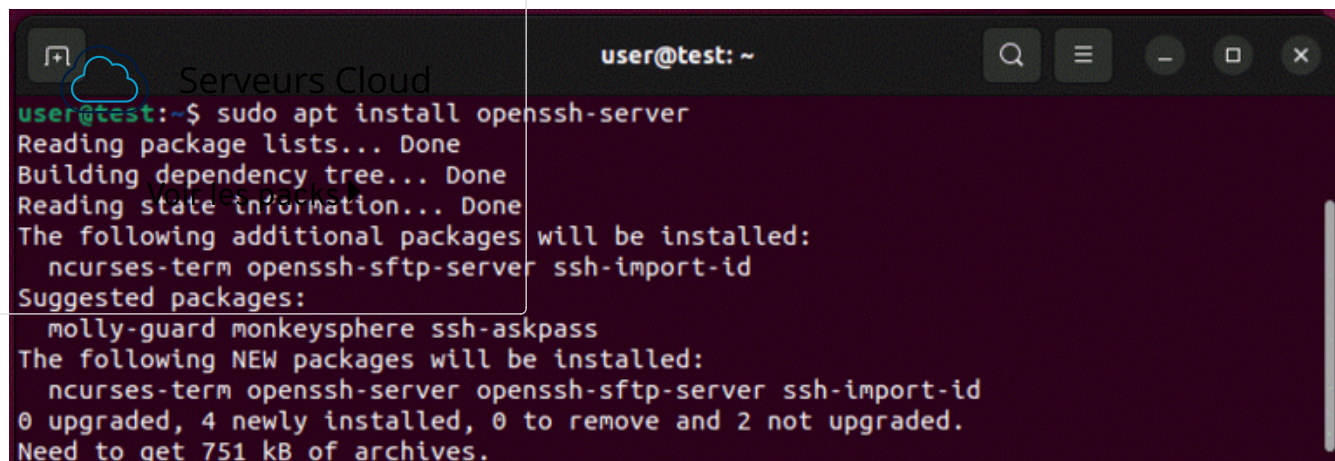
Fonction de recherche d'Ubuntu : recherche du mot-clé « terminal ».

Étape 2 : installer le service SSH d'Ubuntu

Après avoir utilisé la commande *install* d'Ubuntu pour le service SSH, installez la suite logicielle OpenSSH dans l'outil de ligne de commande que vous avez lancé. Renseignez la commande suivante :

```
1 | sudo apt install openssh-server
```

Entrez votre mot de passe utilisateur, puis appuyez sur « Entrée » pour confirmer votre action et commencer l'installation du service SSH d'Ubuntu.



```
user@test:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 2 not upgraded.
Need to get 751 kB of archives.
```

(https://www.ionos.fr/digitalguide/fileadmin/DigitalGuide/Screenshots_2022/openssh-installation-in-the-ubuntu-terminal.png)

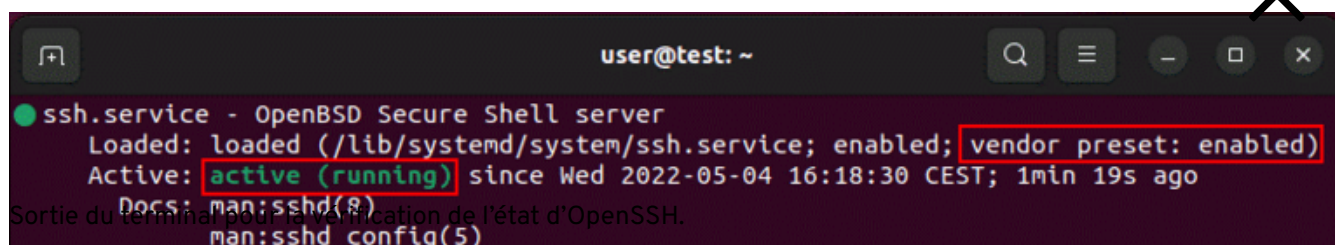
Installation d'OpenSSH dans le terminal Ubuntu.

Étape 3 : vérifier l'état du serveur SSH d'Ubuntu et l'activer (le cas échéant)

Une fois l'installation terminée, utilisez la commande suivante pour savoir si le démon SSH s'exécute correctement :

```
1 | sudo systemctl status ssh
```

Cette sortie de commande renvoie *active (running)* si le service SSH d'Ubuntu est bien en cours d'exécution. Comme le SSH doit aussi être disponible à chaque nouveau démarrage du système, l'entrée *vendor preset: enabled* doit également apparaître dans la ligne *Loaded*.



```
user@test: ~
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-05-04 16:18:30 CEST; 1min 19s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
```

Sortie du terminal pour l'indication de l'état d'OpenSSH.

```
memory: 27M
CPU: 19ms
Group: /system.slice/ssh.service
└─10088 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

(https://www.ionos.fr/digitalguide/fileadmin/DigitalGuide/Screenshots_2022/terminal-for-openssh-status-query.png)

Si le service SSH reste inactif et que son lancement automatique en cas de redémarrage n'est pas activé, vous pouvez alors renseigner deux commandes supplémentaires :

1 | `sudo systemctl enable ssh`
2 | `sudo systemctl start ssh`

Voir les packs ►

! Note

Utilisez la touche « q » pour interrompre la sortie relative à l'état du SSH et revenir à l'entrée de ligne de commande.

Étape 4 : ouvrir le port SSH

Si vous voulez vous connecter à distance à votre système Ubuntu par l'intermédiaire du SSH, le port du protocole réseau (ici le port 22 du TCP, par défaut) doit être activé. Il est le seul à vous permettre de vous connecter à distance à des clients SSH comme PuTTY.

UFW est le programme de configuration d'Ubuntu dédié au pare-feu propriétaire du système. Avec ce programme, configurez une règle appropriée pour la communication depuis le SSH, afin d'ouvrir le port aux données entrantes comme sortantes :

1 | `sudo ufw allow ssh`

```
user@test:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
user@test:~$
```

(https://www.ionos.fr/digitalguide/fileadmin/DigitalGuide/Screenshots_2022/enabling-ss-port-with-ubuntu-terminal.png)

Partage du port SSH par l'intermédiaire du terminal Ubuntu.



! Note

Si vous ne parvenez à établir aucune connexion SSH, il est possible que le port soit fermé. Un

certain nombre de problèmes sont susceptibles de vous empêcher de mettre en place des transferts SSH sécurisés.

Étape 5 : configurer le serveur SSH d'Ubuntu

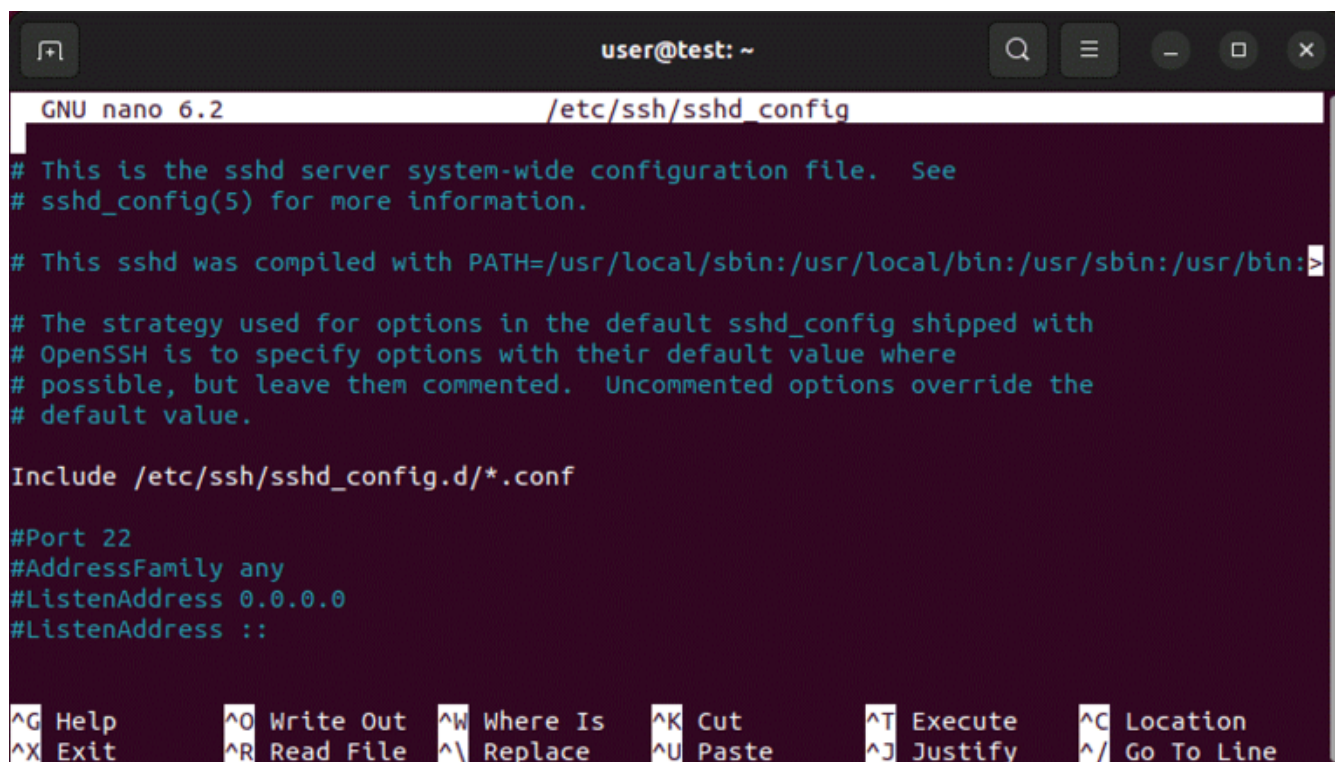
Produits associés

La configuration de base de la suite logicielle OpenSSH est celle qui convient le mieux si vous souhaitez vous connecter à votre système Ubuntu à distance et en toute sécurité. Vous pouvez toutefois modifier les paramètres par défaut, notamment si vous souhaitez utiliser un autre port pour la communication, spécifier une version du protocole Internet ou désactiver la redirection TCP.

`sshd_config` est le fichier de configuration central du package SSH d'Ubuntu. Si vous souhaitez le modifier, ouvrez-le depuis l'éditeur de texte de votre choix (ici, il s'agit de nano) avec ce code :

```
1 | sudo nano /etc/ssh/sshd_config
```

Modifiez le contenu du fichier de configuration en fonction de vos besoins, puis enregistrez ces modifications avant de le fermer. Ensuite, redémarrez la suite logicielle OpenSSH afin que vos modifications s'appliquent :



```
user@test: ~
GNU nano 6.2 /etc/ssh/sshd config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

(https://www.ionos.fr/digitalguide/fileadmin/DigitalGuide/Screenshots_2022/contents-in-openssh-configuration-file-sshd-config.png)

Contenu du fichier de configuration `sshd_config` d'OpenSSH.


```
1 | sudo service ssh restart
```

💡 Conseil

La configuration du SSH peut notamment s'avérer judicieuse si vous prévoyez d'utiliser un serveur FTP Ubuntu (<https://www.ionos.fr/digitalguide/serveur/configuration/serveur-ftp-ubuntu-installation-et-configuration/>). Vous disposerez ainsi de la version FTP sécurisée du protocole SFTP, dont nous avons déjà parlé.

Produits associés



Serveurs Cloud

Voir les packs ▶

05.01.23

Configuration (<https://www.ionos.fr/digitalguide/serveur/configuration/>)

pour la configuration

Sécurité (<https://www.ionos.fr/digitalguide/tags/securite/>)

Tutoriels (<https://www.ionos.fr/digitalguide/tags/tutoriels/>)

Articles similaires



Générer des clés SSH pour votre connexion réseau

🕒 05.01.2023 | Sécurité

Une connexion réseau sécurisée via un protocole SSH est une solution appréciée pour administrer ou commander un serveur à distance. Le processus d'authentification sur le

serveur se déroule de manière conventionnelle, à l'aide d'un identifiant et d'un mot de passe. Mais il existe des méthodes d'authentification alternatives pour une connexion SSH, comme par exemple l'authentification par clé...

SSH
G
W
id

Produits associés



Serveurs Cloud

Voir les packs ▶



Tunnel SSH : introduction à la redirection de ports SSH

🕒 20.09.2022 | Sécurité

Un tunnel SSH est utilisé pour assurer des transferts de données sécurisés et pour accéder à des sites Internet qui seraient inaccessibles sans eux. Les tunnels SSH inversés rendent possible la redirection de ports à l'aide d'adresses IP privées. Lisez cet article dédié pour découvrir en quoi consistent les tunnels SSH, à quelles fins ils sont utilisés et comment en configurer un.

SSH
n à
W
//W



Produits associés



Serveurs Cloud

Voir les packs ►

Articles Populaires

À propos de IONOS (https://www.ionos.fr/apropos)
 Newsroom (https://www.ionos.fr/newsroom/)
 Centre d'Assistance (https://www.ionos.fr/assistance/)
 Startup Guide (https://www.ionos.fr/startupguide/)
 CGV (https://www.ionos.fr/terms-gtc/cgv/)
 Clause de confidentialité (https://www.ionos.fr/terms-gtc/terms-privacy/)
 © 2023 IONOS SARL (https://www.ionos.fr/)

