SSH avec échange de clés

| SSH C'est quoi ? | 2 |
|-----------------------------------------------------|----|
| Installation de SSH sur les deux machines | 3 |
| Configuration initiale des machines virtuelles | 3 |
| Génération de la paire de clés SSH | 3 |
| Vérification de l'empreinte numérique de la clé SSH | 4 |
| Windows ver Debian | 6 |
| Création d'une paire de clés dans PuTTYgen | 6 |
| Connexion avec PuTTY | 12 |
| | |

SSH C'est quoi ?

SSH (Secure Shell) est un protocole de communication sécurisé qui permet d'établir une connexion à distance avec un autre ordinateur ou serveur. Il est utilisé pour l'administration des systèmes à distance, la gestion des fichiers et l'exécution de commandes sur des machines distantes. SSH chiffre les données échangées pour garantir la sécurité des informations lors de la transmission. Il est couramment utilisé pour accéder à des serveurs Linux ou Unix.

Dans ce projet, nous allons configurer deux machines virtuelles pour permettre une connexion SSH sécurisée avec échange de clés. Les deux machines sont configurées comme suit :

srv-home : cette machine aura l'adresse IP <u>192.168.56.101.</u> srv-backup : cette machine sera configurée avec l'adresse IP <u>192.168.56.102.</u> Ces configurations permettent de tester l'authentification sans mot de passe entre les deux machines via SSH.



Installation de SSH sur les deux machines

Pour activer le SSH sur les deux machines, installez le serveur OpenSSH en utilisant la commande suivante sur srv-home (192.168.56.101) puis sur srv-backup (192.168.56.102) :



Configuration initiale des machines virtuelles

Les deux machines virtuelles, **srv-home** et **srv-backup**, sont maintenant correctement configurées pour démarrer le processus d'authentification SSH par clés.

Génération de la paire de clés SSH

La commande suivante permet de générer une paire de clés SSH (clé publique et clé privée), également appelée **empreinte numérique** ou **fingerprint**, que sera utilisée pour l'authentification sans mot de passe :

ssh-keygen

Cela crée la base de l'authentification sécurisée en utilisant des clés SSH.

```
SIO2
```



Vérification de l'empreinte numérique de la clé SSH

Après avoir généré la paire de clés, vous pouvez afficher l'empreinte numérique (fingerprint) de la clé publique en utilisant la commande suivante :

SSH-keygen -lf .ssh/id_rsa

```
sio@srv–backup:~$ ssh–keygen –lf .ssh/id_rsa
2048 SHA256:l3v4dKYxCAxvEzJqDFmqMyBntHWfCLDssHVvDUuzaV0 sio@srv–backup (RSA)
sio@srv–backup:~$ _
```

ssh-copy-id -i sio@192.168.56.101

Cette commande permet de copier la clé publique sur la machine distante afin d'activer l'authentification SSH sans mot de passe.

| sio@srv−backup:~\$ ssh−copy−id −i sio@192.168.56.101 |
|------------------------------------------------------------------------------------------------------|
| /usr/bin/ssh-copy–id: INFO: Source of key(s) to be installed: "/home/sio/.ssh/id_rsa.pub" |
| The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established. |
| ECDSA key fingerprint is SHA256:IADg5f+nBMRFTb8WgL8MscpljKWBH9YkwZbrAWvEquU. |
| Are you sure you want to continue connecting (yes/no)?y |
| Please type 'yes' or 'no': yes |
| /usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr |
| eady installed |
| /usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed if you are prompted now it is to inst |
| all the new keys |
| sio@192.168.56.101's password: |
| Permission denied, please try again. |
| sio@192.168.56.101's password: |
| Permission denied, please try again. |
| sio@192.168.56.101's password: |
| |
| Number of key(s) added: 1 |
| |
| Now try logging into the machine, with: "ssh 'sio@192.168.56.101'" |
| and check to make sure that only the key(s) you wanted were added. |
| |

Une fois la clé publique copiée sur **srv-home**, vous pouvez tester la connexion SSH sans mot de passe depuis **srv-backup** Avec la commande : <u>shh sio@192.168.56.101</u>

```
sio@srv-backup:~* ssh sio@192.168.56.101
Linux svr-home 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Sep 5 13:51:11 2024 from 192.168.56.1
sio@svr-home:~* ip a
1: lo: (LODPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0S3: (BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
link/ether 08:00:27:ce:24:11 brd ff:ff:ff:ff:ff
inet 192.168.56.101/24 brd 192.168.56.255 scope global enp0s3
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fece:2411/64 scope link
valid_lft forever preferred_lft forever
sio@svr-home:~*s
```

Windows ver Debian

Création d'une paire de clés dans PuTTYgen

| ile Key Conversions Help Key | | | | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Key | | | | |
| Discourse and a second | | - Martinese | | |
| Please generate some randomness by | moving the mouse over th | e blank area. | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Actions | | | | |
| Generate a public/private key pair | | | <u>G</u> enerate | E |
| Load an existing private key file | | | Load | |
| Save the generated key | | Save p <u>u</u> blic key | Save private key | |
| Parameters | | | | |
| Type of key to generate: | 0 500.00 | 0.51004 | | |
| <u>Number of hits in a consented loss</u> | <u> </u> | O EdD <u>S</u> A | O SSH-1 (RSA) | |
| Number of bits in a generated key. | | | 2040 | |
| PuTTY Key Generator | | | | ? |
| Key Conversions Help | | | | |
| | | | | |
| HV | | | | |
| ey Public key for pasting into OpenS | SH authorized kevs file | e: | | |
| ey Public key for pasting into Open S ssh-rsa | SH authorized_keys file | ə: | | |
| ey /ublic key for pasting into Open S! ssh+sa AAAAB3NzaC1yc2EAAAADAQA ///WhD111HiH/z0ov7SY/sacC1 isi | SH authorized_keys fik BAAABAQCfxhuT6QZ; PoHMSe/lthavPXw9b | e: y0auyuatBvZ8UFr1+ 5TCGx+kcPA.lfED/T | 4fFvnSfqQM4/ojYkm OgFf3/eOS2CHe5de | alNBIRFadiM4x |
| ey ublic key for pasting into Open S. ish-rsa AAAAB3NzaC1yc2EAAAADAQA yMbDUIHiH/20ox7SY/sacC1is -qZBsO3boTgKwR26TOVlqf6F0 | SH authorized_keys file BAAABAQCfxhuT6QZ; PqHMSe/IrhayPXw9b HA5z7Ajnd54liq1uj1f7 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T iNTJr/L | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds | aINBIRFadiM4x ORnR |
| ey ublic key for pasting into OpenS: ish-rsa AAAAB3NzaC1yc2EAAAADAQA wMbDUHiH/zOox7SY/sacC1is i-qZBsO3boTgKwR26TOWq6F6 GG2FKdfHP9PelxV2mXaUd9IT | SH authorized_keys file BAAABAQCfxhu T6Q.Z; PqHMSe/IrhayPXv9b HA5z7Ajnd54iq 1uj 1f7 ySC/i0mP15vk6F1a1Z | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T INTJr/L Inm | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5de | aINBIRFadiM4x sORnR |
| ey ublic key for pasting into Open S ish-rsa AAAAB3NzaC1yc2EAAAADAQA yMbDUHHH/20ox75Y/sacC1is -qZBsO3boTgKwR26TOVlqf6F0 -OG2FKdfHP9PelxV2mXaUd9IT iey fingerprint: ssh-rsa 204 | SH authorized_keys file BAAABAQCfxhu T6QZ PqHMSe/IrhayPXw9b HA5z7Ajnd54iq1uj 177 9tSO/i0mPI5vk6F1aIZ 8 SHA256fXMkRinLFj 41117 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T 4NTJr/L /nm ywic1YB0+qdU7l8jPr | 4fFvnSfqQM4/ojYkn OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aalNBIRFadiM4x oORnR |
| ey ublic key for pasting into OpenS ssh-rsa AAAAB3NzaC1yc2EAAAADAQA yMbDUIHiH/20ox7SY/sacC1is +qZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PelxV2mXaUd9IT ey fingerprint: ssh-rsa 204 iey <u>c</u> omment: rsa-key-202 | SH authorized_keys fil BAAABAQCfxhu T6Q.Z PqHMSe./inhayPXw9b IHA5z7Ajnd54iq1uj1f7 9t SO./i0mP15vk6F1aIZ 8 SHA256.fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T INTJr/L Inm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkn OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aalNBIRFadiM4x sORnR |
| ey ublic key for pasting into OpenS: ish-rsa AAAAB3NzaC1yc2EAAAADAQA ish-rsa ish-rsa into OpenS: ish-rsa 204 iey gomment: isa-key-202 iey passphrase: | SH authorized_keys fill BAAABAQCfxhu T6Q.Z PqHMSe/IrhayPXw9b IHA5z7Ajnd54iq1uj1f7 9tSO/i0mP15vk6F1alZ 8 SHA256fXMkRinLF; 41017 | ə: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T 4NTJr/L źnm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aalNBIRFadiM4x oRnR |
| ey Jublic key for pasting into Open Si ssh-rsa AAAAB3NzaC 1yc2EAAAADAQA yoMbDUHHH/200x75Y/sacC1is uqZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PetxV2mXaUd9IT key fingerprint: ssh-rsa 204 key comment: rsa-key-202 key passphrase: confirm passphrase: | SH authorized_keys fill BAAABAQCfxhu T6QZ PqHMSe/InhayPXw9b HA5z7Ajnd54iq1uj177 9tSO/10mPI5vk6F1aIZ 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T 4NTJr/L /nm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aalNBIRFadiM4x oORnR |
| ey jublic key for pasting into Open S: sh-rsa AAAAB3NzaC1yc2EAAAADAQA yMbDUHiH/z0ox7SY/sacC1is +qZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PetxV2mXaUd9IT fey fingerprint: ssh-rsa 204 fey gomment: rsa-key-202 fey passphrase: ignfim passphrase: ctions | SH authorized_keys file BAAABAQCfxhu T6QZ PqHMSe/IrhayPXw9b HA5z7Ajnd54iq1uj 177 9tSO/i0mPI5vk6F1aIZ 8 SHA256fXMkRinLFj 41017 | ə: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T NNTJr/L Inm ywic1YB0+qdU7l8jPı | 4fFvnSfqQM4/ojYkn OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aalNBIRFadiM4x sORnR |
| ey tublic key for pasting into Open S: ssh-rsa AAAAB3NzaC1yc2EAAAADAQA yoMbDUIHiH/20ox7SY/sacC1is +qZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PelxV2mXaUd9IT fey fingerprint: ssh-rsa 204 fey comment: rsa-key-202 fey passphrase: confirm passphrase: ctions fenerate a public/private key pair | SH authorized_keys fil BAAABAQCfxhu T6Q.7 PqHMSe./IrhayPXw9b IHA5z 7Ajnd54iq 1uj 1f7 9t SO./i0mP15vk 6F1al2 8 SHA256fXMkRinLF; 41017 | ə: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T INTJr/L Inm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | Generate |
| ey (ublic key for pasting into Open S: ssh-rsa AAAAB3NzaC1yc2EAAAADAQA yoMbDUIHiH/20ox7SY/saC1is: +qZBs03boTgKwR26T0Vlqf6F0 +OG2FKdfHP9PelxV2mXaUd9IT fey fingerprint: ssh-rsa 204 fey gomment: rsa-key-202 fey passphrase: confirm passphrase: ctions fenerate a public/private key pain fenerate a public/private key pain | SH authorized_keys fil BAAABAQCfxhu T6Q.7 PqHMSe/IrhayPXw9b HA5z7Ajnd54iq1uj1f7 9tSO/10mP15vk6F1al2 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T 4NTJr/L /nm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | Generate |
| ey ublic key for pasting into Open Si sh rsa AAAAB3NzaC1yc2EAAAADAQA wMbDUHHH/z0ox75Y/sacC1is rqZBsO3boTgKwR26TOVlqf6F0 rOG2FKdfHP9PelxV2mXaUd9IT iey fingerprint: ssh rsa 204 iey gomment: rsa key-202 iey passphrase: ienfirm passphrase: ctions ienerate a public/private key pair oad an existing private key file | SH authorized_keys fil BAAABAQCfxhu T6QZ PqHMSe/InhayPXw9b HA5z7Ajnd54ig1uji177 9tSO/10mPI5vk6F1aIZ 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T 4NTJr/L 2nm ywic1YB0+qdU7l8jPr | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aaINBIRFadiM4x soRnR <u>G</u> enerate Load |
| ey 2ublic key for pasting into OpenS: ssh-rsa AAAAB3NzaC1yc2EAAAADAQA yMbDUHiH/z0ox75Y/sacC1is +qZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PetxV2mXaUd9IT /ey fingerprint: ssh-rsa 204 /ey comment: rsa-key-202 /ey passphrase: | SH authorized_keys file BAAABAQCfxhu T6QZ PqHMSe/IrhayPXw9b HA5z7Ajnd54iq1uj177 9tSO/10mPI5vk6F1al2 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T INTJr/L Inm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | <u>G</u> enerate Load |
| ey 2ublic key for pasting into OpenS: ssh-rsa AAAAB3NzaC1yc2EAAAADAQA yoMbDUIHiH/20ox7SY/saC1is +qZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PekV2mXaUd9IT Key fingerprint: ssh-rsa 204 Key comment: rsa-key-202 Key passphrase: Confirm passphrase: ctions Senerate a public/private key pair coad an existing private key file Save the generated key larameters | SH authorized_keys fil BAAABAQCfxhu T6QZ PqHMSe/IrhayPXw9b HA5z7Ajnd54iq1uj1f7 9tSO/10mP15vk6F1al2 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T INTJr/L /nm ywic1YB0+qdU7l8jPi | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aaINBIRFadiM4x ORnR <u>G</u> enerate Load ave private key |
| ey ublic key for pasting into OpenS: sh+sa AAAAB3NzaC1yc2EAAAADAQA yMbDUHHI/z0ox75Y/sacC1is +qZBsO3boTgKwR26TOVlqf6F0 +OG2FKdfHP9PelxV2mXaUd9IT fey fingerprint: ssh-rsa 204 fey gomment: rsa-key-202 fey passphrase: for passphrase: ctions enerate a public/private key pair oad an existing private key file ave the generated key arameters ype of key to generate: | SH authorized_keys fil BAAABAQCfxhu T6QZ PqHMSe/InhayPXw9b HA5z7Ajnd54ig1ujif77 9tSO/10mPI5vk6F1aIZ 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T 4NTJr/L /nm ywic1YB0+qdU7l8jPr Save p <u>u</u> bli | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | alNBIRFadiM4x ORnR <u>G</u> enerate Load ave private key |
| ey 2ublic key for pasting into OpenS: ssh-rsa AAAAB3NzaC1yc2EAAAADAQA pvMbDUHiH/z0ox75Y/saC1is +qZBs03boTgKwR26TOVlqf6F0 +OG2FKdfHP9PetxV2mXaUd9IT Key fingerprint: ssh-rsa 204 Key gomment: rsa-key-202 Key passphrase: 2gnfirm passphrase: Senerate a public/private key pair coad an existing private key file Save the generated key 'arameters ype of key to generate: P BSA O DSA | SH authorized_keys fill BAAABAQCfxhu T6QZ PqHMSe/IrhayPXw9b HA5z7Ajnd54ig1uji T7 9tSO/0mPI5vk6F1aIZ 8 SHA256fXMkRinLFj 41017 | e: y0auyuatBvZ8UFr1+ 5TCGx+kgPAJfFD/T tNTJr/L ywic1YB0+qdU7l8jPr Save p <u>u</u> bli | 4fFvnSfqQM4/ojYkm OqEf3/eOS2CHs5ds rvV+Q5KtcYFj3Phw4 | aaINBIRFadiM4x soRnR <u>G</u> enerate Load ave private key) SSH- <u>1</u> (RSA) |

Création de la clé publique

| ate key pair | | Generate |
|--------------|--------------------------|------------------|
| e key file | | Load |
| y | Save p <u>u</u> blic key | Save private key |

Pour activer les transferts de fichiers FTP entre Windows et **srv-home**, installez **vsftpd** (Very Secure FTP Daemon) sur **srv-home** avec apt installe vsftpd

| | Protocole | de <u>fi</u> chier Ch | iffrement : | |
|----------|----------------|-----------------------|-------------------|--------|
| | FTP | ~ Pa | as de chiffrement | ` |
| | Nom d'hôt | te | Numéro de | e port |
| | 192.168. | 56.101 | | 21 🛓 |
| | Nom d'utili | isateur | Mot de passe | |
| | sio | | ••• | |
| | Conne | xion anonyme | | |
| | Sauve | er 💌 | Avancé | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Outils 🔻 | Gestionnaire 🔻 | 🔁 Connexion 💌 | Fermer Ai | ide |
| | | | | |



Il faut couche affichage des fichiers cachés

Modification du fichier de configuration vsftpd

Sur le serveur srv-home, ouvrez le fichier de configuration de vsftpd pour ajuster les paramètres FTP

nano /etc/vsftpd.conf



La clé publique de votre machine hôte a été copiée dans le répertoire /home/sio/.ssh/ de **srv-home**. Ensuite, ajoutez cette clé publique dans le fichier authorized_keys pour permettre l'authentification sans mot de passe.

| | | | | | | | | | | _ |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------------|--|-----------------|--------------|----------------------|--------|---------|---|
| 💫 Desktop – sio@192.168.56.101 – WinSCP | | | | | | | | | | |
| 🖽 🕃 🗽 Synchroniser 🔉 🐙 🔯 🔅 🎒 File d'attente 🔹 Réglages de transfert Défaut 🔹 🧟 🔹 | | | | | | | | | | |
| 💷 sio@192.168.56.101 🗙 📮 sio@192.168.56.101 🗙 📮 Nouvel onglet 👻 | | | | | | | | | | |
| 🔚 Bureau 🔹 🚰 🔹 🗮 🗧 🗮 🗮 🔄 🐂 🔁 👘 😒 🍡 | | | | | | des fichiers | - | | | |
| 🛯 💼 Envoyer 👻 🗾 Éditer | 👔 Envoyer + 📓 Éditer + 🗙 🎿 🖺 Propriétés + 📷 Nouveau + 🖪 📰 🐨 👘 Télécharger + 📓 Éditer + 🗙 🚄 🖺 Propriétés + 📷 Nouveau + 🖬 📰 🐨 | | | | | | | | | |
| C:\Users\piffeteaujames\Desktop\ Local Marquer Fichiers Commandes Onglets Options Distant Aide | | | | | | | | | | |
| Nom | Taille | Туре | Date de modification | | /home/sio/.ssh/ | | | | | |
| 1 | | Répertoire parent | 17/10/2024 14:30:39 | | Nom | Taille | Date de modification | Droits | Proprié | |
| 🔊 desktop.ini | | | | | 1 | | | | | |
| 🔁 Docs.Ink | 2 KB | Raccourci | 17/10/2024 14:04:20 | | authorized kevs | 1 KB | 17/10/2024 16:19 | rw | 1000 | |
| 🖷 DSJamesPiffeteau - SI | 55 KB | Document Micros | 10/10/2024 15:21:44 | | id rsa | 2 KB | 17/10/2024 16:48 | rw | 1000 | |
| 🖷 kk.docx | 2 238 KB | Document Micros | 27/09/2024 15:00:17 | | id_rsa.pub | 1 KB | 17/10/2024 16:48 | rw-rr | 1000 | |
| 🔂 Microsoft Edge.Ink | 3 KB | Raccourci | 03/09/2024 10:22:16 | | known hosts | 1 KB | 17/10/2024 16:34 | rw-rr | 1000 | |
| 🚊 private key.ppk | 2 KB | PuTTY Private Key | 17/10/2024 14:30:39 | | public key | 1 KB | 17/10/2024 14:27:44 | rw | 1000 | |
| public key | 1 KB | Fichier | 17/10/2024 14:27:44 | | <u> </u> | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20241017"

AAAAB3NzaC1yc2EAAAADAQABAAABAQCfxhuT6QZy0auyuatBvZ8UFr1+4fFvnSfq QM4/ojYkmaINBIRFadiM4xpvMbDUIHiH/z0ox7SY/sacC1isPqHMSe/IrhayPXw9 b5TCGx+kgPAJfFD/T0qEf3/e0S2CHs5ds0RnR+qZBs03boTgKwR26T0V1qf6F0HA 5z7Ajnd54iq1uj1f74NTJr/L+0G2FKdfHP9PeIxV2mXaUd9IT9tS0/i0mPI5vk6F 1aIZnm+DM0tYL3vtLQKD1zcmuMV2gaot9WMBNKI5jRuEopSsTkLMGzmxQbNoxKnm 00j+kPRkGzkH25k8z4SeEJSJYW/85yYN47CF0p712fMIxLFe21tn

---- END SSH2 PUBLIC KEY ----

La clé public

ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQCfxhuT6QZy0auyuatBvZ8U Fr1+4fFvnSfqQM4/ojYkmaINBIRFadiM4xpvMbDUIHiH/zOox7SY/sacC1i sPqHMSe/IrhayPXw9b5TCGx+kgPAJfFD/TOqEf3/eOS2CHs5dsORnR+ qZBsO3boTgKwR26TOVIqf6F0HA5z7Ajnd54iq1uj1f74NTJr/L+OG2FKdf HP9PeIxV2mXaUd9IT9tSO/i0mPI5vk6F1aIZnm+DM0tYL3vtLQKD1zcm uMV2gaot9WMBNKI5jRuEopSsTkLMGzmxQbNoxKnm00j+kPRkGzkH2 5k8z4SeEJSJYW/85yYN47CFOp712fMIxLFe21tn sio@srv-home

// /home/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
// Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 = Éditeur = WinSCP -
/ Kome/sio/.ssh/authorized_keys = 192.168.56.101 =
/ Kome/sio/.ssh/author

Connexion avec PuTTY

Après avoir configuré l'authentification par clé publique, vous pouvez maintenant vous connecter à srv-home depuis Windows en utilisant PuTTY. Pour l'authentification, assurez-vous d'ajouter votre clé privée dans les paramètres de PuTTY, dans la section SSH / Auth sous Credentials.



On met l'adresse IP du Srv-home.



| B sio@svr-home: ~ | - | | × |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|------|---|
| login as: sio Authenticating with public key "rsa-key-20241017" Linux svr-home 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) |) x 8 | 6_64 | |
| The programs included with the Debian GNU/Linux system are free sof the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. | twar | e; | |
| Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Fri Oct 18 14:20:09 2024 from 192.168.56.1 sio@svr-home:~\$ | | | |