



Réalisation Technique

Sujet :

**Authentification Sécurisée sur
Debian: Clés SSH et
Cryptographie**

RÉALISÉ par : Darius ILOKI NZOUSSI



TABLE DES MATIERES

| | |
|---|----|
| 1. INTRODUCTION | 3 |
| 1.1 Résumé | 3 |
| 2. PRESENTATION DE LA REALISATION | 3 |
| 2.1 Contexte et enjeux | 3 |
| 2.2 Objectifs et problématique | 3 |
| 2.2.1 Objectifs | 3 |
| 2.2.2 Problématique | 3 |
| 3. ANALYSE FONCTIONNELLE | 4 |
| 4. PLAN D'IMPLEMENTATION | 4 |
| 5. Relisationtion | 5 |
| 5.1 Instalation des deux serveur Debian | 5 |
| 6 Prise en main à distance du serveur Debian par SSH avec MobaXterm | 17 |
| 6.1-1 Rappel..... | 17 |
| 7 Configuration de la Carte Réseau | 19 |
| 8 Configuration de la Carte Réseau | 21 |
| 9 Connexion avec SSH | 23 |
| 10 Sécurisation de la Connexion par Génération de Clé Asymétrique. | 25 |
| 11 Conclusion | 28 |



1. INTRODUCTION

1.1 Résumé

J'ai réalisé un projet technique portant sur la mise en place d'une authentification sécurisée sur un serveur Debian, en utilisant les clés SSH et les principes de cryptographie. Cette réalisation vise à renforcer la sécurité des accès aux infrastructures informatiques en remplaçant les mots de passe traditionnels par une authentification basée sur des clés asymétriques, tout en garantissant la confidentialité et l'intégrité des échanges. Pour ce faire, j'ai :

- ❖ Configuré un serveur Debian avec un service SSH sécurisé,
- ❖ Généré et déployé des paires de clés SSH (publique et privée),
- ❖ Mis en œuvre des bonnes pratiques de cryptographie pour protéger les données sensibles.

Ce projet m'a permis de développer des compétences en sécurisation des systèmes, gestion des accès et application des principes de cryptographie dans un contexte professionnel.

2. PRESENTATION DE LA REALISATION

2.1 Contexte et enjeux

Dans un environnement informatique où les cyberattaques sont de plus en plus fréquentes, garantir la sécurité des accès aux serveurs est une priorité. L'utilisation de mots de passe simples ou réutilisés expose les systèmes à des risques d'intrusion. La mise en place d'une authentification par clés SSH sur Debian répond à cet enjeu en offrant une méthode robuste et sécurisée pour contrôler les connexions à distance, tout en s'appuyant sur des mécanismes cryptographiques fiables.

2.2 Objectifs et problématique

2.2.1 Objectifs

- ❖ Installer et configurer un serveur Debian avec le service SSH,
- ❖ Générer et déployer des clés SSH pour une authentification sécurisée,
- ❖ Appliquer des techniques de cryptographie pour protéger les échanges et limiter les risques d'interception ou de compromission.

2.2.2 Problématique

Comment mettre en place une authentification sécurisée et efficace sur un serveur Debian pour protéger les accès aux infrastructures informatiques tout en assurant une gestion simple et scalable des utilisateurs ?



3. ANALYSE FONCTIONNELLE

Le système repose sur un serveur Debian hébergeant le service SSH (OpenSSH), configuré pour n'autoriser que les connexions par clés SSH, désactivant ainsi l'authentification par mot de passe. Les paires de clés (publique et privée) sont générées avec l'algorithme RSA, offrant un haut niveau de sécurité grâce à la cryptographie asymétrique. La clé publique est stockée sur le serveur, tandis que la clé privée reste sécurisée côté client, protégée par une passphrase si nécessaire. Cette architecture garantit une authentification forte et une protection contre les attaques par force brute.

4. PLAN D'IMPLEMENTATION

1. Installation de Debian : Déploiement de Debian 12 sur une machine virtuelle ou, mise à jour du système et installation du paquet OpenSSH.

2. Configuration du service SSH: Modification du fichier de configuration (`/etc/ssh/sshd_config`) pour désactiver l'authentification par mot de passe (`PasswordAuthentication no`) et activer l'utilisation des clés (`PubkeyAuthentication yes`).

3. Génération et déploiement des clés SSH : Création des paires de clés via la commande `ssh-keygen`, transfert sécurisé de la clé publique sur le serveur avec `ssh-copy-id`, et sécurisation de la clé privée côté client.

4. Tests et validation: Vérification de la connexion SSH avec les clés, simulation d'une tentative d'accès par mot de passe pour confirmer son interdiction, et analyse des logs pour valider le bon fonctionnement.



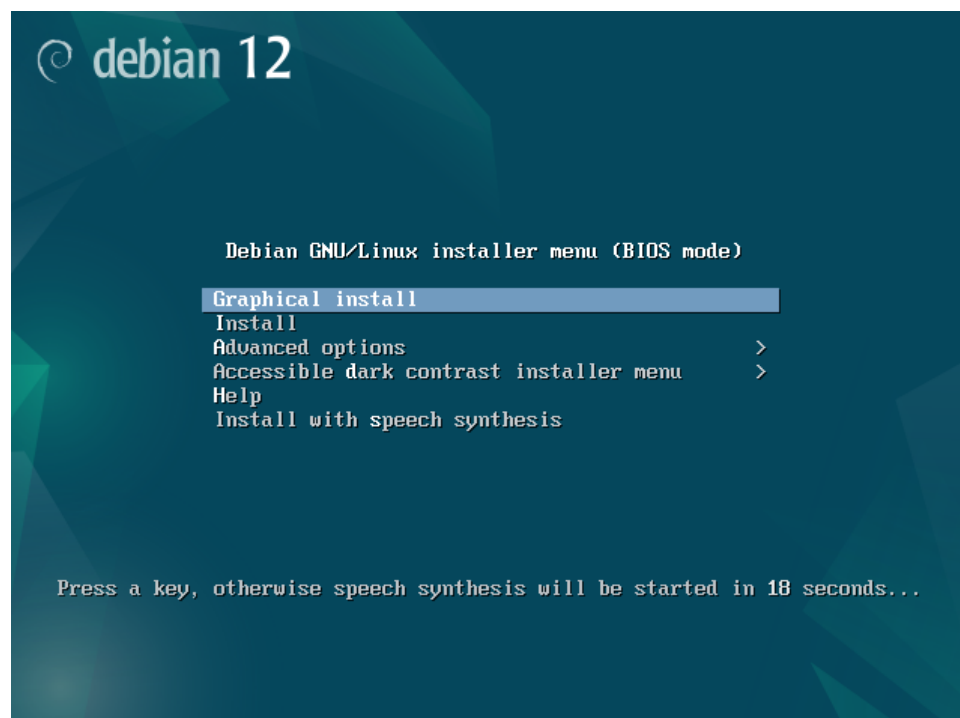
5. RELISATIONTION

5.1 Installation des deux serveur Debian

Rappel

Debian, initié en 1993 par Ian Murdock, est une distribution Linux réputée pour sa stabilité et sa sécurité. Grâce à APT et dpkg, la gestion des paquets est fluide, tandis que systemd facilite l'administration des services. Avec des outils comme adduser et passwd, elle reste flexible et adaptée aussi bien aux serveurs qu'aux développeurs en quête de fiabilité.

❖ Srv-deb1



L'installation de Debian 12 peut se faire en mode graphique ou en mode console, mais nous allons choisir le mode graphique.



debian 12

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

| | |
|-----------------------|-------------------|
| Chinese (Simplified) | - 中文(简体) |
| Chinese (Traditional) | - 中文(繁體) |
| Croatian | - Hrvatski |
| Czech | - Čeština |
| Danish | - Dansk |
| Dutch | - Nederlands |
| Dzongkha | - ཇོང་ཁྱེད་ |
| English | - English |
| Esperanto | - Esperanto |
| Estonian | - Eesti |
| Finnish | - Suomi |
| French | - Français |
| Galician | - Galego |
| Georgian | - ქართული |
| German | - Deutsch |

Screenshot

Go Back

Continue

Comme dans de nombreux assistants d'installation, il faut sélectionner la langue d'installation, de préférence celle du pays d'où la distribution est installée.

debian 12

Choix de votre situation géographique

Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.

La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.

Pays (territoire ou région) :

| |
|---------------|
| Belgique |
| Canada |
| France |
| Luxembourg |
| Suisse |
| Autre |

Capture d'écran

Revenir en arrière

Continuer



debian 12

Configurer le clavier

Disposition de clavier à utiliser :

- Danois
- Néerlandais
- Dvorak
- Dzongkha
- Espéranto
- Estonien
- Éthiopien
- Finnois
- Français**
- Géorgien
- Allemand
- Grec
- Gujarati
- Gourmoukhî
- Hébreu
- Hindi
- Hongrois

Capture d'écran Revenir en arrière Continuer

Il est ensuite possible de sélectionner le type de clavier associé à la machine pour l'installation.

debian 12

Configurer le réseau

Veuillez indiquer le nom de ce système.


Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

Srv-deb1

Capture d'écran Revenir en arrière Continuer

Une fois le CD ou DVD détecté, la configuration est automatiquement déterminée, puis l'assistant propose de nommer la nouvelle machine




Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

Domaine :

On peut proposer un nom de domaine si la machine fait partie d'un ensemble plus large, pour notre cas on laisse ce champ vide.



Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

☐ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

☐ Afficher le mot de passe en clair

Ici on va choisir un mot de passe pour le compte super utilisateur root.



L'assistant propose de créer un compte d'administration distinct de root, permettant de gérer le système avec des droits délégués.

Nous allons garder le même nom pour l'identifiant du compte



debian 12

Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

●●●●●●●●

☐ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

●●●●●●●●

☐ Afficher le mot de passe en clair

Capture d'écran Revenir en arrière Continuer

Il faut également fournir un mot de passe pour ce nouveau compte utilisateur, en veillant à le choisir suffisamment fort, car il dispose des droits d'administration du système.

debian 12

Partitionner les disques

Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.

Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.

Méthode de partitionnement :

- Assisté - utiliser un disque entier
- Assisté - utiliser tout un disque avec LVM
- Assisté - utiliser tout un disque avec LVM chiffré
- Manuel

Capture d'écran Revenir en arrière Continuer

Ensuite, il faut choisir le mode de partitionnement, nous ont choisis Assisté-utiliser un disque entier, et il est possible de chiffrer la partition ou de procéder à un découpage manuel et personnalisé.



debian 12

Partitionner les disques

Veillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.

Disque à partitionner :

SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

Capture d'écran Revenir en arrière Continuer

À ce stade, l'assistant devrait être capable de détecter le disque virtuel préalablement créé, et l'affichage correspondant devrait apparaître.

debian 12

Partitionner les disques

Disque partitionné :

SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB

Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.

Schéma de partitionnement :

Tout dans une seule partition (recommandé pour les débutants)


Partition /home séparée

Partitions /home, /var et /tmp séparées

Capture d'écran Revenir en arrière Continuer

Il faut choisir le mode de partitionnement, nous on choisit Tout dabs une seule partition



 **debian 12**

Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté

Configurer le RAID avec gestion logicielle

Configurer le gestionnaire de volumes logiques (LVM)

Configurer les volumes chiffrés

Configurer les volumes iSCSI

SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

> n° 1 primaire 20.4 GB f ext4 /

> n° 5 logique 1.0 GB f swap swap

Annuler les modifications des partitions

Terminer le partitionnement et appliquer les changements


Capture d'écran

Aide

Revenir en arrière

Continuer

Sur cette page, nous avons les informations sur notre partition.

 **debian 12**

Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :

SCSI3 (0,0,0) (sda)

Les partitions suivantes seront formatées :

partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4

partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

☐ Non

☒ Oui

Capture d'écran

Continuer

On peut alors choisir de répondre "Oui" pour procéder à l'installation, ou annuler si l'on ne souhaite pas écraser le contenu du disque virtuel utilisé.



debian 12

Configurer l'outil de gestion des paquets

L'analyse des supports d'installation a trouvé l'étiquette :

Debian GNU/Linux 12.4.0 _Bookworm_ - Official amd64 NETINST with firmware 20231210-17:56

Vous pouvez maintenant analyser des médias supplémentaires qui seront utilisés par l'outil de gestion des paquets (APT). En principe, ils devraient appartenir au même ensemble que le média d'amorçage. Si vous n'avez pas d'autres supports disponibles, vous pouvez passer cette étape.

Si vous souhaitez analyser d'autres supports, veuillez en insérer un autre maintenant.

Faut-il analyser d'autres supports d'installation ?

☒ Non

☐ Oui

Capture d'écran

Revenir en arrière

Continuer

debian 12

Configurer l'outil de gestion des paquets

L'objectif est de trouver un miroir de l'archive Debian qui soit proche de vous du point de vue du réseau. Gardez à l'esprit que le fait de choisir un pays proche, voire même votre pays, n'est peut-être pas le meilleur choix.

Pays du miroir de l'archive Debian :

- Corée du Sud
- Costa Rica
- Croatie
- Danemark
- Espagne
- Estonie
- Finlande
- France
- Grèce
- Géorgie
- Hong Kong
- Hongrie
- Inde
- Indonésie
- Iran


Capture d'écran

Revenir en arrière

Continuer

L'assistant détecte automatiquement le pays d'installation et propose le meilleur miroir disponible sur Internet.



 **debian 12**

Configurer l'outil de gestion des paquets


Veuillez choisir un miroir de l'archive Debian. Vous devriez utiliser un miroir situé dans votre pays ou votre région si vous ne savez pas quel miroir possède la meilleure connexion Internet avec vous.

Généralement, `deb.debian.org` est un choix pertinent.

Miroir de l'archive Debian :

- `deb.debian.org`
- `ftp.fr.debian.org`
- `debian.proxad.net`
- `ftp.ec-m.fr`
- `deb-mir1.naitways.net`
- `miroir.univ-lorraine.fr`
- `ftp.u-picardie.fr`
- `ftp.u-strasbg.fr`
- `mirror.plusserver.com`
- `debian.mirror.ate.info`
- `debian.univ-tlse2.fr`
- `ftp.rezopole.net`
- `ftp.univ-pau.fr`
- `mirrors.ircam.fr`

Il ne reste plus qu'à l'administrateur de sélectionner le miroir de son choix parmi la liste proposée.

 **debian 12**

Configurer l'outil de gestion des paquets

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée « `http://[utilisateur]:[mot-de-passe]@hôte[:port]/` ».

Mandataire HTTP (laisser vide si aucun) :

Si la configuration du réseau nécessite un serveur mandataire (proxy), l'assistant propose d'en nommer un, sinon il suffit de laisser le champ vide si ce n'est pas nécessaire.



Configuration de popularity-contest

Le système peut envoyer anonymement aux responsables de la distribution des statistiques sur les paquets que vous utilisez le plus souvent. Ces informations influencent le choix des paquets qui sont placés sur le premier CD de la distribution.

Si vous choisissez de participer, un script enverra automatiquement chaque semaine les statistiques aux responsables. Elles peuvent être consultées sur <https://popcon.debian.org/>.

Vous pourrez à tout moment modifier votre choix en exécutant « dpkg-reconfigure popularity-contest ».

Souhaitez-vous participer à l'étude statistique sur l'utilisation des paquets ?

☒ **Non**

☐ **Oui**

Capture d'écran Revenir en arrière Continuer

Si l'on souhaite participer à l'évolution de la distribution, on peut choisir de fournir (ou non) les statistiques d'utilisation des packages téléchargés.

Sélection des logiciels


Actuellement, seul le système de base est installé. Pour adapter l'installation à vos besoins, vous pouvez choisir d'installer un ou plusieurs ensembles prédéfinis de logiciels.

Logiciels à installer :

- ☐ environnement de bureau Debian
 - ☐ ... GNOME
 - ☐ ... Xfce
 - ☐ ... bureau GNOME Flashback
 - ☐ ... KDE Plasma
 - ☐ ... Cinnamon
 - ☐ ... MATE
 - ☐ ... LXDE
 - ☐ ... LXQt
 - ☐ serveur web
 - ☒ serveur SSH
- ☒ utilitaires usuels du système

Capture d'écran Continuer

L'assistant propose de sélectionner les logiciels à installer en plus du socle de base, en cochant simplement les cases correspondant aux fonctionnalités souhaitées.



Installer le programme de démarrage GRUB

Il semble que cette nouvelle installation soit le seul système d'exploitation existant sur cet ordinateur. Si c'est bien le cas, il est possible d'installer le programme de démarrage GRUB sur le disque principal (partition UEFI ou secteur d'amorçage).

Attention : si le programme d'installation ne détecte pas un système d'exploitation installé sur l'ordinateur, cela empêchera temporairement ce système de démarrer. Toutefois, le programme de démarrage GRUB pourra être manuellement reconfiguré plus tard pour permettre ce démarrage.

Installer le programme de démarrage GRUB sur le disque principal ?

☐ Non


☒ **Oui**

Capture d'écran

Revenir en arrière

Continuer

Le processus d'installation est presque terminé. Il reste à installer le chargeur de démarrage, et l'assistant propose automatiquement l'installation de GRUB.



Installer le programme de démarrage GRUB

Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le disque principal (partition UEFI ou secteur d'amorçage). Vous pouvez, si vous le souhaitez, l'installer ailleurs sur un autre disque, une autre partition, ou même sur un support amovible.

Périphérique où sera installé le programme de démarrage :

Choix manuel du périphérique

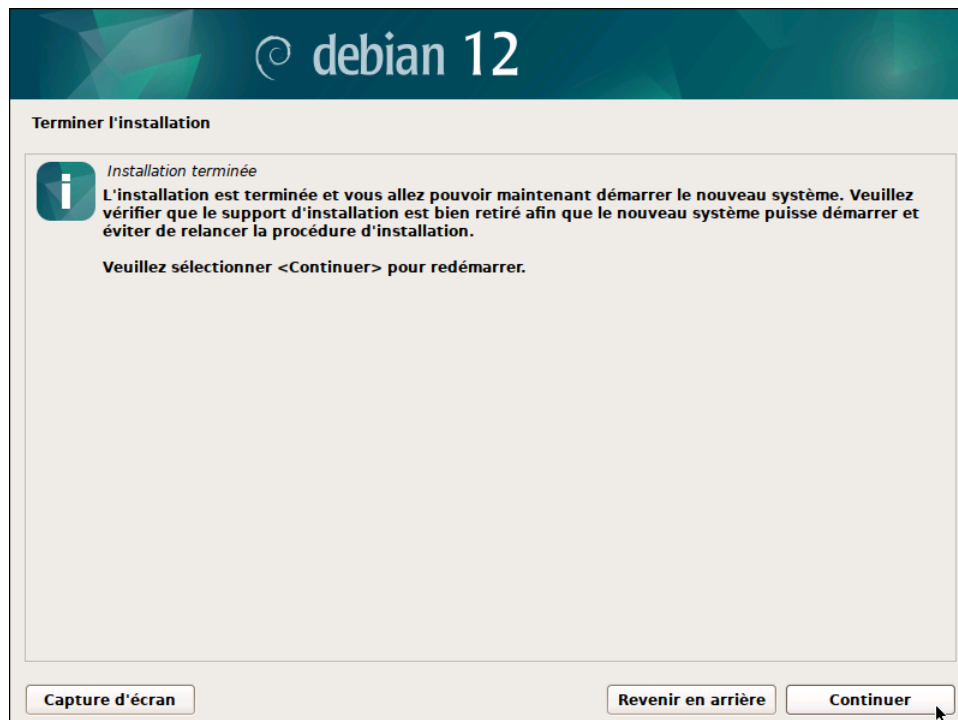
/dev/sda

Capture d'écran

Revenir en arrière

Continuer

Il faut sélectionner le disque sur lequel le secteur de démarrage sera installé, comme dans l'exemple où il s'agit du disque /dev/sda.



Enfin, l'assistant nous avertit que l'installation est terminée et que l'on peut désormais redémarrer le serveur sur le nouveau système.

6 Prise en main à distance du serveur Debian par SSH avec MobaXterm

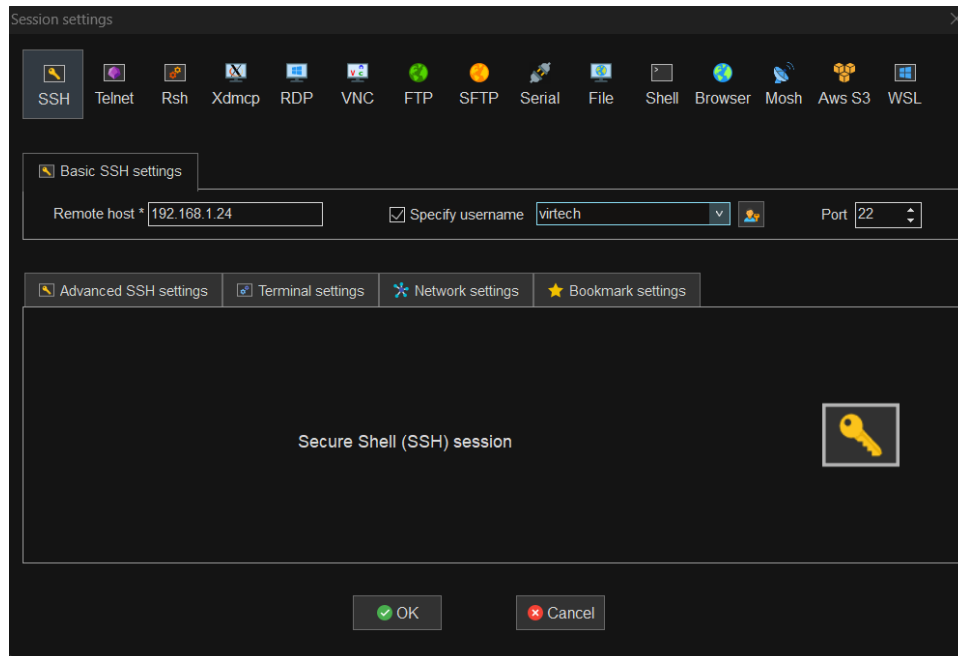
6.1-1 Rappel

SSH (Secure Shell), créé en 1995 par Tatu Ylönen, est un protocole essentiel pour administrer à distance des systèmes Unix/Linux de manière sécurisée. Il repose sur des commandes fondamentales telles que `ssh` pour se connecter, `scp` et `sftp` pour transférer des fichiers en toute sécurité, et `ssh-keygen` pour générer des clés cryptographiques. Avec son chiffrement puissant et ses capacités de tunneling, SSH demeure une référence incontournable pour la gestion des serveurs et le déploiement dans les infrastructures cloud.

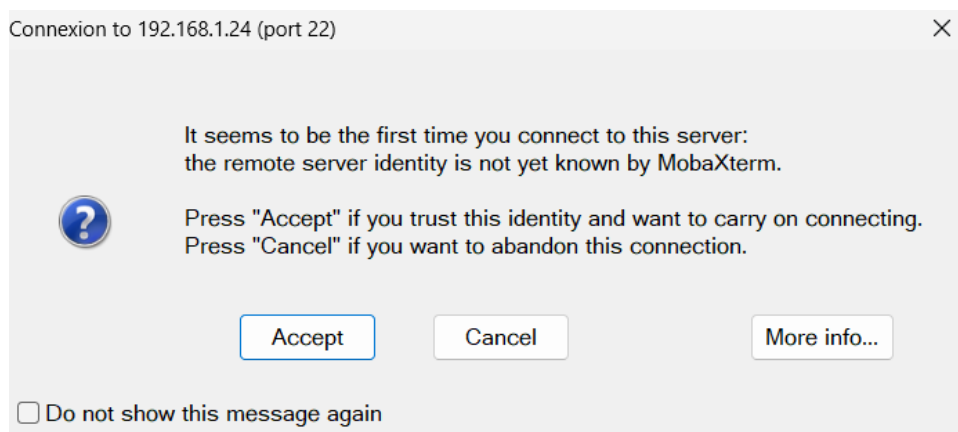
MobaXterm, conçu par Mobatek, est un terminal perfectionné sous Windows qui intègre SSH, SFTP et un serveur X11 dans une interface graphique intuitive. Il simplifie les connexions multiples, permet l'automatisation via des macros et facilite l'exécution de commandes à distance. Cet outil polyvalent est devenu indispensable pour les administrateurs système et les développeurs cherchant efficacité et flexibilité.



Première Connexion SSH avec MobaXterm



Explication : Cette capture montre la première tentative de connexion SSH à l'adresse IP 192.168.1.24 (port 22) via MobaXterm.



Une alerte indique que l'identité du serveur est inconnue, demandant à l'utilisateur d'accepter ou d'annuler la connexion pour établir une relation de confiance.



- ❖ Mettez à jour la liste des paquets disponibles et installez les dernières versions des paquets :

Le # au début de chaque ligne indique que vous devez être connecté au terminal avec les privilèges du compte **root** pour exécuter la commande.

```
# apt-get update && apt-get upgrade
```

7 Configuration de la Carte Réseau

- ❖ Nous allons configurer notre carte:

```
# nano /etc/network/interfaces
```

```
GNU nano 7.2 /etc/network/interfaces *  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
allow-hotplug ens33  
iface ens33 inet static  
    address 192.168.1.24  
    netmask 255.255.255.0  
    gateway 192.168.1.1  
  
# This is an autoconfigured IPv6 interface  
iface ens33 inet6 auto
```

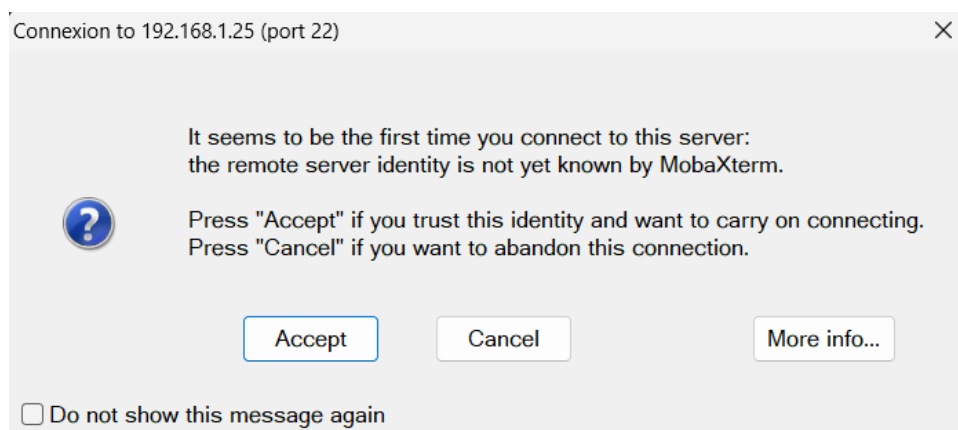
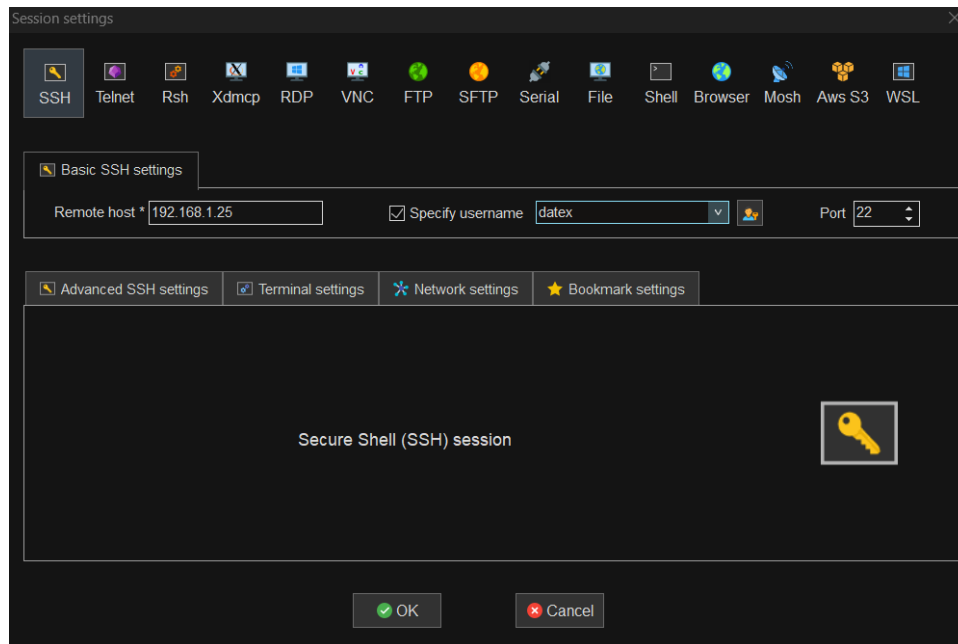
Voici la configuration de notre carte réseau.



- ❖ Ensuite, rechargez la configuration réseau :

```
systemctl restart networking
```

- ❖ On reproduit l'opération sur notre second serveur, Srv-deb2, avec datex comme utilisateur.



Cette figure illustre une nouvelle connexion SSH vers Srv-deb2 à l'adresse 192.168.1.25 (port 22) via MobaXterm, affichant une alerte comparable à celle de Srv-deb1, invitant à confirmer l'identité du serveur pour datex avant de continuer.



8 Configuration de la Carte Réseau

- ❖ Nous allons configurer notre carte:

```
# nano /etc/network/interfaces
```

```
GNU nano 7.2 /etc/network/interfaces *  
  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
allow-hotplug ens33  
iface ens33 inet static  
    address 192.168.1.25/24  
    gateway 192.168.1.1  
  
# This is an autoconfigured IPv6 interface  
iface ens33 inet6 auto
```

Voici la configuration de notre carte réseau.

- ❖ Ensuite, rechargez la configuration réseau :

```
systemctl restart networking
```



❖ Exploration des Serveurs Debian dans l'Écosystème VMware



L'image met en lumière l'environnement VMware hébergeant Srv-deb1 et Srv-deb2,

❖ Diagnostic de l'Activité du Service SSH Vérifions l'état du service SSH avec :

```
systemctl status sshd
```

```
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-03-30 07:59:43 CEST; 47min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 562 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 593 (sshd)
       Tasks: 3 (limit: 2273)
      Memory: 9.5M
         CPU: 557ms
    CGroup: /system.slice/ssh.service
            └─ 593 "sshd: /usr/sbin/sshd -D [listener] 1 of 10-100 startups"
               └─ 1241 "sshd: datex [priv]"
                  └─ 1242 "sshd: datex [net]"

mars 30 08:06:23 Srv-deb2 sshd[821]: Accepted password for datex from 192.168.1.12 port 56317 ssh2
mars 30 08:06:23 Srv-deb2 sshd[821]: pam_unix(sshd:session): session opened for user datex(uid=1000) by (uid=0)
mars 30 08:06:23 Srv-deb2 sshd[821]: pam_env(sshd:session): deprecated reading of user environment enabled
mars 30 08:06:23 Srv-deb2 sshd[823]: Accepted password for datex from 192.168.1.12 port 56321 ssh2
mars 30 08:06:23 Srv-deb2 sshd[823]: pam_unix(sshd:session): session opened for user datex(uid=1000) by (uid=0)
mars 30 08:06:24 Srv-deb2 sshd[823]: pam_env(sshd:session): deprecated reading of user environment enabled
```

La figure révèle la sortie de `systemctl status sshd`, confirmant que le service OpenSSH est actif (running), chargé depuis `/lib/systemd/system/ssh.service`, et prêt à gérer des connexions sécurisées sur le port 22.



❖ Inspection des Ports Actifs du Démon SSH

Identifions les ports SSH actifs via

```
Ss -lptun | grep sshd
```

```
root@Srv-deb2:~# ss -lptun | grep sshd
tcp    LISTEN 0      128      127.0.0.1:6010      0.0.0.0:*    users:((("sshd",pid=828,fd=9))
tcp    LISTEN 0      128      0.0.0.0:22         0.0.0.0:*    users:((("sshd",pid=593,fd=3))
tcp    LISTEN 0      128      [::]:22           [::]:*       users:((("sshd",pid=593,fd=4))
tcp    LISTEN 0      128      [::1]:6010        [::]:*       users:((("sshd",pid=828,fd=7))
root@Srv-deb2:~#
```

Cet écran expose les résultats de `ss -lptun | grep sshd`, indiquant que le démon SSH écoute sur le port 22 pour IPv4 et IPv6, validant son accessibilité réseau dans une configuration standard.

9 CONNEXION AVEC SSH

❖ Établissement de la Connexion SSH Initiale à Srv-deb1

Tentons une connexion SSH avec

```
Ssh user@ip
```

```
root@Srv-deb2:~# ssh virtech@192.168.1.24
The authenticity of host '192.168.1.24 (192.168.1.24)' can't be established.
ED25519 key fingerprint is SHA256:nENzeoB63xbj1QWKBWURmsbcjy5juUJzVE4D8cBgR8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.24' (ED25519) to the list of known hosts.
virtech@192.168.1.24's password:
Linux Srv-deb1 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) 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: Sun Mar 30 08:46:19 2025 from 192.168.1.12
virtech@Srv-deb1:~$
```

L'illustration présente une première connexion SSH vers Srv-deb1 depuis Srv-deb2 (ex. `ssh virtech@192.168.1.24`), affichant l'empreinte de la clé publique pour validation (yes) et demandant le mot de passe de virtech avant l'optimisation par clés.



❖ Liaison SSH par Nom d'Hôte vers Srv-deb1

Nous pouvons aussi faire la même chose avec le nom de notre serveur, Etant donné que nous sommes sur le serveur 2 (Srv-deb2) et que nous voulons nous connecter sur notre serveur 2 (Srv-deb1) nous allons taper `ssh virtech@Srv-deb1`, on fait on appelle le ssh suivi du nom d'utilisateur et du nom de serveur que nous voulons prendre la main.

```
virtech@Srv-deb1:~$ exit
déconnexion
Connection to 192.168.1.24 closed.
root@Srv-deb2:~# ssh virtech@Srv-deb1
The authenticity of host 'srv-deb1 (192.168.1.24)' can't be established.
ED25519 key fingerprint is SHA256:nENzeoB63xbj1QWKBWURmsbcjy5juUJzVE4D8cBgR8.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'srv-deb1' (ED25519) to the list of known hosts.
virtech@srv-deb1's password:
Linux Srv-deb1 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) 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: Sun Mar 30 08:53:41 2025 from 192.168.1.25
virtech@Srv-deb1:~$
```

L'image illustre une connexion SSH initiale depuis Srv-deb2 vers Srv-deb1 en utilisant le nom d'hôte (`ssh virtech@Srv-deb1`). Lors de cette première tentative, l'empreinte de la clé publique est affichée pour acceptation (yes), suivie de la saisie du mot de passe de virtech.

❖ Reconnexion Simplifiée à Srv-deb1.

```
virtech@Srv-deb1:~$ exit
déconnexion
Connection to srv-deb1 closed.
root@Srv-deb2:~# ssh virtech@192.168.1.24
virtech@192.168.1.24's password:
Linux Srv-deb1 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) 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: Sun Mar 30 08:58:47 2025 from 192.168.1.25
virtech@Srv-deb1:~$
```

Cet affichage met en évidence une seconde connexion SSH vers Srv-deb1 (par IP ou nom d'hôte), sans échange d'authentification, car la clé publique est déjà enregistrée dans `./ssh/known_hosts`, facilitant l'accès.



❖ Analyse des Hôtes Authentifiés via Commande

```
Less .ssh/known_hosts
```

```
[1|d6oRQfneXKcmwFrVPOM+/xujCnA=|IQr4FRl0hFnzR+8a1Pv10yoy+0= ssh-ed25519 AAAAC3NzaC1lZD11NTE5AAAAIMj91Zgh0A7p2FWJx1mbE+vFdC951dK3g04g0sKpoCmA  
[1|0y3b/C04puMgrr7B7JQU28nZwIk=|gxHeu0od0b+N8mC60+Bqk22CBVI= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQg0DrBV9YXokLo4kM0LrCD0Yz2rdFyh  
Cv5st1bSN2PeF1tojz747F16vvsjt8tp/6hLXT0pn2ft8GbumZvfGVVg+0812pChv2Xz1j3wqAzkko0zL9YIEcFR1qo03PhTtXl8hUs82knHb:Am55FThKYGMZoIdqm  
YznCbZMw4w45FtLr2Whe4YUkMUGZZTFp3G+YW/c2gwGnytfKCDaeXWdjzaGtpqIR81YF3GjXPWYzrVb1bttYzBj54EkRKGyW0Sj5yqrKITEAdoJvh+IP89F2b  
49Zgv9/Hu5T0apCq1C+WRxeFLZp+z003p0s10Zg7EnmmuP1ts2jvEJue2dXV4D094w0K8q8qshV0GLDFVABTq0umUoVts0CPTBNX/xHIT0L40q4SgLoL7n9rEH  
h1mHuk8dyo5QkZDDK0QM1dJZAWNmS0A10rNjHHPHftc9/eP7j/th78EbVF+UW501vB72vVakuRM05xSIG0HesC0ZdBUZZI3Roc=  
[1|N7dsn401Ye1LQvWF8n6Kx2UM/dc=|Mipmss+Xu0nTEL9L77PAn3qSX0E= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlkZHAyNTYAAAAIbmlkZHAyNTY  
AAABBDV2OpqJzaaRDM7tyi3uVF9GZ10yt7kYhGf0dSE7GRmyJq1K1VSXyKdWlsoj5/H6KXQK5RKEAUe1Rd8ork5RTRI=  
[1|US0bbbtVJ6wy075TDNUW01WC7E=|GTlud1c6/6AHsoocNmB07F18R5k= ssh-ed25519 AAAAC3NzaC1lZD11NTE5AAAAIMj91Zgh0A7p2FWJx1mbE+vFdC951dK3g04g0sKpoCmA  
~  
~
```

La figure montre la sortie de `less ~/.ssh/known_hosts`, permettant de vérifier les empreintes des clés publiques des serveurs précédemment connectés, confirmant que `Srv-deb1` est reconnu par le client SSH.

10 SECURISATION DE LA CONNEXION PAR GENERATION DE CLE ASYMETRIQUE.

Pour aller plus loin dans la connexion ssh et de se connecter sans saisir de mot de passe nous allons échanger des clés entre nos serveurs.

Générons une clé RSA avec :

```
ssh-keygen -t rsa -b 4096 -f /root/.ssh/id_rsa -N ""
```

```
root@Srv-deb2:~# ssh-keygen -t rsa -b 4096 -f /root/.ssh/id_rsa -N ''  
Generating public/private rsa key pair.  
Your identification has been saved in /root/.ssh/id_rsa  
Your public key has been saved in /root/.ssh/id_rsa.pub  
The key fingerprint is:  
SHA256:XGbkL0RoBQAFsCckDyvrT5oLwQLIHaLK7PIca6Lz7Yw root@Srv-deb2  
The key's randomart image is:  
+---[RSA 4096]-----+  
|o.o0o+o..++|  
|+*o.. o+|  
|*..+.. *|  
|B. o . = .|  
|=+ S . .|  
|+ . .|  
|oo..|  
|=o**|  
|o0Eo+|  
+----[SHA256]-----+  
root@Srv-deb2:~#
```

L'écran illustre l'exécution de `ssh-keygen -t rsa -b 4096 -f /root/.ssh/id_rsa -N ""` sur `Srv-deb2`, générant une paire de clés RSA (privée et publique) sans passphrase, avec empreinte et randomart, pour renforcer la sécurité des connexions.



❖ Contrôle de l'Intégrité de la Clé Privée

Nous pouvons voir notre clé en partant dans le fichier que nous avons créé pour stocké (id_rsa) avec la commande

```
Cat /root/.ssh/id_rsa
```

```
root@Srv-deb2:~# cat /root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAABm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEApf65yfHGMsv3lh34alhVsdvtlzEhcPG33dTCZc01HQwJT4yJHe1/
E6A3WbHsbckEYLbLeNhLub8wDjNFuBLIeCZlCvLx8zBtD9ddBJ2CcA/G4BxetWVXTLYGRp
g5lxaH5D7qd5G4kMbE0oXpmrdktejVEiittz7Cv66ac0tVfSRNKZsLn0RkqSzLILhzV4N4
+nshKaZx7zQGdD2QvEL7it3VU2+xGDgtWwexi4ncBIPlKqg/XDIcvy67hLZDBi1Nkouge1
Y7h/4ujTImPz6+rF5ibT80uYC+bPmxHQxLB0N0BLTGC0BNHTKoZncIgZt1oRRTLcxiLRv9
o8BLdx21TzaQLI9sxZQFIac010KN7WdLzNRIBmC3C8ygu2eCeaWsPzAwQYhuC8ndviX9XY
qNraqkJ+bSpulEj9cNkyv7BAb0LuhlbUWxx1FBF5pxHwi1yQsdwFjZi3kh3RtowRlBJYN
vQ4qzwGDL7CpstUtDb0n0KEgeyZDYPdYeMv65BXpm3b9PERkP3DqCyyjp4/me0Svr6kZAH
MuD0CBVW8ogtauGshpPjsh4azshNmYKPWIH0NGyNaYhlnvmzSPXnU6uN4G+PhSPBM56xcW
to85+zSDjQRxLg5Y0C2Fq+Eo1yVysbp7BnQ23mSwbXML+JV5eYfIj59MiUHWu0rVNez4fK
0AAAdIAfhITQH4SE0AAAAHc3NoLXJzYQAAAEApf65yfHGMsv3lh34alhVsdvtlzEhcPG3
3dTCZc01HQwJT4yJHe1/E6A3WbHsbckEYLbLeNhLub8wDjNFuBLIeCZlCvLx8zBtD9ddBJ
2CcA/G4BxetWVXTLYGRpg5lxaH5D7qd5G4kMbE0oXpmrdktejVEiittz7Cv66ac0tVfSRN
KZsLn0RkqSzLILhzV4N4+nshKaZx7zQGdD2QvEL7it3VU2+xGDgtWwexi4ncBIPlKqg/XD
Icvy67hLZDBi1Nkouge1Y7h/4ujTImPz6+rF5ibT80uYC+bPmxHQxLB0N0BLTGC0BNHTKo
ZncIgZt1oRRTLcxiLRv9o8BLdx21TzaQLI9sxZQFIac010KN7WdLzNRIBmC3C8ygu2eCea
WsPzAwQYhuC8ndviX9XYqNraqkJ+bSpulEj9cNkyv7BAb0LuhlbUWxx1FBF5pxHwi1yQs
dwFjZi3kh3RtowRlBJYNvQ4qzwGDL7CpstUtDb0n0KEgeyZDYPdYeMv65BXpm3b9PERkP3
DqCyyjp4/me0Svr6kZAHMuD0CBVW8ogtauGshpPjsh4azshNmYKPWIH0NGyNaYhlnvmzSP
XnU6uN4G+PhSPBM56xcWto85+zSDjQRxLg5Y0C2Fq+Eo1yVysbp7BnQ23mSwbXML+JV5eY
fIj59MiUHWu0rVNez4fK0AAADAQABAACAB6cQTqawchgYRpoEIXcIIGaTCv/vYEMsrHQ
KMGJZIAk1hq7fuFoCQVfijWcAFQFjhub2k5A5UYuAfI8b84vQFUYD6ELs6P7jEFdoCPXwF
RWNIJd+ntNYxocf2/JZuV8Hdd1etvuhbFLVqrUU05a/9GkTJb6tX6TrmqXEpisjel0JL7D
3xJh9EZWomc4XN0Iu+jFiEocDerlFzC7aZ0voX7shgjLEke7JHHWc6GeHNSgT8TChkMsYq
zH04Gv8xBSjnm2EjRspLHhQEGW6GHFenhjN5eaB2cixPvP2F/ZB1CdmeoI/DTa+N2nL/K9
h04R81FvZB9DWB+lh9MJBWHEmsLK5aZRG6g4w57mLQUEIdDKNm9GAxbFHDahjUzTC1is4a
/F6CJ8+f13I4PzHNKECPrR9yCwEzve3k7e/SkjU4q682xi6KA4oNjx7lkTTAD1xrK3ofxL
/AwMvx6qIx66x8tHJ8CUpzH58IXCtA09qU1V4shhmua+dg8g3+zStaTw4aKUNgg7jGmGHl
DPwAjCna6rw2oJu4ve0unirN3TwR9HxtHZ3MPq95GYUkepuzcDrLSGH/zJxqu8/Ku/H0w
/6B4QTHjfgRXm+Qja5m/fongg/g4xVjYmC56p58NXYS7RYyt3rgtw5cHC+MANLS6aFs8lw
0cgtTcCJAEntBCXavBAAABABKiIbI3cLRngtE/Bp38ov+hSpMS2xsZ4CDDiGMMLDvgUmdS
PusF71B2kc02KLQJhkn5SKY1es6u//til0ycQzTzBoX+VWfdj20rYtTY7DiKhqp3vxNQE
7RDoMr9x/d59Nk0UJN70LWY8ANFgVAcqig7Wyb0om+0S0RDT/LIIWu7m3iskUCLB4Z7dqI
33aYvmx9wd+hGHKpi+xlPzWdJm1vbSyV/DaYw51ia/utLEcGSRLKEgVghubxHI9vlyRek
lkCq/T3bomZT07mNce01M3qysyE0MtaA5uEDZE8RElvUSM2IkpTw+KLhdoSBYhm0F864No
o5/NbXSULE72IG8AAAEBAANGW4+kRjhFao6Ghk+3XRxHw1G5wfcHHCLuaEq3IHRtLx5cwj
UcWo8w+V38LdV/QoCQ2fZoyglIbe5wvghWrxorqQFh0sQSJYSTp+n/UE/2aPMEDw9LJ1B8
/rLG7rGmdzpBegJ0V9xvhFZWuikif8U6f2ov+Y7gmhsp0pF41HTdiwY0GIPkNmP5sQpmst
1bzD0JVGqu0knsNL0wyDsLj0gpHz8Up2BRd00aQz0L192eFz88VY4GqhpLhFEkInzP8/Aq
8bh48ch1y40qLB1Pw33f45GgUGmiaUBfLCfQQHmaKtbVn1kKb3xrEWg3qjM24Hdryyz/z
xXjk14C5HPjSkAAAEBAAMrAk4gkWL8T1mmo+tnp+PItkeko5PFVl3wjQlIPsJTKuE10TK2V
rPgPMofZwIdFN+KRuHuKCKDjftAAxpYcmr35JnMznF1RXBRdLLgW0tvRbJNBe1vP23bcbS
bGwT799+yH2eRcrL0gpIFNVpjW2bsWvfn4ZkfXEnI0qSWSIfYPJpkv5y6A3CJsoCmXY+L+
5D3gy0wHnE9+mWAwDpMju2V2dfmnpILmBbLmxSwIFAN112ZovMEM6RaCJ44CYsZBRG/g9
ma1FGfvS0Bn0hfsJdHSB5mSbawLU89RLdfTLvtYfBA+9N/Rqm3emMDi9CxEqvdr6slfpjS
W9EeIMiLX+UAAAANcm9vdEBTcnYtZGVIMgECAwQFBg==
```



La figure présente la vérification de la clé privée via une commande comme `cat /root/.ssh/id_rsa`, confirmant sa création et son stockage dans `/root/.ssh/`, prête pour l'authentification SSH.

❖ Examen de la Clé Publique Générée

Nous allons faire la même opération pour voir à quoi correspond notre clé publique avec la commande :

```
Cat /root/.ssh/id_rsa.pub
```

```
root@Srv-deb2:~# cat /root/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQCL/rnJ8cYyy/eWfHqWfWx22+XMSFw8bfd1MjLzTudDALPjKMd7X8ToDZsextwp5gtst42Eu5vzA0M8VRssh4JmVx
wXHzMG0P110EnYJwD8BgHF61ZVdMtG2GmDmXfokPup3kb1QxstShemat2S16NUSK23PsK/rppzS1V9JE0pmwuc5GSpLmsguHNXg3j6eyEppnHvNAYN3ZC8Sxuk3dVT
b7EYOC1ZZ7GLidwEg+UqQ9cMhy/LruEtKMLU2S16B7VjuH/16NOKY/Pr6sXmJtPw65gLSs+bEdGQUH03QGVMYLQE0dMqhdw1Bm3WhFFMsLGitG/2jwEt3HbVPNPAs
j2zFLAUhpzTU4o3tZ2XMIegYLcLzKC7Z4J5paw/MDBB1G4Lyd2+Jf1d1o2tqqQn5tI+m6USP1w2TK/sEBvQu6GVTrBHHUUEXnnEfCLXJCx1YWNmLeSHdG2jBGUElg29
DirDMY0XsKmy1S0NvSc4oSB7JkNg91h4y/rkFembdv08RG0/c0oLLK0nj+Z45K+vgRkAcY4PQIFVby1C1q4ayGk+0yHr0yE2Zgo9Ygf09b11p1GWe+bnI9edTq43gb4
+FI8EznrFxa2jzn7N1ONBHEuDLj0LYWr45jXJXKxunsGdDbeZJZtcwv4XL5h81Pn0yJQda7Stu17Ph8rQ== root@Srv-deb2
```

Cet affichage expose la sortie de `cat /root/.ssh/id_rsa.pub`, révélant la clé publique au format OpenSSH, préparée pour être partagée avec Srv-deb1 afin d'établir une connexion sécurisée.

❖ Propagation Sécurisée de la Clé Publique vers Srv-deb1

Après avoir réalisé ces opérations nous allons pouvoir partager notre clé publique sur notre deuxième serveur Srv-deb1 afin de se connecter sans tapé de mot de passe. Transférons la clé publique avec :

```
Ssh-copy-id -i /root/.ssh/id_rsa.pub virttech@Srv-deb1
```

```
root@Srv-deb2:~# ssh-copy-id -i /root/.ssh/id_rsa.pub virttech@Srv-deb1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
virttech@srv-deb1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'virttech@Srv-deb1'"
and check to make sure that only the key(s) you wanted were added.

root@Srv-deb2:~#
```

L'image montre l'exécution de `ssh-copy-id -i /root/.ssh/id_rsa.pub virttech@Srv-deb1`, transférant la clé publique de Srv-deb2 vers `~/.ssh/authorized_keys` sur Srv-deb1, avec une saisie initiale du mot de passe pour sécuriser l'opération.



❖ Validation de l'Intégration de la Clé sur l'Hôte Cible

En partant dans le répertoire `.ssh` confirmons la réception via

```
Cd /home/virtech/.ssh/
```

```
root@Srv-deb1:~# cd /home/virtech/.ssh/
root@Srv-deb1:/home/virtech/.ssh#
root@Srv-deb1:/home/virtech/.ssh# ls
authorized_keys
root@Srv-deb1:/home/virtech/.ssh# more authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCL/rnJ8cYyy/ewHfhqWFWx22+XMSFw8bFd1M1zTudDA1PjKMd7X8ToDdZsextwp5gtst42Eu5vzA0M9VRssh4JmVx
wX0lzN69P110EnYJwD8bghF61ZVdHtgZGmDmXoRkPup3Kb10xStShemat2s16NUSK23Psk/rppzS1V9JE9pmwuc565PLKsguHNg3J6eyEppnhVNAVN3ZC8SxK3dVt
b7EYOC1ZZ7GLdWeg4Uq99eMhy/LruEt4KGLU2S6b7Vjsh/r6N0KY/Pro6Xm3TPw65glSs+beDdGUHQ306VMYLQe0dMqmdwT8a3MhFFMsLGT6/2JwET3HbVPNgAs
j2zFLAUhpzTU4o3tZZXm1Eg6YLCLzKC7Z4J5paw/MDBB164Lyd2+Jf1dio2tqg0n5t1+m6USP1w2TK/sEBv0u6GVrBHHUUEXmEfCLXOCx1YmMLeSHdG2jBGUElq29
D1rDMYXSkmy1S8NvSc4oS87JKNg91h4y/rkfembdv88RG0/cDOLLK0nj+Z45K+vgRkAcy4P0IFVby1C1q4ayGk+0yHr0yE2Zgo9YgF08b11p1GWe+bnI9edTq43gb4
+FI8EznrFxa2jzn7N10N8HEuDLjQLYWr4SjXJXKxunsGdDbeZJZtcwv41X15h8iPh0yJQda7StU17Ph8rQ== root@Srv-deb2
```

La figure illustre l'accès à `/home/virtech/.ssh/` sur `Srv-deb1` (`cd /home/virtech/.ssh/`) et la vérification de `authorized_keys` (ex. `cat authorized_keys`), confirmant l'intégration réussie de la clé publique de `Srv-deb2`.

❖ Connexion Optimisée à `Srv-deb1` sans Authentification Manuelle

```
root@Srv-deb2:~# ssh virtech@192.168.1.24
Linux Srv-deb1 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) 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: Sun Mar 30 09:00:50 2025 from 192.168.1.25
virtech@Srv-deb1:~$
```

Cet affichage met en avant une seconde connexion SSH de `Srv-deb2` à `Srv-deb1` (ex. `ssh virtech@Srv-deb1`), réussie sans saisie de mot de passe, prouvant l'efficacité de l'authentification par clé publique pour une interaction sécurisée et fluide.

11 CONCLUSION

Ce projet a permis de sécuriser l'accès à distance sur deux serveurs Debian via des clés SSH, remplaçant les mots de passe par une authentification cryptographique robuste. Les étapes d'installation, de configuration et de validation ont assuré une connexion sécurisée et efficace. Il a renforcé mes compétences en administration Linux et cryptographie, offrant une base solide pour des projets futurs, potentiellement enrichis par une gestion centralisée des clés ou une authentification multi-facteurs.