Création d’un serveur à distance sur Azure

Systèmes d’exploitation II – 2268130

Table des matières

[Clés d’encryption asymétriques 2](#_Toc167700355)

[Comment fonctionne l’encryption asymétrique? 2](#_Toc167700356)

[Création de clés SSH-RSA 2](#_Toc167700357)

[Création d’une machine virtuelle sur Azure 3](#_Toc167700358)

[Ouverture de ports supplémentaires 6](#_Toc167700359)

[SSH 6](#_Toc167700360)

[Qu’est-ce que SSH? 6](#_Toc167700361)

[Connexion à la machine virtuelle par SSH 7](#_Toc167700362)

[Installation du serveur web 8](#_Toc167700363)

[Nom de domaine 8](#_Toc167700364)

[Installation de Nginx 8](#_Toc167700365)

[Sauvegarde du site avec RSync 9](#_Toc167700366)

[Planification de tâches avec Cron 9](#_Toc167700367)

[Serveur FTP 9](#_Toc167700368)

[Sources 10](#_Toc167700369)

# Clés d’encryption asymétriques

Avant de créer notre machine virtuelle Azure, il faudra créer une paire de clés d’encryption asymétrique SSH-RSA pour pouvoir s’identifier en se connectant à la machine.

## Comment fonctionne l’encryption asymétrique?

L’encryption asymétrique permet de s’échanger des clés d’encryption sur un réseau insécure, sans qu’une personne malveillante puisse les intercepter et les utiliser pour décrypter nos messages.

La personne qui souhaite recevoir un message encrypté va générer deux clés :

* La clé publique, qui permet d’encrypter les messages
* La clé privée, qui permet de décrypter des messages

Elle enverra la clé publique à la personne dont elle souhaite recevoir un message et gardera la clé privée pour elle-même.

~~Par exemple, Joe veut envoyer un message secret à John.~~

## Création de clés SSH-RSA

Dans Visual Studio Code, ouvrez PowerShell (CTRL + `)

Pour générer la paire de clés SSH, entrez ssh-keygen

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

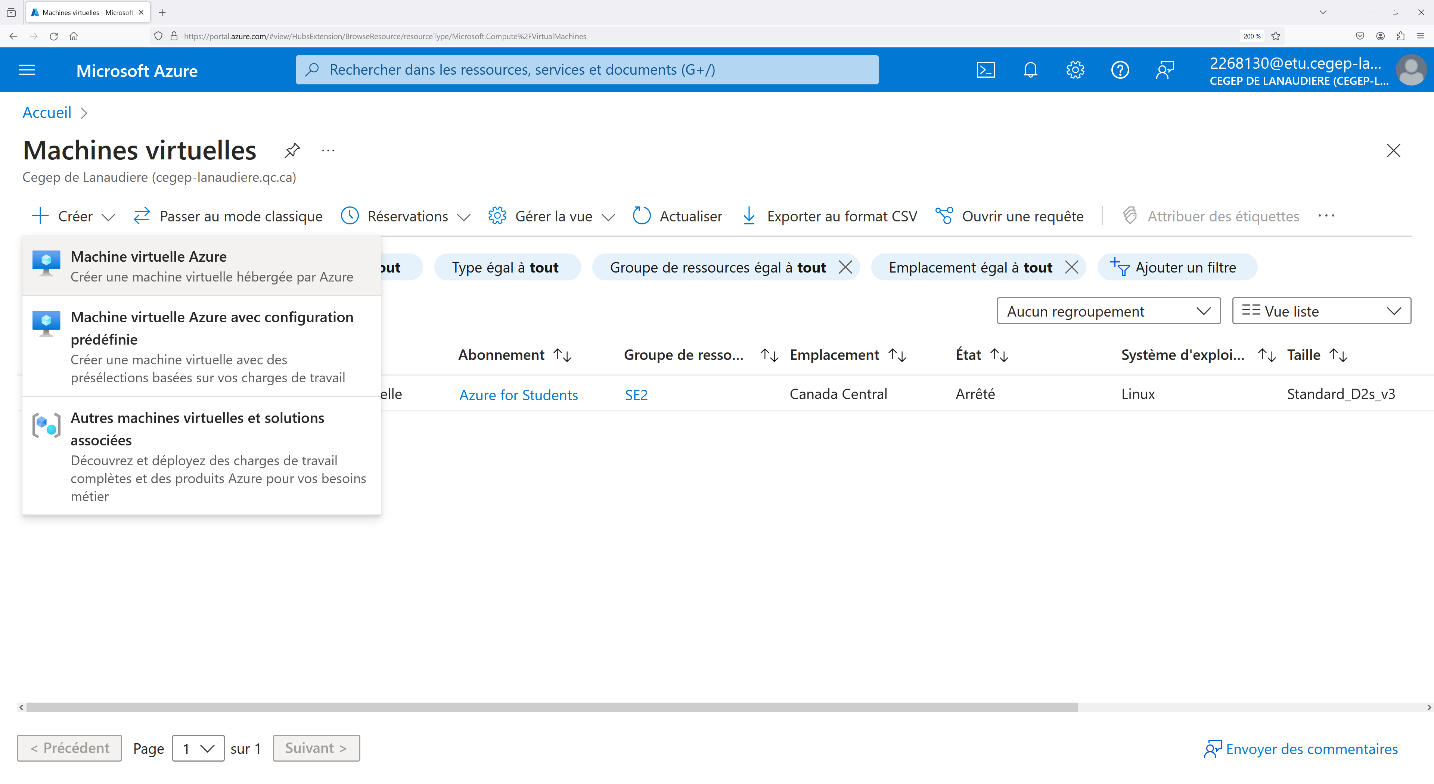
Ensuite, entrez ssh-add *chemin\_clé\_privée* pour ajouter la clé privée à l’agent d’authentification Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

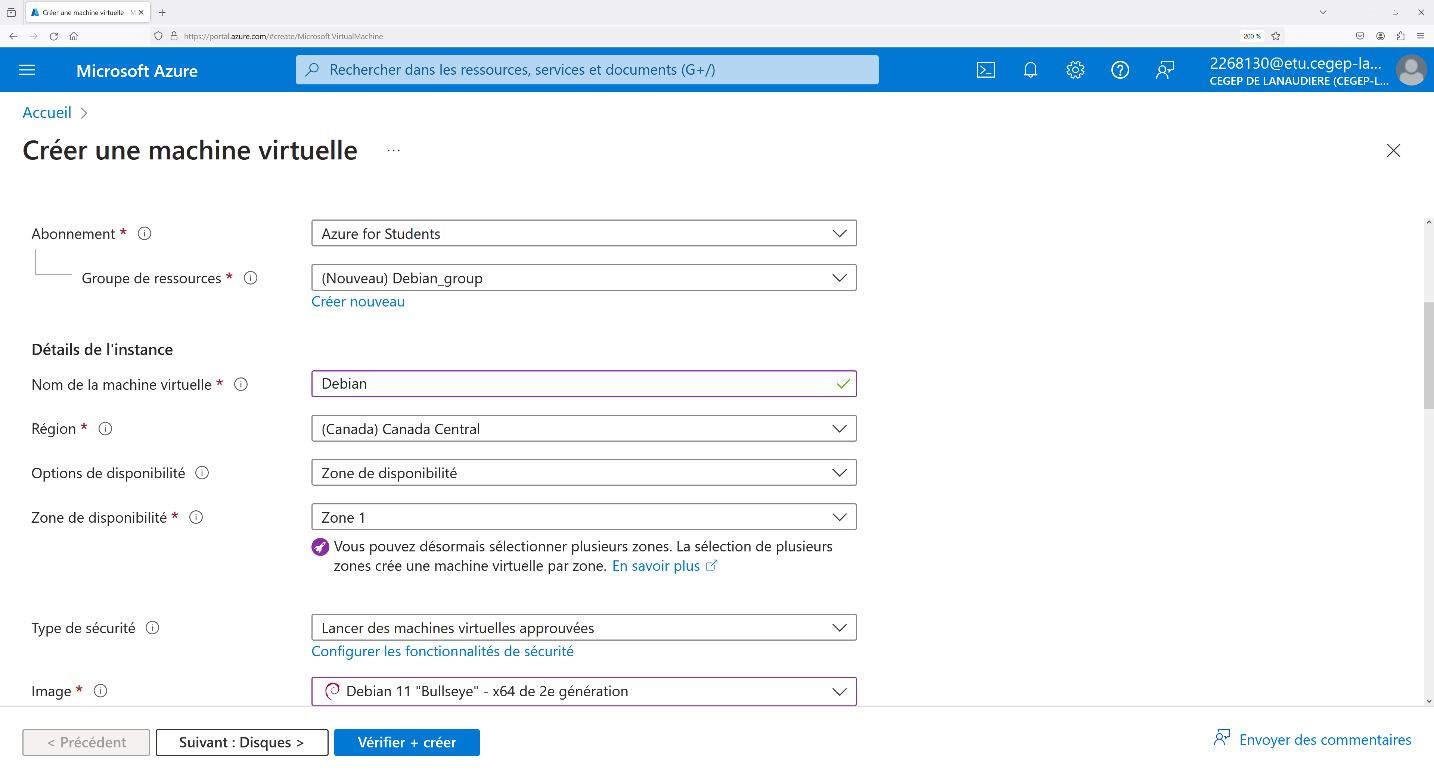
Si ça ne fonctionne pas… ->

# Création d’une machine virtuelle sur Azure

Connectez-vous sur le portail Azure puis cliquez sur Machines virtuelles. Ensuite, en haut à gauche de l’écran, cliquez sur créer >> Machine virtuelle Azure.



Sélectionnez un abonnement puis donnez un nom à votre machine virtuelle.

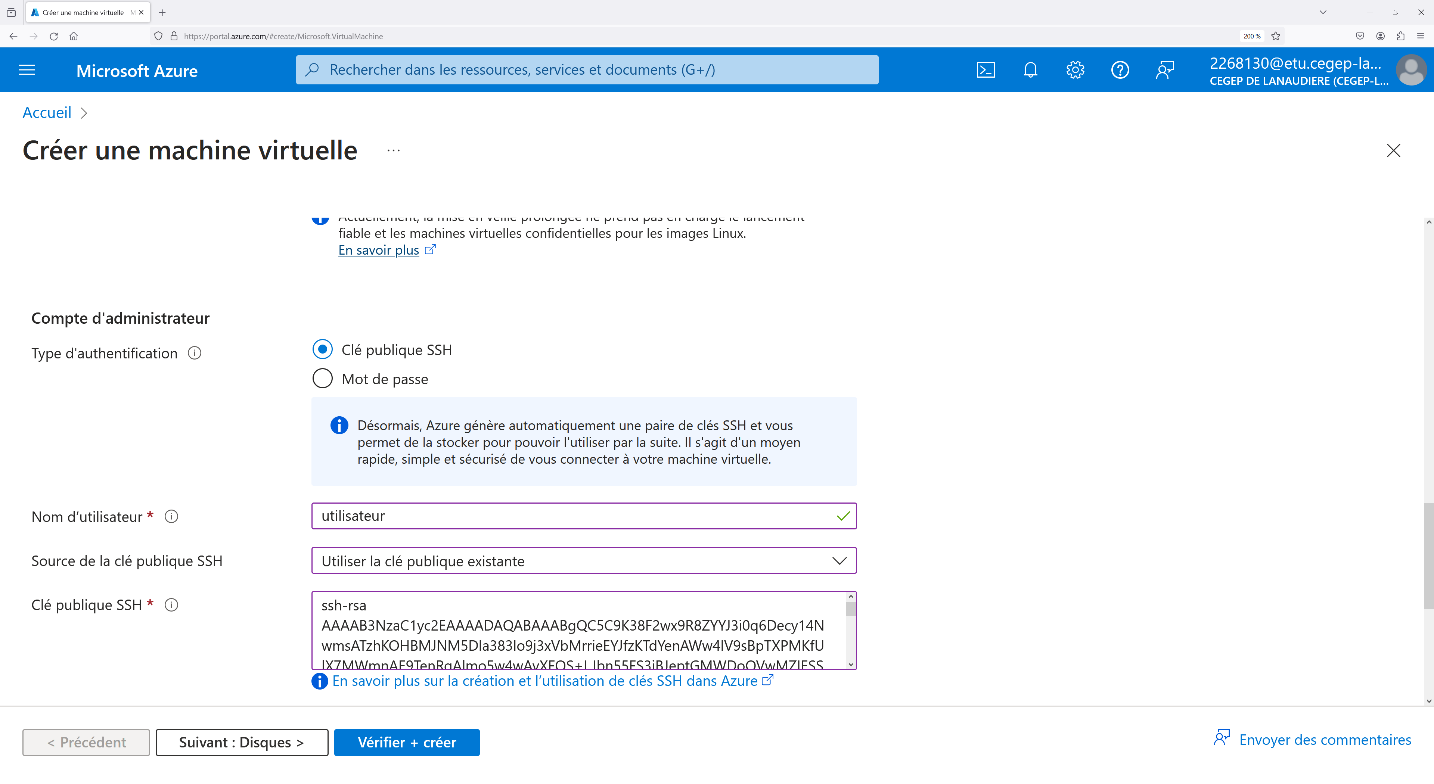


Pour avoir le moins de latence possible dans votre connexion au serveur, choisissez la région Canada central.

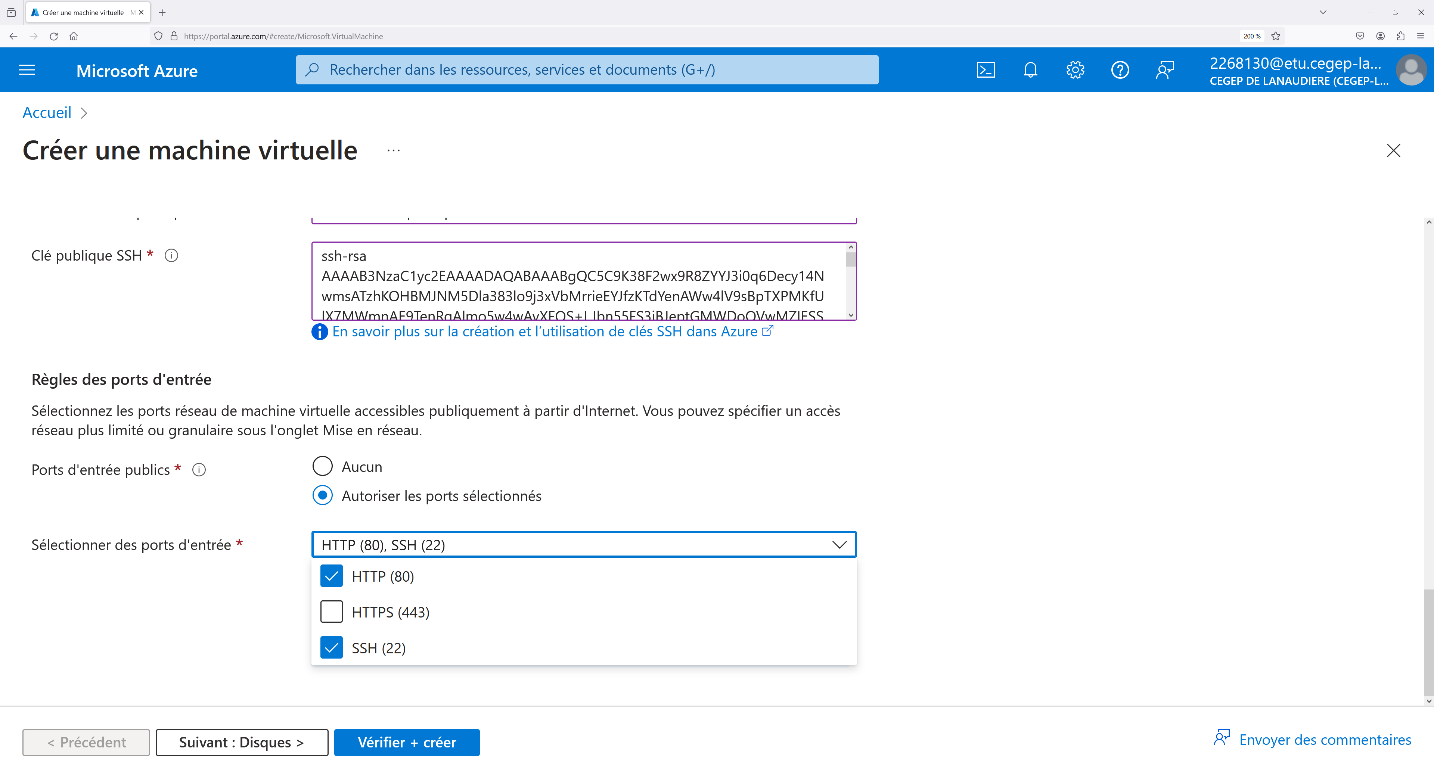
Prenez l’image Debian 11. C’est celle que nous utiliserons dans ce document.

Choisissez un nom d’utilisateur pour le compte d’administrateur.

Pour la section Source de la clé publique SSH, sélectionnez « Utiliser la clé publique existante ». Entrez le texte de votre clé publique SSH[[1]](#footnote-1) dans la boîte de texte.



Pour les règles de ports d’entrée, autorisez les ports 22 (SSH) et 80 (HTTP).



Laissez les autres options à leur valeur par défaut.

Cliquez sur « Vérifier + créer » pour créer votre machine virtuelle.

## Ouverture de ports supplémentaires

Pour pouvoir installer les serveurs FTP et DNS, il faudra ouvrir des ports supplémentaires avec trois nouvelles règles.

Dans vos ressources Azure, cliquez sur le nom de votre machine puis « Mise en réseau »

Cliquez sur Créer une règle de port > Règle de port d’entrée puis choisissez le service DNS (?). Sélectionnez l’action « Autoriser ». Vous pouvez laisser les autres paramètres par défaut.  
Cliquez sur « Ajouter ».

Pour ouvrir le port de contrôle FTP, Répétez la même étape mais choisissez le service FTP.

Pour ouvrir les ports de données FTP, créez une nouvelle règle d’entrée avec le service « Custom ». Entrez la plage de ports de destination 1000-10015. Choisissez le protocole (?)

# SSH

## Qu’est-ce que SSH?

SSH est un protocole qui permet d’accéder à un serveur à distance sécuritairement.

Voici comment la connexion avec le serveur est établie :

1. Le client envoie une demande de connexion au serveur
2. Le serveur envoie sa clé d’encryption publique\*
3. Le client vérifie l’identité du serveur avec la clé qui lui a été envoyée
4. Le client et serveur négocient les paramètres de connexion
5. Le serveur et le client établissent une communication encryptée symétriquement et hachée
6. Le client se connecte sur le système d’exploitation du serveur avec un mot de passe ou une clé publique

SSH peut être utilisé de diverses façons telles que l’exécution de commandes sur le serveur à distance ou le transfert de fichiers (SFTP).

## Connexion à la machine virtuelle par SSH

Dans la ligne de commande, entrez ssh *nom\_utilisateur*@*ip\_machine* pour ouvrir une session en ligne de commande sur la machine virtuelleUne image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

# Installation du serveur web

## Copie du site web vers le serveur à distance

Ouvrez un shell SFTP pour le transfert de fichiers vers le serveur : sftp *utilisateur*@*serveur*

Ensuite transférez récursivement les fichiers du site web : put -r *./racine\_site\_web*

Fermez le shell avec la commande bye.

## Nom de domaine gratuit

Dans le portail azure, cliquez sur votre machine virtuelle puis dans la section « Mise en réseau », cliquez sur l’adresse IP publique de celle-ci.

Entrez l’étiquette de nom DNS de votre choix, cliquez ensuite sur Enregistrer.

## Installation de Nginx

Mettez le système à jour :

sudo apt-get update

sudo apt-get upgrade

Ensuite, installez Nginx : sudo apt-get install nginx

Placez vous dans /etc/nginx/sites-available: cd /etc/nginx/sites-available

Utilisez l’éditeur de texte de votre choix pour créer un fichier avec le nom de votre site :   
*nano mon-site*

Écrivez le code suivant dans le fichier, en remplaçant le texte italique par les bonnes valeurs :

server {  
 listen 80;  
 server\_name *IP\_SERVEUR*;  
  
 location / {  
 root *chemin/répertoire/racine/du/site*;  
 index *index.html*; #Page d’acceuil  
 }  
}

Entrez l’adresse IP de votre serveur dans le fureteur de votre choix pour vérifier si le site fonctionne bien.

# Sauvegarde du site avec RSync

Premièrement, installez RSync : sudo apt-get install rsync

Deuxièmement, créez un dossier de sauvegarde : mkdir *backups*

Finalement faites la sauvegarde RSync avec cette commande : rsync -r *racine-site backups*

Pour restaurer le site avec la sauvegarde, entrez rsync -r *backups*/*racine-site*/ *racine-site*

# Planification de tâches avec Cron

Cron est un logiciel qui permet d’exécuter des tâches automatiquement, à des périodes de l’horaire prédéfinies.

Voici deux scripts pour les tâches différentes qui seront exécutées avec Cron :

* Sauvegarde automatique du site

rsync -r *racine-site* /home/utilisateur/sauvegarde

* Mise à jour système

apt-get update  
apt-get upgrade -y

Créez les scripts sur votre serveur : nano *sauvegarde.sh*, nano *mise-a-jour.sh*

Utilisez chmod pour rendre les scripts exécutables : chmod 700 *sauvegarde.sh* *mise-a-jour.sh*

Ouvrez la crontab de root : sudo crontab -e

Ajoutez-y les deux lignes suivantes pour que les scripts soient exécutés automatiquement selon des fréquences prédéfinies.

0 0 1 \*/6 \* */home/utilisateur/sauvegarde.sh*  
0 0 \* \* 0 */home/utilisateur/mise-a-jour.sh*

* La sauvegarde se fera deux fois par an, car le risque que le site soit endommagé / perdu est très faible.
* La mise à jour se fera une fois par semaine, pour que le système bénéficie des paquets les plus récents.

# Serveur FTP

Installez le logiciel de serveur FTP VSFTPD : sudo apt-get install vsftpd

Arrêtez VSFTPD puisqu’il n’est pas prêt : sudo systemctl stop vsftpd

Créez un utilisateur pour le serveur FTP : sudo useradd -mU ftpuser

Ensuite, donnez-lui un mot de passe : sudo passwd ftpuser

Créez un fichier qui contient la liste d’utilisateurs autorisés à utiliser le serveur FTP :  
sudo nano /etc/vsftpd.userlist

Ajoutez-y le nom de l’utilisateur créé. Si vous souhaitez mettre plus d’un utilisateur, entrez chaque nom sur des lignes différentes.

Ouvrez /etc/vsftpd.conf avec l’éditeur de texte de votre choix : sudo nano /etc/vsftpd.conf

Pour obliger les utilisateurs à se connecter pour utiliser le serveur FTP, assurez-vous que les deux lignes ci-dessous sont présentes, et décommentées.

anonymous\_enable=NO  
local\_enable=YES

Pour que seulement les utilisateurs de la liste soient autorisés à utiliser le serveur FTP, ajoutez les lignes suivantes :

userlist\_enable=YES  
userlist\_file=/etc/vsftpd.userlist  
userlist\_deny=NO

Pour contenir les utilisateurs et uniquement leur donner accès à leur repertoire FTP, ajoutez les lignes suivantes :

chroot\_local\_user=YES  
user\_sub\_token=$USER local\_root=/home/$USER/ftp  
allow\_writeable\_chroot=YES  
write\_enable=YES

Finalement, ajoutez les lignes ci-dessous pour définir la plage de ports qui pourront être utilisés pour le transfert de fichiers :

pasv\_enable=Yes  
pasv\_min\_port=10000  
pasv\_max\_port=10015  
pasv\_address=4.206.177.155

## Connexion au serveur FTP

# Serveur DNS

# Sources

~~Src ssh, def cron~~

1. Clé pour l’encryption de données. Est dans le même dossier que votre clé privée, le nom se termine par « .pub » [↑](#footnote-ref-1)