



Greta

LILLE MÉTROPOLE  
HAUTS-DE-FRANCE

GIP

CFA

AMIENS - LILLE  
HAUTS-DE-FRANCE

euroscol



# RAPPORT DE PROJET

Gestion d'un Parc Informatique : version 1

BTS CIEL

Etudiant1: ROZYCKI Noah  
Etudiant2: GRANDIN Matheo  
Etudiant3: LANGLET Matéo  
Etudiant4: AIT BRAHIM Anass

Juin 2025

Elisa LEMONNIER

# SOMMAIRE

<b>01</b>	<b>INTRODUCTION</b>	p. 3 à 4
<b>02</b>	<b>RÉSUMÉ DU CAHIER DES CHARGES</b>	p. 5 à 11
<b>03</b>	<b>MISSIONS ET TESTS</b>	p. 12 à 90
	ÉTUDIANT 1 (NOAH ROZYCKI)	p. 12 à 31
	ÉTUDIANT 2 (MATHEO GRANDIN)	p. 32 à 51
	ÉTUDIANT 3 (MATÉO LANGLET)	p. 52 à 71
	ÉTUDIANT 4 (ANASS AIT BRAHIM)	p. 72 à 90
<b>04</b>	<b>BILAN ET CONCLUSION</b>	p. 91
<b>05</b>	<b>ATTESTATIONS DE NON-PLAGIAT</b>	p. 92 à 95

# 01 Introduction

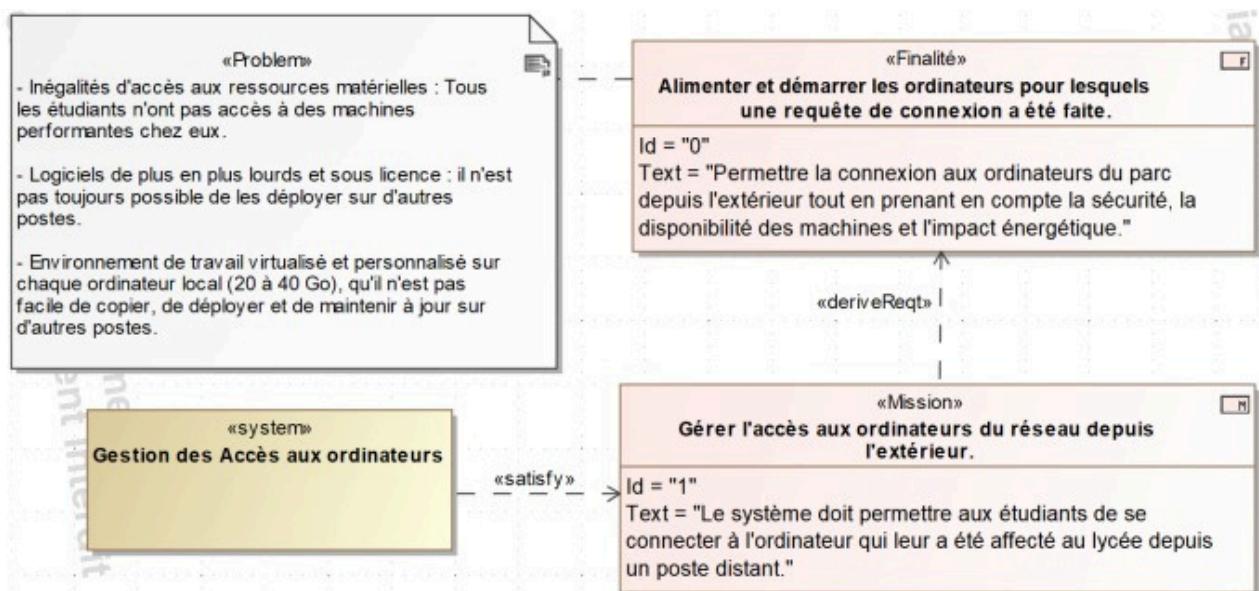
## Le contexte

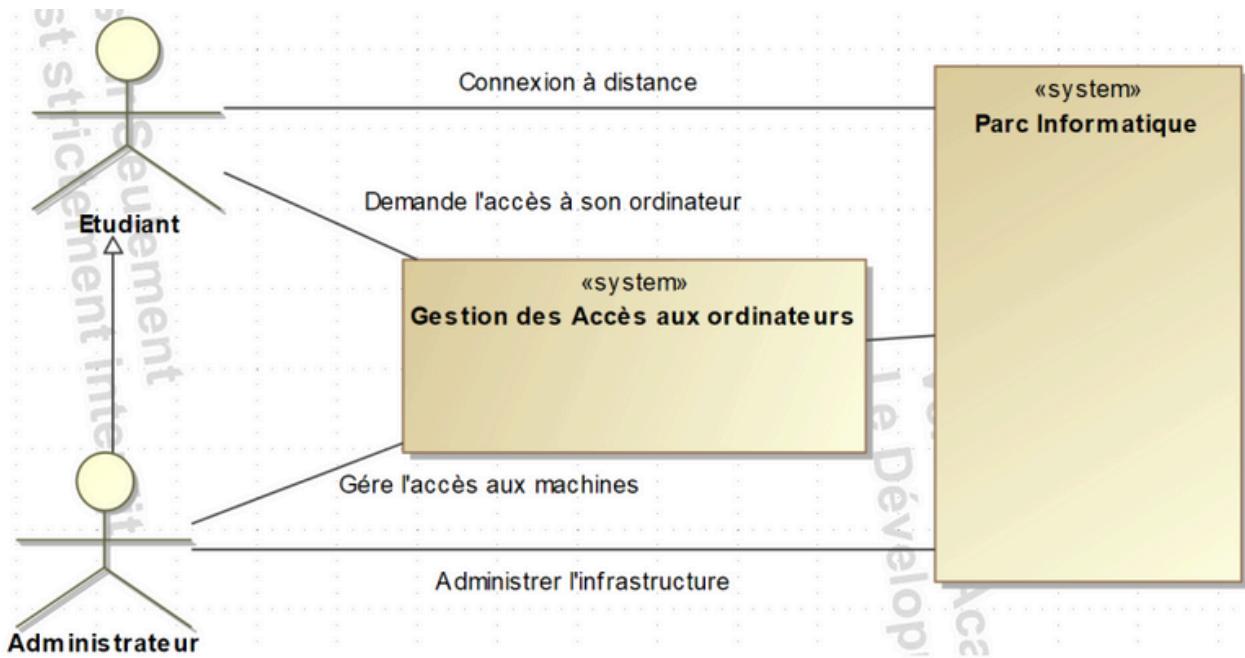
Il est 22h30. Adam, étudiant en BTS CIEL, est devant son ordinateur portable chez lui. Il est plongé dans son projet de développement, les idées fusent, il a trouvé une solution élégante pour optimiser son code. Il est prêt à tester... mais il se rend compte que le logiciel dont il a besoin n'est installé que sur les machines du lycée. Frustré, il essaie de trouver une alternative : il installe une version de démonstration du logiciel sur son PC, mais celle-ci manque de fonctionnalités. Il pense alors aux machines virtuelles, mais son ordinateur personnel n'a pas assez de ressources. Impossible d'avancer. Il doit attendre le lendemain, espérer qu'une machine sera disponible et qu'il pourra finir son projet à temps...

Imaginez maintenant que cette situation ne concerne pas seulement Adam, mais la moitié des étudiants du BTS. Certains doivent abandonner leur travail en pleine progression, d'autres ne peuvent pas pratiquer sur les logiciels professionnels à domicile, et tous perdent un temps précieux.

C'est là que notre projet prend tout son sens. Il répond à un besoin réel et urgent : permettre aux étudiants d'accéder aux machines du lycée à distance, comme s'ils étaient sur place, sans subir les contraintes horaires ou matérielles.

Avec ce projet, Adam et ses camarades ne seraient plus limités. Ils pourraient accéder à leurs outils quand ils en ont besoin, terminer leur projet sans interruption et maximiser leur productivité. Cette solution leur offrirait une nouvelle liberté d'apprentissage et garantirait une meilleure gestion informatique pour l'établissement.





L'équipe pédagogique du BTS CIEL souhaite mettre en place une solution de gestion de son parc informatique qui permettra aux étudiants, l'accès à distance à leur ordinateur du lycée.

Le système devra prendre en compte les aspects suivants :

- Gérer les plages de disponibilité des machines.
- Prendre en compte l'impact énergétique en évitant de laisser en permanence les machines sous tension.
- Gérer la sécurité d'accès aux machines.

Cette solution, au delà d'autoriser un accès à distance aux poste du lycée, doit faciliter l'accès à un outil informatique assez performant pour parfaire leur formation, le but est surtout de permettre aux étudiants d'avoir à leur disposition, un outil informatique assez performant nécessitant un certain budget financier pour l'avoir chez soi.

Ainsi, tous les étudiants inscrit dans la formation pourrons consulter leur fichiers enregistrés sur la machine, leurs machines virtuelles par exemple (ceci étant un dispositif très gourmand en espace de stockage).

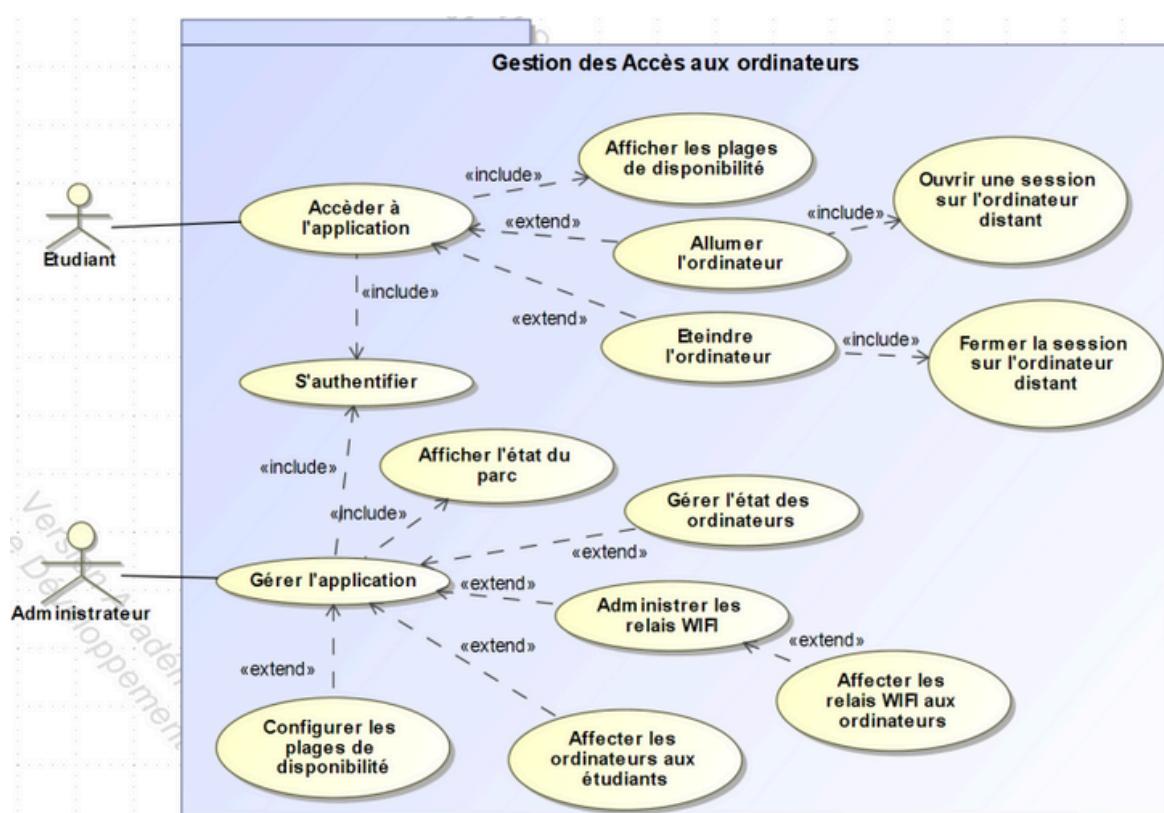
# 02 Résumé du cahier des charges

## Cas d'utilisations principaux

Pour gérer l'application, l'administrateur se connecte depuis un poste distant à l'application, puis s'authentifie pour accéder aux fonctionnalités. L'application affiche alors les ordinateurs utilisés avec les informations suivantes : étudiant connecté et heure de connexion. L'administrateur peut ensuite choisir l'une des autres options pour gérer l'application.

Pour gérer l'état des ordinateurs, l'administrateur sélectionne un ou plusieurs ordinateurs utilisés pour programmer une heure d'extinction ou les arrêter directement. Pour administrer les relais WIFI, l'administrateur gère la base de données pour ajouter, supprimer ou modifier un relais WIFI, caractérisé par un nom d'hôte, une adresse IP et son adresse MAC. Pour affecter les relais WIFI aux ordinateurs, l'administrateur gère la base de données pour associer les relais WIFI aux ordinateurs en respectant le plan de câblage électrique.

Pour affecter les ordinateurs aux étudiants, l'administrateur gère la base de données pour ajouter, supprimer ou modifier une affectation d'ordinateur à un étudiant. Un étudiant ne peut se connecter qu'à l'ordinateur qui lui a été affecté. Pour configurer les plages de disponibilité, l'administrateur configure les plages de disponibilité des ordinateurs par section. Un étudiant ne doit pas pouvoir se connecter à distance sur une machine si elle est déjà utilisée par un autre étudiant en présentiel ou en dehors des plages définies.



Pour accéder à l'application, l'étudiant se connecte depuis un poste distant à l'application, puis s'authentifie pour accéder aux fonctionnalités. L'application affiche alors les plages horaires disponibles et l'état actuel de son ordinateur (disponible ou déjà utilisé). Pour allumer l'ordinateur, l'étudiant demande le démarrage de son ordinateur distant. Le système assure l'alimentation électrique de l'ordinateur via le relais WIFI et envoie un ordre de démarrage (wake-on-LAN). L'étudiant utilise ensuite le bureau à distance pour ouvrir une session sur son ordinateur.

Pour éteindre l'ordinateur, l'étudiant demande l'arrêt de son ordinateur distant après avoir fermé correctement sa session depuis le bureau à distance. Le système vérifie si l'ordinateur a été arrêté correctement, sinon il envoie une requête pour l'arrêter. Enfin, le système envoie une requête au relais WIFI pour couper l'alimentation électrique de l'ordinateur.

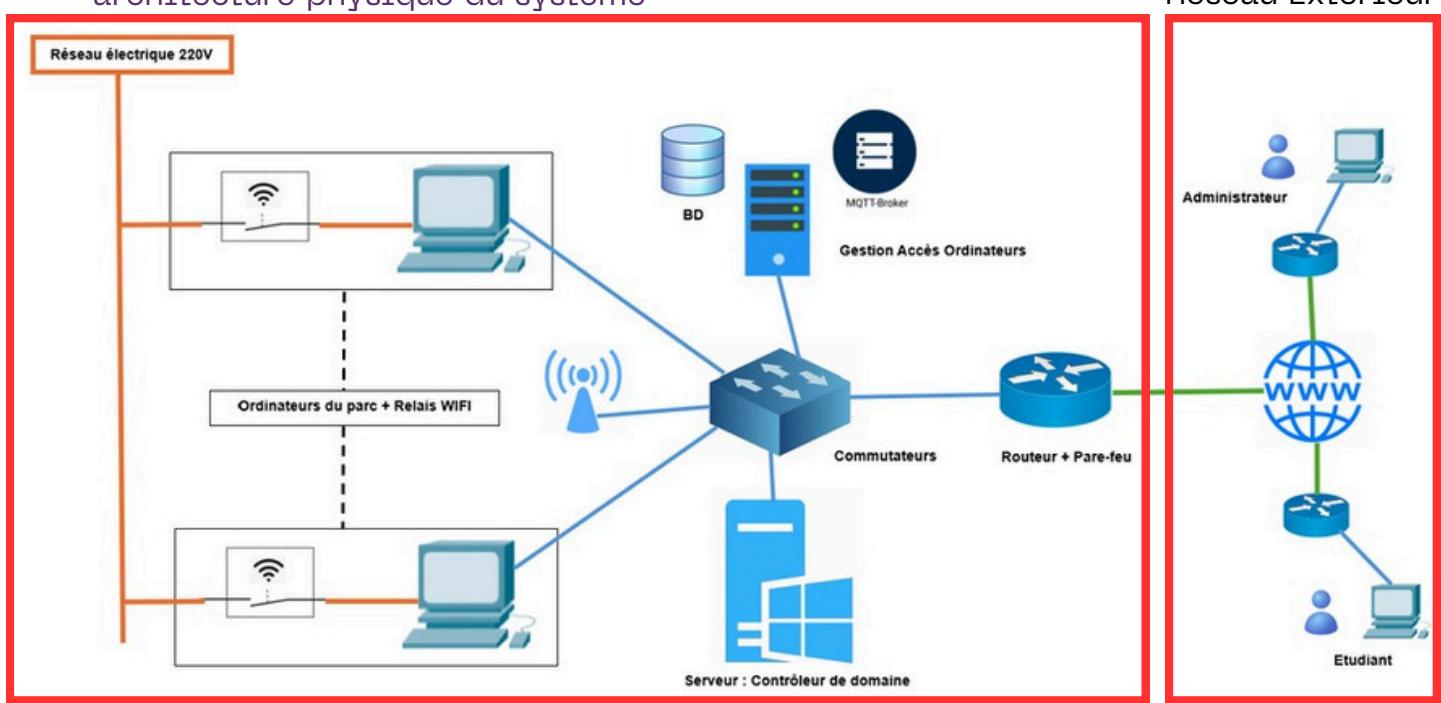
## Exigences du Système

Le système doit permettre l'authentification des utilisateurs, afficher graphiquement les informations, permettre la connexion et l'arrêt à distance des ordinateurs, gérer les plages de disponibilité et les relais WIFI.

## Architecture du Système

Le système repose sur une Raspberry Pi pour héberger l'application, avec un routeur, un pare-feu, des commutateurs, un serveur contrôleur de domaine, des points d'accès WIFI et des relais WIFI.

architecture physique du système



Réseau du lycée

## Tâches Professionnelles

Nos tâches professionnelles comprennent l'installation et la configuration de Windows Serveur 2022, du contrôleur de domaine, des services DNS et DHCP, la création des comptes utilisateurs et des ordinateurs, l'installation et la configuration des règles de filtrage sur le routeur et le pare-feu, la configuration du BIOS (wake-on- LAN) et le développement logiciel pour les modules de connexion, d'authentification, de gestion des plages de disponibilité, de démarrage/arrêt des ordinateurs et de gestion des relais WIFI.

### Répartition des tâches à accomplir

Tâches professionnelles à réaliser	Étudiant 1	Étudiant 2	Étudiant 3	Étudiant 4
<b>Architecture Matérielle</b>				
<b>Serveur</b>				
Installation et configuration de Windows Serveur 2022	✓			
Installation et configuration du contrôleur de domaine	✓			
Installation et configuration des services DNS et DHCP	✓			
Création des comptes utilisateurs et des ordinateurs	✓			
Création des stratégies de groupe nécessaires	✓			
Mise en place et configuration d'une connexion sécurisée d'accès au réseau local (VPN).		✓		
Routeur et pare-feu : Installation et configuration des règles de filtrage.		✓		
<b>Ordinateurs du parc</b>				
Installation et configuration de Windows 11			✓	
Configuration du BIOS (wake-on-LAN)			✓	
Point d'accès WiFi : Installation et configuration				✓
Relais WiFi (Sonoff Basic R2) : Mise à jour du firmware et configuration.				✓
<b>Poste de Gestion Accès Ordinateur</b>				
Installation et configuration du système d'exploitation			✓	
Installation et configuration du serveur de base de données			✓	
Installation et configuration du Broker MQTT				✓
<b>Développement Logiciel</b>				
Conception de la base de données	✓	✓	✓	✓
Implémentation de la base de données		✓		
Module logiciel de connexion et d'authentification		✓		
Module logiciel « Afficher les plages de disponibilité »			✓	
Module logiciel « Allumer l'ordinateur »				✓
Module logiciel « Eteindre l'ordinateur »				✓
Module logiciel « Afficher l'état du parc »		✓		
Module logiciel « Configurer les plages de disponibilité »			✓	
Module logiciel « Gérer l'état des ordinateurs »			✓	
Module logiciel « Administrer les ordinateurs »	✓			
Module logiciel « Administrer les étudiants »	✓			
Module logiciel « Affecter les ordinateurs »		✓		

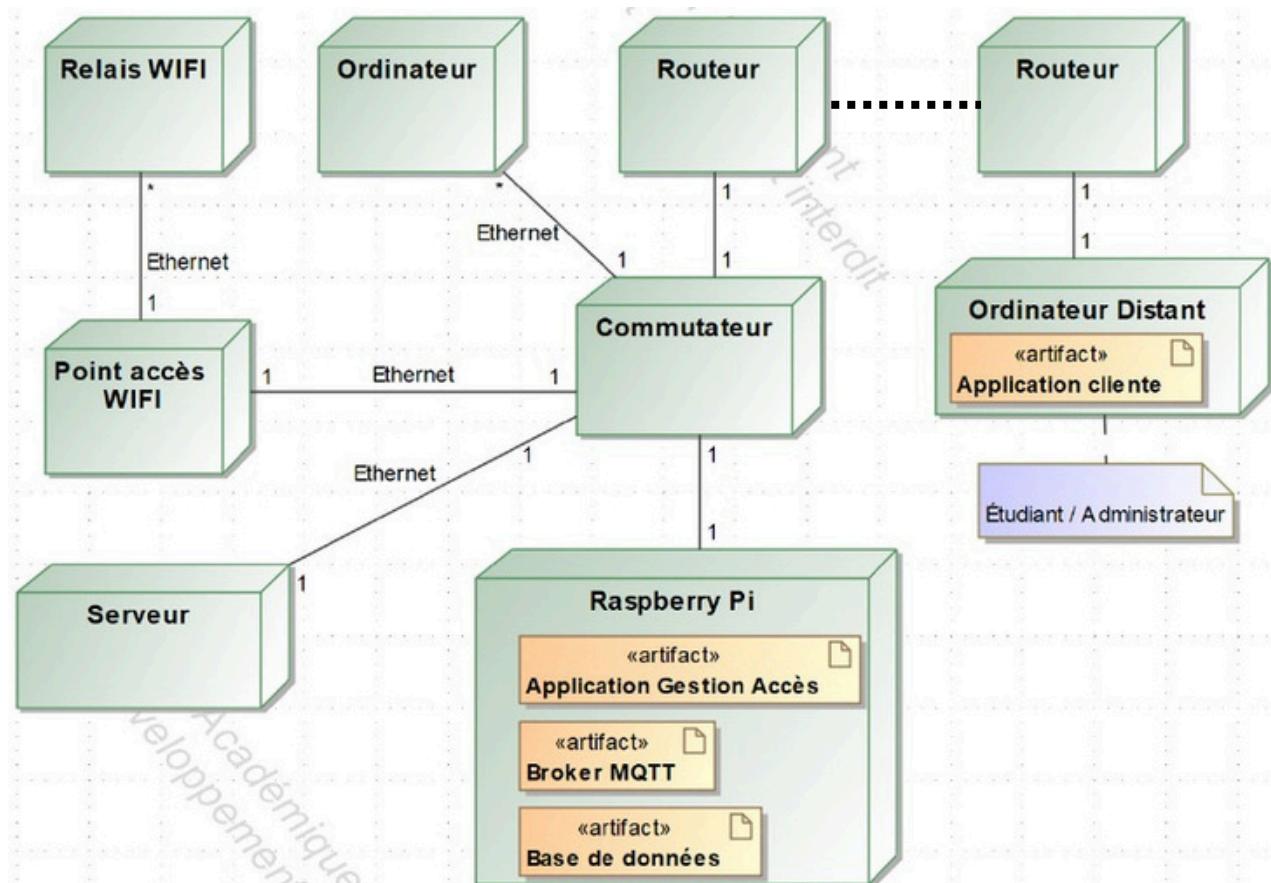
Le système repose sur plusieurs composants interconnectés pour permettre la gestion des accès à distance aux ordinateurs du parc. Tout d'abord, les relais WIFI sont connectés aux ordinateurs du parc pour gérer l'alimentation électrique des machines. Les ordinateurs, quant à eux, sont accessibles à distance par les étudiants et sont connectés au réseau via un commutateur.

Un routeur est utilisé pour gérer le trafic réseau entre les différents composants, tandis que les points d'accès WIFI permettent la connexion sans fil des utilisateurs, qu'ils soient étudiants ou administrateurs. L'application de gestion des accès est hébergée sur un Raspberry Pi, connecté au réseau via Ethernet. Ce Raspberry Pi communique avec le reste du système grâce à un broker MQTT, qui gère la communication entre les différents éléments.

Le serveur héberge la base de données et le broker MQTT. La base de données stocke les informations concernant les utilisateurs, les ordinateurs, les plages de disponibilité et d'autres paramètres essentiels. Les étudiants et les administrateurs se connectent à l'application via le point d'accès WIFI ou directement via le réseau Ethernet pour accéder aux fonctionnalités de gestion des accès.

Le système doit permettre l'authentification des utilisateurs, afficher graphiquement les informations, permettre la connexion et l'arrêt à distance des ordinateurs, gérer les plages de disponibilité et les relais WIFI.

Diagramme de déploiement V1

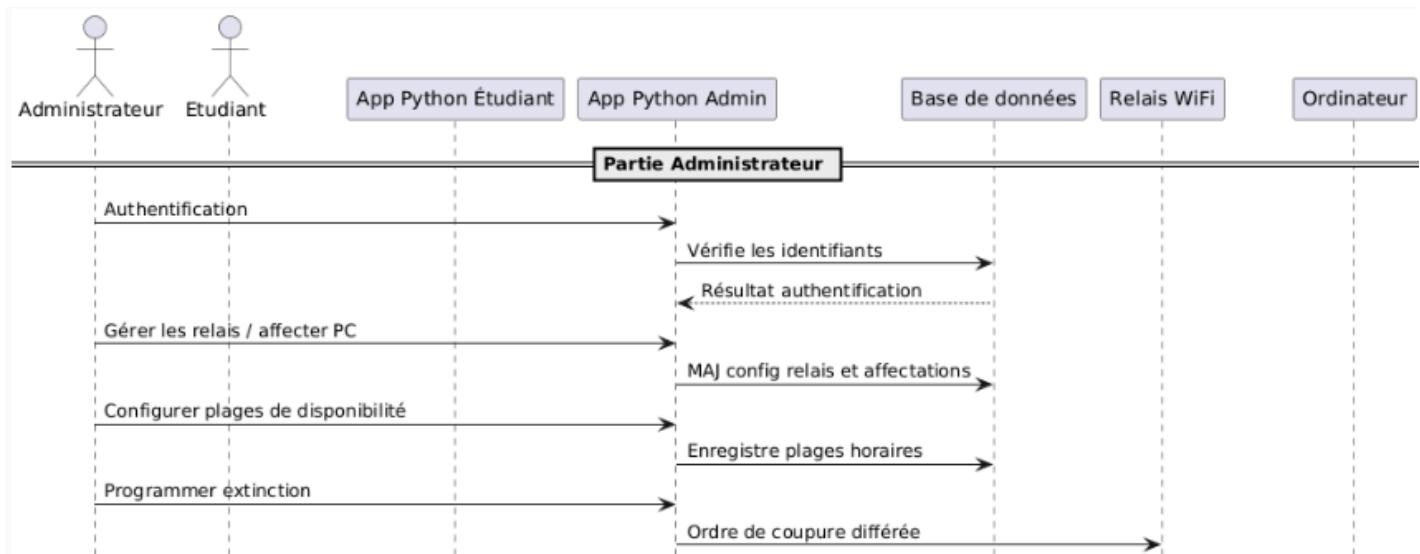


## Diagramme de séquence Administrateur

Ce diagramme de séquence décrit le fonctionnement global du système de gestion du parc informatique, en distinguant clairement deux volets d'interaction : d'une part, celui de l'administrateur qui configure et supervise le système, et d'autre part, celui de l'étudiant qui utilise à distance l'ordinateur qui lui est attribué.

Dans un premier temps, l'administrateur commence par s'authentifier sur l'application Python qui lui est dédiée. L'application communique alors avec la base de données pour vérifier la validité des identifiants. Une fois l'accès validé, l'administrateur peut effectuer différentes opérations de gestion. Il peut par exemple administrer les relais WiFi qui permettent d'alimenter ou d'éteindre les ordinateurs. Cela comprend l'ajout, la suppression ou la modification des relais, ainsi que leur affectation aux ordinateurs selon le plan de câblage électrique existant. Ces actions sont enregistrées dans la base de données.

L'administrateur peut aussi configurer les plages de disponibilité pour chaque section d'élèves, afin de définir précisément les horaires durant lesquels chaque machine peut être utilisée à distance. Cette configuration empêche les conflits d'accès et renforce la sécurité du système. Enfin, il peut programmer des extinctions automatiques des postes à des horaires spécifiques, en envoyant des ordres différés au relais WiFi pour couper l'alimentation des ordinateurs.



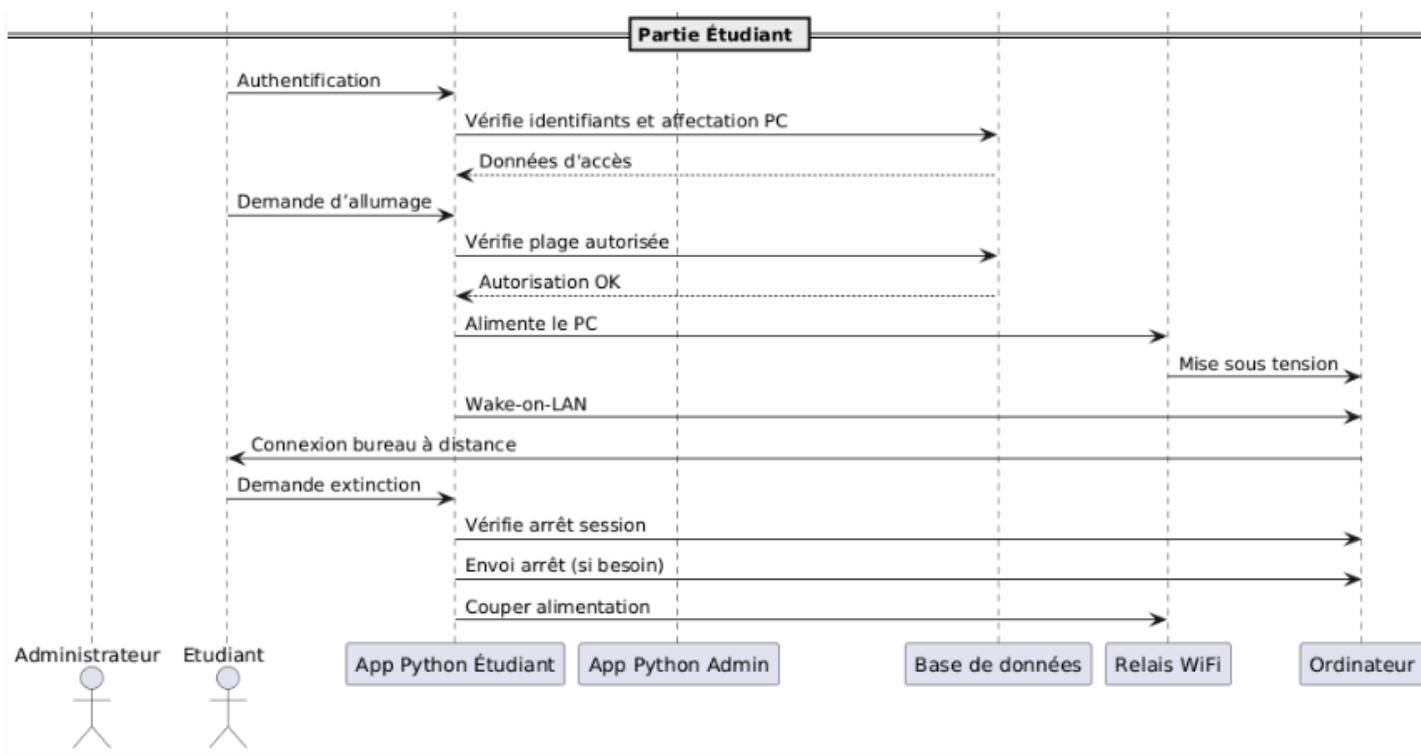
## Diagramme de séquence Etudiant

Dans un second temps, le diagramme décrit le parcours de l'étudiant. Celui-ci commence également par s'authentifier via l'application Python côté étudiant. L'application interroge la base de données afin de confirmer son identité, de vérifier l'affectation de son ordinateur, et de s'assurer qu'il tente de se connecter pendant une plage horaire autorisée. Si toutes ces conditions sont remplies, l'étudiant peut demander l'allumage de son poste distant.

L'application étudiante envoie alors une commande via MQTT au relais WiFi associé pour alimenter électriquement le poste. Une fois que le courant est délivré, elle émet une commande Wake-on-LAN afin de démarrer l'ordinateur à distance. L'étudiant peut ensuite se connecter à sa session Windows via un bureau à distance.

Lorsque l'étudiant termine son travail, il peut initier la procédure d'extinction de son poste. L'application vérifie d'abord si la session a bien été fermée, puis si l'ordinateur est arrêté. Si ce n'est pas le cas, elle envoie une commande réseau pour forcer l'arrêt. Une fois la machine correctement éteinte, elle envoie une dernière commande MQTT au relais WiFi pour couper définitivement l'alimentation électrique.

Ce diagramme illustre ainsi un cycle complet de gestion de l'accès aux ordinateurs du lycée, depuis la configuration par l'administrateur jusqu'à l'utilisation par l'étudiant. Il met en évidence les interactions entre les différents modules du système : applications Python, base de données, relais WiFi et ordinateurs, tout en respectant les contraintes de sécurité, d'organisation, et d'économie d'énergie.

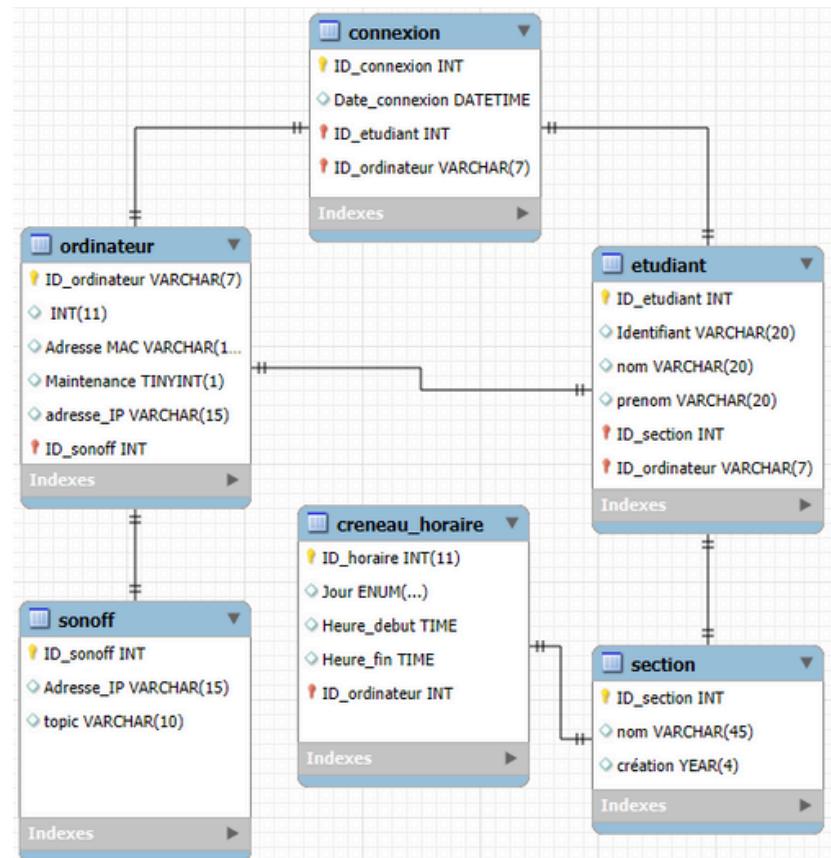


## Schéma relationnel de la Base de données

Notre base de données (voir Figure Y - Schéma Relationnel) est structurée pour une gestion efficace du parc informatique. Chaque table a une finalité précise :

- sonoff : Identifie et permet d'adresser chaque module Sonoff (relais physique) via son IP et son topic MQTT pour le contrôle de l'alimentation.
- ordinateur : Répertorie les PC du parc avec leurs identifiants réseau (IP, MAC) et les associe à un module sonoff pour leur pilotage.
- etudiant : Gère les utilisateurs, leurs informations d'identification et l'ordinateur spécifique qui leur est affecté.
- section : Regroupe les étudiants, facilitant l'application de règles et d'horaires d'accès communs.
- creneau\_horaire : Définit les plages de disponibilité autorisées pour l'utilisation des ordinateurs, souvent par section.
- connexion : Journalise les sessions d'utilisation (qui, quel PC, quand) pour le suivi et la traçabilité.

Ensemble, ces tables structurent les informations essentielles pour permettre l'identification, l'affectation, le contrôle horaire et le pilotage à distance des postes informatiques, ainsi que le suivi de leur utilisation.



# 03 Missions et tests

## Mes tâches assignées

## Etudiant n°1

Comme cela a été mis en évidence dans le tableau de répartition des tâches, chaque membre de l'équipe s'est vu attribuer des responsabilités spécifiques, aussi bien dans le développement logiciel que dans la conception matérielle. Il a donc fallu hiérarchiser les différentes missions en fonction de leur importance, en traitant en priorité celles jugées les plus essentielles.

### Architecture Matérielle

#### Windows Server 2022

**01**

Installation et configuration de Windows Server 2022 afin de gérer les services réseau et centraliser les ressources du système

#### Contrôle de domaine (Active Directory)

Installation et configuration du contrôle de domaine afin de centraliser la gestion des utilisateurs, des groupes et des stratégies de sécurité du réseau

**03**

#### DHCP / DNS

Installation et configuration des services DHCP et DNS afin d'automatiser l'attribution des adresses IP et d'assurer la résolution des noms de domaine au sein du réseau

**02**

#### Comptes utilisateurs et GPO

Création des comptes utilisateurs et des GPO afin de gérer les accès, appliquer des stratégies de sécurité et uniformiser la configuration des postes au sein du domaine.

**04**

### Développement Logiciel

**05**

#### Modules logiciels

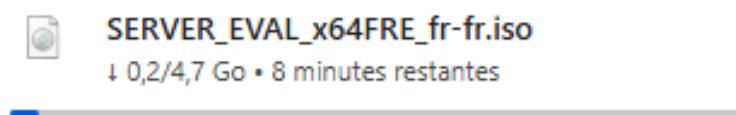
Création des modules logiciels permettant d'administrer les ordinateurs et les étudiants.

# 01 Windows Server 2022

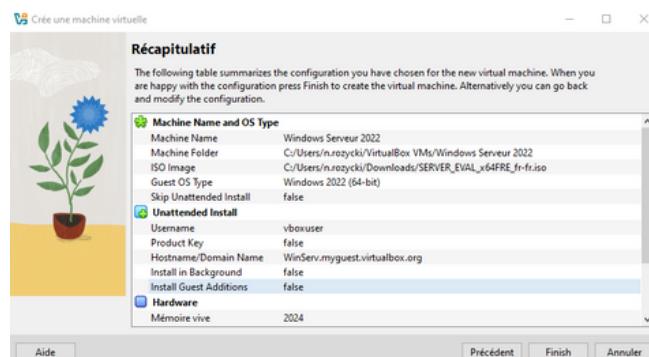
## Etape 1: Phase de test

Cette prototypage est nécessaire pour comprendre l'utilisateur de Windows Server 2022 à partir d'une VM avant de passer à la réalisation physique.

Nous allons procéder à l'installation de l'ISO de Windows Serveur 2022  
<https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2022>

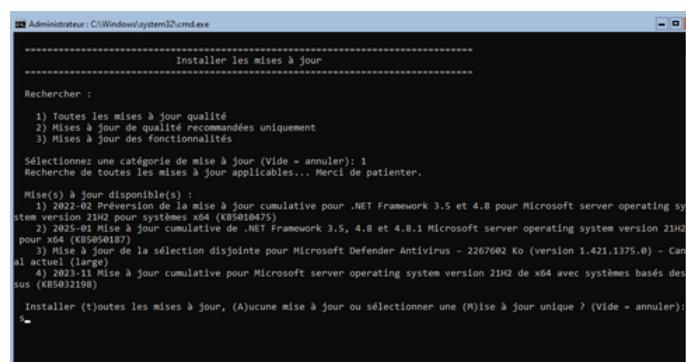


Après avoir installer l'ISO, nous procédons directement à la configuration de Windows Serveur 2022 sur Oracle VirtualBox afin d'installer le serveur sur notre VM.



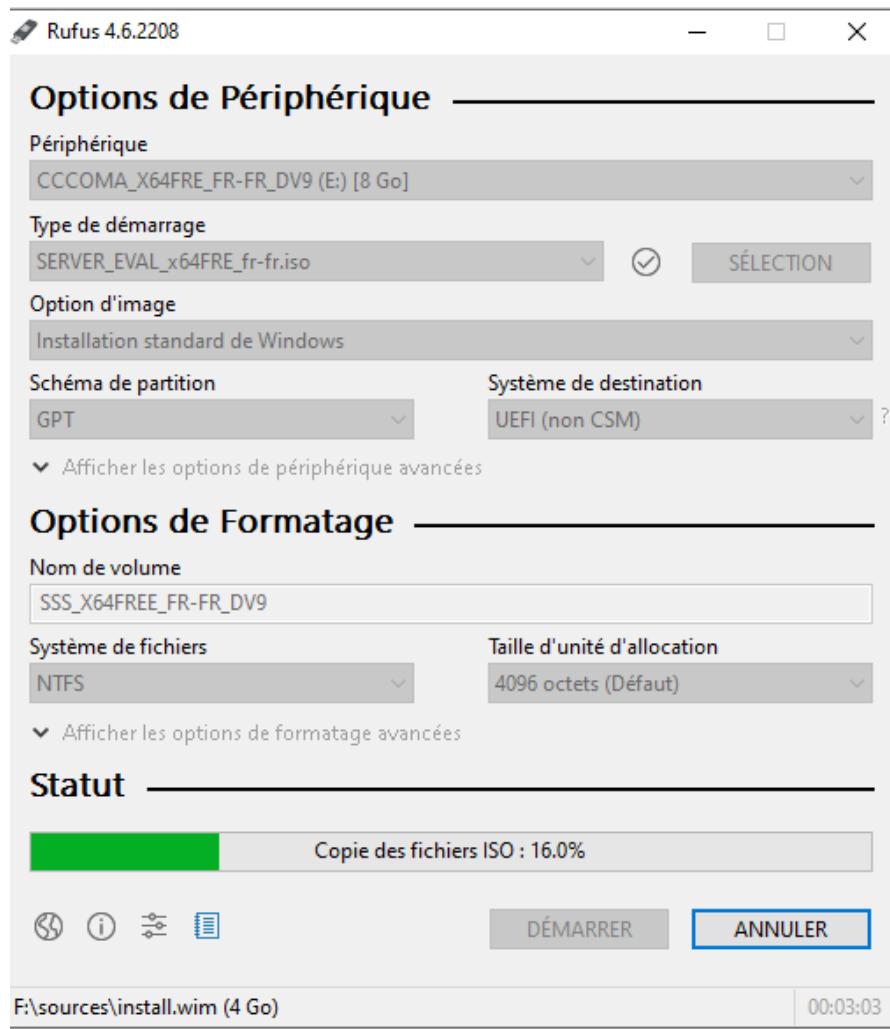
L'installation a été réalisée, nous pouvons accéder à Windows Serveur 2022 à partir de notre machine virtuelle, voici ci-dessous l'illustration.

Lors de la manipulation nous avons modifié quelques détails. En effet, nous avons configuré l'installation des mises à jour de sorte qu'elles se fassent de manière spontané et automatique. Dans le doute qu'elles n'ont pas été faites lors de la préparation de notre machine virtuelle, nous avons recherché les mises à jours applicables pour les réaliser.



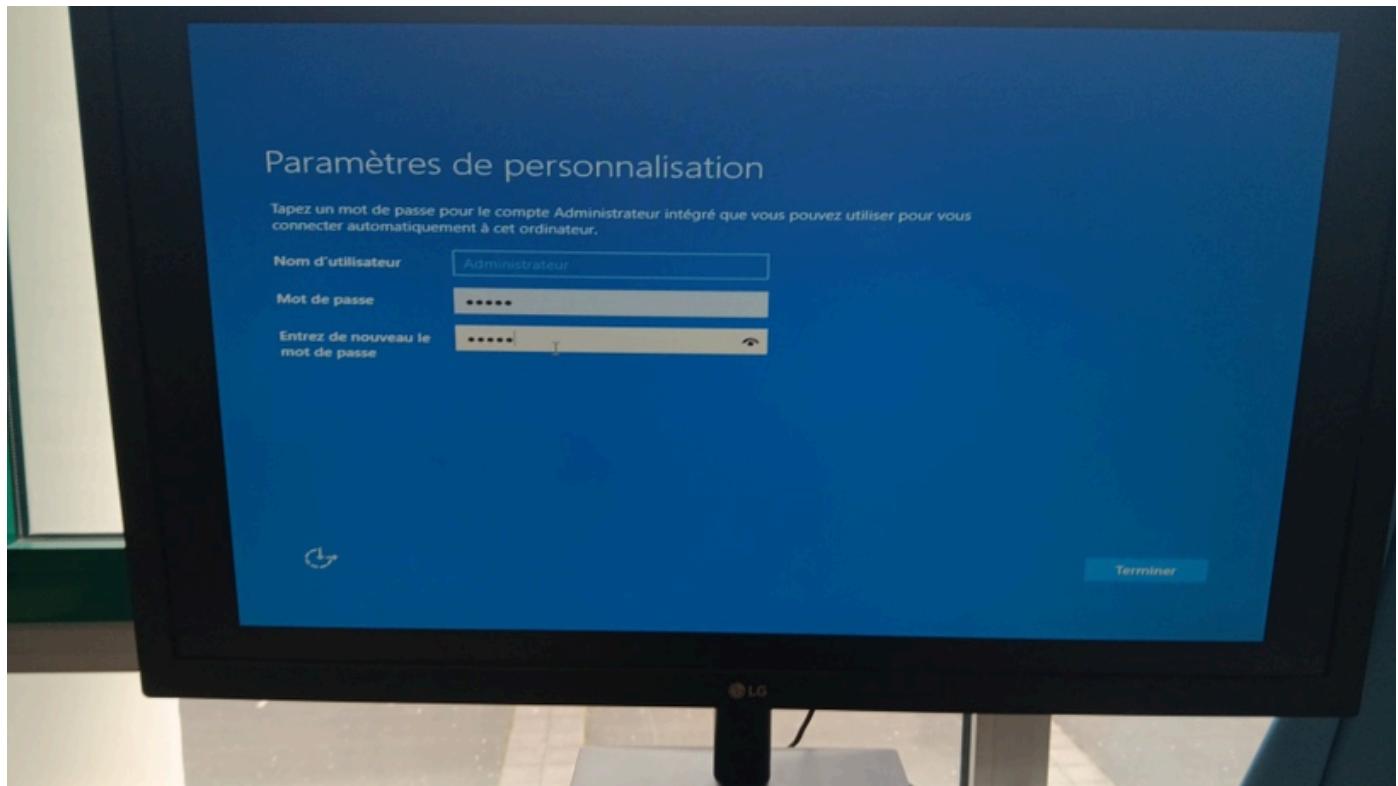
## Etape 2: La clé bootable

L'installation de Rufus va nous permettre de créer une clé bootable avec l'ISO de la version standard d'évaluation de Windows Serveur 2022



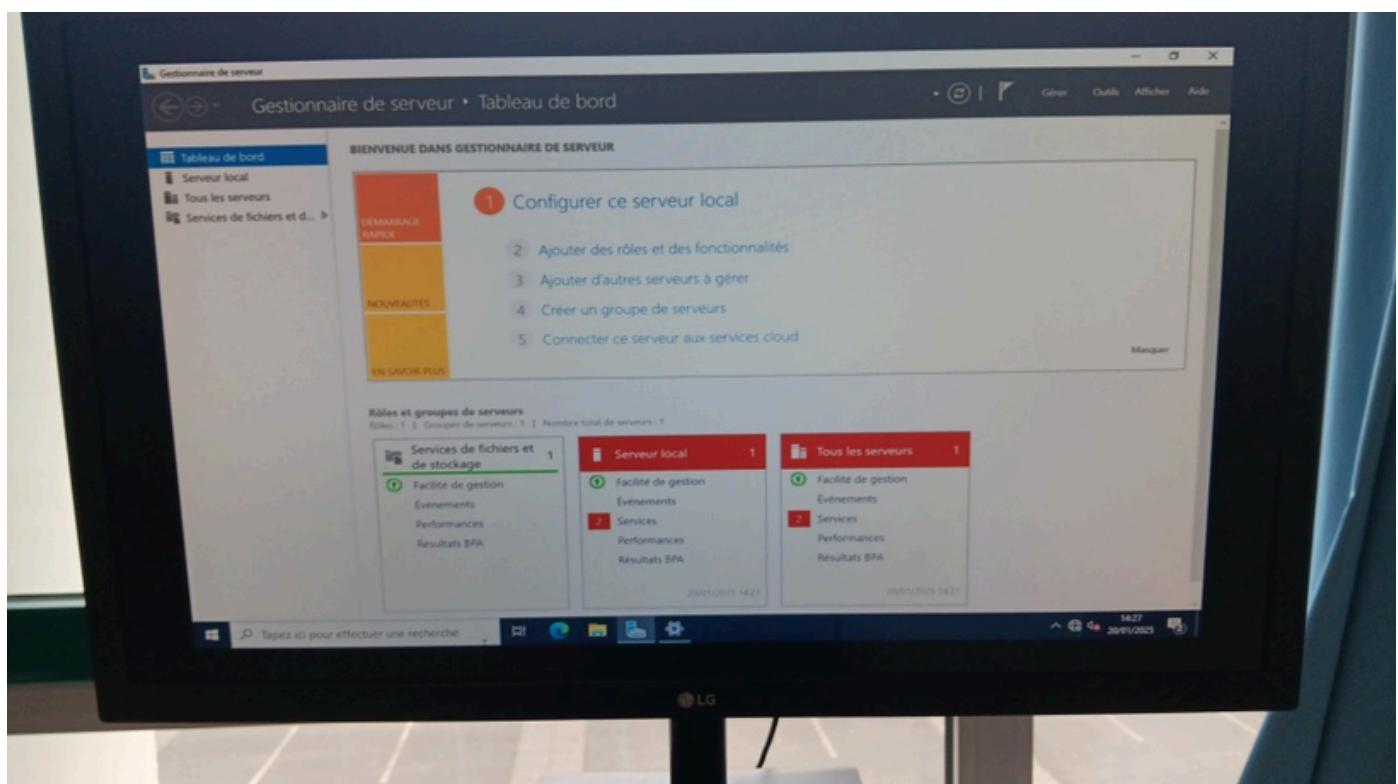
Une fois que nous avons installé l'ISO Windows Server 2022 sur notre clé bootable, nous l'avons branché sur un poste qui fera office de serveur. Lors de l'installation nous avons du supprimer le système d'exploitation déjà présent pour permettre la configuration de Windows Server.

Un mot de passe est demandé pour se connecter à notre utilisateur Administrateur, le mot de passe que nous avons donné est Admin123!



### Etape 3: Configuration de l'installation

Le gestionnaire de serveurs ci-dessous nous est directement présenté lors du démarrage de Windows Server 2022.

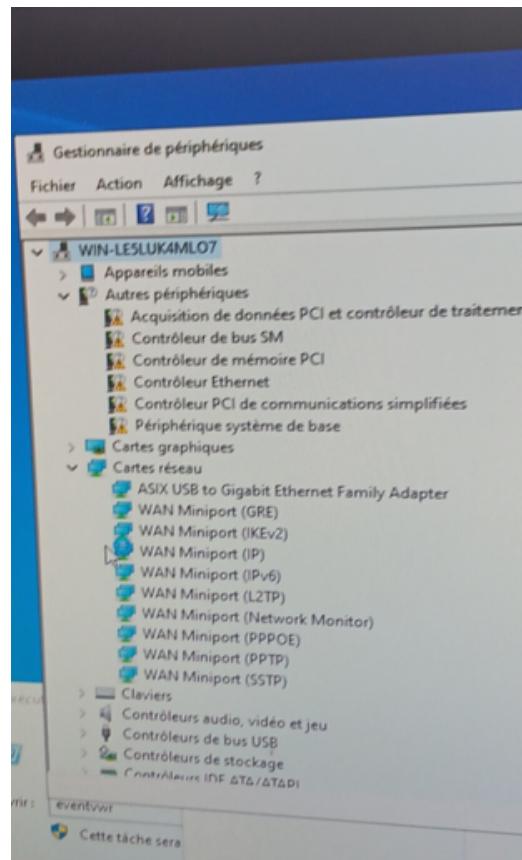


Avant de passer aux parties suivantes, il faut que nous mettons à jour les pilotes en se connectant au réseau du lycée. Le problème que nous avons rencontré est que le pilote pour la connexion au réseau n'est pas reconnu par le serveur. Un téléchargement des pilotes est nécessaire à partir du modèle de notre carte mère MSI H310M PRO-M2 PLUS.

Cette étape est nécessaire pour la configuration du contrôleur de domaine, et des serveurs DHCP, DNS.

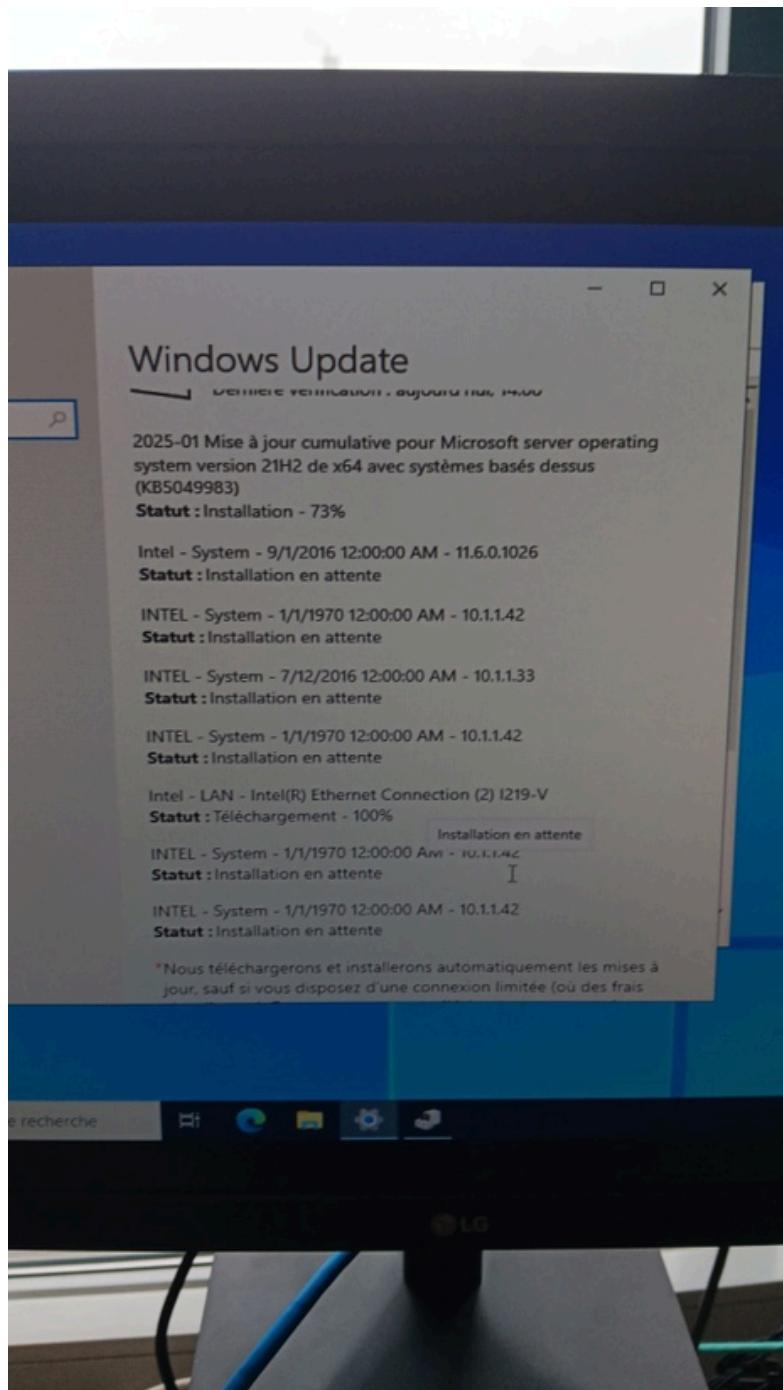
#### **Etape 4: Problèmes rencontrés et solutions**

Le téléchargement des pilotes a été effectué, mais malencontreusement ils n'ont pas été pris en compte par Windows Serveur 2022. La carte réseau n'est toujours pas reconnu. Pour remédier à ce problème nous avons pris un adaptateur Ethernet



Cet adaptateur nous est nécessaire pour installer les pilotes par l'intermédiaire de Windows Update. La réalisation de cette tâche nous est nécessaire pour confirmer la configuration complète de Windows Serveur 2022.

Lorsqu'un système d'exploitation (comme Windows Server 2022) est installé, il ne reconnaît pas toujours automatiquement tous les composants matériels de l'ordinateur, comme la carte réseau (adaptateur Ethernet). Sans le bon pilote, la carte réseau ne fonctionne pas : il est alors impossible d'accéder à Internet ou au réseau local.



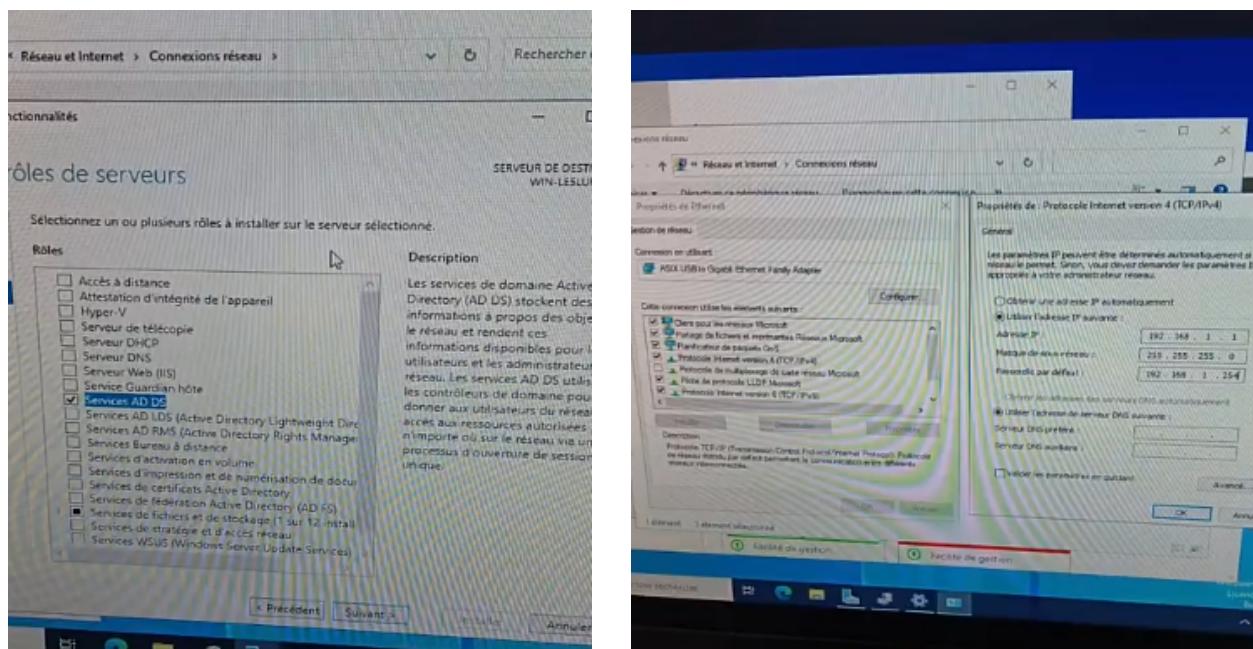
Une fois l'installation finie nous procédons directement à l'installation et la configuration du contrôle de domaine. Un redémarrage est nécessaire pour continuer la réalisation des tâches.

# 02 Contrôle de domaine

## Etape 1: Adressage statique du serveur

Ma deuxième tâche consistant à installer un contrôle de domaine. Aussi appelé « Active Directory », c'est un outil de gestion qui permet de centraliser toutes les informations des utilisateurs dans un seul et même endroit. Cette base de données facilite l'administration de ces informations.

[https://www.cyber-management-school.com/outils-logiciels-et-technologies/active-directory-quest-ce-que-cest/#:~:text=Active%20Directory%20\(AD\)%20est%20un,%20informations.](https://www.cyber-management-school.com/outils-logiciels-et-technologies/active-directory-quest-ce-que-cest/#:~:text=Active%20Directory%20(AD)%20est%20un,%20informations.)



La condition de déployer les différents services prérequis, en particulier l'Active Directory, une configuration d'adressage sur le serveur est nécessaire, que nous passerons en 192.168.2.1, la passerelle en 192.168.1.254 .

## Etape 2: Installation et configuration des services AD DS

Avant de passer à la configuration du contrôle de domaine, cet étape de recherche est nécessaire pour soutirer les informations.

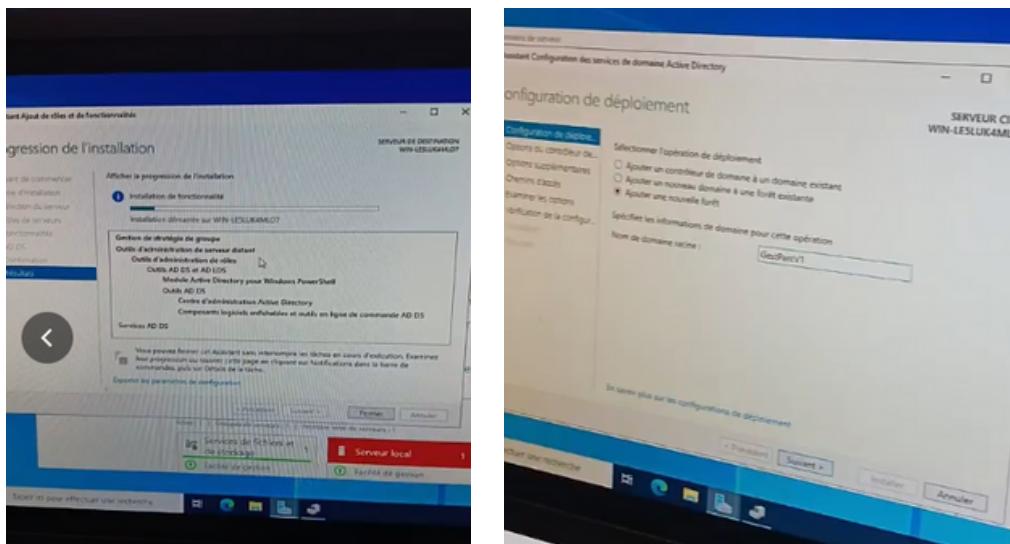
<https://www.ibm.com/docs/fr/rpa/23.0.x>

## Configuration du service Active Directory

1. Dans Configuration de déploiement, sélectionnez Ajouter une nouvelle forêt.
2. Dans la zone Domaine racine , entrez votre domaine racine, par exemple zpa . ibm. com, puis cliquez sur Suivant pour continuer.
3. Attendez que la configuration soit terminée, définissez un mot de passe pour le mode de restauration des services d'annuaire (DRSM), puis cliquez sur Suivant.
4. Dans Options DNS, cliquez sur Suivant.
5. Dans Options supplémentaires, passez en revue votre nom de domaine NetBIOS et modifiez-le si nécessaire.
6. Dans Chemins, passez en revue les chemins d'accès aux dossiers dans lesquels vos fichiers et journaux sont stockés, puis cliquez sur Suivant.
7. Dans Options de révision, consultez les détails de votre service d'annuaire et cliquez sur Suivant.
8. Dans Prerequisites Check, vérifiez si votre ordinateur répond à toutes les exigences et recherchez les avertissements ou les erreurs susceptibles de bloquer l'installation. Cliquez sur Installer pour installer le service.
9. Vous êtes invité à être déconnecté. Cliquez sur Fermer et reconnectez-vous à votre compte utilisateur pour confirmer que Active Directory est installé.

Les prérequis réalisés pour la mise en place des services AD DS ont été réalisés pour qu'ils puissent être déployés.

Ces services sont nécessaires pour stocker les informations sur le réseau et faciliter l'utilisation de ces informations pour les administrateurs et les utilisateurs.



Nous accédons à l'Assistant Configuration des services de domaine Active Directory pour permettre la configuration du déploiement

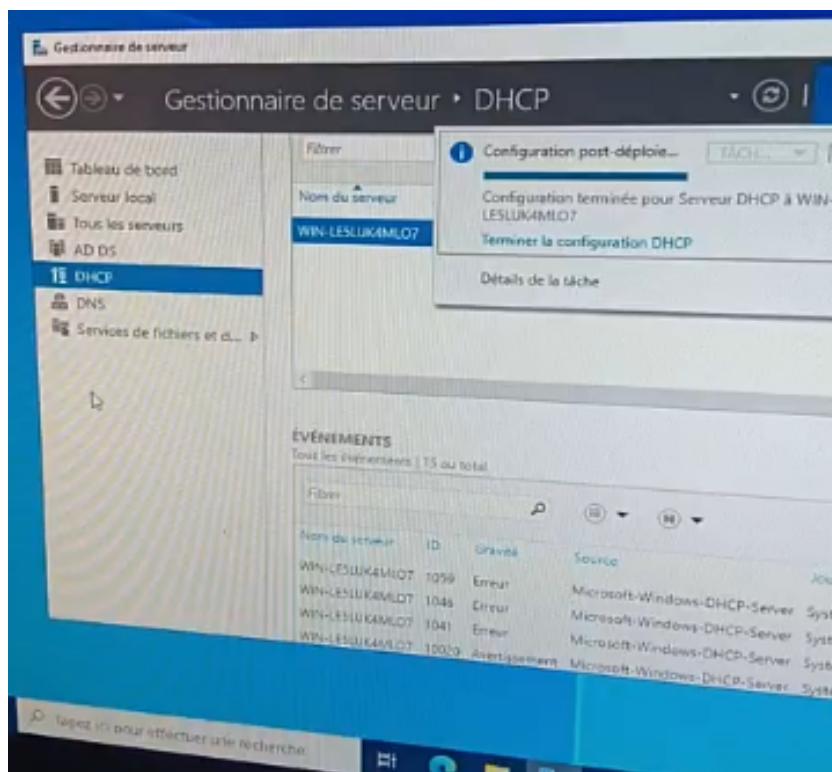
Nous décidons de créer une nouvelle forêt, où le nom de notre domaine racine attribué sera « GestParc.v1 ». Ce nom de domaine représente la base hiérarchique de toute l'infrastructure Active Directory. Il permet également de retracer les ordinateurs et les utilisateurs à partir du chemin LDAP que nous utiliserons pour la réalisation nos modules logiciels.

La configuration terminée en suivant le protocole étape par étape il faut redémarrer le serveur afin de vérifier si la configuration du déploiement a été effectué.

# 03 DHCP / DNS

## Etape 1: Installation des services DNS et DHCP

L'installation des services DNS et DHCP doit être nécessaire pour effectuer une bonne configuration du serveur.



Aussi appelé « Dynamic Host Configuration Protocol » (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.  
[fr.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](http://fr.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)

L'Active Directory dépend totalement du DNS pour fonctionner, car lorsqu'un PC se connecte au domaine il utilise le DNS pour localiser le contrôle de domaine. Il joue un rôle critique dans la résolution de noms et le bon fonctionnement de l'infrastructure réseau.

## Etape 2: Configuration du service DHCP

Nous nous basons sur la capture d'écran ci-dessous pour configurer le service DHCP. Cette capture d'écran nous permettra de configurer une nouvelle étendue en suivant les étapes à la clé. <https://www.editions-eni.fr/livre/windows-server-2022-les-bases-indispensables-pour-administrer-et-configurer-votre-serveur-9782409037641/implementation-d-un-serveur-dhcp>

- Cliquez sur **Valider** puis sur **Fermer**.
- Dans le menu **Démarrer**, cliquez sur **Outils d'administration**.
- Double cliquez sur **DHCP**.

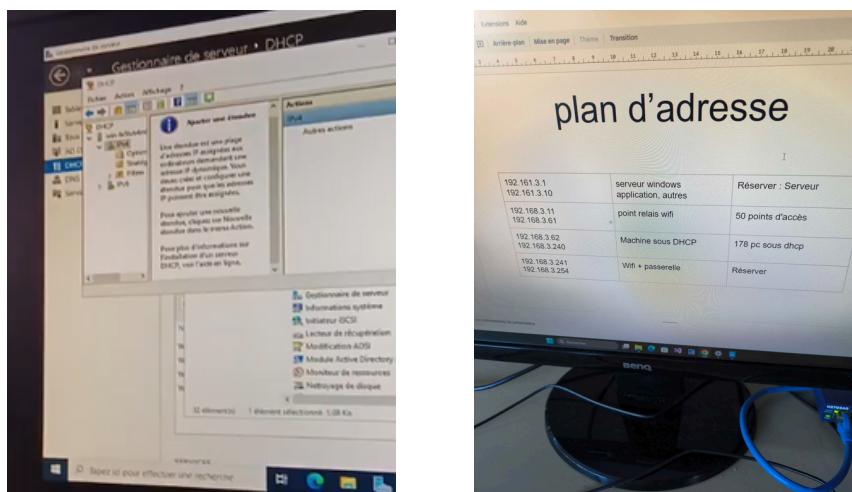
Le rôle est bien installé mais il n'est pas configuré.

### 1. Ajout d'une nouvelle étendue

Une **étendue DHCP** est constituée d'un pool d'adresses IP (par exemple, 192.168.1.80 à 192.168.1.86). Lorsqu'un client effectue une demande, le serveur DHCP lui attribue une des adresses du pool.

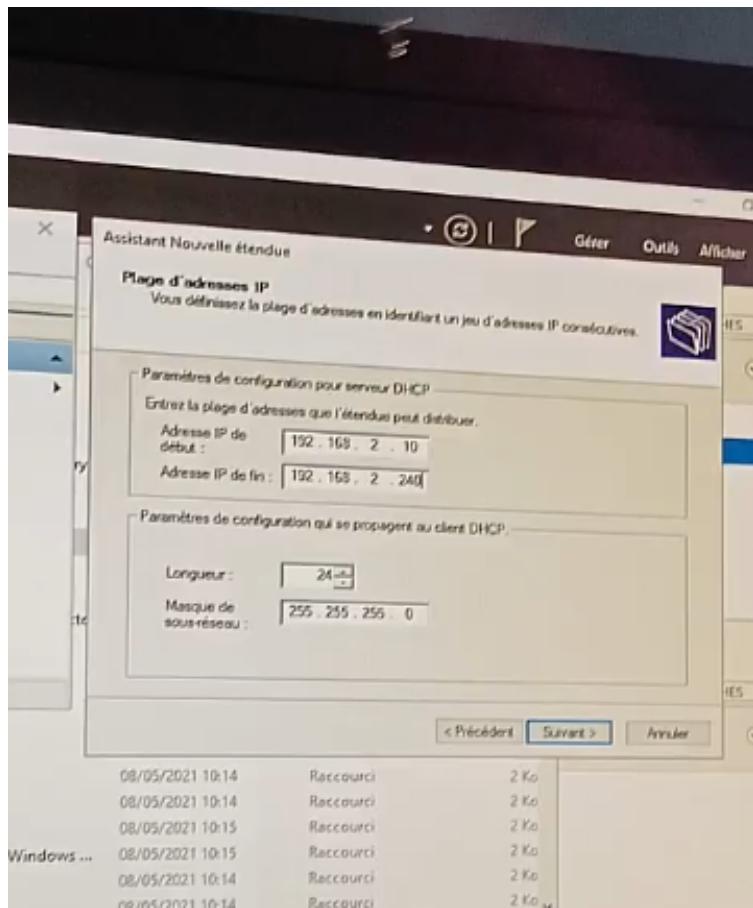
La plage d'adresses IP distribuables par l'étendue est nécessairement contiguë. Pour éviter la distribution de certaines adresses, il est possible de mettre en place des exclusions d'une adresse ou d'une plage contiguë. Ces dernières peuvent être assignées à un poste de façon manuelle sans risquer un conflit d'IP puisque...

Comme dit sur cette capture d'écran, le rôle DHCP a été installé mais pas configuré. Nous suivons les étapes comme demandés pour accéder au module DHCP sur lequel nous ajoutons une nouvelle étendue.



La nouvelle étendue doit respecter un plan d'adressage « prototype » que nos camarades ont proposé. Quelques modifications ont été suggérés et apportés pour apporter une meilleure organisation du réseau, car mettre un serveur DHCP sur un point d'accès WiFi, alors qu'un DHCP est déjà actif sur Windows Server 2022 n'est généralement pas utile.

Un plan d'adressage IP est un document ou une stratégie qui définit comment les adresses IP sont distribuées et organisées dans un réseau. Elle permet de configurer la nouvelle étendue en respectant les consignes de ce plan d'adressage.



On aperçoit que la plage d'adresses IP a été configuré en fonction du plan d'adressage prototype et des modifications suggérées, et que la configuration du DHCP a été complétée.

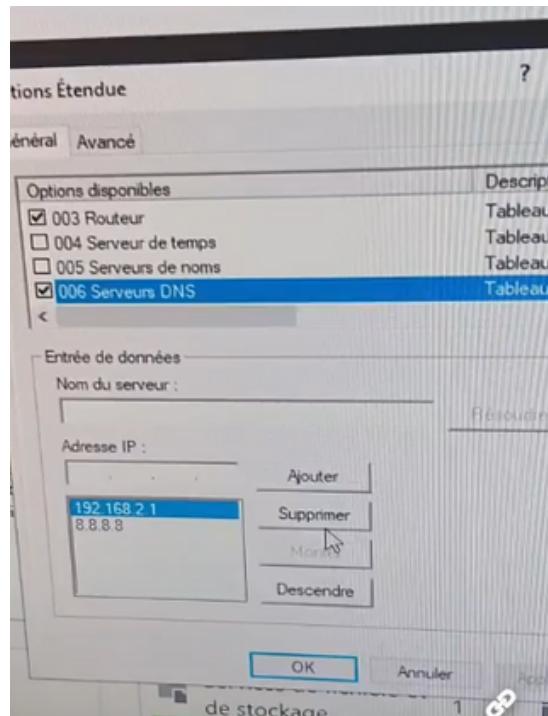
### **Etape 3: Configuration des services DNS**

Nous suivons la configuration du service DNS à partir de l'Assistant Configuration d'un serveur DNS



Des modifications ont été apportés notamment sur la zone de recherche directe à créer, et l'adresse IP du redirecteur, correspondant à rédiger la requête vers Google DNS pour résoudre les noms Internet.

La zone de recherche directe à créer est « GestParc.v1 » car il doit correspondre au nom de domaine racine créé à partir de la configuration de l'Active Directory.

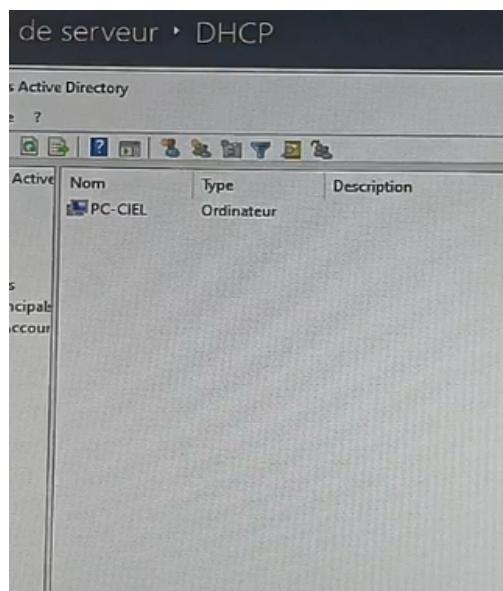


La modification sur l'adresse IP du redirecteur a été apporté. Le serveur DNS principale est 192.168.2.1 correspondant à l'adresse de notre serveur. Le serveur DNS transitoire est 8.8.8.8 afin de permettre aux ordinateurs de notre réseau d'accéder aux services Internet.

# 04 Comptes utilisateurs et GPO

## Etape 1: Création de l'ordinateur dans l'Active Directory

Dans l'Active Directory, nous avons créer un ordinateur avec le nom « PC-CIEL » correspond au nom du « PC-CIEL » rattaché à notre serveur. C'est le PC avec lequel l'étudiant se connectera sur la session à distance en entrant ses identifiants à partir de l'application.



## Etape 2: Création du compte utilisateur "Etudiant"

On crée un nouvel objet à partir de l'Active Directory, nous permettant de créer un nouvel objet « Utilisateur » que on nommera Étudiant.

The screenshot shows the 'Nouvel objet - Utilisateur' (New Object - User) wizard in the 'Gestionnaire de serveur > DHCP' snap-in. The left pane shows the 'Utilisateurs' (Users) container. The right pane shows a list of existing groups and the newly created 'Etudiant' user account.

Nom	Type	Description
Administrat...	Groupe de séc...	Administrateur
Admins du ...	Groupe de séc...	Administrateurs
Contrôleurs ...	Groupe de séc...	Tous les contrô...
Contrôleurs ...	Groupe de séc...	Les membres d...
Contrôleurs ...	Groupe de séc...	Les membres d...
DnsAdmins...	Groupe de séc...	Groupe des ad...
DnsUpdateP...	Groupe de séc...	Les clients DNS
Éditeurs de c...	Groupe de séc...	Les membres d...
Groupe de ...	Groupe de séc...	Les mots de pa...
Groupe de r...	Groupe de séc...	Les mots de pa...
Invité	Utilisateur	Compte d'utilis...
Invités du d...	Groupe de séc...	Tous les invité...
Ordinateurs ...	Groupe de séc...	Toutes les stati...
Propriétaires...	Groupe de séc...	Les membres de ...
Protected Us...	Groupe de séc...	Les membres de ...
Serveurs RA...	Groupe de séc...	Les serveurs de ...
Utilisateurs ...	Groupe de séc...	Les membres qu...
Utilisateurs ...	Groupe de séc...	Tous les utilisat...
Etudiant	Utilisateur	

Dans Active Directory, deux GPO sont créées par défaut.

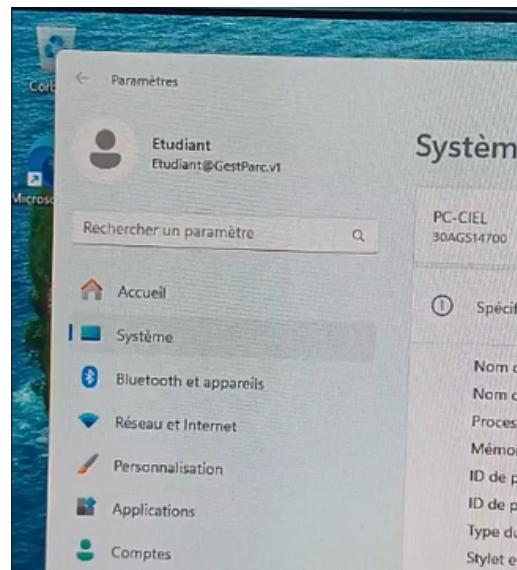
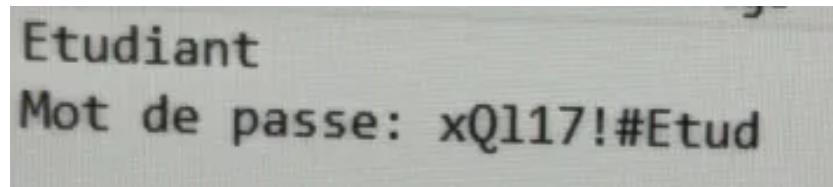
La Default Domain Policy, qui s'applique à tout le domaine pour définir notamment les exigences de mot de passe et les paramètres de sécurité globaux.

La Default Domain Controllers Policy, appliquée uniquement aux serveurs contrôleurs de domaine afin d'y configurer les droits utilisateur, l'audit et les réglages de sécurité spécifiques.  
chatgpt.com

Nom de la GPO	Appliquée à...	Contenu principal
Default Domain Policy	Le domaine entier	Paramètres de sécurité des comptes, stratégie de mot de passe, verrouillage de compte, etc.
Default Domain Controllers Policy	L'OU "Domain Controllers" (les contrôleurs de domaine)	Paramètres sécurité locale, audit, droits utilisateurs, etc.

L'environnement cible comporte un nombre limité de machines et d'utilisateurs, ce qui ne justifie pas la mise en œuvre de GPO complexes. Une gestion manuelle ou locale restait suffisante et plus rapide à mettre en œuvre

Les conditions ont été remplis, permettant à un étudiant d'entrer sa session sur « PC-CIEL » en entrant son identifiant et son mot de passe.



# 05 Modules logiciels

## Etape 1: Connexion à la base de données à partir d'un code

La création des modules logiciels nécessite de réaliser des tests pour nous permettre de comprendre le fonctionnement d'une application interactive.

Le premier test était de réaliser un code nous permettant de nous connecter à la base de donnée et vérifier si nous pouvions nous connecter à cette dernière. Cette étape est cruciale pour que les membres du groupe et moi pouvons avancer sur la réalisation de nos modules respectifs.

La bibliothèque que nous allons devoir utiliser pour permettre une connexion sur la base de données et de faire des requêtes SQL est « mysql-connector-python »

### mysql-connector-python

**Dernière version stable:** 9.3.0  
**Résumé:** A self-contained Python driver for communicating with MySQL servers, using an API that is compliant with the Python Database API Specification v2.0 (PEP 249).  
**Auteur:** Oracle and/or its affiliates  
**Licence:** GNU GPLv2 (with FOSS License Exception)  
**Page PyPI:** <https://pypi.org/project/mysql-connector-python/>  
**Nécessite:**  
|

Le code permettant de créer une connexion à distance à la base de donnée en entrant les identifiants de l'administrateur, le nom de la base de données, ainsi que l'adresse IP de la Raspberry Pi 5 pour communiquer avec cette dernière, et renvoie une réponse favorable ou non.

```
import mysql.connector
from mysql.connector import Error

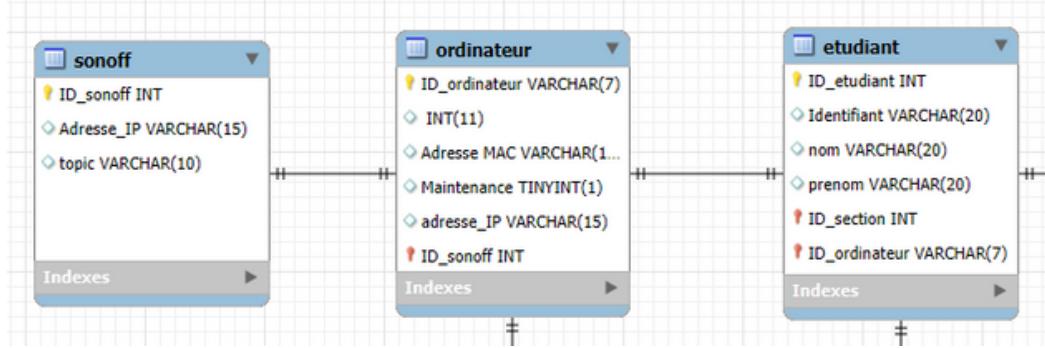
try:
    conn = mysql.connector.connect(
        host="192.168.2.5",
        user="a.admin",
        password="admin.CIEL!",
        database="VirtualPilot"
    )

    if conn.is_connected():
        print("Connexion réussie à la base de données")

except Error as e:
    print(f"Erreur de connexion : {e}")
```

La réalisation des modules « Administrer les étudiants » et « Administrer les ordinateurs » nécessite de saisir les champs respectifs de nos tables sonoff, ordinateur, et etudiant.

Le but est de permettre une interactivité entre l'administrateur et la base de donnée, comme s'il pouvait directement la manipuler à partir de l'application. Mais c'est indispensable pour la mise en place de notre code.

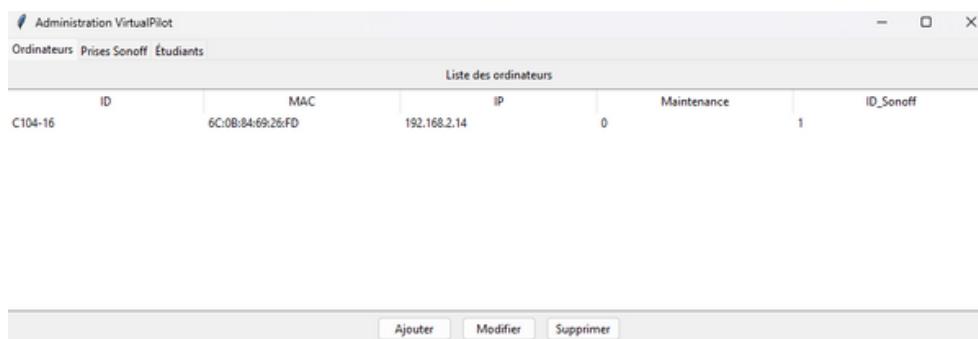


## Etape 2: "Administrer les ordinateurs"

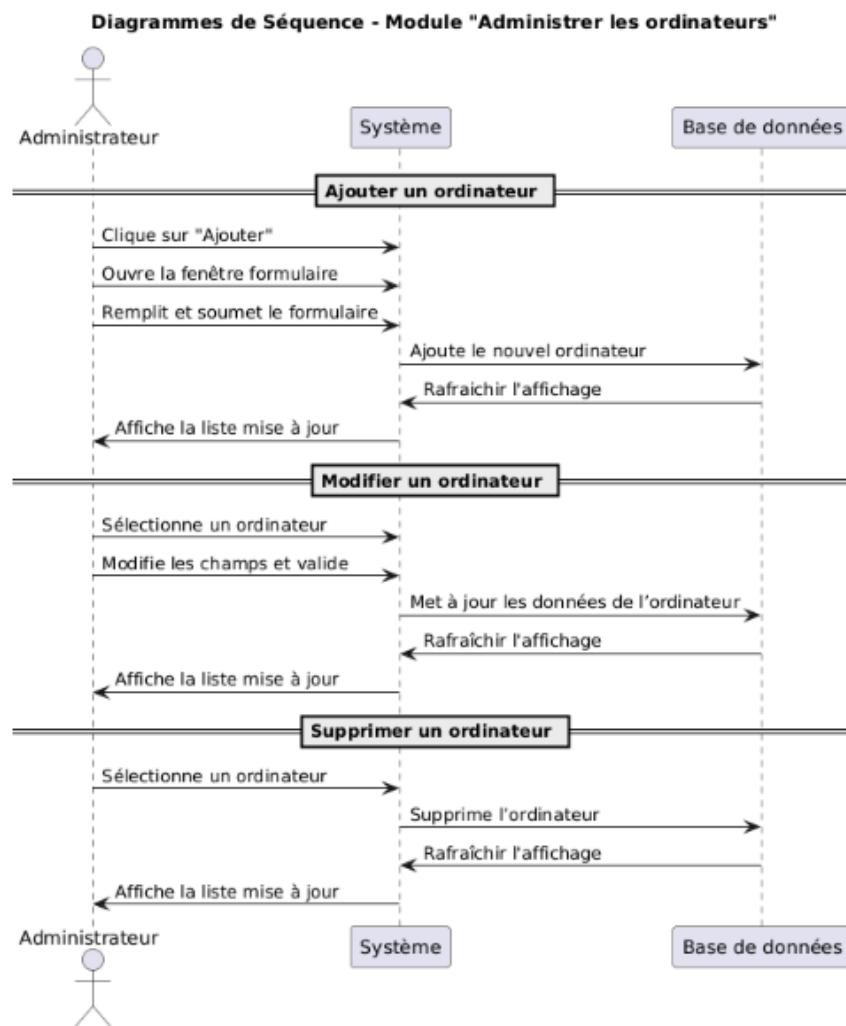
La réalisation du module logiciel “Administrer les ordinateurs” fonctionne comme un CRUD (Create, Read, Update, Delete), offrant une interface complète pour gérer les données des ordinateurs.

Il permet de centraliser et de gérer efficacement les informations sur les ordinateurs du parc, comme leur configuration, leur affectation aux utilisateurs, leur état ou leur emplacement. Grâce à ce module, les administrateurs peuvent ajouter de nouveaux équipements, consulter les détails d'un poste, mettre à jour des informations ou supprimer des machines obsolètes, assurant ainsi un suivi précis et une meilleure gestion du matériel informatique.

L'interface graphique de notre module “Administrer les ordinateurs” se présente de la façon suivante:



Ce diagramme de séquence illustre les interactions entre un Administrateur, le système et la base de données pour trois cas d'utilisation : ajouter, modifier et supprimer un ordinateur.



Une fenêtre de formulaire s'ouvre lorsque l'administrateur clique sur "Ajouter" lui permettant de rentrer les différentes informations liés à un ordinateur, son ID, son adresse MAC, son adresse IP, son état (maintenance) ainsi qu'au relais wifi dont il a été attribué

ID_ordinateur	Adresse_MAC	Adresse_IP	Maintenance	ID_Sonoff
C104-17	00:00:00:00:00:00	192.168.2.15	1	2

Administration VirtualPilot						
Ordinateurs Prises Sonoff Étudiants						
Liste des ordinateurs						
ID	MAC	IP	Maintenance	ID_Sonoff		
C104-16	6C:0B:84:69:26:FD	192.168.2.14	0	1		
C104-17	00:00:00:00:00:00	192.168.2.15	1	2		

Lorsque l'administrateur clique sur un ordinateur, et clique sur le bouton "Modifier" une fenêtre de formulaire s'ouvre avec les informations déjà rentrées, où ce dernier pourra modifier l'information qu'il souhaite

ID	MAC	IP	Maintenance	ID_Sonoff
C104-16	6C:0B:84:69:26:FD	192.168.2.14	0	1
C104-17	00:00:00:00:00:00	192.168.2.15	1	2

ID_ordinateur	C104-17
Adresse_MAC	00:00:00:00:00:01
Adresse_IP	192.168.2.15
Maintenance	1
ID_sonoff	2

Lorsqu'un ordinateur a été sélectionné et qu'on clique sur "Supprimer", l'ordinateur est supprimé de la liste.

ID	MAC	IP	Maintenance	ID_Sonoff
C104-16	6C:0B:84:69:26:FD	192.168.2.14	0	1
C104-17	00:00:00:00:00:01	192.168.2.15	1	2

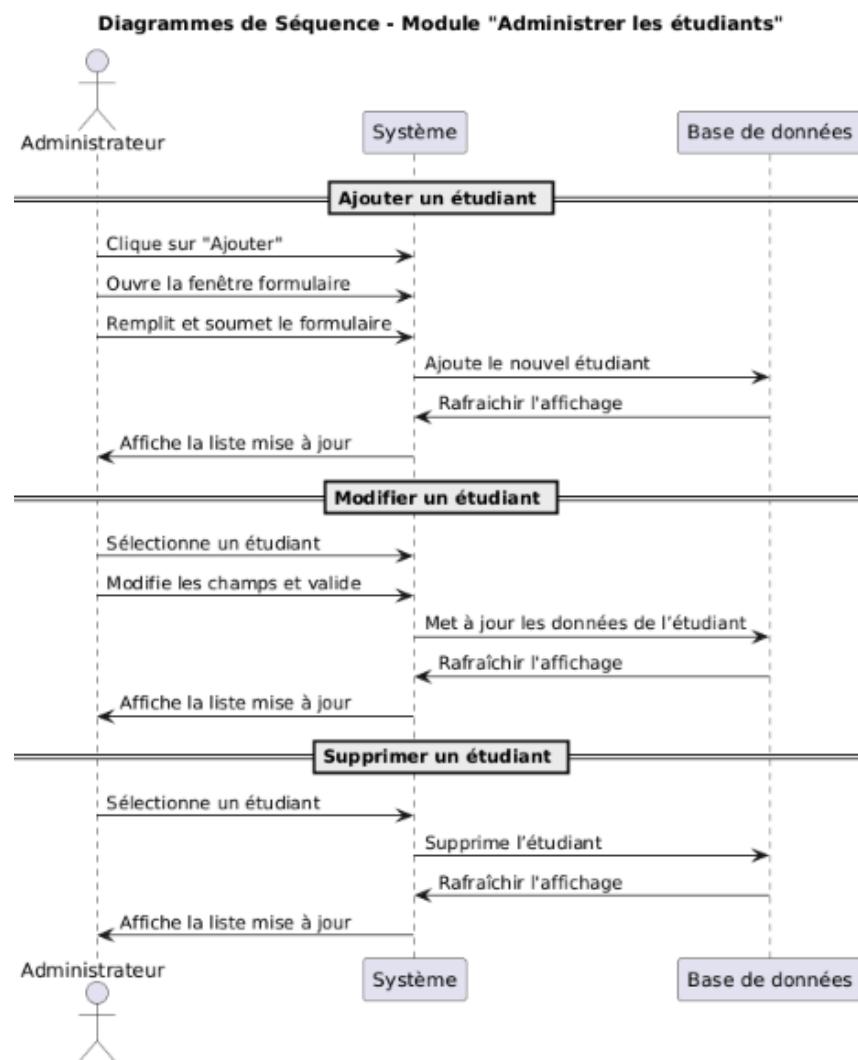
### Etape 3: "Administrer les étudiants"

A l'instar de notre module logiciel précédent, celui concernant l'administration des étudiants est également un CRUD offrant une interface complète pour gérer les données des étudiants.

L'administrateur aura la possibilité d'ajouter, de modifier, et de supprimer comme nous pouvons apercevoir sur l'interface graphique de notre module "Administrer les étudiants"

ID	Identifiant	Nom	Prenom	ID_ordinateur
1	e.etud	edmond	etudiant	C104-16

Ce diagramme de séquence illustre les interactions entre un Administrateur, le système et la base de données pour trois cas d'utilisation : ajouter, modifier et supprimer un étudiant.



Une fenêtre de formulaire s'ouvre lorsque l'administrateur clique sur "Ajouter" lui permettant de rentrer les différentes informations liés à un étudiant, son ID, son identifiant, son nom, son prénom, et l'ID de l'ordinateur auquel il a été affecté

The screenshot shows two windows side-by-side:

- Left Window (Étudiant Form):**

ID_etudiant	2
Identifiant	n.rozycki
nom	rozycki
prenom	noah
ID_ordinateur	C104-16

**Right Window (Administration VirtualPilot):**

ID	Identifiant	Nom	Prenom	ID_ordinateur
1	e.etud n.rozycki	edmond	etudiant	C104-16
2		rozycki	noah	C104-16

Buttons at the bottom of the right window: Ajouter, Modifier, Supprimer.

Lorsque l'administrateur clique sur un étudiant, et clique sur le bouton "Modifier" une fenêtre de formulaire s'ouvre avec les informations déjà rentrées, où ce dernier pourra modifier l'information qu'il souhaite

ID	Identifiant	Nom	Prenom	ID_ordinateur
1	e.etud	edmond	etudiant	C104-16
2	n.rozycki	rozycki	noah	C104-16

<b>Étudiant</b>	X
ID_etudiant	3
Identifiant	n.rozycki
nom	rozycki
prenom	noah
ID_ordinateur	C104-16
<b>Valider</b>	

Lorsqu'un étudiant a été sélectionné et qu'on clique sur "Supprimer", l'étudiant est supprimé de la liste.

ID	Identifiant	Nom	Prenom	ID_ordinateur
1	e.etud	edmond	etudiant	C104-16
2	n.rozycki	rozycki	noah	C104-16

Nous pouvons conclure que le projet est à un stade avancé, avec la majorité des fonctionnalités principales déjà développées, testées et intégrées. Plusieurs composants sont entièrement opérationnels, et bien qu'il y ait toujours des axes d'améliorations à trouver autour de ces composants, ils répondent correctement au cahier des charges.

### **Tâches réalisées:**

- Installation et configuration de Windows Server 2022
- Installation et configuration de l'Active Directory
- Installation et configuration des services DHCP et DNS
- Création des comptes utilisateurs et ordinateurs
- Création des stratégies de groupes nécessaires
  
- Conception de la base de données
- Module logiciel "Administrer les ordinateurs"
- Module logiciel "Administrer les étudiants"

## Mes tâches assignées

Comme nous avons pu le constater dans le tableau de la répartition des tâches, chaque étudiant avait des missions différentes dans chaque partie, que ce soit dans le développement du logiciel ou dans l'architecture matérielle. nous avons dû classer les tâches en fonction de leur importance, faisant ainsi passer la plus importante en premier :

### Architecture Matérielle

#### Routeur et pare-feu

**01**

Pour installer un routeur et pare-feu, l'équipement Stormshield SN160 sera utilisé. Celui-ci permettra de sécuriser la connexion entre différents réseaux

#### VPN (Virtual Private Network)

Installation et configuration d'un serveur VPN pour permettre une connexion sécurisée à distance à l'infrastructure du lycée.

**02**

### Développement Logiciel

#### Base De Données / Implémentation

Conception et réalisation de la base de données servant à stocker l'ensemble des informations essentielles à la gestion du parc informatique

**03**

**04**

#### Connexion et authentification

Développement du module servant à garantir l'accès sécurisé des utilisateurs au parc informatique.

**05**

#### Affichage de l'état du parc

Création du module logiciel permettant d'afficher l'état de chaque ordinateur du park.

**06**

#### Affecter les ordinateur

Développement du module servant à attribuer chaque étudiant à un ordinateur unique via la base de donnée.

# 01 Routeur et pare-feu

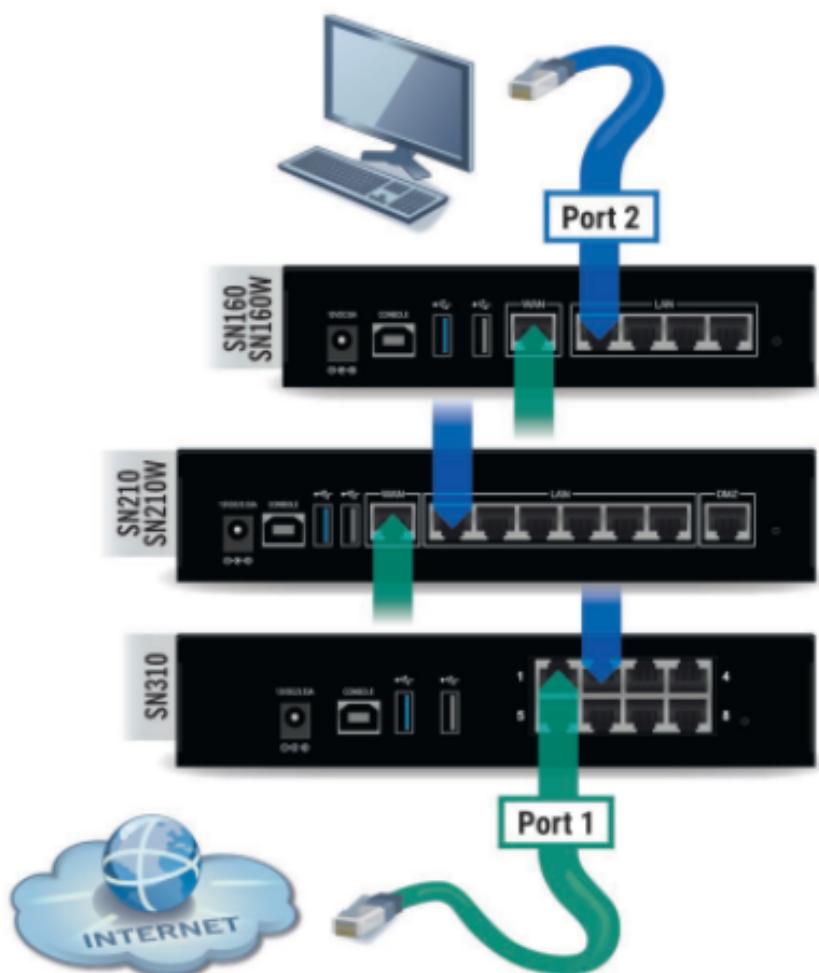
Dans le cadre de la mise en place de l'architecture réseau en environnement isolé (réseau bac à sable), l'équipement Stormshield SN160 a été retenu pour sa double fonctionnalité : il assure à la fois les rôles de routeur et de pare-feu. Ce modèle a été choisi principalement pour deux raisons : son coût réduit et sa compatibilité avec les configurations de sécurité déployées sur le réseau du lycée.

L'objectif n'est pas de l'intégrer directement à l'infrastructure finale, mais de l'utiliser comme support de test pour la création et la validation des règles de filtrage. Une fois ces règles établies et testées dans cet environnement contrôlé, elles seront transférées vers l'équipement Stormshield en production, utilisé au sein du réseau principal de l'établissement.

## Installation

Dans un premier temps j'ai dû réinitialiser et installer le Stormshield, mais à cause de problème je n'ai pas pu directement le connecter à internet, mais j'ai dû passer par un autre réseau, qui lui est connecté à internet.

Une fois installé, j'ai dû me connecter sur le LAN (au niveau du Port2) avec un PC et en tapant l'adresse IP du Stormshield, on accède à l'interface de configuration.





Une fois connecté à l'interface de gestion du Stormshield SN160, plusieurs onglets sont accessibles depuis le menu latéral gauche. Ces onglets permettent de configurer l'ensemble des fonctionnalités réseau et de sécurité de l'équipement.

Dans le cadre de la mise en place du routeur, seuls les onglets Network et Security Policy seront utilisés.

Pour la configuration du pare-feu, l'intervention se limite exclusivement à l'onglet Security Policy.

## NetWork

IP address	Network mask	Comments
192.168.2.254	255.255.255.0	

L'interface LAN, correspondant à l'intérieur du réseau, a été configurée en adresse IP statique. Cette interface jouant le rôle de passerelle par défaut pour l'ensemble des postes du réseau, il est essentiel qu'elle conserve une adresse fixe.

L'interface WAN, correspondant à la partie externe du réseau, a été configurée en mode DHCP. Cette interface n'étant pas directement connectée à Internet mais reliée à un réseau en amont, aucune adresse IP fixe ne peut lui être attribuée manuellement.

IP address	Network mask	Comments
192.168.2.254	255.255.255.0	

## Security Policy



The screenshot shows the 'FILTER - NAT' configuration screen. At the top, there are buttons for 'Block all', 'Activate this policy', 'Edit', 'Export', and a help link. Below is a table with columns for 'Status', 'Source', 'Destination', 'Dest. port', 'Source', 'Src. port', 'Destination', 'Dest. port', 'Options', and 'Comment'. Two rules are listed:

Status	Original traffic (before translation)				Traffic after translation				Options	Comment
	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port			
1 on	Network_LAN	Network_WAN	Any	Firewall_WAN	Any	Firewall_WAN	Any		Créée le 2025-01-28 16:17:48, par admin (192...)	
2 on	Network_LAN	Internet	Any	Firewall_WAN	Any	Firewall_WAN	Any		Créée le 2025-01-28 16:17:48, par admin (192...)	

Dans la section Network / NAT de l'interface de configuration du Stormshield SN160, il est nécessaire de définir les règles permettant la communication entre le réseau LAN interne et le réseau WAN externe, ainsi que l'accès à Internet.

Le paramétrage du NAT (Network Address Translation) est essentiel pour que les machines du réseau local, utilisant des adresses IP privées, puissent être traduites en une adresse publique ou routable au sein du réseau amont. Cette étape permet à l'ensemble des postes clients du réseau LAN de sortir vers Internet via l'interface WAN.

Il est également possible, dans ce module, de configurer des règles de redirection de port (DNAT) si des services internes doivent être accessibles depuis l'extérieur — ce qui n'est pas le cas dans notre configuration actuelle, orientée uniquement vers un accès sortant.

Une fois le routage effectué il me reste à mettre en place les règles du pare-feu.

Index	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comment
<b>Remote Management: Go to System - Configuration to setup the web administration application access (contains 4 rules, from 1 to 4)</b>								
1	on	pass	[Any]	firewall_all	firewall_srv https	IPS	Admin from everywhere	
2	on	pass	Network_LAN	Internet	isakmp_natt isakmp	IPS	Allow Ping from everywhere - Updated on 202...	
3	on	pass	Network_LAN	Internet	[Any]	IPS	Allow Ping from everywhere - Updated on 202...	
4	on	pass	[Any]	[Any]	icmp (Echo request (Ping))	IPS	Allow Ping from everywhere	
<b>Default policy (contains 2 rules, from 5 to 6)</b>								
5	on	pass	[Any]	Network_LAN	[Any]	IPS	Block all	
6	off	block	[Any]	[Any]		IPS	Créée le 2025-03-13 12:41:36, par admin (192...	

Dans l'onglet Security Policy / Filtering, plusieurs règles ont été définies afin de contrôler précisément les communications entre les différents réseaux.

- Les trois premières règles ont pour objectif d'autoriser la communication entre les réseaux. Elles permettent le passage des flux nécessaires au bon fonctionnement des services entre le LAN, le WAN et internet.
- La quatrième règle autorise le trafic ICMP. Cette autorisation est essentielle pour effectuer des tests de connectivité, tels que les commandes ping, sans que le pare-feu n'interfère ou bloque ces requêtes. Cela permet de vérifier facilement si les machines peuvent se joindre entre elles à travers les différents réseaux.
- La sixième règle, quant à elle, est désactivée par défaut (off) et ne doit être activée qu'en cas de dysfonctionnement ou de tentative d'accès non autorisé. Elle a pour fonction de bloquer intégralement les communications entre les différents réseaux, agissant ainsi comme une mesure de sécurité d'urgence.

## 02 VPN (Virtual Private Network)

Un VPN (Virtual Private Network) est un réseau privé virtuel permettant de créer une connexion sécurisée entre deux points sur Internet, en chiffrant les données échangées. Cela permet notamment d'accéder à distance à des ressources d'un réseau (comme un serveur d'entreprise ou d'école) tout en protégeant ses informations personnelles.

**Il existe deux grands types de VPN :**

### 1. VPN Client-to-Site (ou Remote Access VPN)

Ce type de VPN permet à un utilisateur distant (client) de se connecter de manière sécurisée à un réseau privé (par exemple, le réseau d'un lycée ou d'une entreprise).

Exemple : Un étudiant ou un employé travaillant à distance qui se connecte au réseau du lycée via le client OpenVPN pour accéder aux fichiers et services.

Caractéristiques :

- Chaque client établit un tunnel VPN sécurisé avec le serveur VPN.
- Permet de se connecter depuis n'importe quel endroit (Wi-Fi public, maison...).

### 2. VPN Site-to-Site (ou LAN-to-LAN VPN)

Ce type de VPN connecte deux réseaux entiers entre eux de manière sécurisée.

Par exemple, relier deux sites d'une entreprise ou deux bâtiments d'un lycée (principal et antenne).

Exemple : Un site principal (lycée) est relié à un site distant (antenne) via un tunnel VPN.

Caractéristiques :

- Permet à tous les appareils d'un réseau d'accéder à un autre réseau distant comme s'ils étaient physiquement connectés.
- Configuration souvent réalisée sur des routeurs ou des pare-feux (comme le Stormshield SN160).

Aucune contrainte particulière ne nous a été imposée concernant la mise en place du VPN. J'ai donc étudié plusieurs possibilités afin de choisir la solution la plus adaptée au contexte de notre infrastructure. Deux options principales se présentaient : utiliser le serveur Windows déjà intégré à notre réseau, ou bien tirer parti du routeur Stormshield SN160.

### **Option 1 : Mise en place du VPN via le serveur Windows**

#### Avantages :

- Intégration native à l'environnement Active Directory, ce qui facilite la gestion des utilisateurs et des droits d'accès.
- Facilité de mise en œuvre pour des connexions PPTP ou L2TP simples.



#### Inconvénients :

- Moins sécurisé que d'autres solutions si des protocoles obsolètes (comme PPTP) sont utilisés.
- Performances limitées si le serveur Windows est déjà sollicité pour d'autres services (contrôleur de domaine, DNS...).

### **Option 2 : Mise en place du VPN via le Stormshield SN160**



**STORMSHIELD**

- Intégration directe au pare-feu, permettant un contrôle précis du trafic VPN (filtrage, journalisation).

#### Avantages :

- Sécurité renforcée grâce au support natif des protocoles IPsec, avec chiffrement fort et gestion centralisée des clés.

#### Inconvénients :

- Moins d'intégration directe avec l'annuaire Active Directory (configuration des utilisateurs en local ou via certificat).

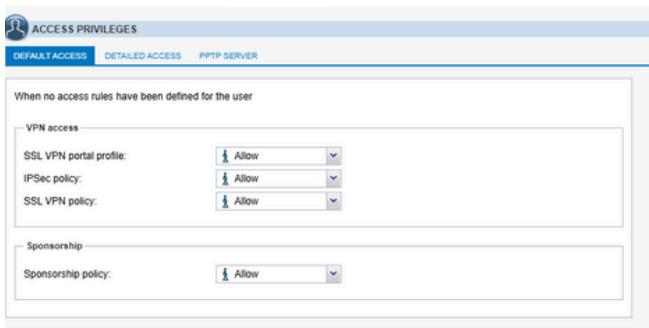
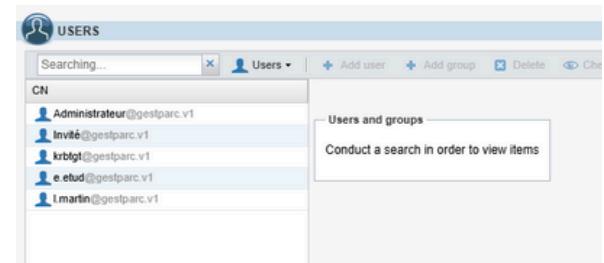
## Choix final : Implémentation du VPN via le Stormshield SN160

Après analyse des différentes options, le choix s'est porté sur l'utilisation du Stormshield SN160 pour la mise en place du VPN. Ce choix a été motivé principalement par des considérations de sécurité, le Stormshield offrant un niveau de protection plus élevé grâce à sa gestion avancée des protocoles IPsec et SSL, ainsi qu'un meilleur contrôle des flux via son module pare-feu intégré.

Pour mettre en œuvre cette solution, trois sections de l'interface d'administration du Stormshield seront utiliser, Security Policy, User et VPN.

### User

La première étape de la configuration consiste à récupérer les comptes utilisateurs existants depuis le serveur Active Directory. Cette opération permet d'importer les identifiants déjà utilisés dans l'infrastructure du lycée, tout en conservant les priviléges associés à chaque utilisateur



Une fois les comptes utilisateurs récupérés depuis le serveur Active Directory, il est nécessaire de définir les droits d'accès aux services VPN pour chacun d'eux.

Cette configuration s'effectue dans la section Users > Access privileges de l'interface d'administration Stormshield. À ce niveau, les différentes politiques d'accès VPN doivent être explicitement autorisées pour permettre la connexion des utilisateurs à distance.

## Security Policy

Une fois les comptes utilisateurs correctement configurés et les droits d'accès VPN attribués, il est nécessaire de définir une règle de filtrage dans le pare-feu pour autoriser le trafic entrant depuis les connexions VPN vers le réseau local.

Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comment
on	pass	Any	firewall_all	https		IPS	Admin from everywhere
on	pass	Network_LAN	Internet	isakmp_natt	isakmp	IPS	Allow Ping from everywhere - Updated on 202...
on	pass	Network_LAN	Internet	Any		IPS	Allow Ping from everywhere - Updated on 202...
on	pass	Any	Any	Any	icmp (Echo request (Ping))	IPS	Allow Ping from everywhere
on	pass	any	Network_LAN	Any		IPS	Block all
off	block	Any	Any	Any		IPS	Créée le 2025-03-13 12:41:36, par admin (192...

Cette configuration s'effectue dans l'onglet Security Policy > Filtering – NAT. La règle n°5 a été ajoutée à cet effet. Elle permet à tous les utilisateurs connectés via le VPN d'accéder aux ressources du réseau LAN interne.

## VPN

Après avoir autorisé les accès VPN aux utilisateurs et défini les règles de filtrage, l'étape suivante consiste à configurer le serveur SSL VPN intégré au Stormshield SN160.

Network settings	
UTM IP address (or FQDN) used:	192.168.1.114
Available networks or hosts :	Network_internals
Network assigned to clients (UDP):	SSL_VPN
Network assigned to clients (TCP):	SSL_VPN2
Maximum number of simultaneous tunnels allowed:	6

DNS settings sent to client	
Domain name:	gestparc.v1
Primary DNS server:	DNSserv
Secondary DNS server:	Configured for the fi

Cette configuration s'effectue dans l'onglet VPN / SSL VPN, où plusieurs paramètres essentiels sont définis :

UTM IP address : L'adresse IP enregistrer dois être le même que l'interface WAN sur stormshield.

Available networks or hosts : Ce champ détermine les ressources internes accessibles par les utilisateurs VPN.

Network assigned to clients (UDP / TCP): ici on enregistre un 3eme réseau qui fait office de DMZ a des fin de sécurité .



### **Côté client : connexion VPN avec OpenVPN**

Pour permettre aux étudiants de se connecter au réseau du lycée à distance, le client OpenVPN a été utilisé. Ce logiciel libre est compatible avec la configuration VPN mise en place sur le Stormshield SN160.

trib

Installation et configuration

Le client OpenVPN a été installé sur les postes utilisateurs.

La configuration repose sur l'importation d'un fichier .ovpn généré depuis l'interface du Stormshield. Ce fichier contient les paramètres nécessaires à l'établissement du tunnel VPN (adresse IP, type de protocole, certificats, etc.).

Des modifications ont été apportées à ce fichier afin de l'adapter à notre infrastructure et de régler des problème rencontré.

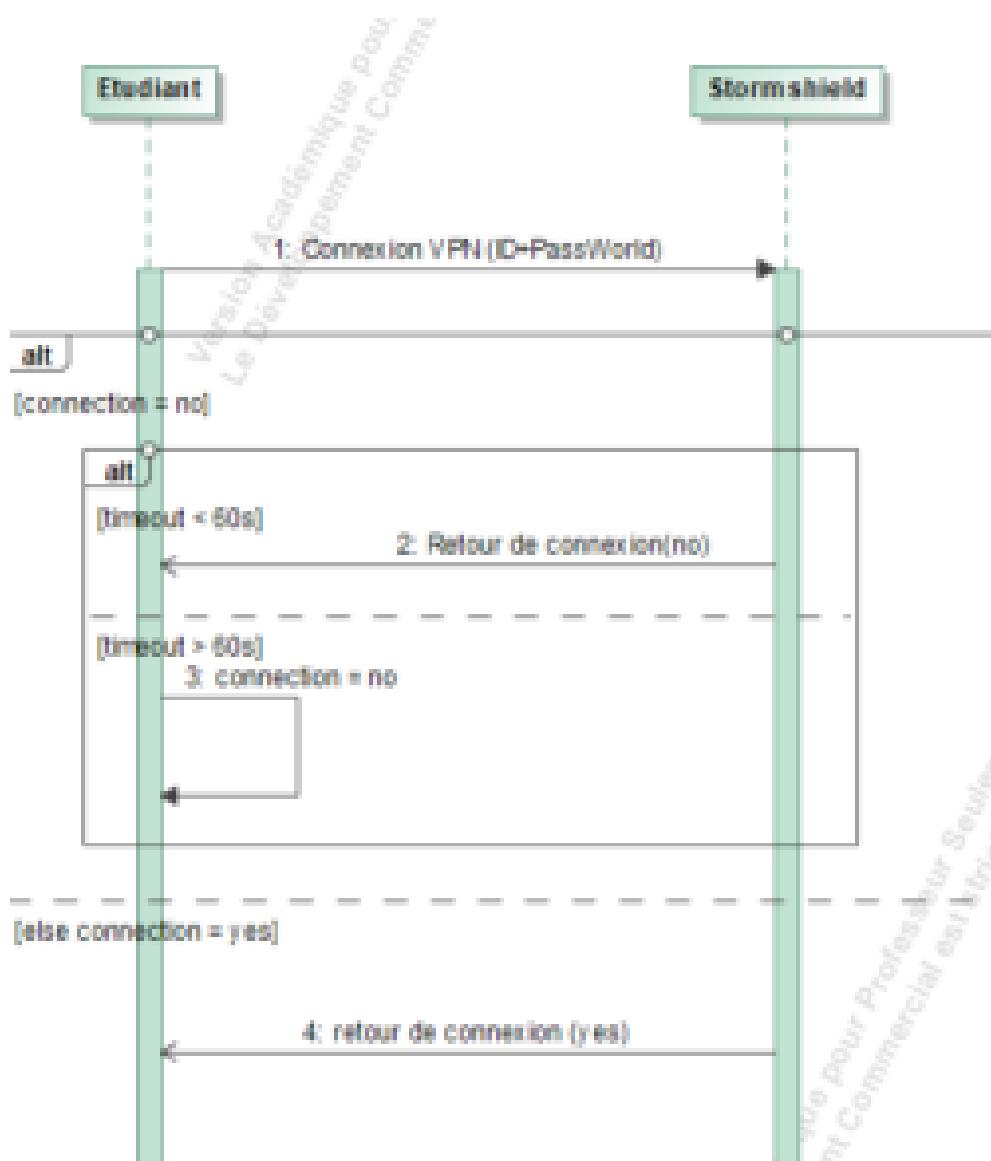
Afin d'intégrer OpenVPN à notre application , un fichier *auth.txt* a été utilisé. Ce fichier contient :

- ligne 1 : Identifiant
- ligne 2 : Mot de passe

Le fichier *.ovpn* est ensuite modifié pour inclure ce fichier d'authentification automatique, via la ligne :

auth-user-pass "C:\\Program Files\\OpenVPN\\config\\auth.txt"

Une fois l'ensemble de la configuration terminé — côté pare-feu, utilisateur, et client OpenVPN — la connexion VPN peut être établie depuis n'importe quel poste extérieur au réseau LAN, permettant ainsi un accès sécurisé aux ressources internes du lycée.



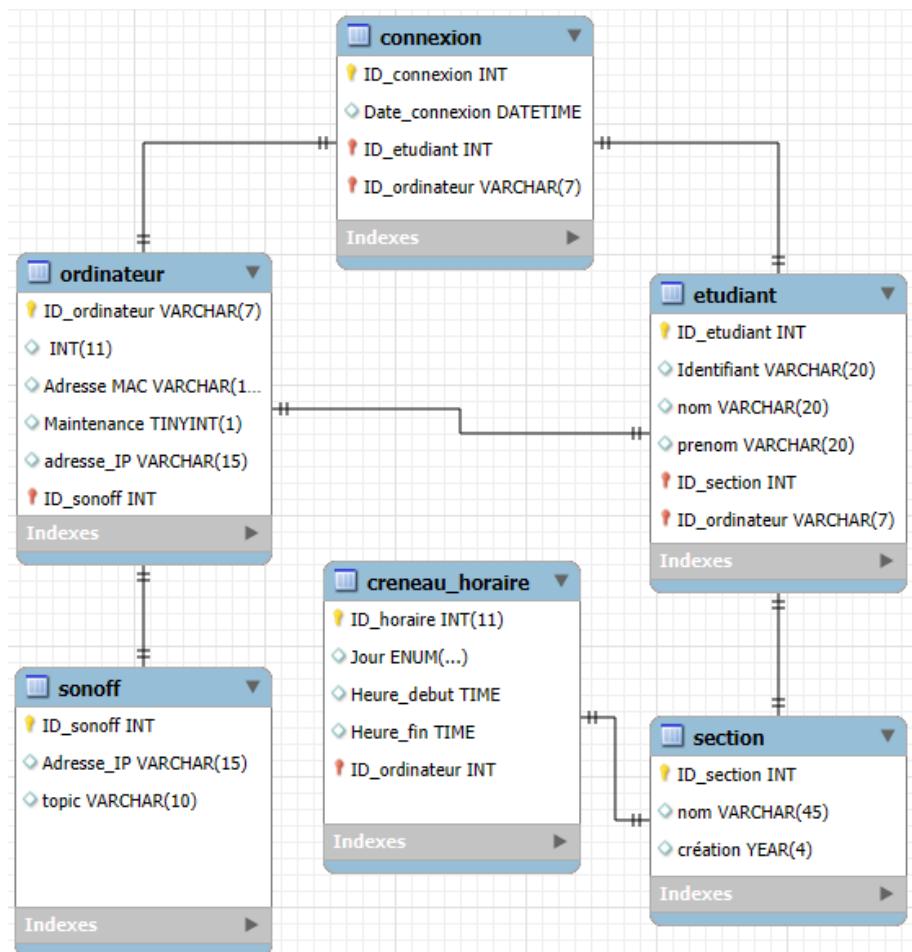
# 03 Base De Données / Implémentation

La base de données a été implémentée à l'aide de MariaDB, un moteur SQL libre, rapide et compatible avec MySQL.

L'implémentation repose sur 6 tables relationnelles, toutes créées manuellement via des requêtes SQL. Des clés primaires et étrangères ont été définies pour assurer l'intégrité des relations.

Exemple de l'implémentation de la table étudiant :

```
CREATE TABLE etudiant (
    ID_etudiant INT AUTO_INCREMENT PRIMARY KEY,
    ID_ordinateur VARCHAR(7),
    ID_section INT,
    Identifiant VARCHAR(20),
    nom VARCHAR(20),
    prenom VARCHAR(20),
    FOREIGN KEY (ID_ordinateur) REFERENCES ordinateur(ID_ordinateur),
    FOREIGN KEY (ID_section) REFERENCES section(ID_section)
);
```



## 04 Connexion et authentification

L'application développée en Python intègre une procédure de connexion automatisée basée sur le VPN. Contrairement à un système classique où l'utilisateur saisit manuellement ses identifiants, ici, l'authentification repose directement sur la réussite de la connexion VPN.

### Déclenchement automatique du VPN

Au lancement, l'application exécute OpenVPN en ligne de commande à l'aide de openvpn.exe, en fournissant deux fichiers essentiels :

- un fichier de configuration .ovpn, généré depuis l'interface Stormshield et adapté à notre infrastructure ;
- un fichier auth.txt contenant l'identifiant et le mot de passe de l'utilisateur sur deux lignes.

Cette commande est lancée par le script Python à l'aide de la bibliothèque subprocess.

### Vérification de la connexion VPN:

L'application surveille les logs générés par OpenVPN pour détecter si la connexion a bien été établie.

Elle analyse notamment la présence de messages tels que :

Initialization Sequence Completed

Ce message confirme que le tunnel VPN est actif et fonctionnel.

Si ce message est détecté, l'utilisateur est considéré comme authentifié et autorisé à accéder aux fonctionnalités de l'application.

### Sécurité et simplicité

Ce système permet une authentification automatisée et transparente pour l'utilisateur, tout en conservant un haut niveau de sécurité :

- les identifiants sont vérifiés par le pare-feu Stormshield ;
- seules les personnes autorisées peuvent établir une connexion VPN ;
- l'application bloque l'accès si le tunnel VPN n'est pas actif ou si la connexion échoue.

Ce fonctionnement évite les doublons de vérification et garantit que seuls les utilisateurs ayant des droits réseau valides peuvent utiliser la plateforme.

## 05 Affichage de l'état du parc

L'application intègre un module permettant d'afficher l'état de chaque poste du parc informatique, en indiquant si la machine est actuellement allumée ou éteinte.

Pour déterminer l'état d'un ordinateur, l'application utilise la commande ping. Si la machine répond, elle est considérée comme allumée. Dans le cas contraire, elle est déclarée comme éteinte ou injoignable.

Le comportement de ce module varie selon le profil de l'utilisateur connecté :

- Étudiant :

Lorsqu'un étudiant se connecte, l'application interroge la base de données pour connaître l'identifiant de l'ordinateur qui lui est associé.

Seul cet ordinateur est ensuite testé via un ping, afin d'optimiser les performances et éviter des requêtes inutiles.

- Administrateur :

En mode administrateur, l'application doit tester l'ensemble des machines du parc. Cela implique d'envoyer un ping vers chaque adresse IP répertoriée dans la base de données des ordinateurs.

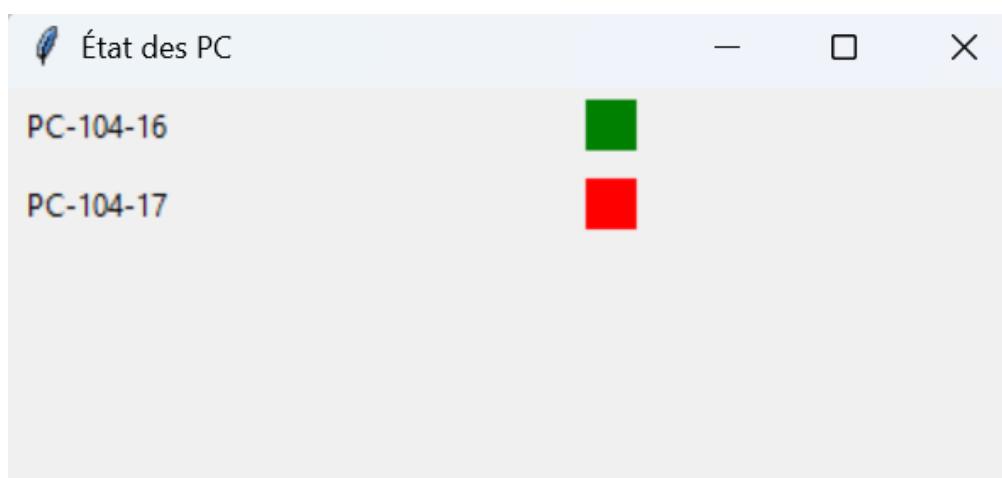
Tester tout le parc informatique peut être lourd en ressources et en temps.

Pour cette raison, le test des machines ne s'effectue pas automatiquement en temps réel.

Un bouton "Rafraîchir" est mis à disposition de l'administrateur, lui permettant de lancer manuellement une mise à jour de l'état des postes.

Cette approche garantit un bon équilibre entre précision de l'information et optimisation des performances du système.

voilà le module séparé administrateur :



# 06 Affecter les ordinateurs

Le module d'affectation des ordinateurs aux étudiants est une fonctionnalité essentielle du système de gestion du parc informatique. Bien que cette partie n'ait pas encore été implémentée au moment de la rédaction de ce rapport, le mécanisme prévu est décrit ci-dessous.

## Mécanisme prévu pour l'affectation

L'affectation d'un ordinateur à un étudiant se fera par une modification simple dans la base de données MariaDB. Plus précisément, il s'agira de :

- Mettre à jour le champ ID\_ordinateur dans la table étudiant avec l'identifiant de l'ordinateur à affecter

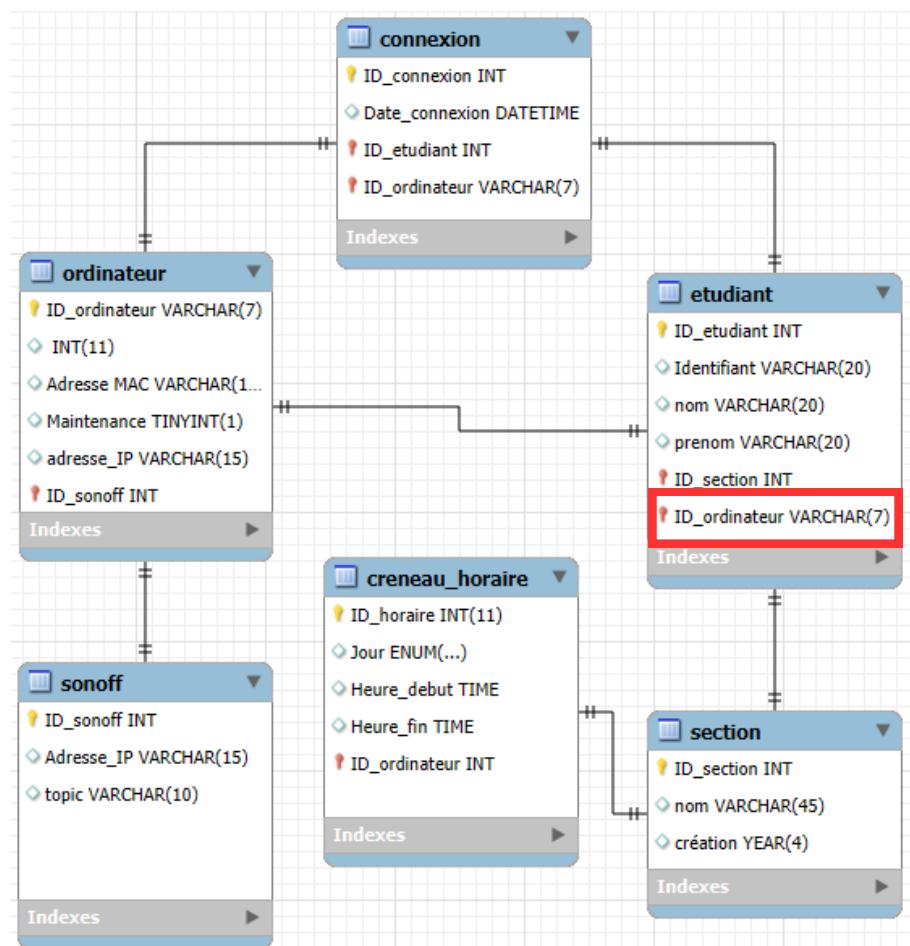
UPDATE étudiant

```
SET ID_ordinateur = [ID_ordinateur] WHERE ID_etudiant = [ID_etudiant];
```

- Vérifier que l'ordinateur n'est pas déjà attribué à un autre étudiant

Cette opération pourra être effectuée :

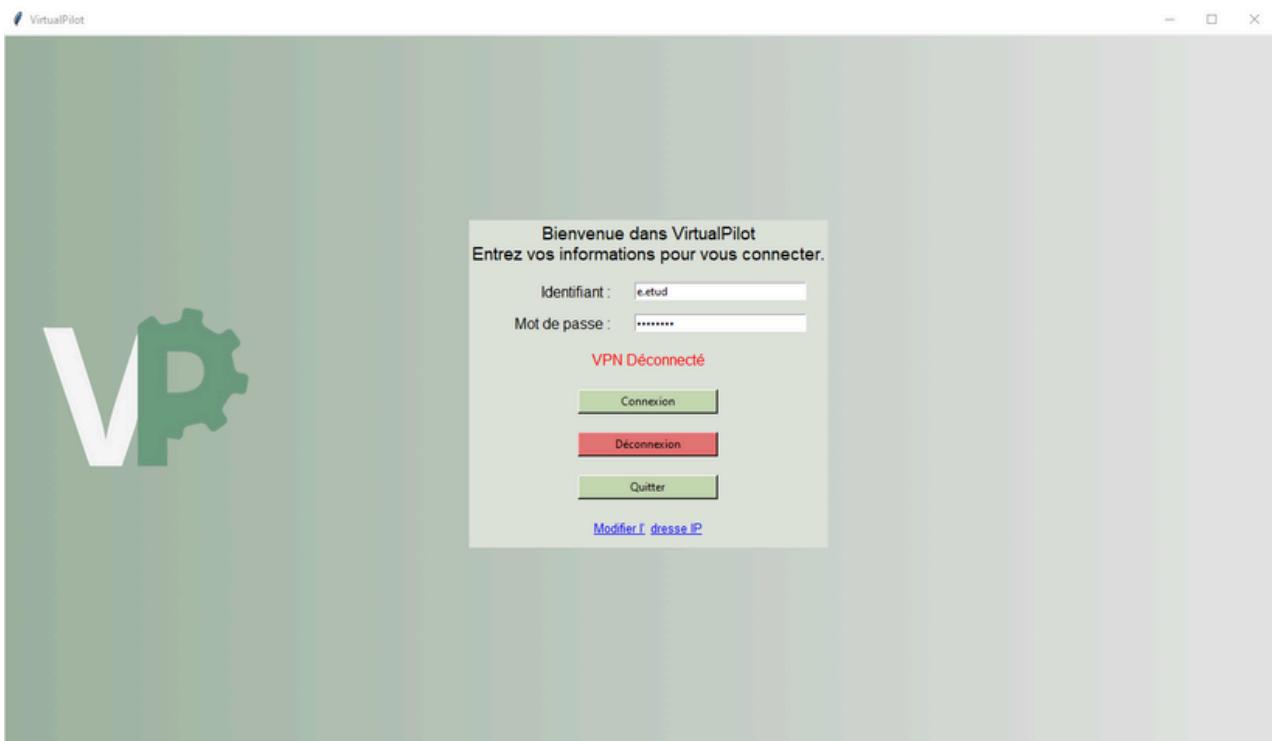
directement sur l'application administrateur, en créant le conte étudiant ou en modifiant les information de l'étudiant.



# Application Etudiant

Ici je vais vous expliquer comment marche et les modifications à apporter à l'application côté étudiant.

il y a ci-dessous une image qui montre ce que l'application affichera une fois l'application lancée



il y a 4 boutons et chacun a sa particularité :

## 1. Connexion

- Action : Démarrer la connexion VPN via OpenVPN.
- Ce que fait le bouton :
  - Vérifie les identifiants saisis.
  - Écrit l'identifiant et le mot de passe dans le fichier auth.txt.
  - Lance OpenVPN avec le fichier de configuration spécifié.
  - Affiche une animation de connexion.
  - Met à jour l'état : "VPN Connecté" si la connexion réussit.

## 2. Déconnexion

- Action : Arrête la connexion VPN.
- Ce que fait le bouton :
  - Termine le processus openvpn.exe.
  - Interrompt l'animation de connexion s'il y en a une.
  - Met à jour l'état : "VPN Déconnecté".
  - L'application reste ouverte pour une future reconnexion.

## 3. Quitter

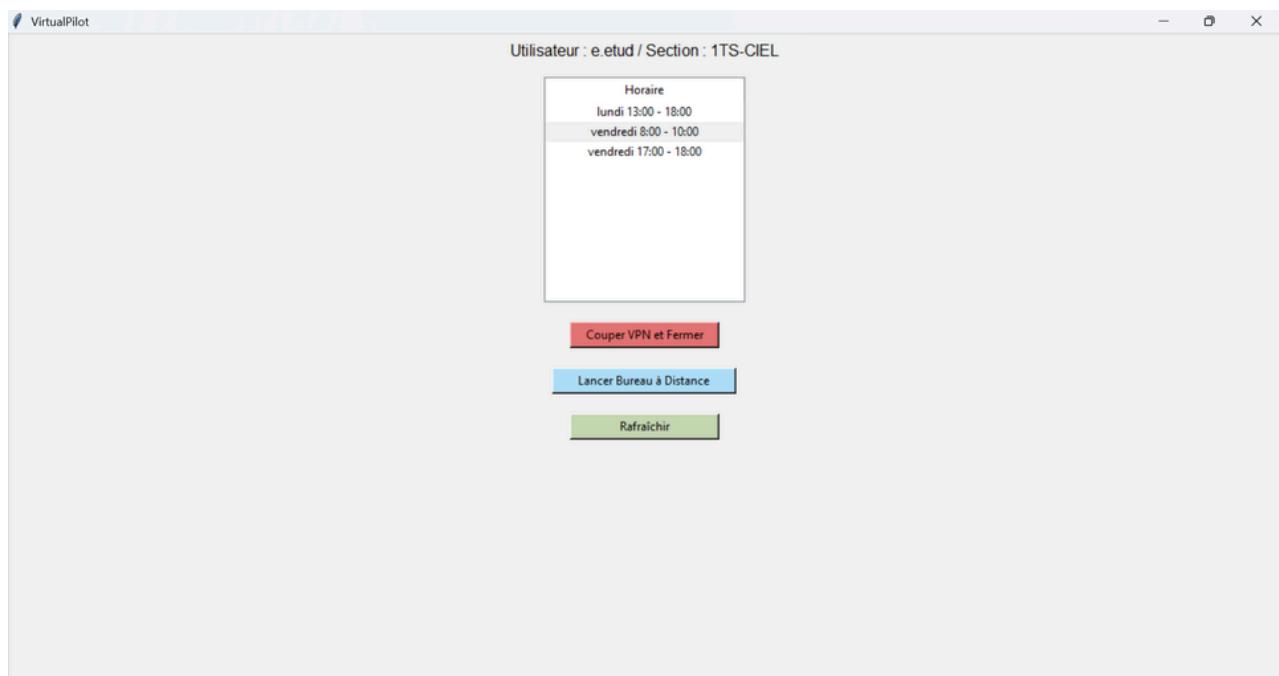
- Action : Ferme complètement l'application.
- Ce que fait le bouton :
  - Vérifie si un VPN est en cours, et le stoppe proprement.
  - Ferme la fenêtre Tkinter (l'interface graphique).
  - Met fin à l'exécution du programme.



## 4. Modifier l'adresseIP

- Action : modifier l'adresse IP enregistrée du port WAN du stormshield
- Ce que fait le bouton :
  - Vérifie que l'adresse IP/port saisis est valide
  - Modifie le fichier .ovpn en remplaçant l'ancienne IP
  - Affiche un message de confirmation/erreur
  - La nouvelle IP sera utilisée pour les prochaines connexions

Une fois connecter on arrive sur la page montré ci-dessous.



il y a 3 boutons et chacun a sa particularité :

#### 1. Lancer Bureau à Distance

- Action : Établit une connexion bureau à distance vers l'ordinateur attribué.
- Ce que fait le bouton :
  - Récupère l'identifiant de l'étudiant à partir du fichier auth.txt.
  - Accède à la base de données pour obtenir l'adresse IP du PC attribué à cet étudiant.
  - Allume le relais Sonoff associé à l'ordinateur (via MQTT).
  - Allume le PC distant via un script SSH (WOL).
  - Attend le démarrage complet de la machine.
  - Ajoute automatiquement les identifiants au gestionnaire d'identifiants Windows.
  - Lance la connexion Bureau à distance (mstsc) vers l'IP du PC.

## 2. Couper VPN et Fermer

- Action : Déconnecte le VPN et quitte l'application.
- Ce que fait le bouton :
  - Récupère l'IP du PC distant associé à l'étudiant.
  - Exécute un script SSH pour éteindre le PC (WOL2\_A <ip>).
  - Éteint le relais Sonoff via MQTT.
  - Termine le processus OpenVPN (taskkill).
  - Ferme l'application (fermeture de la fenêtre principale).

## 3. Rafraîchir

- Action : Met à jour la liste des créneaux horaires.
- Ce que fait le bouton :
  - Interroge la base de données pour récupérer les créneaux de la section de l'étudiant connecté.
  - Trie les créneaux :
    - Ceux d'aujourd'hui à venir.
    - Puis ceux des jours suivants.
  - Met à jour dynamiquement l'interface (Treeview) avec la liste triée.

# Conclusion

Le projet est dans un état avancé, avec une grande partie des fonctionnalités principales déjà mises en place et opérationnelles. Plusieurs éléments ont été entièrement développés, testés et intégrés, tandis que certaines parties restent à finaliser ou à améliorer.

Fonctionnalités finalisées :

- Configuration du routeur/pare-feu Stormshield SN160, avec routage, NAT et règles de sécurité personnalisées.
- Mise en place du serveur VPN, avec gestion des utilisateurs via l'interface Stormshield.
- Création et configuration des fichiers .ovpn et auth.txt pour l'authentification automatisée.
- Connexion VPN automatique via l'application Python.
- Implémentation complète de la base de données (MariaDB), avec relations entre étudiants, machines, sections, horaires et relais.
- Affichage de l'état du parc côté administrateur, avec un système de rafraîchissement manuel.
- Attribution des ordinateurs aux étudiants dans la base.

Fonctionnalités en cours de développement :

- Interface étudiante après connexion VPN : en cours de finalisation.
- Affichage de l'état de la machine personnelle pour l'étudiant, après vérification de la connexion VPN.
- Uniformisation graphique de l'application pour une meilleure expérience utilisateur.

Fonctionnalités à prévoir ou à améliorer :

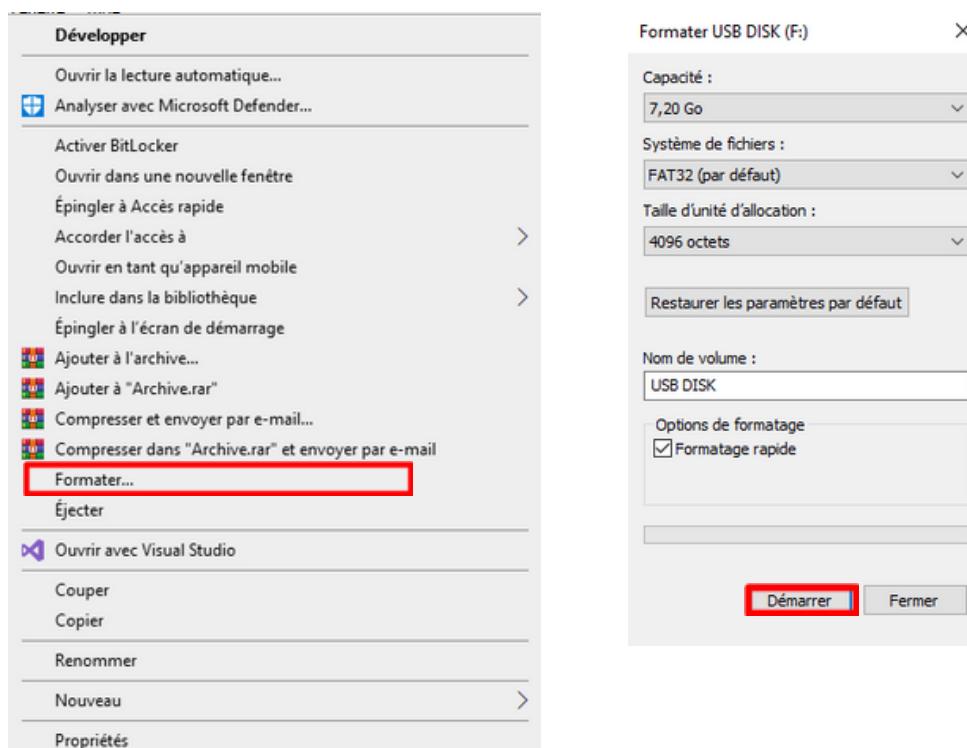
- Finalisation de l'interface étudiante complète.
- Optimisation de la gestion des logs et erreurs pour les administrateurs.

# INSTALLATION ET CONFIGURATION DE WINDOWS 11

Ma première tâche a été la mise en place de l'ordinateur du parc.  
Dans un premier temps, j'ai installer le système d'exploitation sur l'ordinateur.

Le système d'exploitation qu'il m'est demandé d'installer sur l'ordinateur est Windows 11, et dans notre cas j'ai choisi d'installer windows 11 Pro qui est le plus approprié.

La première étape a été de formater une clé USB afin d'en faire par la suite une clé bootable.



Une fois cela fait je me suis assuré que la clé USB était bien vide, c'était bien le cas, j'ai donc pu passer à l'étape suivante.

La seconde étape consistait à se rendre sur le site de Microsoft afin de créer notre clé bootable : <https://www.microsoft.com/fr-fr/windows?r=1>

# Bienvenue dans Windows

Nous savons que vous avez beaucoup à faire. Chaque jour s'accompagne d'un nouveau défi. Avec Windows 11, il est plus facile de relever ces défis.

[Obtenir Windows 11](#)

[Continuer vers la version professionnelle >](#)

## Création d'un support d'installation de Windows 11

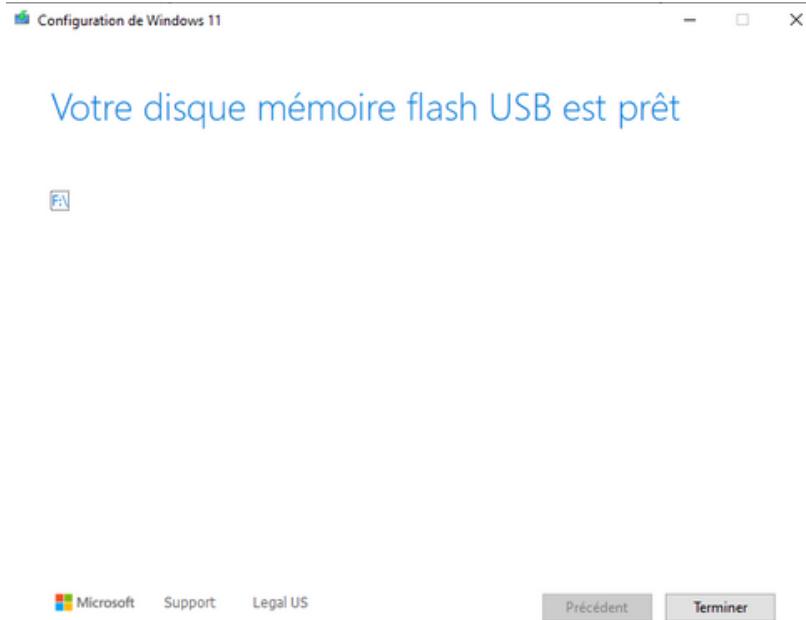
Si vous voulez réinstaller ou effectuer une nouvelle installation de Windows 11 sur un PC neuf ou déjà utilisé, cette option permet de télécharger l'outil de création de supports afin de créer une clé USB ou un DVD de démarrage.

Remarque : l'outil de création multimédia de Windows 11 ne peut pas être utilisé pour créer un contenu multimédia d'installation pour les PC dotés d'un processeur ARM. Il ne peut créer des contenus multimédias que pour les processeurs x64.

> Avant de commencer à utiliser l'outil de création de supports

[Télécharger](#)

Notre clé bootable est maintenant prête :



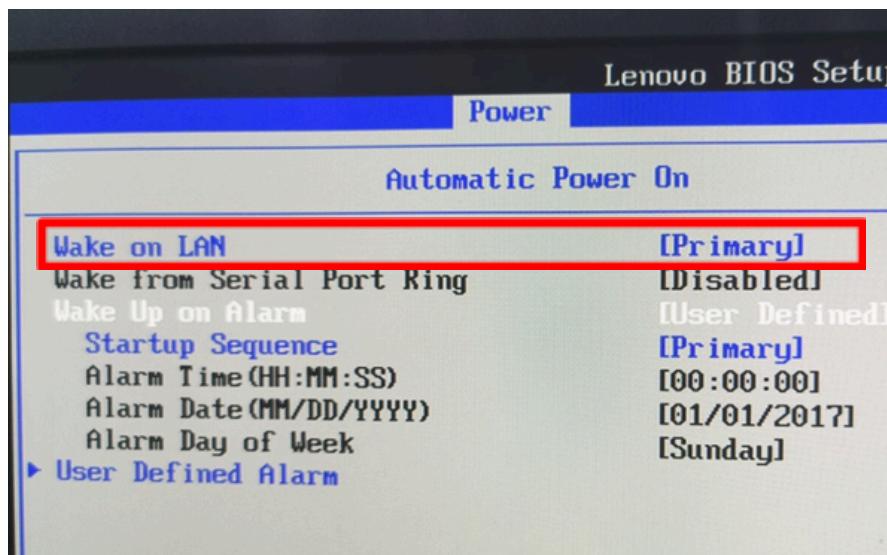
L'étape suivante est de brancher la clé USB sur l'ordinateur puis de l'allumer afin de démarrer l'ordinateur sur la clé USB, ce qui lancera l'installation du système d'exploitation.

L'installation s'est bien réalisé, j'ai donc pu passer à la suite.

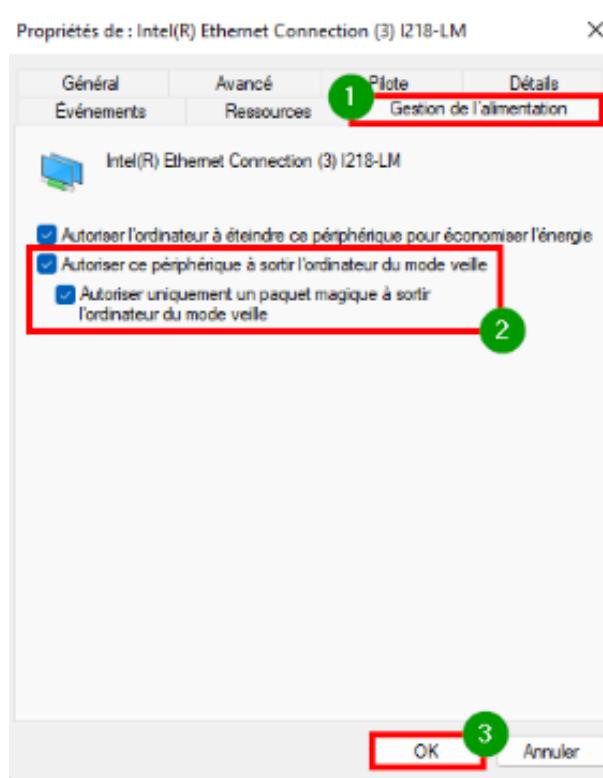
# CONFIGURATION DU BIOS (WAKE-ON-LAN)

Le wake-on-LAN est un protocole qui fait en sorte de laisser allumer le port Ethernet d'un ordinateur lorsqu'il est éteint et qui permet l'allumage d'un ordinateur éteint à distance par l'envoi d'une trame que l'on appelle paquet magique.

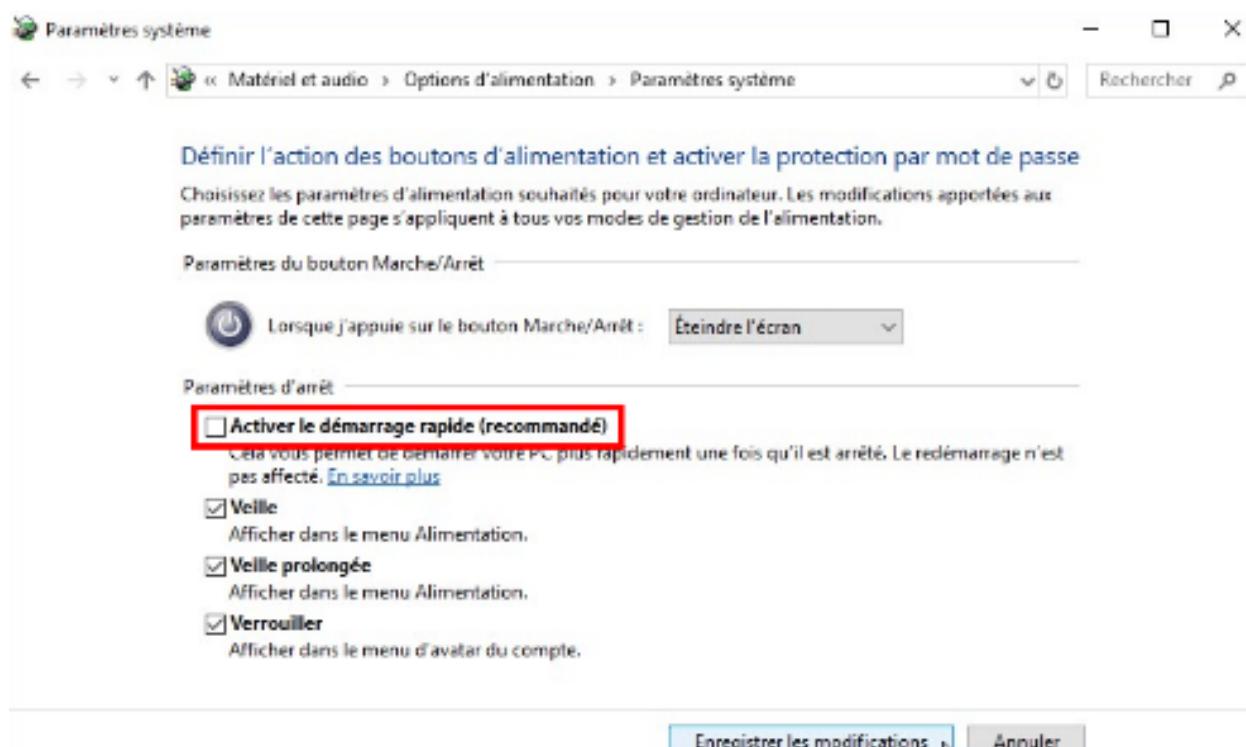
J'ai tout d'abord été dans le bios afin d'activer le wake-on-LAN sur le PC du parc.



Une fois cela fait j'ai dû me rendre sur l'ordinateur afin d'aller dans les propriétés de la carte réseau pour cocher les éléments suivant dans la catégorie « Gestion de l'alimentation » : « Autoriser ce périphérique à sortir l'ordinateur du mode veille », « Autoriser uniquement un paquet magique à sortir l'ordinateur du mode veille », ce qui permettra à la carte réseau qui sera allumer lorsque l'ordinateur sera éteint de réveiller l'ordinateur une fois qu'elle aura reçu le paquet magique.



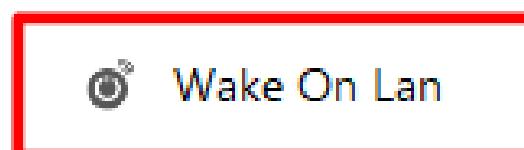
J'ai ensuite dû me rendre dans les options d'alimentation de Windows afin de décocher l'option qui se nomme « Activer le démarrage rapide » de l'ordinateur, qui pourrait poser certain problème lors du démarrage de l'ordinateur à distance.



Le Wake-on-LAN étant maintenant bien configurer, j'ai ensuite réalisé des test afin de garantir le fonctionnement.

Pour ce faire j'ai installé l'application « ManageEngine » qui est une application de gestion informatique, qui permet l'utilisation du Wake-on-LAN.

Une fois l'application installé, je me suis rendu dans la rubrique « Wake On Lan » :



Une fois dans cette rubrique, je suis arrivé sur une page qui me demandais de renseigner l'adresse MAC ainsi que l'adresse IP de l'ordinateur que je souhaite réveiller.

MAC Address	:	<input type="text" value="Enter the Mac address like 5C-A9-E2-H5-D2-L9"/>
IP Address	:	<input type="text" value="Enter the IP address"/> <span style="background-color: green; color: white; padding: 2px 10px;">Wake Up</span>

Une fois les informations de l'ordinateur entrées, je me suis assuré que l'ordinateur était bien éteint, puis j'ai appuyé sur le bouton « Wake Up ».

MAC Address	:	<input type="text" value="6C-0B-84-69-26-FD"/>
IP Address	:	<input type="text" value="192.168.1.107"/> <span style="background-color: green; color: white; padding: 2px 10px;">Wake Up</span>

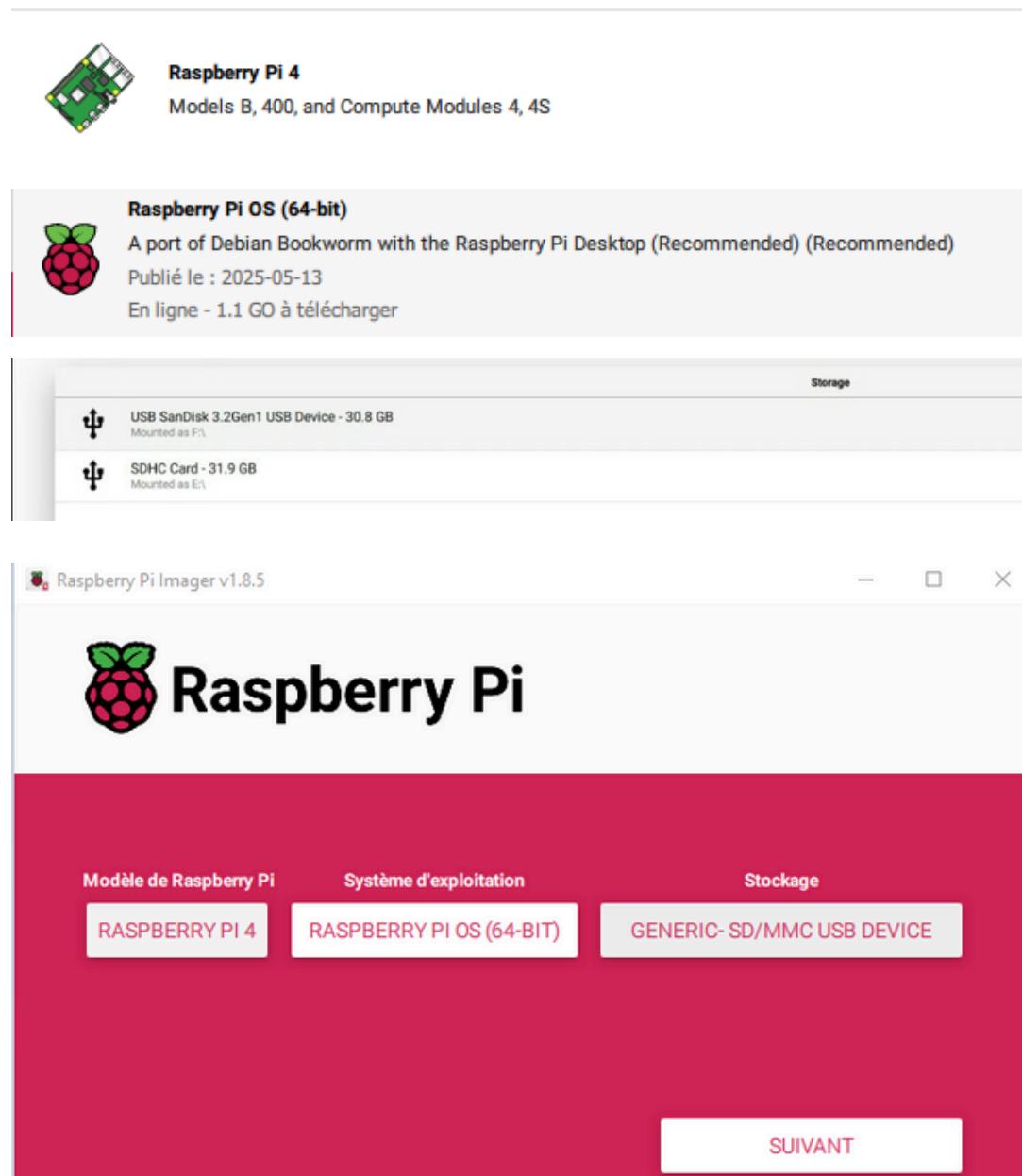
Une fois cela fait, comme on peut le voir, le paquet magique a bien été envoyé. Et l'ordinateur s'est bien allumé, ce qui veut dire que le wake on LAN est bien fonctionnel sur l'ordinateur du parc.

Status	:	Success
Remarks	:	Successfully sent the magic packets

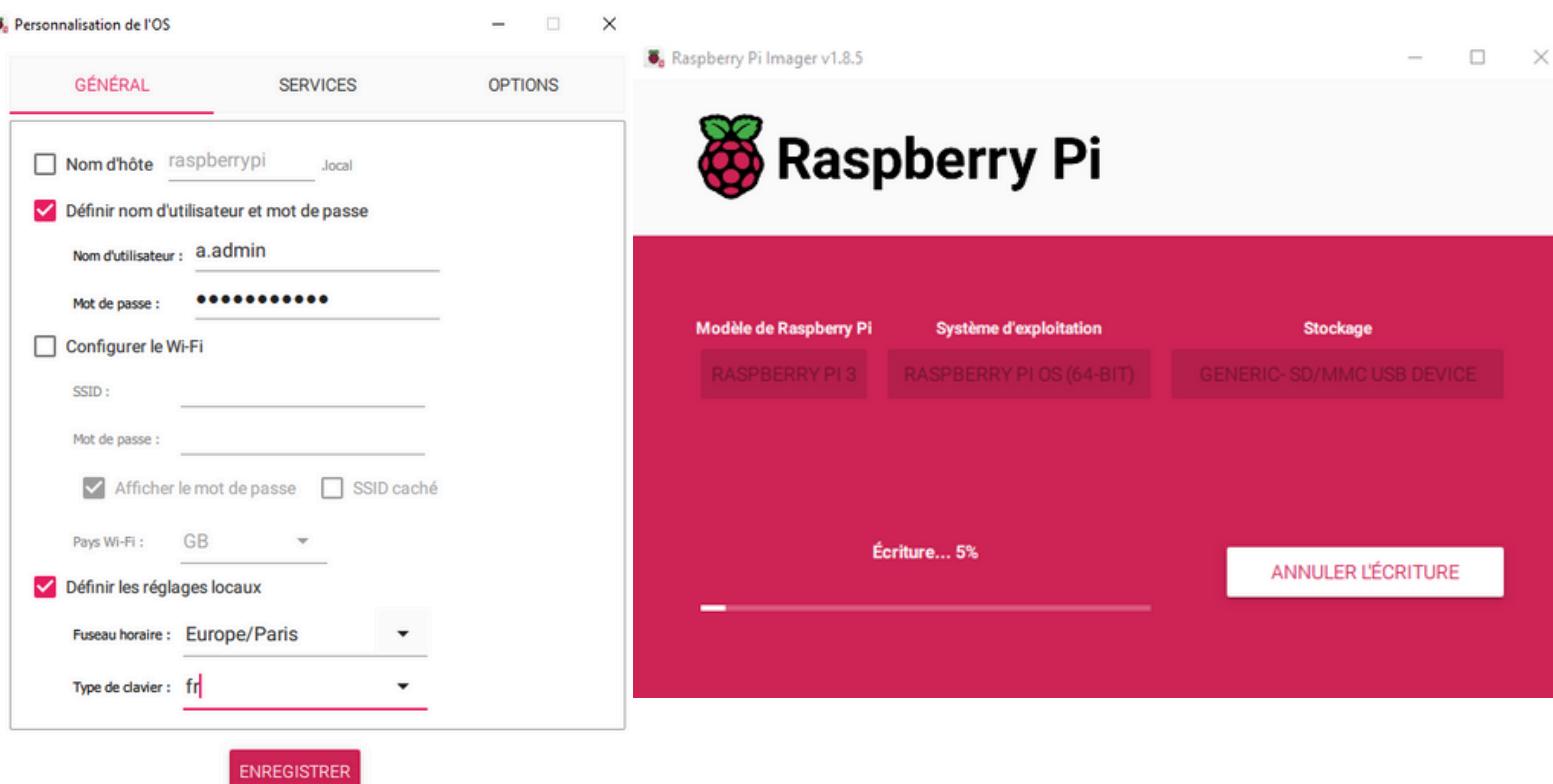
# INSTALLATION DU SYSTÈME D'EXPLOITATION DE LA RASPBERRY

Pour réaliser cette installation, je me suis tout d'abord rendu sur le site officiel de Raspberry afin de télécharger le logiciel qui va par la suite me permettre d'installer le système d'exploitation sur une carte sd : <https://www.raspberrypi.com/software/>

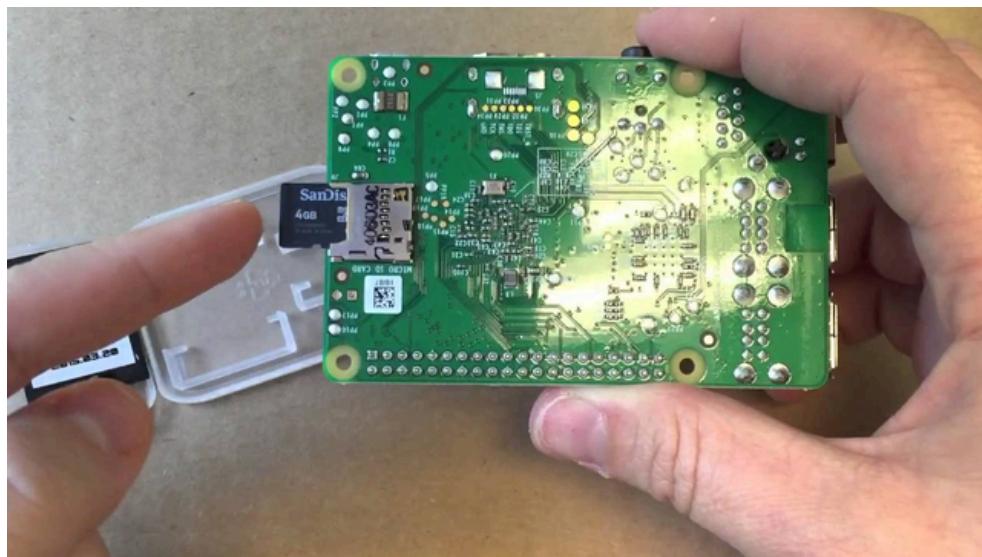
Une fois le logiciel installé, j'ai renseigné toutes les informations, en commençant par le modèle de la raspberry que l'on utilise, puis par la version du système d'exploitation qui nous intéresse, puis pour finir par le choix du stockage dans notre cas, une carte sd.



Une fois cela fait j'ai renseigné le nom d'utilisateur ainsi que le mot de passe que nous avons décidé de mettre sur la raspberry, puis j'ai lancé l'installation du système d'exploitation sur la carte SD



Une fois l'installation terminé, j'ai entré la carte SD sur la raspberry Pi afin de lancer le téléchargement du système d'exploitation



puis une fois cela fait, je me suis occupé d'installer le Wake on LAN directement sur la raspberry puisque c'est par la raspberry que nous devrons passer pour allumer l'ordinateur à distance.



A terme, l'utilisateur pourras alors déclencher le Wake on LAN depuis l'application, ce qui va ensuite envoyer un paquet magique de la raspberry à la carte réseau de l'ordinateur cible qui s'allumera si l'adresse MAC de l'ordinateur est reconnu par la carte réseau.

Pour réaliser l'installation du Wake on LAN, j'ai dû utiliser la ligne de commande « sudo apt install wakeonlan »

```
a.admin@SGBDR:~ $ sudo apt install wakeonlan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wakeonlan is already the newest version (0.41-12.1).
```

Une fois l'installation terminé, j'ai réalisé des tests afin de voir si le Wake On LAN fonctionne pour allumer un PC à distance depuis la raspberry. Pour ce faire j'ai utilisé la commande « wakeonlan + @MAC »

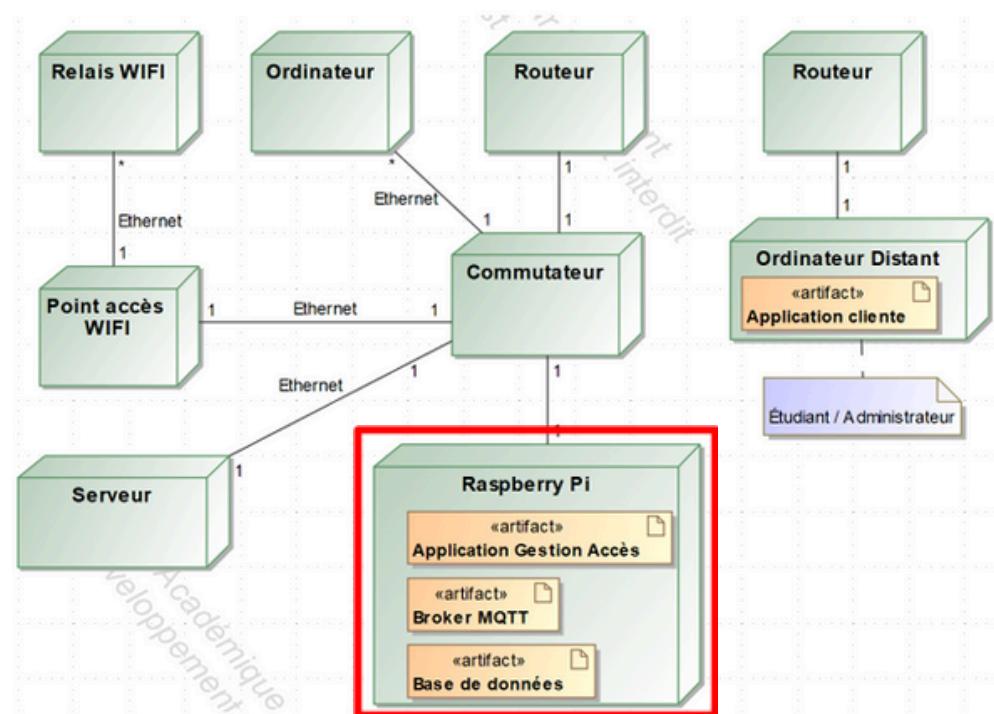
```
a.admin@SGBDR:~ $ wakeonlan 6C:0B:84:69:26:FD
Sending magic packet to 255.255.255.255:9 with 6C:0B:84:69:26:FD
```

Comme nous pouvons le voir, le paquet magique a bien été envoyé, et l'ordinateur s'est bien allumé à distance.

Nous pouvons donc en conclure que l'installation du système d'exploitation de la raspberry ainsi que la mise en place du Wake On LAN est maintenant terminé.

# INSTALLATION ET CONFIGURATION DU SERVEUR DE BASE DE DONNÉES

Comme nous pouvons le voir sur ce diagramme de déploiement, la base de données doit se situer sur la raspberry



Dans un premier temps j'ai procéder à l'installation de mariadb qui est un système de gestion de base de données sur la raspberry, en utilisant la commande « sudo apt install mariadb-server -y »

```
a.admin@SGBDR:~ $ sudo apt install mariadb-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Une fois l'installation réalisé, j'ai vérifié que le service était bien lancé, et comme nous pouvons le voir, le service mariadb est bien lancé.

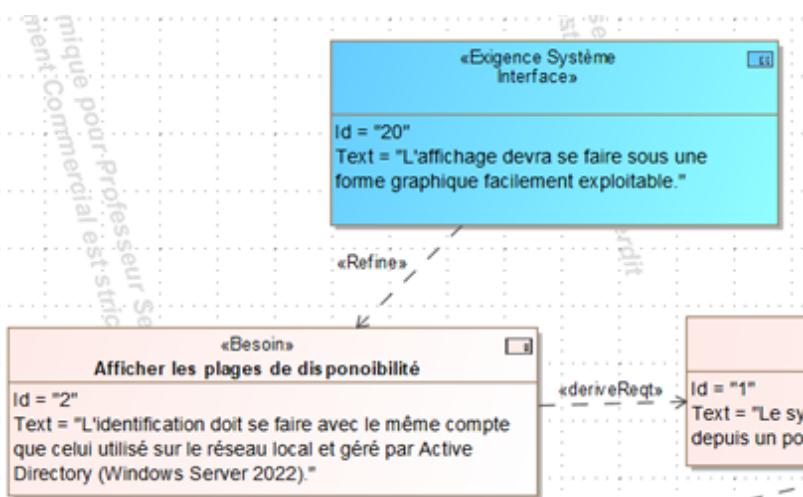
```
a.admin@SGBDR:~ $ sudo systemctl status mysql
● mariadb.service - MariaDB 10.11.11 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-05-05 14:46:41 CEST; 1 week 6 days ago
    Docs: man:mariadb(8)
```

# MODULE LOGICIEL : AFFICHAGE DES PLAGES DE DISPONIBILITÉS

Le but de ce module logiciel est de permettre à l'étudiant de voir les différentes plages de disponibilités qui lui sont attribué une fois qu'il se connecte à l'application, comme nous pouvons le voir dans le diagramme des cas d'utilisation



Le diagramme des spécification technique nous impose une seule chose qui est que l'affichage se fasse sur sous une forme graphique et facilement exploitable





A terme, ce module fonctionnera de cette façon : Dans un premier temps l'étudiant va se connecter à l'application, une fois cela fait une connexion SSH s'effectuera avec la raspberry, puis on se connectera à la base de données située sur la raspberry afin de récupérer la section de l'élève ainsi que les créneaux horaires associés à cette section afin de les afficher sur l'application de l'élève comme le montre ce diagramme de séquence

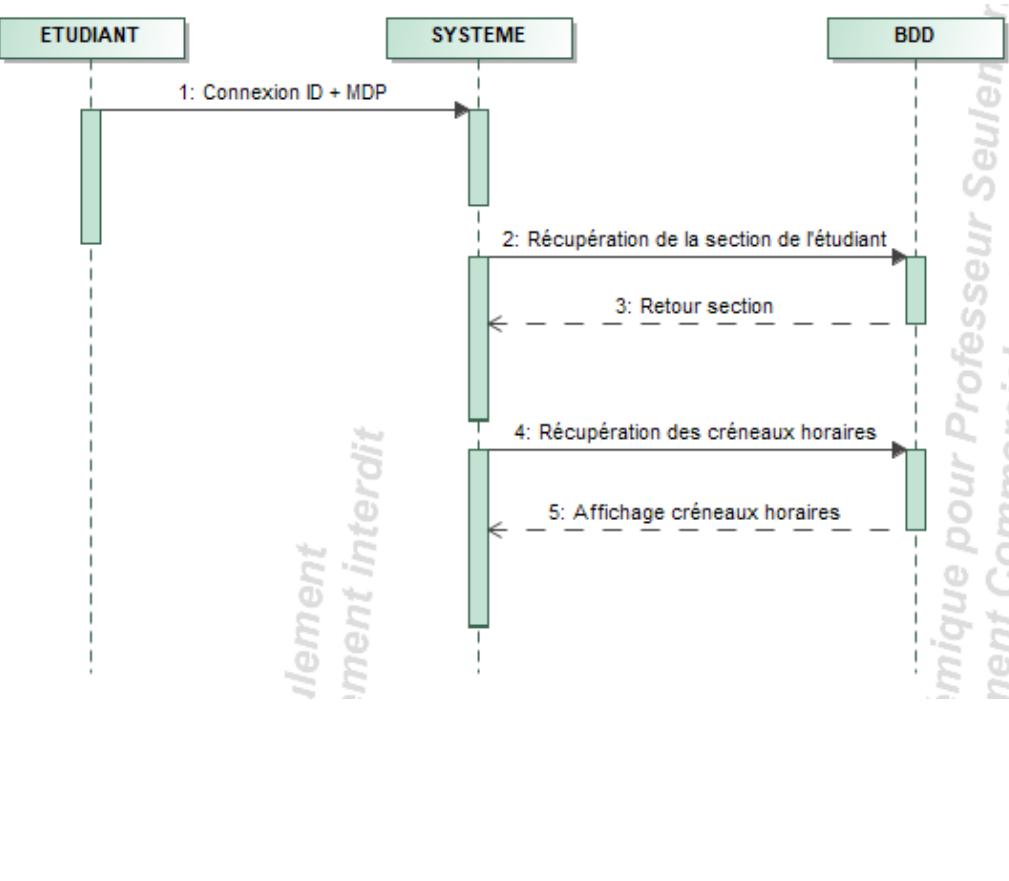


Table dans laquelle nous récupérons la section de l'étudiant :

section	
ID_section	INT
nom	VARCHAR(45)
création	YEAR(4)
Indexes	

Table dans laquelle nous récupérons les créneaux horaires selon la section :

creneau_horaire	
ID_horaire	INT(11)
Jour	ENUM(...)
Heure_debut	TIME
Heure_fin	TIME
ID_ordinateur	INT
Indexes	

Pour me rapprocher le plus possible de l'objectif final, j'ai dû faire en sorte que la section de l'étudiant soit récupérée grâce à un fichier texte qui enregistre le nom de l'étudiant. Cela me permet de me rapprocher le plus possible de l'objectif final puisque lorsque l'étudiant va se connecter à l'application, son nom sera enregistrer dans un fichier texte. Cela me permet donc de récupérer son nom à partir de ce fichier afin de retrouver sa section dans la base de données, pour lui afficher uniquement les créneaux horaires qui lui sont attribué une fois qu'il sera connecté

Dans un premier temps il faut effectuer une connexion en SSH avec la raspberry ainsi qu'une connexion avec la base de données nommée "VirtualPilot"

```

connection = mysql.connector.connect(
    host="192.168.2.5",
    user="a.admin",
    password="admin.CIEL!",
    database="VirtualPilot"
)
    
```

Pour réaliser cela, j'ai tout d'abord ajouté une fonction qui me permet de récupérer l'identifiant de l'étudiant à partir du fichier texte en y renseignant le chemin de ce fichier

```
# Fonction pour lire l'identifiant depuis un fichier auth.txt
def fetch_student_identifier_from_file():
    try:
        # Chemin vers le fichier auth.txt (modifiez le chemin selon vos besoins)
        file_path = r"C:\Users\m.langlet\Desktop\auth.txt"
        with open(file_path, "r") as file:
            student_identifier = file.readline().strip() # Lire la première ligne
        return student_identifier # Renvoie l'identifiant tel quel (VARCHAR)
    except FileNotFoundError as e:
        print(f"Erreur : Fichier auth.txt introuvable : {e}")
        return None
```

Ensuite je récupère la section de l'étudiant grâce à la ligne de commande "SELECT ID\_section FROM etudiant WHERE Identifiant = %s;"

```
cursor = connection.cursor()
cursor.execute("SELECT ID_section FROM etudiant WHERE Identifiant = %s;", (student_identifier,))
result = cursor.fetchone()
return result[0] if result else None
```

Je vais maintenant utiliser cette commande "SELECT Jour, Heure\_debut, Heure\_fin FROM creneau\_horaire WHERE ID\_section = %s;" afin de récupérer les créneaux horaire de l'étudiant selon sa section

```
cursor = connection.cursor()
cursor.execute("SELECT Jour, Heure_debut, Heure_fin FROM creneau_horaire WHERE ID_section = %s;", (section_id,))
results = cursor.fetchall()

# Date et heure actuelles
now = datetime.now()
english_to_french_days = {
    "monday": "lundi",
    "tuesday": "mardi",
    "wednesday": "mercredi",
    "thursday": "jeudi",
    "friday": "vendredi",
    "saturday": "samedi",
    "sunday": "dimanche"
}
```

Voici à quoi ressemble le module logiciel une fois terminé. Comme nous pouvons le voir, la section ainsi que les créneaux horaires changent selon l'étudiant choisi conformément à la base de données. Pour réaliser les tests, je n'ai pas enregistré de créneaux horaires pour la section 2 afin de bien distinguer le changement de section

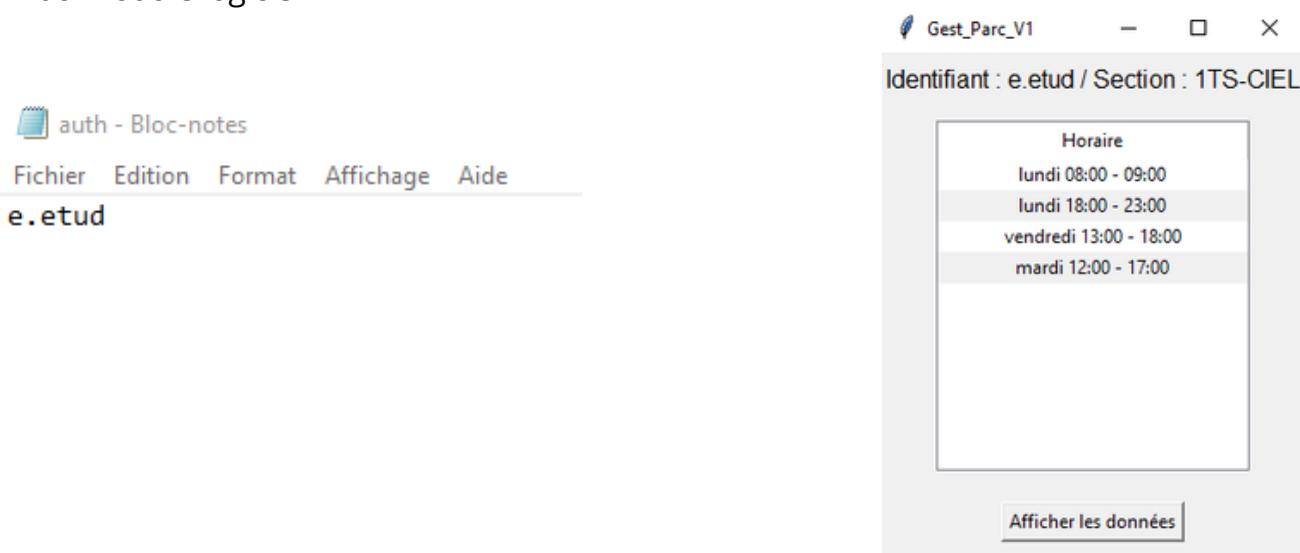
TABLE "creneau\_horaire" :

ID_horaire	ID_section	Jour	Heure_debut	Heure_fin
1	1	lundi	18:00:00	23:00:00
2	1	mardi	12:00:00	17:00:00
4	1	vendredi	13:00:00	18:00:00
28	1	mardi	12:00:00	18:00:00

TABLE "etudiant" :

ID_etudiant	ID_ordinateur	ID_section	Identifiant	nom	prenom
1	C124-16	1	e.etud	edmon	etud
9	C124-17	2	n.rozycki	rozycki	noah

J'ai réalisé les tests avec un étudiant de la section 1, et comme nous pouvons le voir, une fois l'identifiant de l'étudiant renseigné dans le fichier, nous avons une modification du module logiciel



J'ai ensuite réalisé les tests pour l'élève de la section 2, et comme nous pouvons le voir, la section, le nom de l'étudiant, ainsi que les créneaux horaire ont bien été modifié en fonction de la section de l'élève

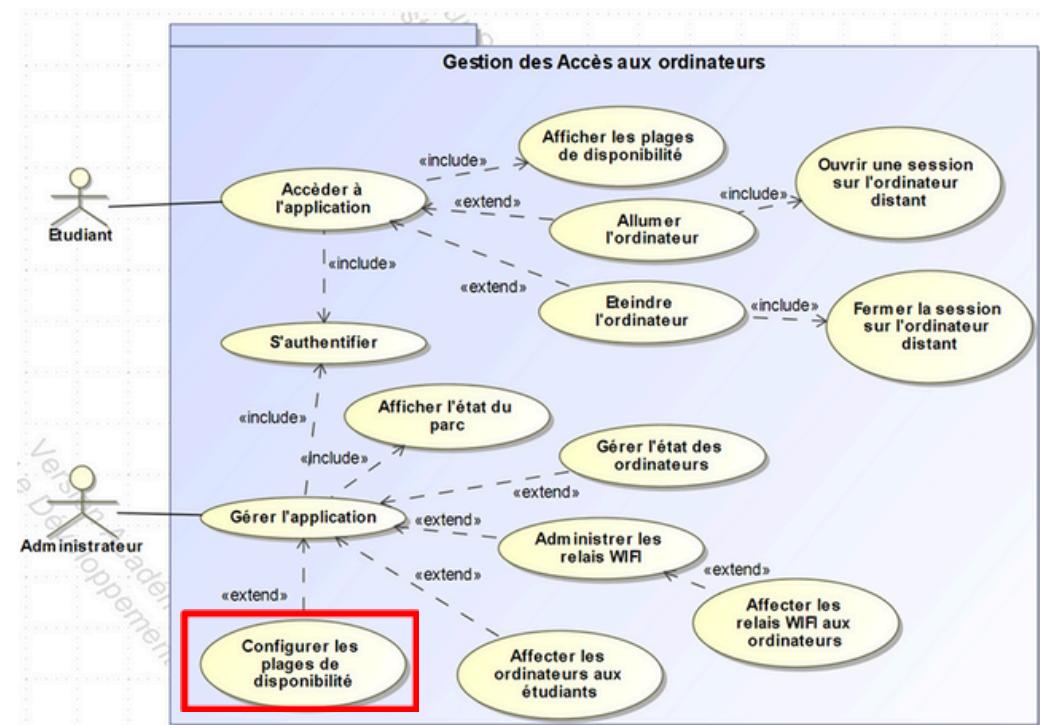


Ce module logiciel est maintenant terminé, nous récupérons bien la section de l'étudiant en fonction de son identifiant de connexion situé dans le fichier texte, pour ensuite afficher les différents créneaux horaires qui lui sont attribué dans la base de données.

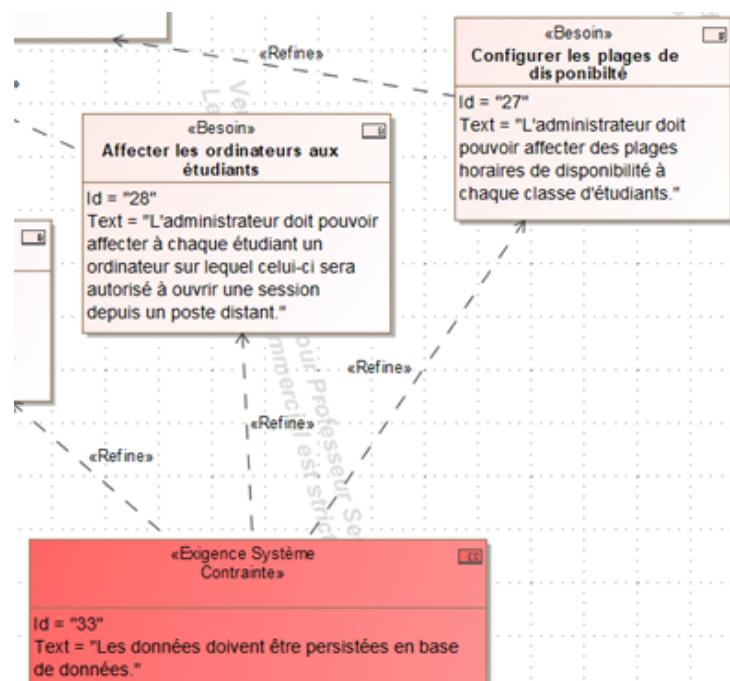
# MODULE LOGICIEL : CONFIGURER LES PLAGES DE DISPONIBILITÉS

Le but de ce module logiciel est de permettre à l'administrateur, de pouvoir configurer les créneaux horaires pour les étudiants en ayant le choix de la section, du jour de la semaine ainsi que de l'heure de début et de fin du créneaux. Ce module devra aussi pouvoir avertir l'administrateur dans les cas suivant : l'heure de début est supérieur à l'heure de fin ou le créneaux horaire chevauche un autre créneaux.

L'administrateur pourras aussi à partir de ce module, supprimer les créneaux horaires qu'il désire enlever aux étudiants.



Le diagramme des spécification technique nous impose une seule chose qui est que les données soit stocker en base de données



A terme, ce module fonctionnera de cette façon : Dans un premier temps l'administrateur va se connecter à l'application, une fois cela fait une connexion SSH s'effectuera avec la raspberry, puis on se connectera à la base de données situé sur la raspberry afin de récupérer les créneaux horaires déjà enregistrer dans la table "creneau\_horaire", une fois cela fait l'administrateur pourras sélectionner un créneau horaire en choisissant la section ainsi que le jour et l'heure de début et de fin afin de l'ajouter dans la base de données. L'administrateur pourras si il le souhaite, supprimer un créneau horaire depuis le module logiciel afin de le supprimer au sein de la base de données, comme le montre ce diagramme de séquence

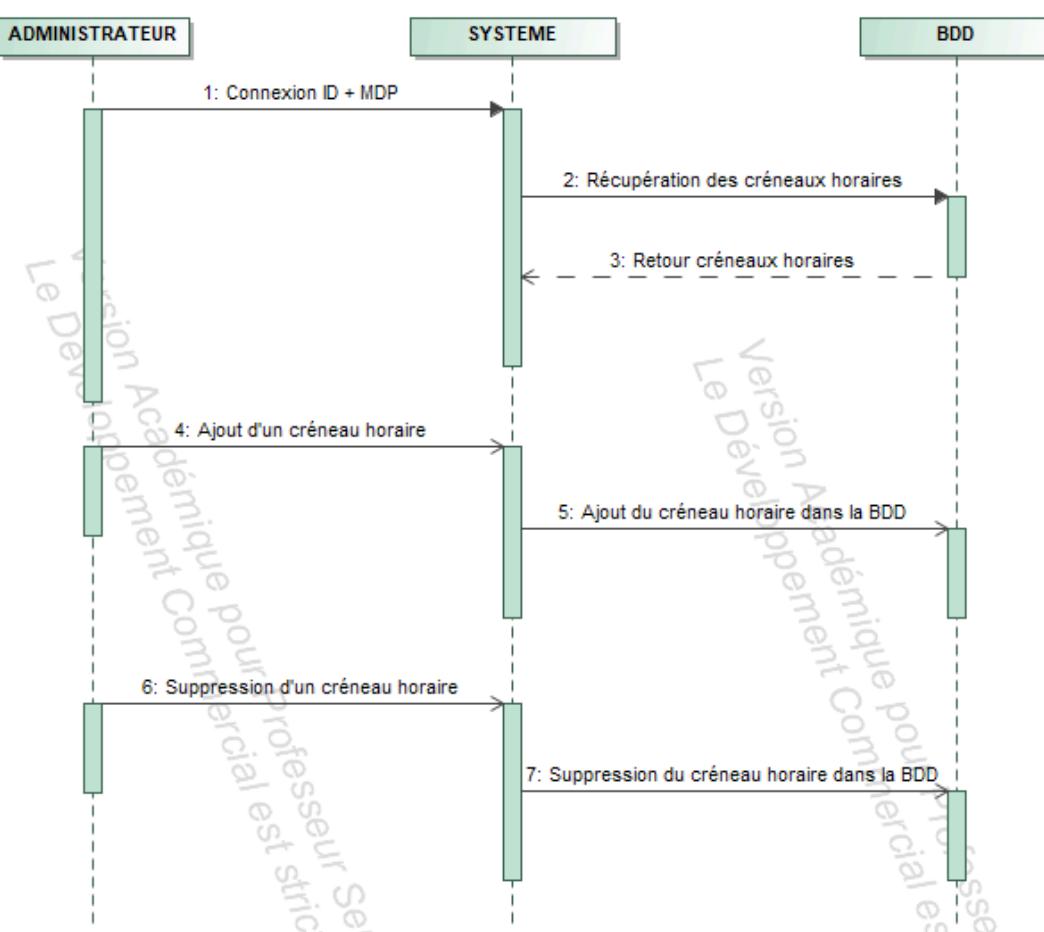


Table dans laquelle nous venons enregistrer les créneaux horaires :

creneau_horaire	
ID_horaire	INT(11)
Jour	ENUM(...)
Heure_debut	TIME
Heure_fin	TIME
ID_ordinateur	INT
Indexes	

Pour réaliser ce module, j'ai une nouvelle fois réalisé un code en python qui permet à l'administrateur d'ajouter à la base de données un nouveau créneau horaire pour la section, le jour, l'heure de début et de fin qu'il souhaite. Tout en gardant la possibilité de supprimer un créneau de la base de données s'il le souhaite. Ce module devra prévenir l'administrateur en cas d'incohérence des données entré, comme une heure de début supérieur à l'heure de fin ou lorsque qu'un créneau chevauche un créneau déjà enregistré

Une connexion en SSH avec la raspberry est encore une fois nécessaire afin de récupérer les créneaux horaire enregistrer dans la table “creneau\_horaire” à l'aide de cette partie de code

```
try:
    cursor = conn.cursor()
    query = "SELECT ID_horaire, ID_section, Jour, Heure_debut, Heure_fin FROM creneau_horaire"
    cursor.execute(query)
    rows = cursor.fetchall()
```

L'étape suivante est d'enregistrer le créneau horaire en envoyant les sélection faite par l'administrateur directement dans la table “creneau\_horaire” en vérifiant au préalable s'il n'y a pas de chevauchement, et si l'heure de début est bien inférieur à l'heure de fin avec cette partie de code

```
def enregistrer_creneau(section, jour, heure_debut, heure_fin):
    conn = connecter_raspberry()
    if conn:
        try:
            cursor = conn.cursor()

            # Vérifier chevauchements inter-sections
            requete_verif = """
                SELECT * FROM creneau_horaire
                WHERE Jour = %s
                AND (
                    (Heure_debut < %s AND Heure_fin > %s)
                    OR (Heure_debut >= %s AND Heure_debut < %s)
                    OR (Heure_fin > %s AND Heure_fin <= %s)
            """
            cursor.execute(requete_verif, (
                jour.lower(),
                heure_fin, heure_debut,
                heure_debut, heure_fin,
                heure_debut, heure_fin
            ))
            conflits = cursor.fetchall()
            if conflits:
                messagebox.showerror("Chevauchement", "Un créneau horaire existe déjà à ce moment-là, dans l'une des sections.")
                return

            requete = """
                INSERT INTO creneau_horaire (ID_section, Jour, Heure_debut, Heure_fin)
                VALUES (%s, %s, %s, %s)
            """
            id_section = 1 if section == "ITS-CIEL" else 2
            valeurs = (id_section, jour.lower(), heure_debut, heure_fin)
            cursor.execute(requete, valeurs)
            conn.commit()
            messagebox.showinfo("Succès", "Le créneau horaire a été enregistré.")
        except Error as e:
            messagebox.showerror("Erreur", f"Erreur lors de l'enregistrement:\n{e}")
        finally:
            cursor.close()
            conn.close()
```

La dernière étape importante de ce code est de permettre la suppression d'un créneau horaire sélectionné par l'administrateur à l'aide de ce code qui supprime la sélection réalisé par l'administrateur en faisant appel à la fonction “supprimer\_creneaux” qui elle va se rendre sur la raspberry afin de supprimer le créneau en ligne de commande

```
def supprimer_selection():
    selected = treeview_c.selection()
    if not selected:
        messagebox.showwarning("Avertissement", "Veuillez sélectionner un créneau à supprimer.")
        return
    ids = [treeview_c.item(sel)["values"][0] for sel in selected]
    supprimer_creneaux(ids)
    refresh_treeview()

def supprimer_creneaux(ids):
    conn = connecter_raspberry()
    if conn:
        try:
            cursor = conn.cursor()
            query = "DELETE FROM creneau_horaire WHERE ID_horaire = %s"
            for id_ in ids:
                cursor.execute(query, (id_,))
            conn.commit()
            messagebox.showinfo("Succès", "Le(s) créneau(x) sélectionné(s) ont été supprimé(s).")
        except Error as e:
            messagebox.showerror("Erreur", f"Erreur lors de la suppression:\n{e}")
        finally:
            cursor.close()
            conn.close()
```

Dans un premier temps j'ai réalisé les tests en ajoutant un créneau horaire à la base de données, et comme nous pouvons le voir celui ci a bien été ajouté

The screenshot shows a user interface for creating a new time slot. On the left, there's a form with fields for 'Section' (set to '2TS-CIEL'), 'Jour' (set to 'Dimanche'), 'Heure de début' (set to '11:00'), and 'Heure de fin' (set to '16:00'). A 'Valider' button is at the bottom. To the right is a terminal window showing the MySQL command: 'select \* from creneau\_horaire;' followed by its output:

```
MariaDB [VirtualPilot]> select * from creneau_horaire;
+-----+-----+-----+-----+
| ID_horaire | ID_section | Jour      | Heure_debut | Heure_fin   |
+-----+-----+-----+-----+
|      1 |      1 | lundi    | 18:00:00  | 23:00:00  |
|      2 |      1 | mardi    | 12:00:00  | 17:00:00  |
|      4 |      1 | vendredi | 13:00:00  | 18:00:00  |
|     28 |      1 | mardi    | 12:00:00  | 18:00:00  |
|     29 |      2 | dimanche | 11:00:00  | 16:00:00  |
+-----+-----+-----+-----+
```

Below the terminal is a success message dialog: 'Succès' with the text 'Le créneau horaire a été enregistré.' and an 'OK' button.

Pour finir j'ai vérifier que la suppression se déroule bien et que cela supprime bien le créneau dans la BDD . Comme nous pouvons le voir, cela fonctionne bien

The screenshot shows a table of existing time slots and a confirmation dialog. The table has columns: ID, Section, Jour, Heure Début, and Heure Fin. One row is selected: '29 2TS-CIEL Dimanche 11:00:00 16:00:00'. Below the table is a success message dialog: 'Succès' with the text 'Le(s) créneau(s) sélectionné(s) ont été supprimé(s).' and an 'OK' button. To the right is a terminal window showing the MySQL command: 'select \* from creneau\_horaire;' followed by its output:

```
MariaDB [VirtualPilot]> select * from creneau_horaire;
+-----+-----+-----+-----+
| ID_horaire | ID_section | Jour      | Heure_debut | Heure_fin   |
+-----+-----+-----+-----+
|      1 |      1 | lundi    | 18:00:00  | 23:00:00  |
|      2 |      1 | mardi    | 12:00:00  | 17:00:00  |
|      4 |      1 | vendredi | 13:00:00  | 18:00:00  |
|     28 |      1 | mardi    | 12:00:00  | 18:00:00  |
+-----+-----+-----+-----+
```

J'ai ensuite vérifié que les messages d'erreur s'affiche bien en cas de créneau déjà existant ou en cas d'heure de début supérieur à l'heure de fin, cela est bien fonctionnel

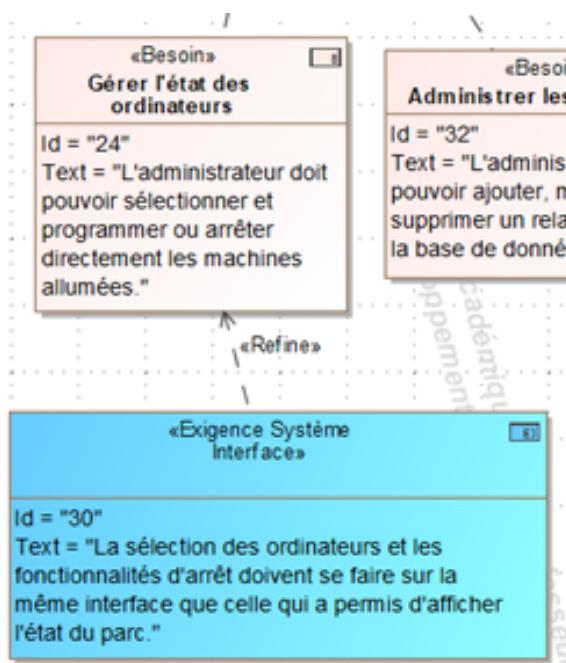
The screenshot shows two error dialogs. The left one is titled 'Erreur' and says 'L'heure de début doit être strictement inférieure à l'heure de fin.' with an 'OK' button. The right one is titled 'Chevauchement' and says 'Un créneau horaire existe déjà à ce moment-là, dans l'une des sections.' with an 'OK' button. Between the dialogs are two small windows showing invalid input examples: one with '15:00' as start and '11:00' as end, and another with '18:00' as start and '23:00' as end.

# MODULE LOGICIEL : GERER L'ÉTAT DES ORDINATEURS

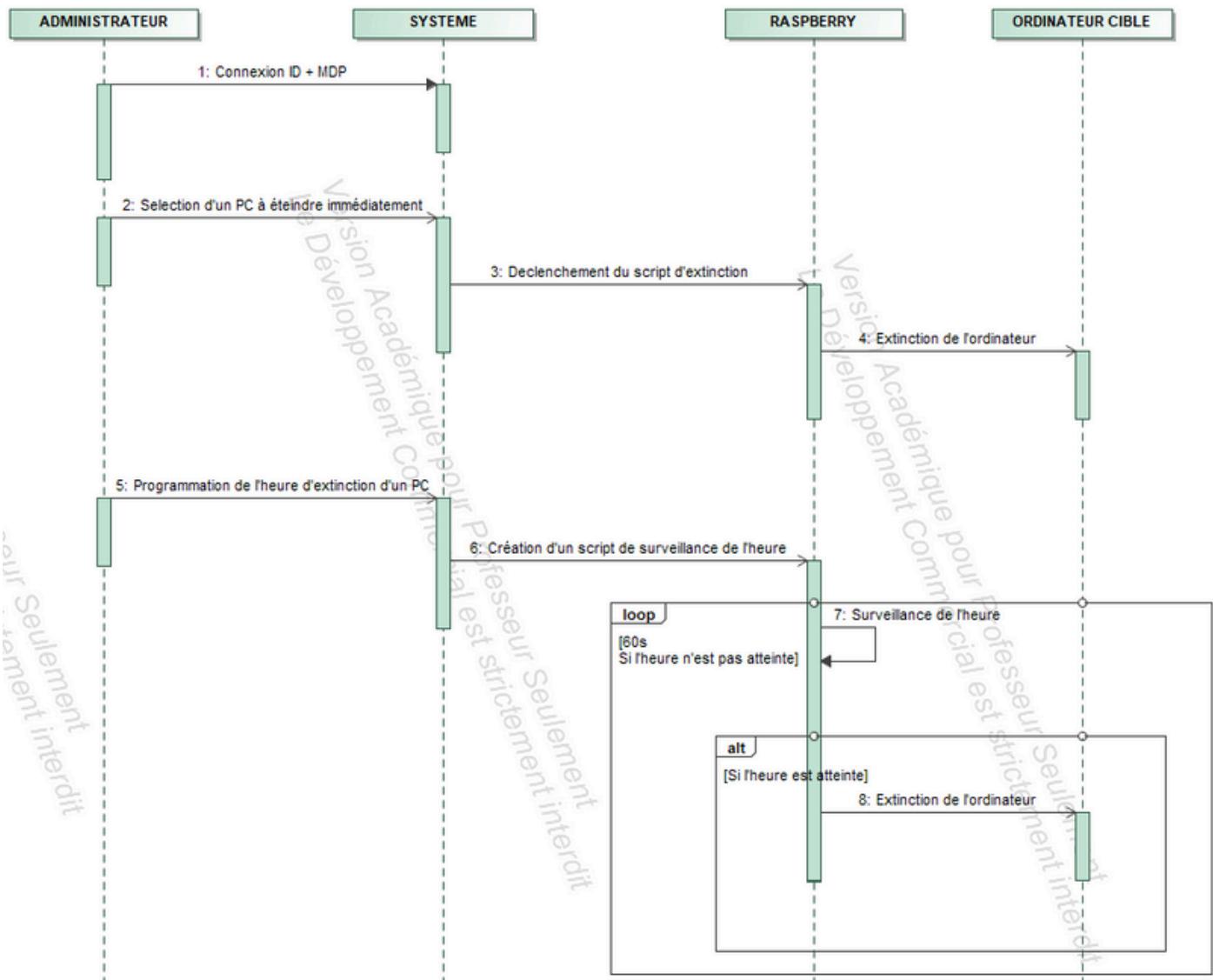
Le but de ce module logiciel est de s'appuyer sur le module logiciel "Afficher l'état du parc" de l'étudiant 2 afin de permettre à l'administrateur à partir de ce module, de pouvoir sélectionner un ordinateur afin de l'éteindre ou de programmer son extinction pour un jour et une heure choisie



Le diagramme des spécification technique nous impose une seule chose qui est que la sélection des ordinateurs ainsi que les fonctionnalités d'arrêt se fasse à partir du module logiciel qui permet d'afficher l'état du parc



A terme, ce module devrait fonctionner de cette façon : Dans un premier temps l'administrateur va se connecter à l'application, une fois cela fait une connexion SSH s'effectuera avec la raspberry, puis on se connectera à la base de données situé sur la raspberry, ensuite l'administrateur pourra sélectionner un des ordinateur situé dans le module logiciel "afficher l'état du parc" afin de l'éteindre à partir d'un script situé sur la raspberry, ou pourra choisir de programmer l'extinction d'un ordinateur à un jour et une heure choisi ce qui lancera le script d'extinction situé sur la raspberry à l'heure choisi par l'administrateur, comme le montre ce diagramme de séquence

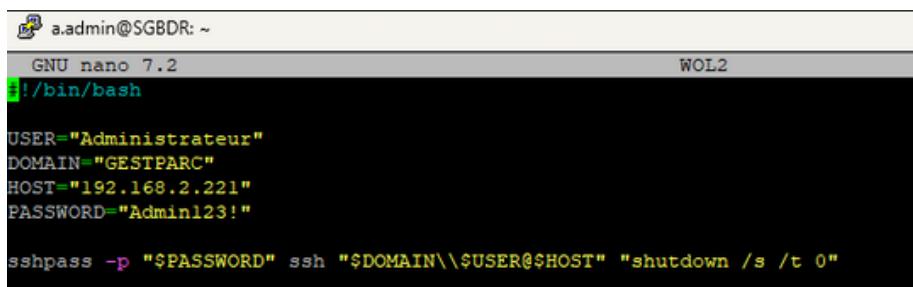


Par manque de temps, je n'ai pas eu le temps de finaliser ce module logiciel mais j'ai tout de même réussi à réaliser quelques étapes préliminaire du module n'étant pas viable pour une version finale comme nous allons le voir.

Mon collègue n'ayant pas terminé son module "Afficher l'état du parc", j'ai donc dans un premier temps essayé de le simulé afin de pouvoir tout de même essayer de développer mon propre module.

Dans le but de réaliser les premiers test et d'éteindre l'un des ordinateurs sélectionné par l'administrateur, j'ai utilisé ce script provisoire.

Ce script nommé "WOL2" est dit provisoire puisque le script final lui ne devra pas comporté le nom d'utilisateur, le mot de passe ainsi que l'adresse IP de l'ordinateur à éteindre, puisque l'administrateur pourras choisir n'importe lequel des ordinateurs du parc



```
a.admin@SGBDR: ~
GNU nano 7.2
#!/bin/bash

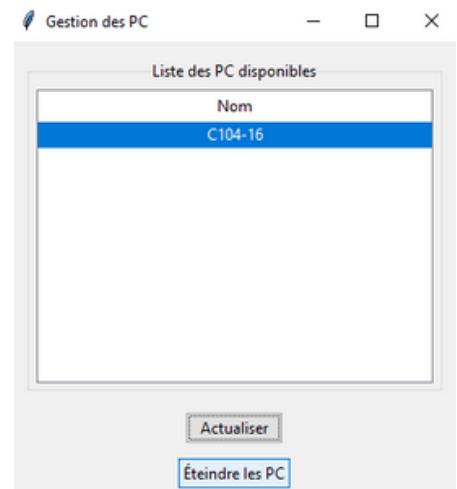
USER="Administrateur"
DOMAIN="GESTPARC"
HOST="192.168.2.221"
PASSWORD="Admin123!"

sshpass -p "$PASSWORD" ssh "$DOMAIN\$USER@$HOST" "shutdown /s /t 0"
```

Dans un premier temps j'ai réaliser un code qui permet de sélectionner un des ordinateurs du parc puis qui déclenche le script "WOL2" lorsque l'on appuie sur le bouton "éteindre les PC", Ce code éteint bien le pc de notre parc informatique

Voici la partie du code qui permet de lancer le script "WOL2" qui permet l'extinction de l'ordinateur en se connectant à la raspberry en SSH :

```
try:
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh.connect(
        hostname="192.168.2.5",
        username="a.admin",
        password="admin.CIEL!")
)
stdin, stdout, stderr = ssh.exec_command("/home/a.admin/WOL2")
```



J'ai ensuite réalisé un code qui va permettre de programmer le jour et l'heure d'extinction d'un ordinateur du parc en faisant en sorte que lorsque l'administrateur programme l'extinction d'un ordinateur, un script qui permet de surveiller l'heure toute les minutes afin de déclencher le script "WOL2" une fois l'heure programmé atteinte se crée automatiquement sur la raspberry et se supprime une fois l'heure passé

## Programmation d'extinction PC

Jour de la semaine:	<input type="text" value="Mercredi"/>
Heure:	<input type="text" value="17"/>
Minute:	<input type="text" value="42"/>
<input type="button" value="Programmer l'extinction"/>	

Extinction programmée avec succès le Mercredi à 17:42

Partie du script créée par le code qui permet de surveiller le jour et l'heure et de lancer le script "WOL2" si l'heure programmé est atteinte :

```
# Boucle principale qui vérifie l'heure et le jour
while True:
    # Obtenir la date et l'heure actuelles
    maintenant = datetime.datetime.now()
    jour_actuel = jours[maintenant.weekday()] # Obtient le jour de la semaine actuel

    # Vérifier si c'est le jour et l'heure d'extinction
    if jour_actuel == jour and maintenant.hour == heure and maintenant.minute == minute:
        print(f"C'est {jour} {heure}:02d", exécution du script d'extinction...")
```

Ce module n'est donc pas finalisé. Afin de le finalisé, il faudrait dans un premier temps créer un script sur la raspberry qui permet de récupérer les informations du PC sélectionné par l'administrateur afin de remplacer le script "WOL2". La seconde étape serai de rassembler la programmation ainsi que l'extinction dans le même code python. Puis la dernière étape serai d'associer le code qui rassemble la programmation ainsi que l'extinction d'un PC, avec le module logiciel "Afficher l'état du parc" ce qui permettra à l'administrateur de sélectionner un ordinateur allumer au sein du parc afin de l'éteindre directement, ou alors de programmer son extinction en cas de besoin.

## Mes tâches assignées

Comme nous avons pu le constater dans le tableau de la répartition des tâches, chaque étudiant avait des missions différentes dans chaque partie, que ce soit dans le développement du logiciel ou dans l'architecture matérielle. Après s'être attribué les différents rôles, nous avons du classer les tâches en fonction de leur importance, faisant ainsi passer la plus importante en premier :

### Architecture Matérielle



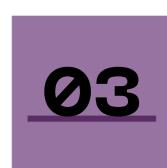
#### Broker MQTT

Installation et configuration du broker MQTT pour gérer les différents relais. Simple et efficace, il permet un usage complet et un coût nul pour une utilisation à distance



#### Point d'accès WiFi

Installation et configuration du pont d'accès WiFi pour permettre la connexion des différents relais sur l'infrastructure réseau.



#### relais WiFi (Sonoff Basic R2)

Mise à jour du firmware et configuration pour une utilisation optimale de l'appareil. Le firmware à installer permet de faciliter l'usage qu'il en sera fait.

### Développement Logiciel



#### Base De Données

Conception de la base de données servant à lier ordinateurs et relais, utilisateurs et machines.



#### Allumage de l'ordinateur

Création du module logiciel permettant d'allumer le couple relais/machine après authentification

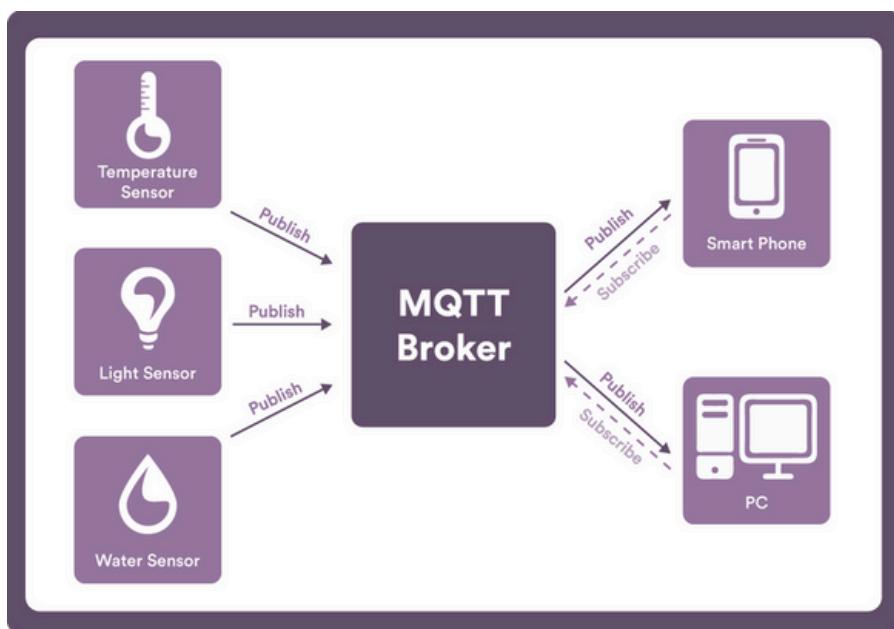


#### Extinction de l'ordinateur

Création du module logiciel permettant d'éteindre le couple relais/machine après utilisation.

# 01 Broker MQTT

MQTT, qui signifie Message Queuing Telemetry Transport, est un protocole de messagerie léger conçu pour faciliter les communications entre appareils, en particulier dans les environnements où la connexion réseau est faible ou instable. Ce protocole fonctionne selon un modèle dit "publish/subscribe", ce qui signifie qu'un appareil peut publier un message sur un sujet donné, et un ou plusieurs autres appareils peuvent s'abonner à ce sujet pour recevoir automatiquement ces messages.



Le broker MQTT est le cœur du système de communication. C'est un serveur qui reçoit tous les messages envoyés par les appareils connectés (appelés clients) et les redistribue à ceux qui se sont abonnés aux sujets correspondants. Il joue le rôle d'intermédiaire : les appareils ne communiquent pas directement entre eux, mais uniquement par l'intermédiaire du broker. Cela permet de gérer facilement un grand nombre de connexions, de simplifier les échanges, et d'assurer que chaque message arrive au bon destinataire.

Ce système est particulièrement bien adapté aux projets liés à la domotique ou à l'Internet des objets (ce qu'on appelle plus souvent l'IoT pour Internet of Things), car il permet une communication simple, rapide et efficace entre les différents composants. En plus, il peut être sécurisé à l'aide d'un système d'authentification, comme nous allons le voir ci-dessous. C'est pour toutes ces raisons que nous avons choisi MQTT pour notre projet, plutôt qu'un protocole plus lourd ou plus complexe à mettre en œuvre.

L'installation du Broker MQTT se fait sur la carte Raspberry Pi 4, une carte fiable et pas du tout encombrante. En ce qui concerne notre projet, on utilise Mosquitto comme logiciel pour le broker mqtt.

Pour l'installer, il suffit d'entrer la commande suivante, appuyer sur 'y' et valider avec la touche entrer :

```
a.admin@SGBDR:~ $ sudo apt-get install mosquitto
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdlt2 libmosquittol
The following NEW packages will be installed:
  libdlt2 libmosquittol mosquitto
0 upgraded, 3 newly installed, 0 to remove and 142 not upgraded.
Need to get 524 kB of archives.
After this operation, 1,573 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Pour sécuriser la connexion au broker, il est nécessaire d'activer un mot de passe et d'empêcher toute personne anonyme d'y accéder avec cette commande :

```
a.admin@SGBDR:~ $ sudo mosquitto_passwd -c /etc/mosquitto/passwd adminMqtt
Password:
Reenter password:
a.admin@SGBDR:~ $
```

Avec la commande ci-dessous, il est permis à la carte Raspberry Pi 4 de lancer automatique notre broker MQTT au démarrage de l'appareil :

```
a.admin@SGBDR:~ $ sudo systemctl enable mosquitto.service
Synchronizing state of mosquitto.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mosquitto
```

Ensuite, il faut modifier le fichier mosquitto.conf du logiciel pour activer l'authentification avec un mot de passe et un identifiant, mais aussi le port 1883 qui sert à écouter les requêtes mqtt. On y ajoute les 3 dernières lignes :

```
GNU nano 7.2          /etc/mosquitto/mosquitto.conf
# Place your local configuration in /etc/mosquitto/conf.d/
#
# A full description of the configuration file is at
# /usr/share/doc/mosquitto/examples/mosquitto.conf.example

pid_file /run/mosquitto/mosquitto.pid

persistence true
persistence_location /var/lib/mosquitto/

log_dest file /var/log/mosquitto/mosquitto.log

include_dir /etc/mosquitto/conf.d

listener 1883
allow_anonymous false
password_file /etc/mosquitto/passwd
```

Le protocole MQTT est un choix idéal pour la gestion à distance des relais en raison de sa légèreté et de son efficacité.

Voici comment il fonctionne :

- Communication des messages : Le protocole MQTT permet aux appareils de communiquer en envoyant des messages au broker MQTT. Le broker joue le rôle d'intermédiaire en relayant ces messages aux appareils abonnés.
- Gestion des abonnements : Chaque relais connecté au réseau s'abonne à des sujets spécifiques gérés par le broker MQTT. Lorsqu'un appareil envoie un message à un sujet auquel un relais est abonné, le relais reçoit et exécute l'instruction correspondante (par exemple, allumer ou éteindre un appareil).
- Pilotage à distance : Grâce à ce système, il est possible de contrôler les relais à distance de manière centralisée. Par exemple, un administrateur peut envoyer une commande via le broker MQTT pour activer un relais situé à plusieurs kilomètres, permettant ainsi de gérer des équipements sans avoir besoin d'une connexion directe à chaque appareil.

Le protocole MQTT offre une solution robuste et flexible pour le contrôle à distance des relais, facilitant ainsi la gestion de plusieurs appareils depuis un point centralisé.

## Choix du Qos (Quality of Service)

Le protocole MQTT définit plusieurs niveaux de QoS pour la transmission des messages :

- QoS 0 (Au plus une fois) : Le message est envoyé sans accusé de réception. Ce niveau est rapide mais ne garantit pas la livraison du message en cas de problème réseau.
- QoS 1 (Au moins une fois) : Le message est garanti d'être délivré au moins une fois. L'expéditeur reçoit un accusé de réception (PUBACK) du destinataire (le broker dans un premier temps, puis le broker vers le client abonné). Si l'accusé n'est pas reçu, le message est renvoyé.
- QoS 2 (Exactement une fois) : Le message est garanti d'être délivré exactement une fois, grâce à un mécanisme d'échange en quatre étapes. C'est le niveau le plus fiable mais aussi le plus consommateur en ressources et en temps.

Dans le cadre de ce projet, les messages MQTT sont principalement utilisés pour envoyer des commandes d'allumage ("ON") et d'extinction ("OFF") aux relais qui contrôlent l'alimentation des ordinateurs du parc. Le choix s'est porté sur le QoS 1 car il représente le meilleur compromis pour ce cas d'usage :

- Fiabilité suffisante : Il assure que les commandes critiques (allumer ou éteindre un PC) sont bien transmises au relais, même en cas de brèves instabilités du réseau. La réception d'un accusé de réception confirme la prise en charge du message par le broker.
- Gestion des duplicitas acceptable : Bien que le QoS 1 puisse entraîner la réception de messages dupliqués par le relais (si l'accusé de réception du premier envoi se perd mais que le message a été reçu), les commandes "ON" et "OFF" sont idempotentes. Recevoir plusieurs fois la même commande d'allumage sur un relais déjà allumé, ou d'extinction sur un relais déjà éteint, n'a pas d'effet indésirable sur l'état final du relais.
- Performance : Il est moins gourmand en bande passante et en temps de traitement que le QoS 2.

Le QoS 0 a été écarté en raison du risque de perte de commandes, ce qui pourrait par exemple laisser un ordinateur allumé involontairement. Le QoS 2, bien que plus robuste contre les duplicitas, a été jugé comme introduisant une complexité et une surcharge de communication non nécessaires pour la nature des commandes envoyées aux relais.

Ainsi, le QoS 1 offre l'assurance que les commandes de pilotage des relais sont transmises de manière fiable, ce qui est essentiel pour le bon fonctionnement de la gestion énergétique et de la disponibilité des postes informatiques, tout en maintenant une communication efficace.

## 02 Point d'accès WiFi

Le point d'accès WiFi est un composant fondamental de l'infrastructure de notre projet "Gestion d'un parc informatique", jouant un rôle indispensable pour le contrôle à distance des ordinateurs.

Son caractère essentiel repose sur sa capacité à :

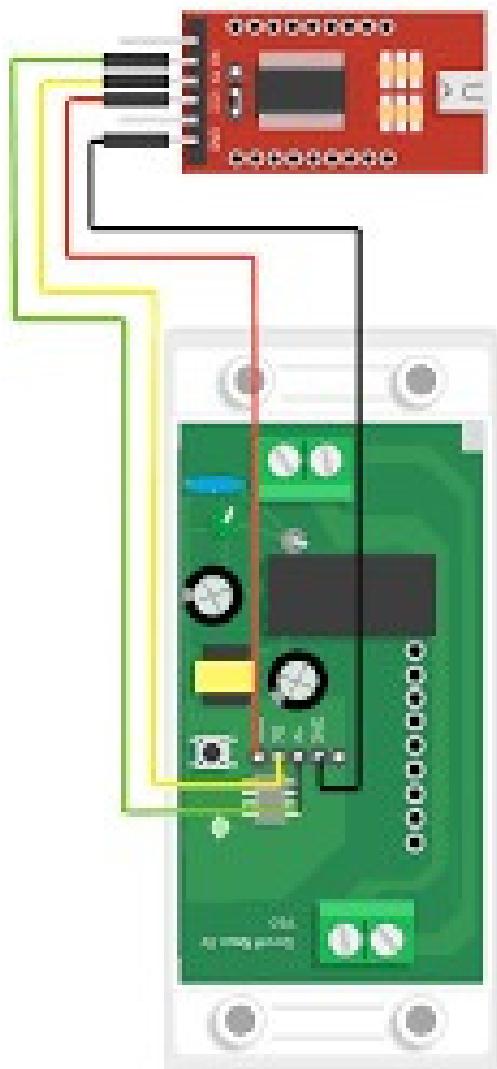
- Fournir la Connectivité Sans Fil : Il crée le réseau sans fil nécessaire pour que les relais WiFi (Sonoff), qui commandent l'alimentation des PC, puissent se connecter à l'infrastructure réseau du projet. Sans cette connectivité, ces relais ne pourraient pas communiquer.
- Permettre le Contrôle à Distance : En tant que pont entre les relais et le réseau local, le point d'accès est crucial pour acheminer les commandes (via le broker MQTT) vers ces relais. C'est ce qui permet aux utilisateurs de contrôler l'allumage et l'extinction des PC à distance.
- Assurer l'Intégration Réseau : Sa configuration spécifique (adressage IP, passerelle, DNS) l'intègre de manière cohérente au réseau du projet (192.168.2.0/24), garantissant que les communications des relais et autres dispositifs sans fil sont correctement gérées au sein de l'infrastructure.

En résumé, le point d'accès WiFi est indispensable car il établit la liaison de communication pour les relais de commande. Sans lui, la fonctionnalité principale de gestion à distance de l'alimentation des postes informatiques, qui est un objectif central du projet, ne pourrait être réalisée.



# 03 relais WiFi (Sonoff Basic R2)

Dans le cadre du projet, les relais WiFi sont utilisés pour permettre l'alimentation en courant des différents ordinateurs du parc à distance. Ils jouent un rôle clé dans le coût énergétique du parc informatique. En effet, en contrôlant l'alimentation en courant des nombreux ordinateurs qui constituent ou constitueront le parc, on débloque une somme économisée qui peut s'avérer être conséquente pour l'établissement.



Flasher un relais avec Tasmota consiste à remplacer son logiciel d'origine (le firmware) par un firmware libre et personnalisable appelé Tasmota. Ce nouveau logiciel permet de contrôler le relais localement, sans dépendre d'un service cloud, et de le faire communiquer avec des systèmes comme MQTT.

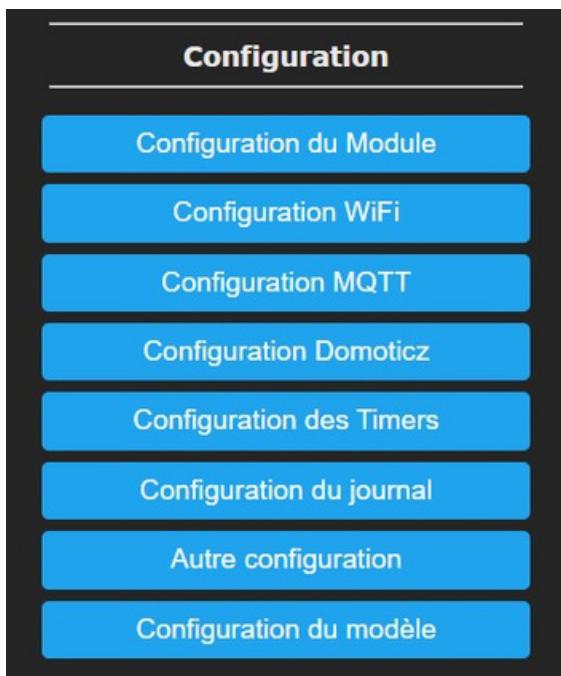
Pour effectuer ce flashage, il faut connecter physiquement le relais à un ordinateur à l'aide d'un adaptateur USB-série, souvent basé sur la puce FT232. Cet adaptateur permet de relier les broches du relais (TX, RX, GND, et 3.3V) aux ports USB du PC afin de transférer le nouveau firmware. Le logiciel le plus couramment utilisé pour envoyer Tasmota dans le relais est Tasmotizer ou ESPHome-Flasher.

Avant le flashage, on doit mettre le relais en mode "programmation" (appelé aussi flash mode) en maintenant un bouton ou en reliant certaines broches selon le modèle, puis on branche l'adaptateur au PC. Une fois le firmware installé, le relais redémarre avec Tasmota, prêt à être configuré.



Comme évoqué ci-dessus, nombreuses possibilités de configuration témoignent de l'efficacité de ce logiciel.

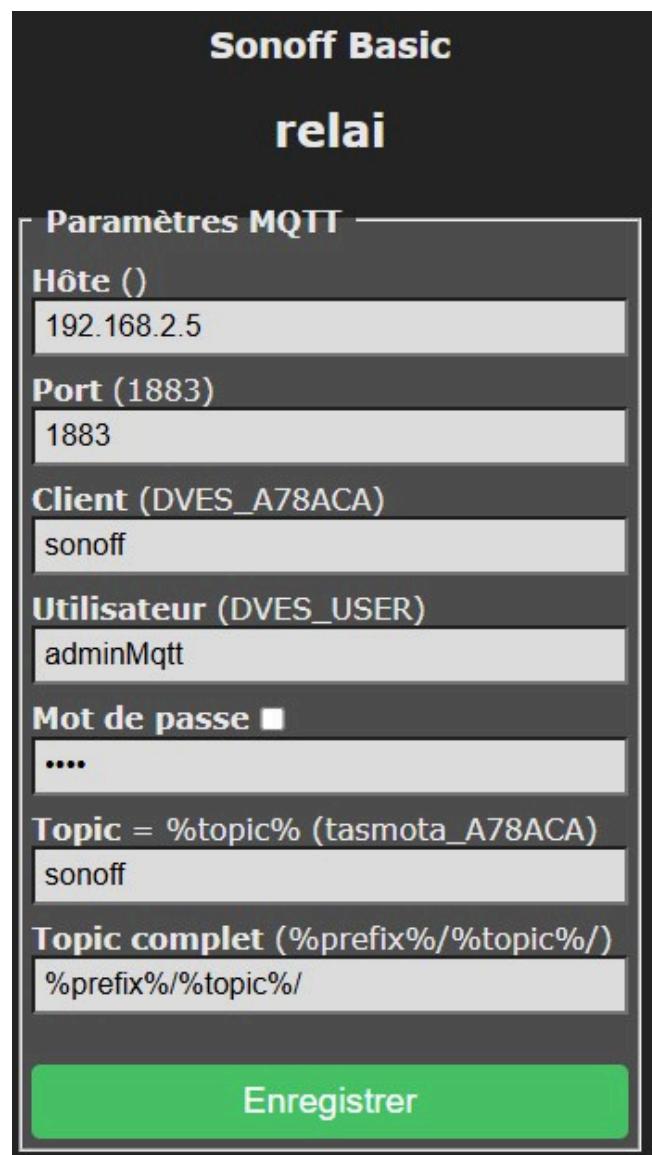
en ce qui concerne la liaison mqtt, il est nécessaire de configurer l'appareil en cliquant sur le bouton "Configuration MQTT".



La configuration du relais WiFi se fait ensuite sur l'interface WEB du serveur embarqué. pour s'y rendre, il suffit d'entrer l'adresse IP du relais et la page de configuration s'ouvre.

Cette interface permet également de contrôler le relais via le bouton ON/OFF situé en première position.

Le choix de flasher le microgiciel avec tasmota relève de l'efficacité. En effet, ce firmware admet tant de possibilité liées à la domotique, mais principalement, au protocole mqtt.



Une fois le relais Wi-Fi (Sonoff Basic) flashé avec le firmware Tasmota, une interface web devient accessible pour configurer le module. Voici les étapes principales mises en œuvre dans le projet :

### Connexion au WiFi

Lors du premier démarrage du relais après le flashage, Tasmota crée un point d'accès Wi-Fi temporaire. Il faut s'y connecter avec un smartphone ou un ordinateur, puis accéder à l'interface via l'adresse 192.168.2.16. On renseigne ensuite les identifiants du réseau Wi-Fi local dans les paramètres, afin que le relais puisse s'y connecter automatiquement à l'avenir.

### Accès à l'interface Web

Une fois connecté au réseau Wi-Fi, le relais obtient une adresse IP locale via DHCP. Cette adresse est utilisée pour accéder à l'interface web de Tasmota depuis un navigateur. L'interface permet d'allumer ou éteindre le relais, et d'accéder aux menus de configuration.

### Configuration MQTT

Pour permettre la communication entre le relais et le système central (Raspberry Pi avec Mosquitto), le protocole MQTT doit être activé et configuré dans l'interface Tasmota :

- Aller dans le menu Configuration, puis Configuration MQTT
- Renseigner :
  - Host : adresse IP du broker MQTT (dans ce projet, 192.168.2.5)
  - Port : généralement 1883 (par défaut)
  - User : identifiant du broker, ici adminMqtt
  - Password : mot de passe du broker, ici mosquitto123!
  - Topic : nom du relais (par exemple sonoff)
  -
- Enregistrer les paramètres et redémarrer le module si nécessaire

Une fois configuré, le relais peut recevoir des messages MQTT sur son topic pour contrôler son état (ON/OFF), et également publier son statut ou d'autres informations.

# 04 Base De Données

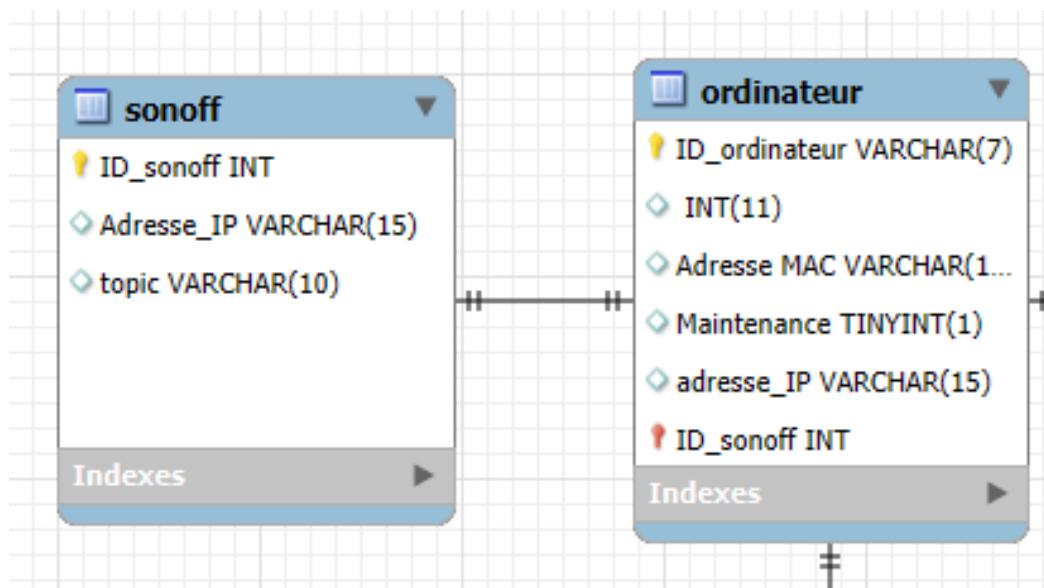
Pour assurer le suivi, la traçabilité et la gestion des équipements utilisés dans le projet, une base de données relationnelle a été conçue et implémentée à l'aide de MariaDB, un système de gestion de base de données open source, performant et compatible avec MySQL. La base est hébergée localement sur la Raspberry Pi servant de serveur. La base de données créée se nomme VirtualPilot. Elle permet de relier des informations sur les étudiants, les ordinateurs, les relais Sonoff, les créneaux horaires d'utilisation, et les sections pédagogiques. Elle a été pensée de manière à être évolutive et facilement exploitable à l'aide de requêtes SQL simples.

## Structure relationnelle

La base de données repose sur une structure relationnelle cohérente, avec plusieurs tables reliées entre elles par des clés étrangères, permettant de maintenir l'intégrité des données tout en assurant la souplesse des mises à jour.

Les tables les plus importantes dans les modules d'allumage et d'extinction des relais et des ordinateurs sont les tables "sonoff" qui regroupe les données de chaque relais, et "ordinateur" qui regroupe les données de chaque ordinateur et relie chaque relais à celui-ci.

Ces deux tables vont permettre au logiciel de récupérer l'adresse MAC des ordinateurs à allumer ou à éteindre, et le relais relié ou plus précisément le topic mqtt du relais en question, afin d'alimenter l'ordinateur avant de procéder à l'allumage. Ce sont ces mêmes données enregistrées dans ces tables qui permettront d'éteindre par la suite, les appareils voulus.



Toutes les relations sont gérées avec le moteur InnoDB, qui prend en charge les contraintes d'intégrité référentielle, notamment les comportements ON DELETE et ON UPDATE spécifiés sur les clés étrangères.

Lorsqu'une clé étrangère est utilisée, on peut définir ce qu'il se passe lorsqu'un enregistrement lié est modifié ou supprimé :

- Le mot-clé ON UPDATE CASCADE signifie que si la valeur de la clé primaire dans la table de référence est modifiée, cette modification est automatiquement répercutée dans toutes les tables qui la référencent. Le mot-clé ON DELETE SET
- NULL indique que si une entrée est supprimée dans la table de référence (par exemple une section ou un ordinateur), alors la valeur correspondante dans la table dépendante (comme étudiant) est mise à NULL, c'est-à-dire qu'on "supprime le lien" sans supprimer l'enregistrement lui-même.

Ce mécanisme est essentiel pour éviter les incohérences tout en conservant les données utiles. Par exemple, si une section est supprimée, les étudiants liés à cette section ne sont pas supprimés de la base : leur champ ID\_section devient simplement vide (NULL), ce qui indique qu'ils ne sont plus rattachés à une section.

Des index ont été créés sur certaines colonnes de jointure afin d'optimiser les performances des requêtes SQL entre tables, notamment lors de recherches ou d'associations de données fréquentes.

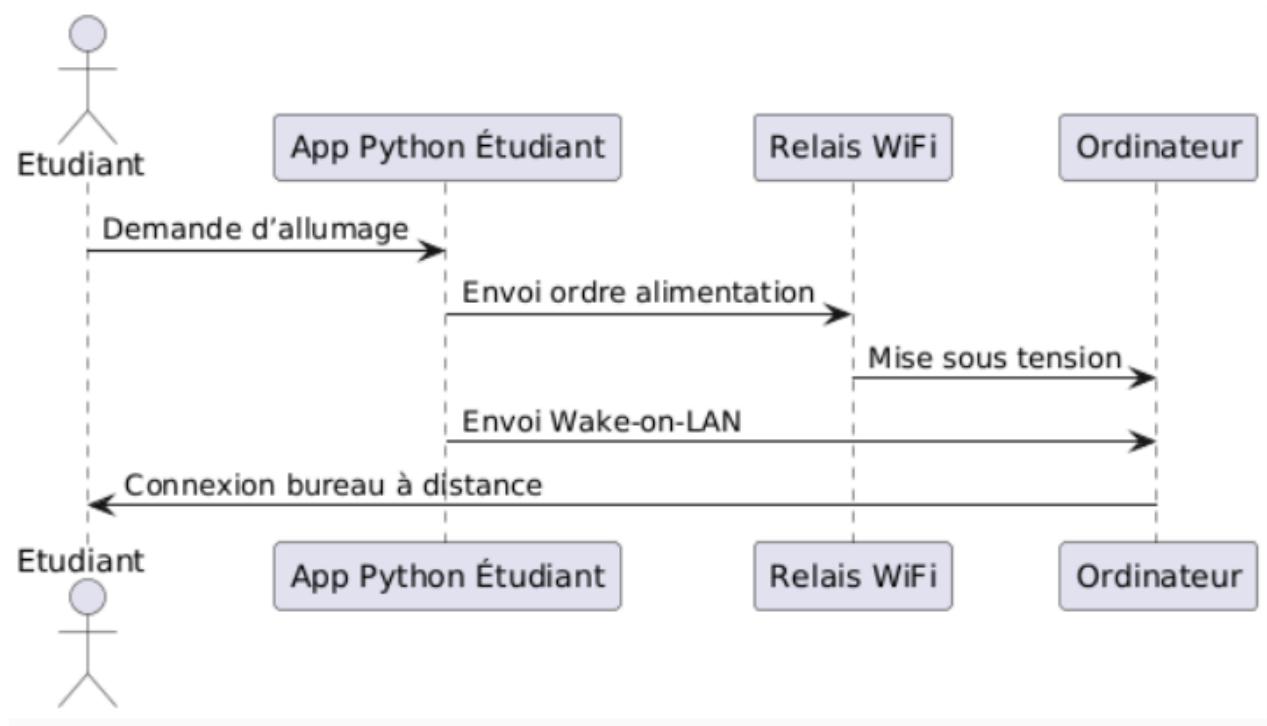
La base de données ne sert pas uniquement à stocker des informations, elle permet aussi de réaliser concrètement des opérations automatisées dans le système. Dans notre projet, chaque tâche est reliée à des champs précis de la base de données, facilitant ainsi l'intégration et la coordination entre les modules.

# 05 Allumage de l'ordinateur

Le module « Allumer l'ordinateur » permet à un étudiant d'allumer à distance l'ordinateur qui lui est attribué. Une fois authentifié dans l'application, l'étudiant peut consulter les plages horaires durant lesquelles il est autorisé à se connecter. S'il est dans une plage autorisée, l'application vérifie que l'ordinateur concerné n'est pas déjà utilisé, puis lance la procédure d'allumage.

L'allumage se déroule en deux temps. Dans un premier temps, une commande est envoyée via le protocole MQTT à un relais WiFi (de type Sonoff Basic R2) afin de fournir l'alimentation électrique à l'ordinateur. Dans un second temps, l'application envoie une commande Wake-on-LAN pour démarrer la machine. Une fois l'ordinateur allumé, l'étudiant peut établir une connexion via le bureau à distance pour ouvrir sa session.

Ce module contribue à l'autonomie des étudiants tout en garantissant que seuls les postes autorisés peuvent être utilisés dans les créneaux définis.



Pour l'allumage du PC, Il est nécessaire d'envoyer un paquet magique Wake On Lan comme constaté précédemment. le procédé utilisé permet au module de :

- o se connecter grâce au protocole SSH sur la raspberry.
- o récupérer l'adresse MAC de l'ordinateur que l'on veut démarrer
- o lancer le script "ON\_PC" enregistré sur la raspberry avec l'argument \$1 correspondant à l'adresse MAC.
- o effectuer un PING à l'adresse IP de la machine pour savoir si celle-ci s'est correctement allumée.

Voici une capture du script qui est lancé par l'application pour allumer les ordinateurs :

```
GNU nano 7.2                                     ON PC
#!/bin/bash

# Vérifie si un argument (adresse MAC) a été fourni
if [ -z "$1" ]; then
    echo "Erreur : Veuillez fournir une adresse MAC en argument."
    echo "Usage : $0 <adresse_mac>"
    exit 1
fi

# Récupère l'adresse MAC depuis l'argument
MAC_ADDRESS="$1"

# Utilise l'outil wakeonlan pour envoyer le paquet magique
wakeonlan "$MAC_ADDRESS"

# Vérifie si la commande s'est bien exécutée
if [ $? -eq 0 ]; then
    echo "Paquet Wake-on-LAN envoyé avec succès à $MAC_ADDRESS"
else
    echo "Échec de l'envoi du paquet Wake-on-LAN"
fi
```

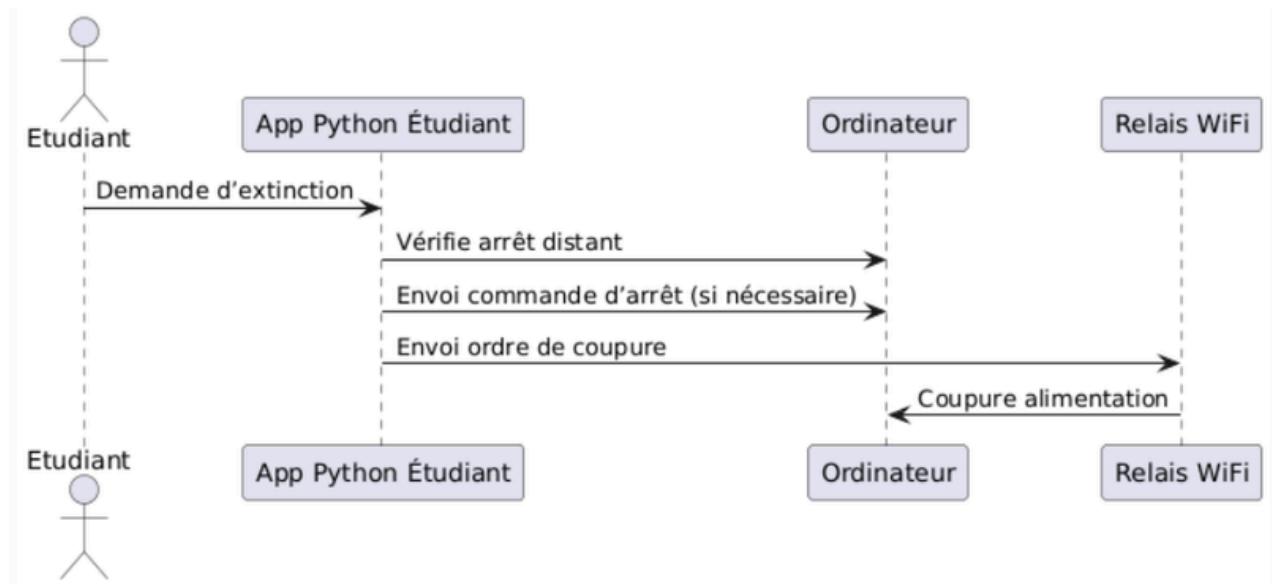
Il permet de récupérer l'adresse MAC de la machine à allumer, et envoi le paquet wake on lan.

# 06 Extinction de l'ordinateur

Le module « Éteindre l'ordinateur » permet à l'étudiant de couper proprement et complètement son poste distant après utilisation. Une fois sa session Windows fermée via le bureau à distance, l'étudiant déclenche l'extinction depuis l'application.

L'application commence par vérifier si l'ordinateur est bien éteint. Si ce n'est pas le cas, elle lui envoie une commande d'arrêt via le réseau. Une fois que l'arrêt est confirmé, une commande MQTT est transmise au relais WiFi pour couper l'alimentation électrique de l'ordinateur.

Ce module permet d'éviter que les ordinateurs restent inutilement sous tension, ce qui représente un gain significatif en matière de consommation énergétique. Il s'inscrit ainsi dans l'un des objectifs principaux du projet : réduire l'impact environnemental du parc informatique tout en assurant sa disponibilité.



Pour l'extinction du PC, Il est nécessaire d'envoyer une commande Wake On Lan inversé stockée dans un script comme constaté précédemment. le procédé utilisé permet au module de :

- o se connecter grâce au protocole SSH sur la raspberry.
- o effectuer un PING à l'adresse IP de la machine pour savoir si celle-ci est allumée.
- o récupérer l'adresse IP de l'ordinateur que l'on veut éteindre
- o lancer le script "OFF\_PC" enregistré sur la raspberry avec l'argument \$1 correspondant à l'adresse IP.
- o effectuer un PING à l'adresse IP de la machine pour savoir si celle-ci s'est correctement éteinte.

Voici une capture du script qui est lancé par l'application pour allumer les ordinateurs :

```
GNU nano 7.2 OFF_PC
#!/bin/bash

# Script : OFF_PC
# Objectif : Retrouve l'IP d'une machine via son adresse MAC et l'éteint via SSH.

# --- Configuration des identifiants ( repris de WOL2_A ) ---
USER_REMOTE="Administrateur"
DOMAIN_REMOTE="GestParc"
PASSWORD_REMOTE="Admin123!" # Attention : Mettre un mot de passe en clair dans un script est un risque de sécurité.

# Vérifier si une adresse MAC a été fournie en argument
if [ -z "$1" ]; then
    echo "Erreur : Veuillez fournir une adresse MAC en argument."
    echo "Usage : ./OFF_PC <adresse_mac>"
    exit 1
fi

TARGET_MAC_ADDRESS="$1"

echo "Script OFF_PC en cours..."
echo "Recherche de l'adresse IP pour la MAC : $TARGET_MAC_ADDRESS..."

# --- 1. Récupération de l'adresse IP à partir de l'adresse MAC (logique de IP_PC) ---
# Il peut être nécessaire d'exécuter ce script avec sudo si 'arp -a' le requiert.
# Ou spécifiez le chemin complet de arp, ex: /usr/sbin/arp
arp_output=$(arp -a)
ip_address=$(echo "$arp_output" | grep -i "$TARGET_MAC_ADDRESS" | awk '{print $2}' | tr -d '()' )

# --- 2. Vérification et extinction ---
if [ -n "$ip_address" ]; then
    echo "Adresse IP trouvée : $ip_address pour la MAC $TARGET_MAC_ADDRESS."
    echo "Tentative d'extinction de la machine à l'adresse IP : $ip_address..."

    # Commande d'extinction (logique de WOL2_A)
    # L'option -o StrictHostKeyChecking=no et -o UserKnownHostsFile=/dev/null
    # est ajoutée pour éviter les demandes de confirmation de clé d'hôte,
    # ce qui peut être utile pour les scripts automatisés.
    # Attention aux implications de sécurité de ces options.
    sshpass -p "$PASSWORD_REMOTE" ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null "$DOMAIN_REMOTE\${USER_REMOTE}@$ip_address" "shutdown /s /t 0"

    # Vérification simple du code de sortie de sshpass
    if [ $? -eq 0 ]; then
        echo "La commande d'extinction a été envoyée avec succès à $ip_address."
        echo "Script OFF_PC terminé."
    else
        echo "Erreur lors de l'envoi de la commande d'extinction à $ip_address."
        echo "Vérifiez la connectivité, les identifiants, ou si le serveur SSH est bien configuré sur la machine cible."
        echo "Assurez-vous également que 'sshpass' est installé."
        echo "Script OFF_PC terminé avec erreur."
        exit 3 # Code de sortie spécifique pour erreur SSH/shutdown
    fi
else
    echo "Aucune adresse IP n'a été trouvée pour l'adresse MAC : $TARGET_MAC_ADDRESS."
    echo "L'ordinateur ne peut pas être éteint."
    echo "Script OFF_PC terminé avec erreur."
    exit 2 # Code de sortie spécifique pour IP non trouvée
fi

exit 0
```

Ce script OFF\_PC utilise une technique différente de celui qui permet d'allumer les ordinateurs.

Pour éteindre un ordinateur, il faut renseigner l'adresse IP de celui-ci dans une ligne de commande permettant de l'éteindre. Or les adresses IP peuvent changer étant donné qu'elles sont attribuées par le serveur DHCP du contrôleur de domaine. Donc la solution qu'apport ce script se sert d'une technique logicielle qui permet de retrouver l'adresse IP en fonction de l'adresse MAC de la machine, qui elle, reste immuable, il s'agit de la table ARP.

Cette technique est également utilisée afin d'effectuer des requêtes "ping" pour connaître l'état des machines en temps réel. Il est utilisé dans le code sous le nom de ETAT\_PC et il renvoie l'état de l'ordinateur en fonction du succès ou de l'échec du ping :

```
GNU nano 7.2                                     ETAT_PC
#!/bin/bash

# Script : ETAT_PC
# Objectif : Retrouve l'IP d'une machine via son adresse MAC et vérifie son statut avec ping.

# Vérifier si une adresse MAC a été fournie en argument
if [ -z "$1" ]; then
    echo "Erreur : Veuillez fournir une adresse MAC en argument."
    echo "Usage : ./ETAT_PC <adresse_mac>"
    exit 2 # Code d'erreur pour mauvaise utilisation
fi

TARGET_MAC_ADDRESS="$1"

echo "Script ETAT_PC en cours..."
echo "Recherche de l'adresse IP pour la MAC : $TARGET_MAC_ADDRESS..."

# --- 1. Récupération de l'adresse IP à partir de l'adresse MAC ---
# Il peut être nécessaire d'exécuter ce script avec sudo si 'arp -a' le requiert.
# Ou spécifiez le chemin complet de arp, ex: /usr/sbin/arp
arp_output=$(arp -a)
ip_address=$(echo "$arp_output" | grep -i "$TARGET_MAC_ADDRESS" | awk '{print $2}' | tr -d '()' )

# --- 2. Vérification du statut par Ping si l'IP est trouvée ---
if [ -n "$ip_address" ]; then
    echo "Adresse IP trouvée : $ip_address pour la MAC $TARGET_MAC_ADDRESS."
    echo "Vérification de l'état de la machine (ping)...""

    # Effectue 3 tentatives de ping, avec 1 seconde de timeout par paquet,
    # et un intervalle de 0.2 secondes entre les paquets.
    # Redirige stdout et stderr vers /dev/null car seul le code de retour nous intéresse.
    ping -c 3 -W 1 -i 0.2 "$ip_address" > /dev/null 2>&1

    if [ $? -eq 0 ]; then
        echo "ÉTAT : EN LIGNE (la machine $ip_address répond au ping)."
        echo "Script ETAT_PC terminé."
        exit 0 # Succès, le PC répond
    else
        echo "ÉTAT : HORS LIGNE (la machine $ip_address ne répond pas au ping)."
        echo "Script ETAT_PC terminé."
        exit 1 # Échec, le PC ne répond pas
    fi
else
    echo "Aucune adresse IP n'a été trouvée pour l'adresse MAC : $TARGET_MAC_ADDRESS."
    echo "Impossible de vérifier l'état."
    echo "Script ETAT_PC terminé avec erreur."
    exit 3 # Code d'erreur spécifique pour IP non trouvée
fi
```

# Modules logiciels

Les modules « Allumer » et « Éteindre » utilisent le protocole MQTT pour communiquer avec les relais WiFi (Sonoff Basic R2 configurés avec Tasmota). Afin de piloter efficacement l'alimentation des ordinateurs, plusieurs topics MQTT sont utilisés.

Pour allumer ou éteindre un relais, l'application publie un message ON ou OFF sur le topic cmnd/nom\_du\_relais/POWER

Pour connaître l'état actuel du relais (savoir s'il est allumé ou éteint), l'application interroge ou écoute le topic stat/nom\_du\_relais/POWER. Le relais renvoie ON si l'alimentation est active, ou OFF si elle est coupée.

Enfin, pour savoir si le relais est connecté au réseau, l'application écoute le topic tele/nom\_du\_relais/LWT.

Le message renvoyé est Online si le relais est bien connecté au réseau WiFi, ou Offline s'il est déconnecté.

Cette structure de communication permet à l'application Python d'assurer à la fois le pilotage en temps réel des ordinateurs et la vérification de la fiabilité des relais, garantissant ainsi un fonctionnement sûr et contrôlé du système.

Premièrement, l'utilisateur est face à cette page, il choisit donc le rôle qui lui correspond, ADMIN s'il est administrateur, et e.etud qui est un bouton permettant de simuler la connexion de l'identifiant e.tud qui est dans la section 1TS-CIEL, qui est dans la base de données pour me permettre de faire mes tests :

The diagram illustrates the user selection process. On the left, a window titled "Sélection du Rôle" shows two options: "ADMIN" and "e.etud". The "ADMIN" option is highlighted with a blue border. An arrow points from this window to the right, where a second window titled "Utilisateur : e.etud / Section : 1TS-CIEL" is displayed. This window contains a "Horaire" section with three time intervals: "lundi 13:00 - 18:00", "vendredi 8:00 - 10:00", and "vendredi 17:00 - 18:00". Below this are three buttons: a red "Couper VPN et Fermer", a blue "Lancer Bureau à Distance", and a green "Rafraîchir". A large downward-pointing arrow originates from the "e.etud" button in the first window and points to the bottom of the second window. To the right of the second window, a third window titled "Contrôle Alimentation PCs - Admin (Admin (Accès Direct))" is shown. This window has a title bar "Panneau de Contrôle PCs & Relais (Admin):". It displays a table with two rows:

Sél.	ID PC	Info PC (État)	Info Relais (État)	Actions Relais	Actions PC
1 <input type="checkbox"/>	C104-16	192.168.2.14 État PC: INDÉT.	Topic: sonoff État Relais: ON	<input type="button" value="Relais ON"/> <input type="button" value="Relais OFF"/>	<input type="button" value="PC ON"/> <input type="button" value="PC OFF"/>
2 <input type="checkbox"/>	C107-17	192.168.2.15 État PC: INDÉT.	Topic: coucou État Relais: UNKNOWN	<input type="button" value="Relais ON"/> <input type="button" value="Relais OFF"/>	<input type="button" value="PC ON"/> <input type="button" value="PC OFF"/>

At the bottom of this window are three buttons: "Rafraîchir États" (green), "Allumer Sél." (green), and "Éteindre Sél." (red). Below the table is a status bar showing "Scan PCs: 0%" and "MQTT: Connecté". A scrollable "Journal des événements:" section at the bottom lists log entries:

```
[2025-05-28 17:49:05] Admin Relais 'sonoff' Online. Demande état...
[2025-05-28 17:49:05] Admin MQTT RX: stat/sonoff/POWER -> ON
[2025-05-28 17:49:05] Admin Relais 'sonoff' -> ON
[2025-05-28 17:49:05] Admin MQTT RX: stat/sonoff/POWER -> ON
[2025-05-28 17:49:05] Admin Relais 'sonoff' -> ON
[2025-05-28 17:49:05] Admin Lancement scan PCs (ping RPi)...
[2025-05-28 17:49:05] --- RPi CMD: Tentative sur 192.168.2.5 ---
[2025-05-28 17:49:05] Cmd: bash /home/a.admin/ping_check.sh 192.168.2.14
[2025-05-28 17:49:06] RPi CMD: Connecté.
```

Les tests précédemment effectués sont faits en partant du principe que l'authentification de l'administrateur et de l'étudiant, tous deux enregistrés, a bien été effectuée. la base de donnée est alimentée de sorte à ce que les tests puissent vérifier les exigences du système du point de vue du module prix en charge par l'étudiant 4. En effet, on vérifie la présence de chaque détail permettant la connexion et l'allumage avec l'extinction.

Pour arriver à l'allumage, il faut prendre en compte plusieurs variables, il faut un ordinateur enregistré, un relais configuré et qui lui est relié, un compte utilisateur qui lui donne le droit d'accéder à cet ordinateur en question. Ensuite, il faut vérifier la plage horaire attribuée disponible pour la section à laquelle le compte utilisateur appartient.

Prenons exemple sur les captures des pages précédentes. On voit que l'étudiant dont l'identifiant est "e.etud" est connecté à l'application, et qu'il appartient à la section appelée "1TS-CIEL", à laquelle les horaires de connexion sont visibles sur le panneau des créneaux horaires. L'étudiant peut consulter les horaires durant lesquelles il peut accéder à son ordinateur. Il a donc la possibilité d'allumer son ordinateur en appuyant sur le bouton "Lancer le bureau à distance", et l'extinction en appuyant sur le bouton "Couper VPN et Fermer".

La phase d'intégration permettra donc d'instaurer le VPN et de rendre obligatoire l'authentification. Elle permettra également de mettre en place la solution complète du système afin de répondre au problème.

Les modules d'allumage et d'extinction sont la finalité de ce système, car ils permettent de clôturer la solution logiciel que nous apportons. En effet, après toutes les vérifications d'utilisateurs, des machines et des relais, ainsi que les vérifications de connectivité, l'utilisateur parvient enfin à allumer ou éteindre la machine selon son rôle.

# 04 Bilan et Conclusion

## Bilan général

Le projet "Gestion d'un parc informatique v1" avait pour ambition de fournir une solution d'accès à distance aux ordinateurs du lycée, en mettant l'accent sur la sécurité, la disponibilité et l'optimisation énergétique.

D'importantes avancées ont été réalisées : les principaux composants matériels (serveurs, Raspberry Pi, relais Sonoff flashés Tasmota, point d'accès WiFi) ont été configurés. Parallèlement, les modules logiciels clés, incluant le broker MQTT, la base de données MariaDB (VirtualPilot), les interfaces et les mécanismes de commande ON/OFF des postes (Wake-on-LAN, MQTT), ont été développés et leurs fonctionnalités individuelles confirmées par des tests unitaires.

Cependant, un défi majeur est survenu en phase finale : des problèmes d'assemblage et d'interconnexion des différents éléments ont empêché la finalisation de l'intégration complète du système. En conséquence, les tests d'intégration globaux n'ont pu être conduits, laissant le système avec des modules fonctionnels individuellement mais sans validation de leur interaction globale en situation réelle.

Malgré cet obstacle, ce projet a offert un apprentissage significatif en administration réseau (Active Directory, services DNS/DHCP), configuration de services IoT (MQTT, Tasmota), développement Python pour l'IoT et gestion de bases de données. L'importance cruciale de la phase d'intégration a également été fortement soulignée par cette expérience.

La base technique établie demeure solide. La résolution des difficultés d'assemblage constitue la prochaine étape évidente pour permettre une intégration complète et la validation finale de la solution.

## Conclusion générale

En conclusion, le projet "Gestion d'un parc informatique v1" a permis de développer et de valider individuellement la majorité des briques technologiques nécessaires à la solution d'accès distant envisagée. Bien que les défis liés à l'assemblage final aient empêché la démonstration d'un système pleinement intégré, les connaissances et les compétences acquises dans la conception, le développement et la configuration de chaque composant sont considérables.

Ce projet met en lumière l'importance critique des phases d'intégration et la nécessité d'anticiper les difficultés qui peuvent y survenir. Les fondations techniques posées restent néanmoins pertinentes et la solution conserve son potentiel pour répondre, une fois l'intégration finalisée, aux besoins initiaux de gestion optimisée du parc informatique de l'établissement.

## ATTESTATION DE NON PLAGIAT

SESSION 2025

BTS CIEL

Session 2025

EPREUVE E6 (Stage et Projet).

Je soussigné(e) :

Nom de naissance : Rozicki ..... Prénom : Noah .....

Nom d'usage : .....

Inscrit(e) dans l'établissement : Lycée Elisa Lemonnier, Douai

Certifie que le dossier support de l'épreuve E6 est strictement le fruit de mon travail personnel.

Tout emprunt à un tiers (ouvrage, article, documents, sources internet incluses dont ChatGPT) est obligatoirement précisé. Les documents propres à la structure évoquée dans le dossier et repris sans être retravaillés sont indiqués par la mention « *Document interne à la structure* ».

Le dossier constitue une production originale et personnelle soumise à la réglementation de la fraude aux examens. Tout plagiat sera considéré comme une situation de fraude.

Fait à Douai ..... le ..... 03/06 .....

Signature manuscrite :



## ATTESTATION DE NON PLAGIAT

SESSION 2025

BTS CIEL

Session 2025

EPREUVE E6 (Stage et Projet).

Je soussigné(e) :

Nom de naissance : grandin ..... Prénom : Mathéo .....Nom d'usage : grandin .....Inscrit(e) dans l'établissement : Elisa Lemonnier .....

Certifie que le dossier support de l'épreuve E6 est strictement le fruit de mon travail personnel.

Tout emprunt à un tiers (ouvrage, article, documents, sources internet incluses dont ChatGPT) est obligatoirement précisé. Les documents propres à la structure évoquée dans le dossier et repris sans être retravaillés sont indiqués par la mention « *Document interne à la structure* ».

Le dossier constitue une production originale et personnelle soumise à la réglementation de la fraude aux examens. Tout plagiat sera considéré comme une situation de fraude.

Fait à ..... Douai ..... le ..... 03/06/2025

Signature manuscrite :



## ATTESTATION DE NON PLAGIAT

SESSION 2025

BTS CIEL

Session 2025

EPREUVE E6 (Stage et Projet).

Je soussigné(e) :

Nom de naissance : Langlet ..... Prénom : Marion .....

Nom d'usage : .....

Inscrit(e) dans l'établissement : Lycée Elisa Lemire .....

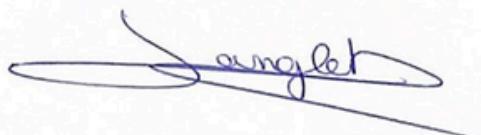
Certifie que le dossier support de l'épreuve E6 est strictement le fruit de mon travail personnel.

Tout emprunt à un tiers (ouvrage, article, documents, sources internet incluses dont ChatGPT) est obligatoirement précisé. Les documents propres à la structure évoquée dans le dossier et repris sans être retravaillés sont indiqués par la mention « *Document interne à la structure* ».

Le dossier constitue une production originale et personnelle soumise à la réglementation de la fraude aux examens. Tout plagiat sera considéré comme une situation de fraude.

Fait à .... Domrémy ..... le ..... 03/06/2025.....

Signature manuscrite :



## ATTESTATION DE NON PLAGIAT

SESSION 2025

BTS CIEL

Session 2025

EPREUVE E6 (Stage et Projet).

Je soussigné(e) :

Nom de naissance : AIT BRAHIM..... Prénom : ANASS.....Nom d'usage : AIT BRAHIM.....Inscrit(e) dans l'établissement : LPO ELISA LEMONNIER.....

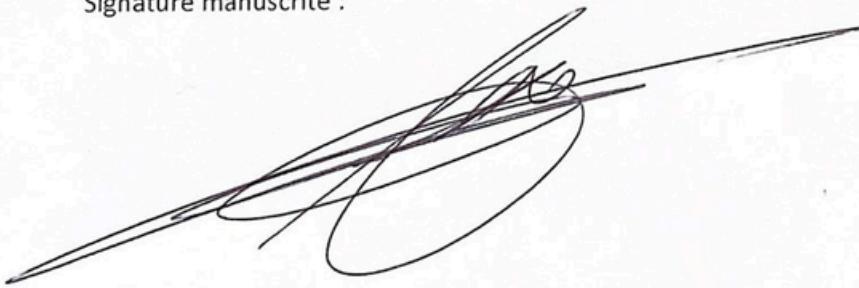
Certifie que le dossier support de l'épreuve E6 est strictement le fruit de mon travail personnel.

Tout emprunt à un tiers (ouvrage, article, documents, sources internet incluses dont ChatGPT) est obligatoirement précisé. Les documents propres à la structure évoquée dans le dossier et repris sans être retravaillés sont indiqués par la mention « *Document interne à la structure* ».

Le dossier constitue une production originale et personnelle soumise à la réglementation de la fraude aux examens. Tout plagiat sera considéré comme une situation de fraude.

Fait à ..... Domai ..... le ..... 03/06/2025 .....

Signature manuscrite :





# RAPPORT DE PROJET

BTS CIEL

Elisa LEMONNIER

juin 2025