

DELOUIS kylian

BAY Enzo

SICOT-DURIVEAU Alexia

Infrastructure Assurmer

**Un nouvel équipement Nomade et Sécurisé
ASSURMER**

ASSURMER

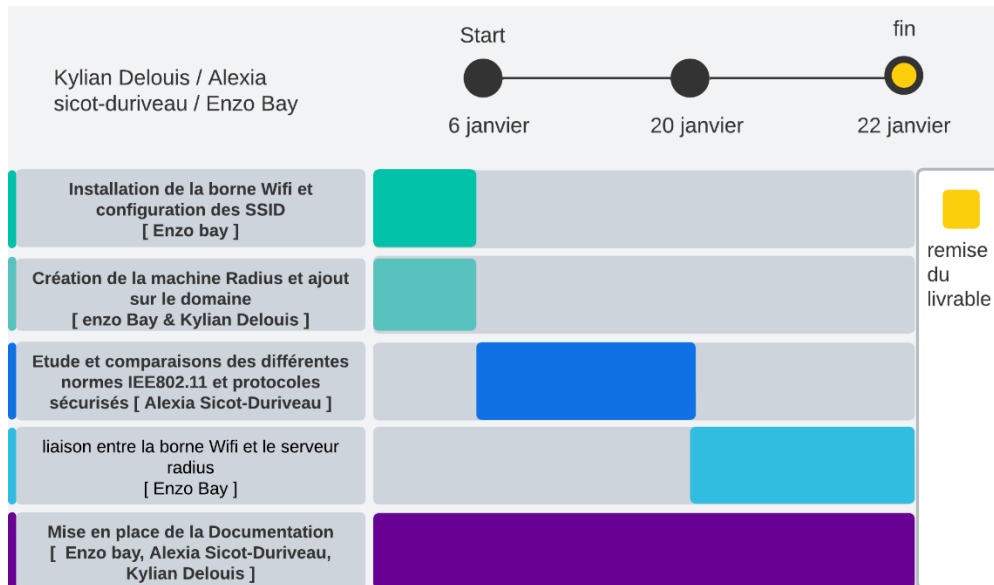


Sommaire

- **Planning de travail et répartition des tâches.....3**
 - Diagramme de Gant.....3
- **Présentation de la norme IEE802.114**
 - Différents types de normes.....4
 - Différentes Couches radio.....5
- **Etude comparative des protocoles de sécurité wifi.....5**
 - Tableau de comparaison.....5
- **Procédure d'installation de la borne Wifi cisco et configuration SSID....6**
 - Configuration de l'adresse IP.....6
 - Mise en place d'un mot de passe robuste.....6
 - Création d'une cellule wifi en 5Ghz.....7
- **Présentation du fonctionnement d'une solution Radius et certificats.....9**
 - Définition d'un serveur Radius et certificat.....9
- **Procédure d'installation d'un serveur Radius10**
 - Création du serveur Radius.....10
 - Ajout de la borne Wifi.....19

Planning de travail et répartition des tâches

Un diagramme de Gantt est un outil essentiel pour la gestion de projet, en particulier lorsqu'il s'agit de répartir efficacement les tâches au sein d'une équipe. Dans notre cas, l'utilisation d'un diagramme de Gantt nous a permis de structurer notre travail de manière claire et organisée.



- **Enzo Bay**
 - Installation de la borne WiFi et configuration des SSID
 - Création de la machine Radius et ajout sur le domaine (avec Kylian Delouis)
 - Liaison entre la borne WiFi et le serveur Radius
 - Mise en place de la documentation (avec Alexia Sicot-Duriveau et Kylian Delouis)
- **Kylian Delouis**
 - Création de la machine Radius et ajout sur le domaine (avec Enzo Bay)
 - Mise en place de la documentation (avec Enzo Bay et Alexia Sicot-Duriveau)
- **Alexia Sicot-Duriveau**
 - Étude et comparaisons des différentes normes IEEE 802.11 et protocoles sécurisés + comparaison
 - Mise en place de la documentation (avec Enzo Bay et Kylian Delouis)

Chaque membre de l'équipe a ainsi contribué à différentes phases du projet, certaines tâches étant réalisées en collaboration afin d'assurer une meilleure répartition du travail et une complémentarité des compétences.

Présentation de la norme IEEE802.11

Le standard IEEE802.11 a été créé par le groupe de travail 11 du comité de normalisation LAN/MAN de l'Institute of Electrical and Electronics Engineers (IEEE). Ce groupe de travail a publié la première version de la norme en 1997, établissant les bases des réseaux WIFI. La norme IEEE 802.11 a été créée pour répondre à la demande croissante de connectivité sans fil et pour établir un standard commun permettant l'interopérabilité entre différents appareils et fabricants. Cette norme se réfère à la couche 1 et à la couche 2 du modèle OSI :

- Elle utilise la couche physique (1) pour la transmission des données sur les différents supports physiques. Les ondes radios en sont une.
- Elle utilise aussi la sous-couche MAC (2) pour la liaison de données. Elle gère l'accès au canal de communication et assure la transmission des données entre les appareils.

Différents types de Normes :

Il existe 3 variantes de la norme IEEE 802.11

- IEEE 802.11 FHSS** (Frequency Hopping Spread Spectrum) utilise la technique de l'étalement de spectre par saut de fréquence.
- IEEE 802.11 DSSS** (Direct Sequence Spread Spectrum) utilise la technique de l'étalement de spectre par fréquence directe.
- IEEE 802.11 IR** utilise la lumière infrarouge pour la transmission des données.

Ses trois types de produits ne sont d'ailleurs pas compatibles entre eux au niveau physique.

Le standard IEEE 802.11 a évolué avec l'ajout de nouvelles couches physiques :

- **IEEE 802.11b** : Utilise la bande ISM avec des débits jusqu'à 11 Mbit/s, compatible avec IEEE 802.11 DSSS.
- **IEEE 802.11a** : Utilise la bande U-NII autour de 5 GHz avec des débits jusqu'à 54 Mbit/s, mais n'est pas compatible avec les précédents standards.
- **IEEE 802.11g** : Utilise la bande ISM avec des débits jusqu'à 20 Mbit/s, compatible avec IEEE 802.11 DSSS et IEEE 802.11b.
- **IEEE 802.11n** : Évolution de 802.11g intégrant la technologie MIMO.

La norme IEEE 802.11 définit les deux premières couches du modèle OSI : la couche physique et la couche liaison de données, cette dernière étant subdivisée en sous-couches LLC et MAC. La couche physique est divisée en sous-couches PMD et PLCP.

Différentes Couches Radio :

Les couches radio du standard IEEE 802.11/a/b/g utilisent des bandes sans licence :

- **Bande ISM** : Utilisée par 802.11/b/g autour de 2,4 GHz.
- **Bande U-NII** : Utilisée par 802.11a autour de 5 GHz, divisée en trois sous-bandes distinctes.

Les bandes de fréquences varient selon les pays et sont régulées par des organismes comme la FCC aux États-Unis, l'ETSI en Europe, et le MKK au Japon.

Etude comparative des protocoles de sécurité wifi

Protocole	Année d'introduction	Cryptage	Clé	Avantages	Inconvénients
WEP	1997	RC4	40/104 bits	Facile à configurer	Très vulnérable
WPA	2003	TKIP	128 bits	Amélioration par rapport à WEP	Vulnérable aux attaques par dictionnaire
WPA2	2004	AES	256 bits	Sécurité renforcée	Nécessite plus de puissance de traitement
WPA3	2018	SAE	128/192 bits	Protection contre les attaques par force brute	Adoption en cours

- **WEP (1997)** : Protocole obsolète avec chiffrement RC4 (40/104 bits), facile à configurer mais très vulnérable.
- **WPA (2003)** : Amélioration de WEP avec TKIP (128 bits), mais vulnérable aux attaques par dictionnaire.
- **WPA2 (2004)** : Sécurité renforcée avec AES (256 bits), nécessitant plus de puissance de traitement.
- **WPA3 (2018)** : Protection avancée contre les attaques avec SAE (128/192 bits), adoption en cours.

Configuration de l'adresse IP

Access Point Setup Wizard

Welcome

Configuration

IP Address

Single Point Setup

Time Settings

Device Password

Radio 1 (5 GHz)

Network Name

Wireless Security

VLAN ID

Radio 2 (2.4 GHz)

Network Name

Configure Device - IP Address

Select either Dynamic or Static IP address for your device.

☒ Dynamic IP Address (DHCP) (Recommended)

☐ Static IP Address

Static IP Address: 172 . 16 . 0 . 10

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 172 . 16 . 0 . 254

DNS: 172 . 16 . 0 . 1

Secondary DNS (optional): 8 . 8 . 8 . 8

[Learn more about the different connection types](#)

Click **Next** to continue

Back Next Cancel

Mise en place de l'adresse « 172.16.0.10 » comme adresse principale de la borne wifi, « 172.16.0.254 » comme adresse de la passerelle, « 172.16.0.1 » comme adresse DNS puis appuyez sur « **Next** »

Mise en place d'un mot de passe robuste

Access Point Setup Wizard

Welcome

Configuration

✓ IP Address

✓ Single Point Setup

✓ Time Settings

Device Password

Radio 1 (5 GHz)

Network Name

Wireless Security

VLAN ID

Radio 2 (2.4 GHz)

Network Name

Configure Device - Set Password

The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New password should not match with current password

New Password:

Confirm Password:

Password Strength Meter: Weak

Password Complexity: ☒ Enable

[Learn more about passwords](#)

Click **Next** to continue

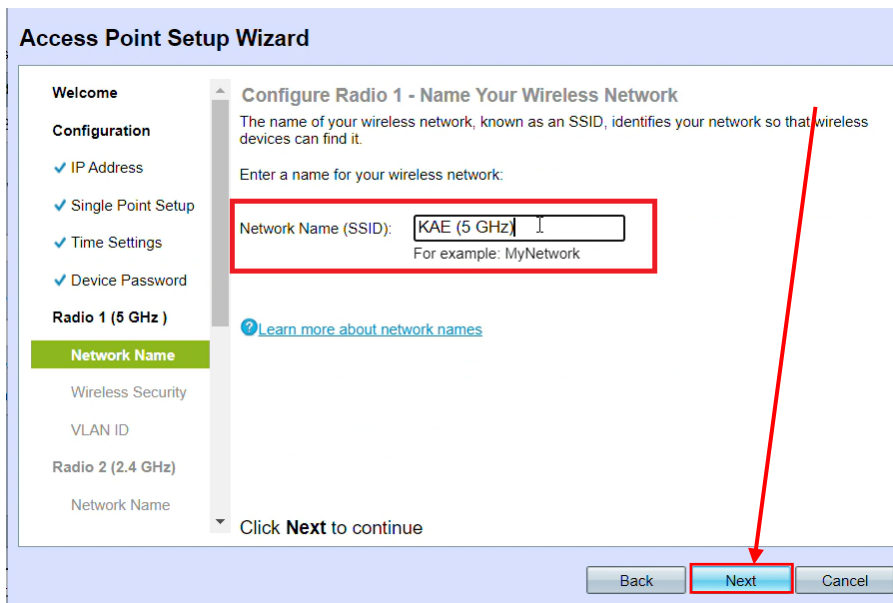
Back Next Cancel

Mot de passe robuste ?

Un mot de passe robuste est un mot de passe difficile à deviner ou à casser, même à l'aide d'attaques automatisées. Il doit être suffisamment long (au moins 12 à 16 caractères) et inclure une combinaison de majuscules, de minuscules, de chiffres et de caractères spéciaux.

Mise en place du mot de passe robuste de votre choix qui permettra de se connecter au la borne wifi puis appuyez sur « **Next** »

Création d'une cellule wifi en 5Ghz



Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- ✓ Device Password

Radio 1 (5 GHz)

- Network Name**
- Wireless Security
- VLAN ID
- Radio 2 (2.4 GHz)
- Network Name

Configure Radio 1 - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

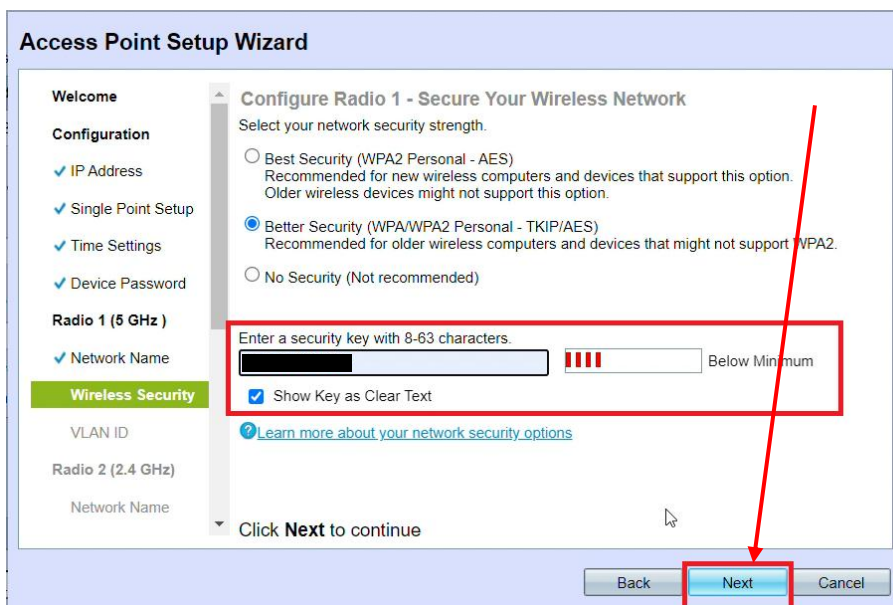
For example: MyNetwork

[Learn more about network names](#)

Click **Next** to continue

Back Next Cancel

Création d'une cellule wifi en radio 5 GHz qui permettra de diffuser un réseau wifi, ici appeler « KAE (5 GHz) » puis appuyez sur « **Next** »



Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- ✓ Device Password

Radio 1 (5 GHz)

- Wireless Security**
- VLAN ID
- Radio 2 (2.4 GHz)
- Network Name

Configure Radio 1 - Secure Your Wireless Network

Select your network security strength.

- ☐ Best Security (WPA2 Personal - AES)
Recommended for new wireless computers and devices that support this option.
Older wireless devices might not support this option.
- ☒ Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.
- ☐ No Security (Not recommended)

Enter a security key with 8-63 characters.

Below Minimum

☒ Show Key as Clear Text

[Learn more about your network security options](#)

Click **Next** to continue

Back Next Cancel

Mise en place d'un mot de passe robuste nous permettant de nous connecter à notre réseau wifi puis appuyez sur « **next** »

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- ✓ Device Password
- Radio 1 (5 GHz)**
 - ✓ Network Name
 - ✓ Wireless Security
 - VLAN ID**
- Radio 2 (2.4 GHz)
 - Network Name

Configure Radio 1 - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: (Range: 1 - 4094)

[Learn more about vlan ids](#)

Click **Next** to continue

Back **Next** Cancel

Attribution du vlan correspondant au réseau wifi, ici le vlan est « 80 » puis appuyez sur « **Next** ».

Il nous suffit donc de prévoir différents types de réseaux selon le service de l'utilisateur

Ainsi, 7 réseaux seront donc opérationnel tel que :

- Direction
- Compta
- Assurance Pro
- Assurance Particuliers
- Ressource Humaine
- D&C Numérique
- Support Utilisateur

Virtual Access Points (SSIDs)				
	VAP No.	Enable	VLAN ID	SSID Name
☐	0	☒	80	KAE (5 GHz)
☐	1	☒	10	KAE-Direction
☐	2	☒	20	KAE-Compta
☐	3	☒	30	KAE-Assurance-Pro
☐	4	☒	40	KAE-Assurance Particuliers
☐	5	☒	50	KAE-Ressource Humaine
☐	6	☒	60	KAE-D&C numérique
☐	7	☒	70	KAE-Support utilisateurs

Définition d'un serveur Radius et Certificat :

Une solution RADIUS (Remote Authentication Dial-In User Service) est un protocole permettant l'authentification, l'autorisation des utilisateurs souhaitant accéder à un réseau, notamment en WiFi ou via VPN. Son fonctionnement repose sur un modèle client-serveur où les équipements réseau (comme les points d'accès WiFi ou les pare-feux) agissent en tant que clients RADIUS, et le serveur RADIUS gère les requêtes d'authentification en se basant sur une base de données d'identifiants.

Connexion de l'utilisateur :

- Lorsqu'un utilisateur essaie de se connecter au réseau, son appareil **envoie une demande** d'accès au serveur RADIUS via un point d'accès WiFi ou un autre équipement réseau.
- Au lieu d'utiliser un mot de passe, la connexion peut se faire avec un **certificat numérique**, un fichier sécurisé qui prouve l'identité de l'utilisateur.

Vérification du certificat :

- Le serveur RADIUS vérifie si le certificat est valide et s'il a été délivré par une autorité de confiance.
- Si tout est correct, l'accès est accordé, sinon il est refusé.

Attribution des droits :

- Une fois connecté, l'utilisateur est placé dans un groupe spécifique selon son profil (par exemple, accès limité pour les invités, accès total pour les employés).

Suivi des connexions :

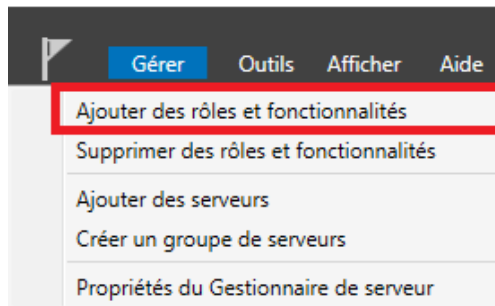
- Le serveur RADIUS enregistre les connexions pour savoir qui s'est connecté, quand et pendant combien de temps, ce qui est utile pour la sécurité du réseau.

En résumé, une solution RADIUS avec certificats permet de sécuriser les connexions réseau de manière efficace et automatique, en garantissant que seules les personnes autorisées peuvent se connecter.

Procédure d'installation d'un serveur Radius

Création du serveur Radius

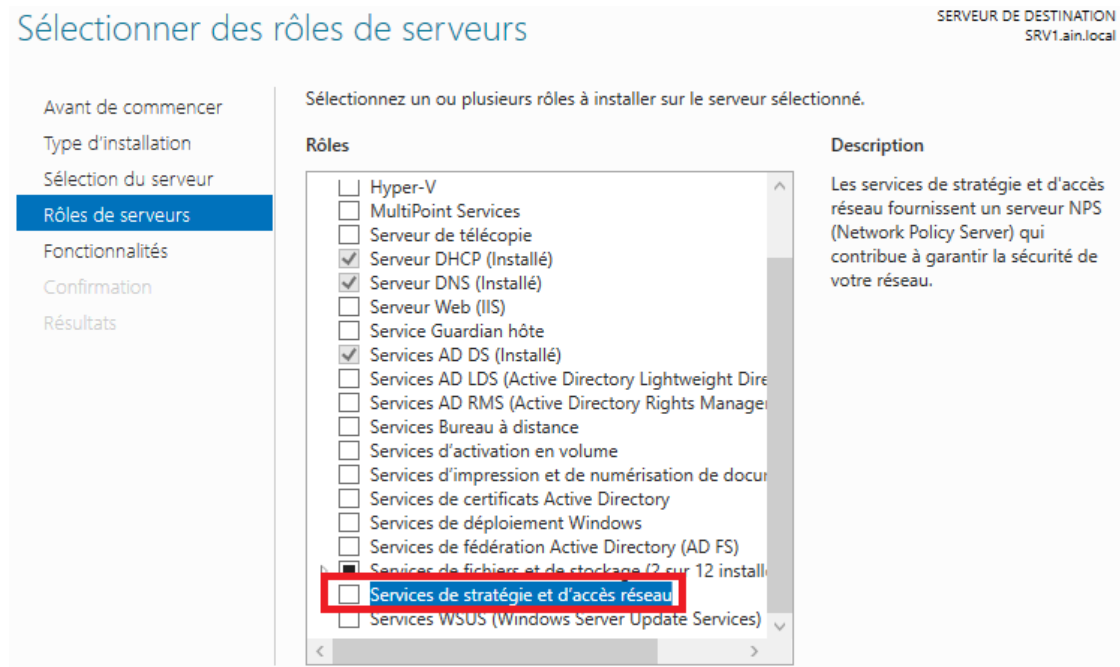
Pour commencer, allez dans le **gestionnaire de serveur**, cliquez sur « **Gérer** » puis « **Ajouter des rôles et fonctionnalités** ».



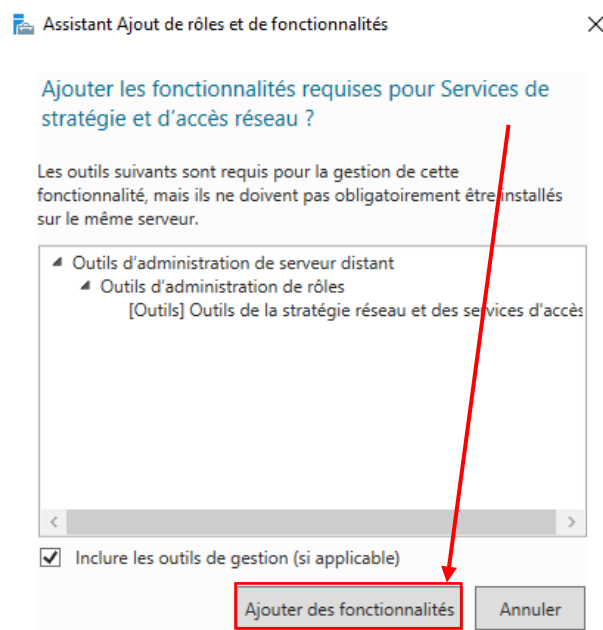
Sur la première fenêtre laissez cocher « **Installation basée sur un rôle ou une fonctionnalité** ».



Sur la fenêtre suivante « **Sélection du serveur** » laissez par défaut et cliquez à nouveau sur « **Suivant** ». Vous arriverez sur la fenêtre de sélection des rôles, cochez « **Services de stratégie et d'accès réseau** ».



Cliquez sur « **Ajouter des fonctionnalités** » et cliquez sur « **Suivant** ».



Cliquez sur « **Suivant** » jusqu'à arriver sur la fenêtre de confirmation d'installation du rôle et cliquez sur « **Installer** ».

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
SRV1.ain.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmer
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☒ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

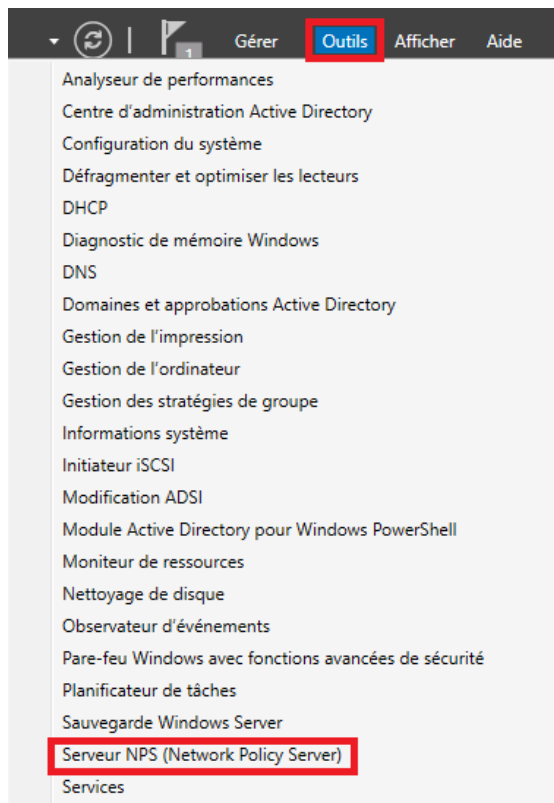
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de la stratégie réseau et des services d'accès
Services de stratégie et d'accès réseau

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

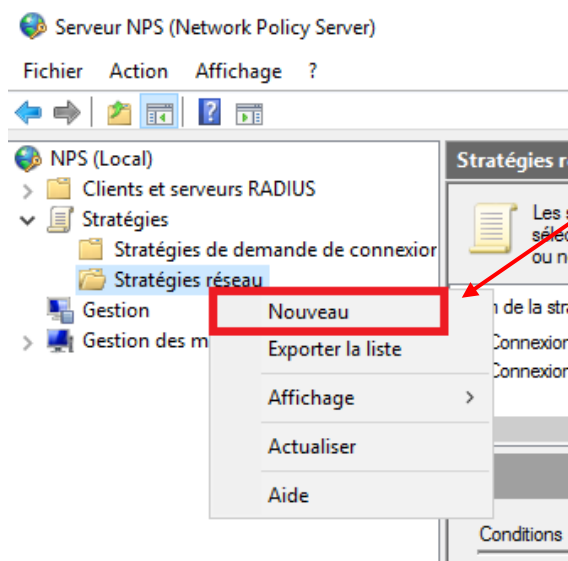
< Précédent Suivant > **Installer** Annuler

Patiencez quelques minutes jusqu'à l'installation du rôle.

Maintenant que le rôle est installé nous allons devoir le configurer. Pour cela dans le gestionnaire de serveur cliquez sur « **Outils** » puis sur « **Serveur NPS (Network Policy Server)** ».



Vous arriverez sur la fenêtre d'administration de **RADIUS**. Nous allons commencer par configurer la stratégie de connexion à notre réseau Wifi. Dépliez le menu « **Stratégie** », faites un clic droit sur « **Stratégies réseau** » et sélectionnez « **Nouveau** ».



Vous allez arriver sur la fenêtre ci-dessous. Entrez le nom de votre stratégie et cliquez sur « **Suivant** ».

Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :

connexion_wifi

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :

Non spécifié

☐ Spécifique au fournisseur :

10

Pour la condition cliquez sur « **Ajouter** » et sélectionnez « **Groupes Windows** » et cliquez à nouveau sur « **Ajouter** »

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

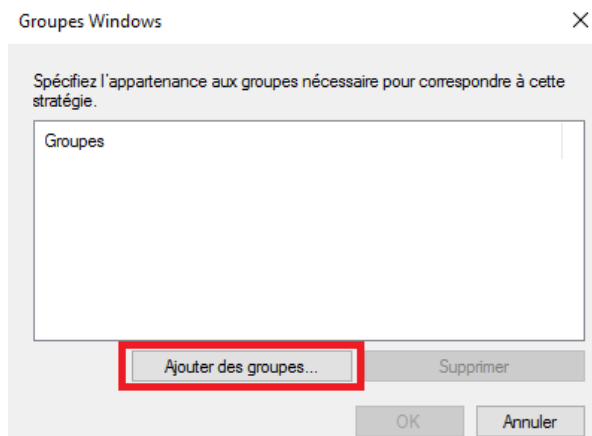
- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

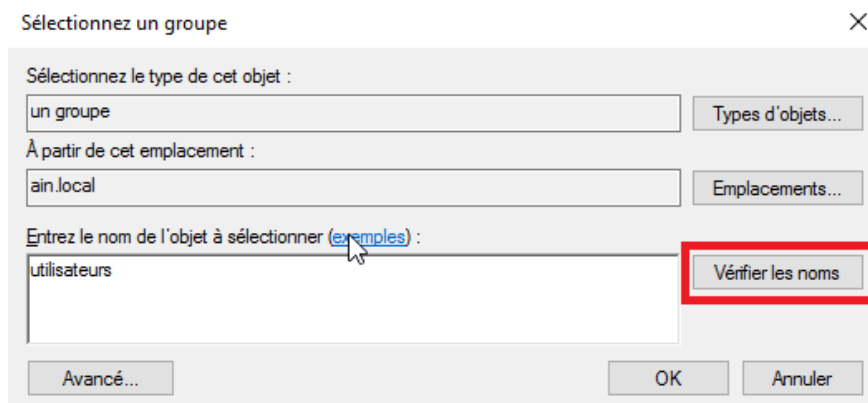
Ajouter... Annuler

Cliquez sur « **Ajouter des groupes** ».

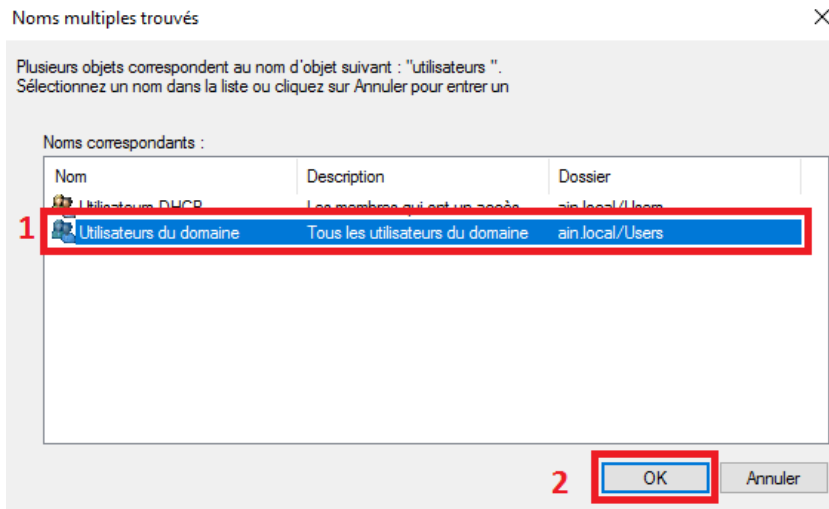


Vous allez ensuite devoir sélectionner le groupe des utilisateurs pouvant se connecter au réseau WiFi en question.

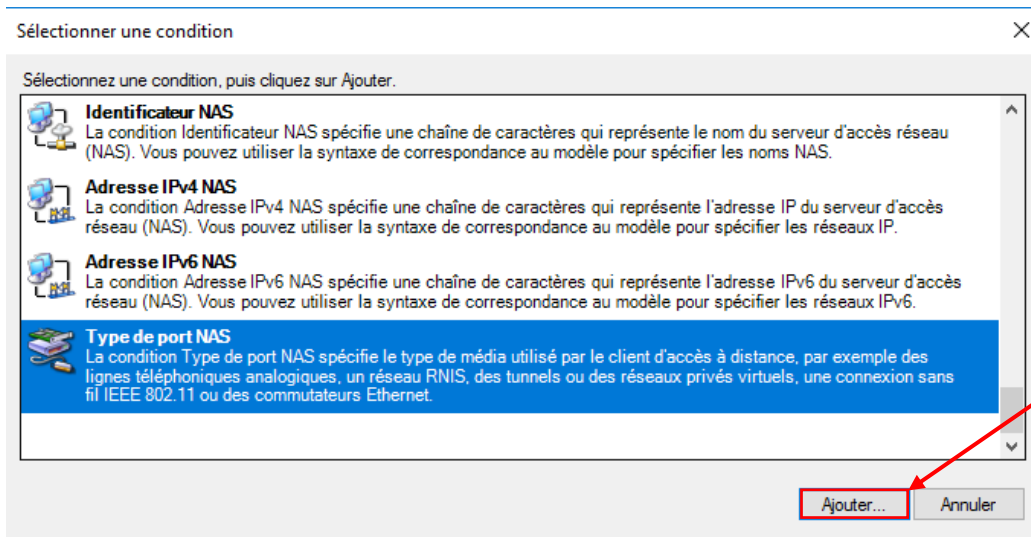
Écrivez utilisateurs et cliquez sur « **Vérifier les noms** »



Sélectionnez « **Utilisateurs du domaine** » et cliquez sur « **OK** » jusqu'à revenir sur la fenêtre pour spécifier les conditions et cliquez de nouveau sur « **Ajouter** ».



Cette fois ci sélectionnez « **Type de port NAS** » et cliquez sur « **Ajouter** ».



Sélectionnez les 2 options comme ci-dessous et cliquez sur « **OK** ». Cliquez sur « **Suivant** » sur la fenêtre des conditions.

Spécifiez les types de médias d'accès nécessaires pour correspondre à cette stratégie.

Types de tunnels pour connexions d'accès à distance et VPN standard

- ☐ Asynchrone (Modem)
- ☐ RNIS synchrone
- ☐ Synchrone (ligne T1)
- ☐ Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

- ☐ Ethernet
- ☐ FDDI
- ☒ Sans fil - IEEE 802.11
- ☐ Token Ring

Autres

- ☐ RNIS synchrone
- ☒ Sans fil - Autre
- ☐ SDSL - DSL symétrique
- ☐ Synchrone (ligne T1)

OK Annuler

Laissez cocher « **Accès accordé** » et cliquez sur « **Suivant** ».

Nouvelle stratégie réseau

Spécifier l'autorisation d'accès

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

☒ **Accès accordé**
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ **Accès refusé**
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

Pour les méthodes authentification, cliquez sur « **Ajouter...** ».

Nouvelle stratégie réseau X

 **Configurer les méthodes d'authentification**
Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter

Descendre

Ajouter...

Modifier...

Supprimer

Méthodes d'authentification moins sécurisées :

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.

Précédent

Suivant

Terminer

Annuler

Sélectionnez « **Microsoft PEAP** » cliquez sur « **OK** » et cliquez sur « **Suivant** » sur l'autre fenêtre.

Ajouter des protocoles EAP X

Méthodes d'authentification :

Microsoft: Carte à puce ou autre certificat

Microsoft: PEAP (Protected EAP)

Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)

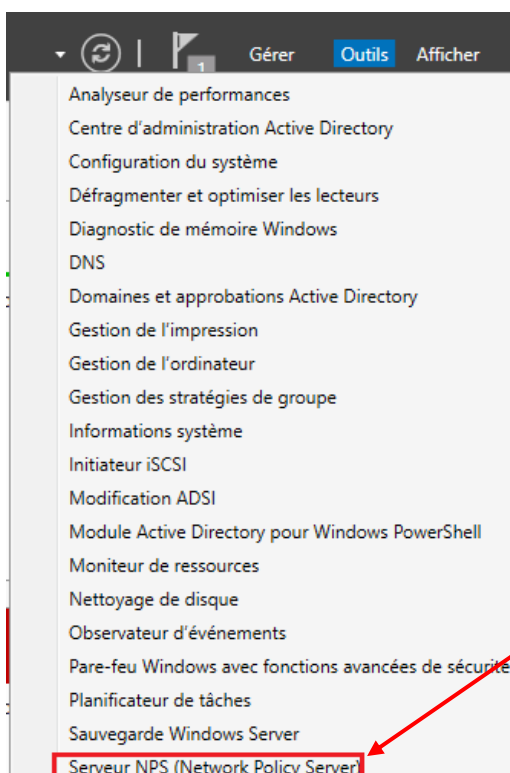
OK

Annuler

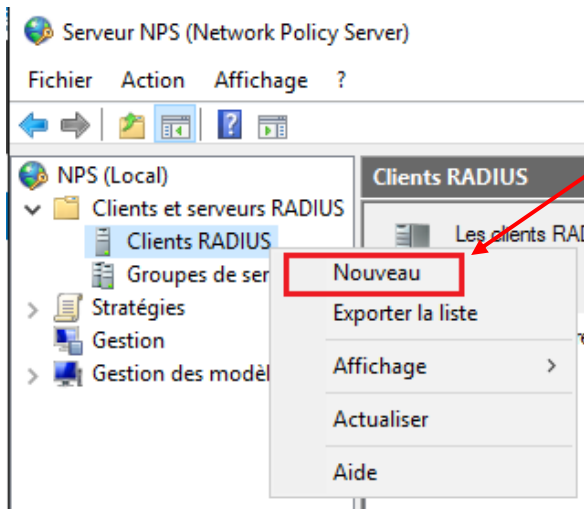
Sur la fenêtre suivante « **Configurer des contraintes** », laissez par défaut et cliquez sur « **Suivant** ». Faites de même pour la fenêtre « **Configurer les paramètres** ». Une fenêtre récapitulant la configuration va apparaître cliquez sur « **Terminer** ».

Ajout de la borne

Pour que l'accès fonctionne, nous allons devoir ajouter la borne WiFi sur le serveur **RADIUS**. Elle va avoir le rôle de NAS (Network Access Server) qui est un équipement intermédiaire entre le serveur **RADIUS** et l'utilisateur. Allez dans le gestionnaire de serveur et cliquez sur « **Outils** » puis sur « **Serveur NPS (Network Policy Server)** »



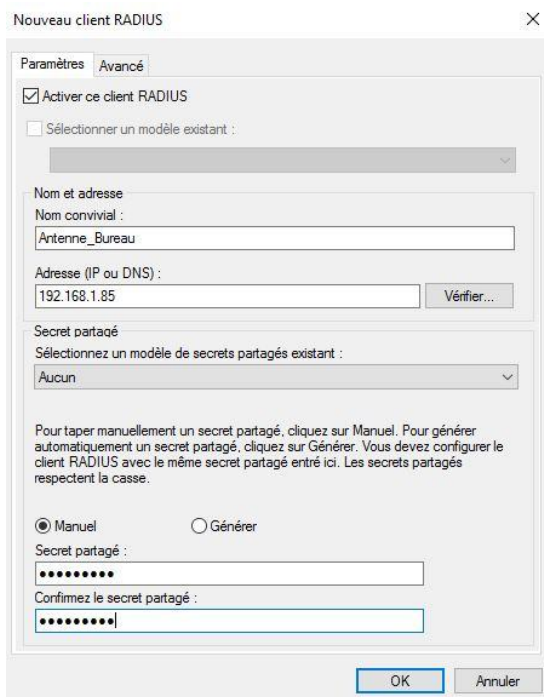
Dans la fenêtre qui vient de s'ouvrir, déroulez le menu « **Client et serveurs RADIUS** », faites un clic droit sur « **Clients RADIUS** » et sélectionnez « **Nouveau** »



Nous allons renseigner les informations de la borne wifi sur le serveur.

- Laissez cocher « **Activer ce client RADIUS** ».
- Nom convivial : Entrez le nom d'hôte de la borne WiFi.
- Adresse IP : Renseignez l'adresse IP de la borne WiFi.
- Pour le secret laissez cocher « **Manuel** » et renseignez la clé que vous saisissez aussi sur la borne WiFi.

Cliquez ensuite sur « **OK** ».



BAY Enzo
DELOUIS Kylian
IDJELLIDINE Amina

BTS SIO SISR 1A

Un nouvel équipement Nomade et Sécurisé
ASSURMER

ASSURMER



Table des matières

• Présentation de l'outils GLPI	3
○ Fonctionnalités.....	3
▪ Optimisation des ressources.....	3
▪ Amélioration de la productivité.....	3
▪ Gestion proactive des incidents.....	3
▪ Conformité et sécurité.....	4
▪ Prise de décision éclairée.....	4
○ Version.....	5
▪ Interface utilisateur.....	5
▪ Sécurité.....	5
▪ Performance.....	5
▪ Compatibilité.....	5
○ Licence.....	6
• Topologie Numérique	8
• Procédure d'installation	9
○ Préparation du serveur avant installation.....	11
○ Installation GLPI.....	14
○ Installation du plugin GLPI inventory.....	24
• Teste et création de tickets	29
○ Création du compte « Utilisateur »	30
○ Création du compte « Technicien »	31
• Logigramme du style de vie d'un ticket	35
• Procédure de destination Utilisateur	38

Présentation de l'outils GLPI



GLPI est un fantastique logiciel de Service Management basé sur des technologies open source. Il vous aide à planifier et à gérer facilement les changements informatiques, à résoudre efficacement les problèmes, à automatiser vos processus métier et à prendre le contrôle de votre infrastructure informatique.

Ainsi il nous propose plusieurs fonctionnalités tel que :

1. Optimisation des ressources :

En centralisant la gestion des actifs informatiques, GLPI permet aux organisations d'optimiser l'utilisation de leurs ressources matérielles et logicielles. Cela peut se traduire par une réduction des coûts liés à l'acquisition et à la maintenance des actifs, ainsi qu'une meilleure utilisation des licences logicielles.

2. Amélioration de la productivité :

En offrant un système efficace de gestion des tickets d'assistance, GLPI contribue à réduire les temps d'arrêt des utilisateurs et à améliorer leur productivité. Les demandes d'assistance sont traitées de manière plus rapide et plus efficace, ce qui permet aux utilisateurs de revenir rapidement à leurs activités principales.

3. Gestion proactive des incidents :

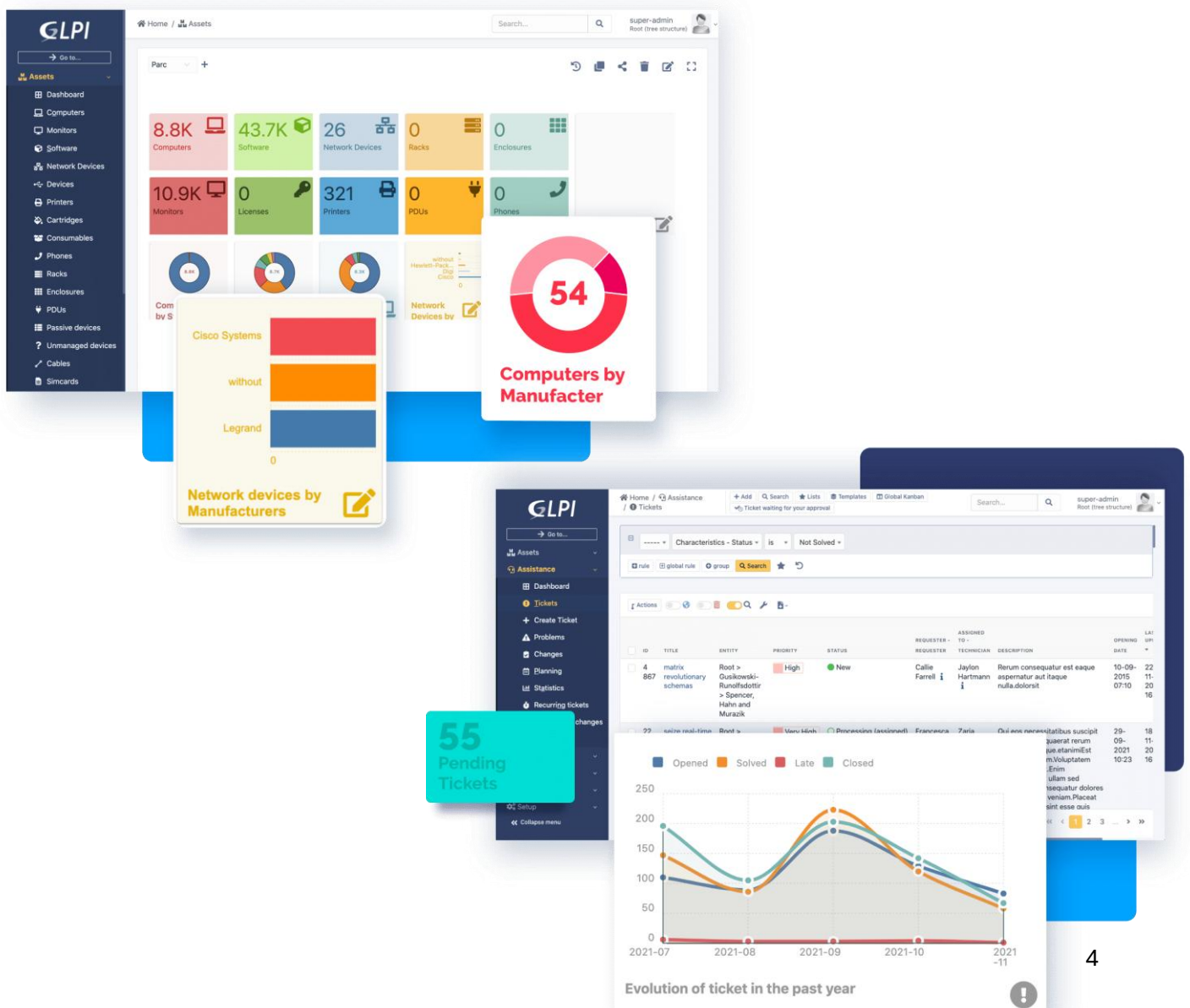
Grâce à ses fonctionnalités de gestion des problèmes, GLPI permet aux organisations d'adopter une approche proactive pour identifier et résoudre les causes sous-jacentes des incidents informatiques. Cela contribue à réduire le nombre d'incidents récurrents et à améliorer la stabilité globale du système informatique.

4. Conformité et sécurité :

En fournissant des fonctionnalités de suivi des actifs informatiques et des contrats de maintenance, GLPI aide les organisations à garantir leur conformité aux réglementations et aux normes de sécurité. Cela permet de réduire les risques liés à la non-conformité et de renforcer la sécurité des données.

5. Prise de décision éclairée :

GLPI est hautement personnalisable et extensible, ce qui permet aux organisations de l'adapter à leurs besoins spécifiques. Des plugins et des modules complémentaires peuvent être ajoutés pour étendre les fonctionnalités de base de GLPI et répondre à des exigences métier spécifiques.



Version de l'outils

LA DERNIÈRE VERSION GLPI STABLE

GLPI VERSION 10.0.15

La version 10.0.15 de GLPI apporte de nombreuses améliorations par rapport au version antérieur de GLPI. Voici quelques-unes des principales nouveautés :

Interface utilisateur :

La version 10.0.15 bénéficie d'une refonte majeure de l'interface utilisateur, ce qui améliore l'expérience utilisateur et la facilité d'utilisation.

Sécurité :

La version 10.0.15 corrige plusieurs problèmes de sécurité qui ont été découverts récemment, ce qui garantit une sécurité renforcée pour les utilisateurs.

Performances :

La version 10.0.15 apporte des améliorations significatives en termes de performances, notamment pour les vues kanban et l'initialisation des plugins.

Compatibilité :

La version 10.0.15 est compatible avec les versions PHP 8.1 et supérieures, ce qui permet aux utilisateurs de bénéficier des dernières fonctionnalités de PHP.

Licence

Souscription GLPI Network

Que comprend l'offre GLPI Network ?



Garantie Éditeur



Support correctif (N3)



Plugins exclusifs

(Tous sous licence libre GPL)



Accès aux partenaires-
intégrateurs

GLPI Network Cloud

19€/mois

Prix pour 1 agent
informatique

Actifs illimités

Utilisateurs finaux illimités

Correction de bugs illimitée

Plugins communautaires *

Plugins GLPI Network

Mises à jour incluses

Sauvegardes journalières

Maintenance du serveur

On-premises Basic

* HT

100€/mois

(engagement 12 mois)

Jusqu'à **10 agents**
informatiques

Jusqu'à **500 actifs**
informatiques

Utilisateurs finaux
illimités

Correction de bugs
illimitée

Plugins
communautaires *

Plugins GLPI Network

Plugins Standard **

Plugins Advanced ***

+ 2 tickets d'expertise
technique à distance
de TECLIB

Mises à jour

Sauvegardes

Maintenance du
serveur

SOUSCRIRE

On-premises Standard

* HT

300€/mois

(engagement 12 mois)

Jusqu'à **50 agents**
informatiques

Jusqu'à **5000 actifs**
informatiques

Utilisateurs finaux
illimités

Correction de bugs
illimitée

Plugins
communautaires *

Plugins GLPI Network

Plugins Standard **

Plugins Advanced ***

+ 8 tickets d'expertise
technique à distance
de TECLIB

Mises à jour

Sauvegardes

Maintenance du
serveur

SOUSCRIRE

On-premises Advanced

* HT

1000€/mois

(engagement 12 mois)

Plus que > **51 agents**
informatiques

Plus que > **5001**
actifs informatiques

Utilisateurs finaux
illimités

Correction de bugs
illimitée

Plugins
communautaires *

Plugins GLPI Network

Plugins Standard **

Plugins Advanced ***

+ 20 tickets
d'expertise technique
à distance de TECLIB

Mises à jour

Sauvegardes

Maintenance du
serveur

SOUSCRIRE

Qu'est-ce que GLPI Network ?

GLPI Network est un service de support niveau 3 (correctifs de bugs en illimité) sur une distribution de notre logiciel libre et opensource « GLPI » correctement packagée pour une utilisation professionnelle.

Assistance technique à distance de l'équipe de Teclib'

Niveau de support 3 pour les plugins supportés

Garantie de l'éditeur

BASIC

1 instance de production et 1 instance de test. Jusqu'à 500 matériels ou jusqu'à 10 utilisateurs avec un profil standard.

STANDARD

2 instances de production et 2 instances de test. Jusqu'à 5000 matériels ou jusqu'à 50 utilisateurs avec un profil standard.

ADVANCED

4 instances de production et 4 instances de test. Plus que 5001 matériels ou plus que 51 utilisateurs avec un profil standard.

Plugins exclusifs Teclib'



Le niveau de souscription est établi en fonction de deux critères :



Le nombre total de matériels administrés par GLPI
Nous prenons en compte les matériels suivants : Ordinateurs fixes, portables, clients légers, nano-ordinateurs, serveurs physiques, virtuels, hyperviseurs, appliances.



Le nombre d'utilisateurs ayant au moins un profil "Interface standard"
Parfois appelés "techniciens", "agents helpdesk".

Versions de GLPI Supportées

Version majeure actuelle (N)

Version majeure précédente (N-1)

Le client doit conserver une version (N) ou (N-1) tout au long de la souscription.

Calendrier d'ouverture du Support

Lundi au vendredi de 09h00 à 17h00

(Europe / Paris timezone)

Week-ends et jours fériés (Français) exclus

Langues Supportées

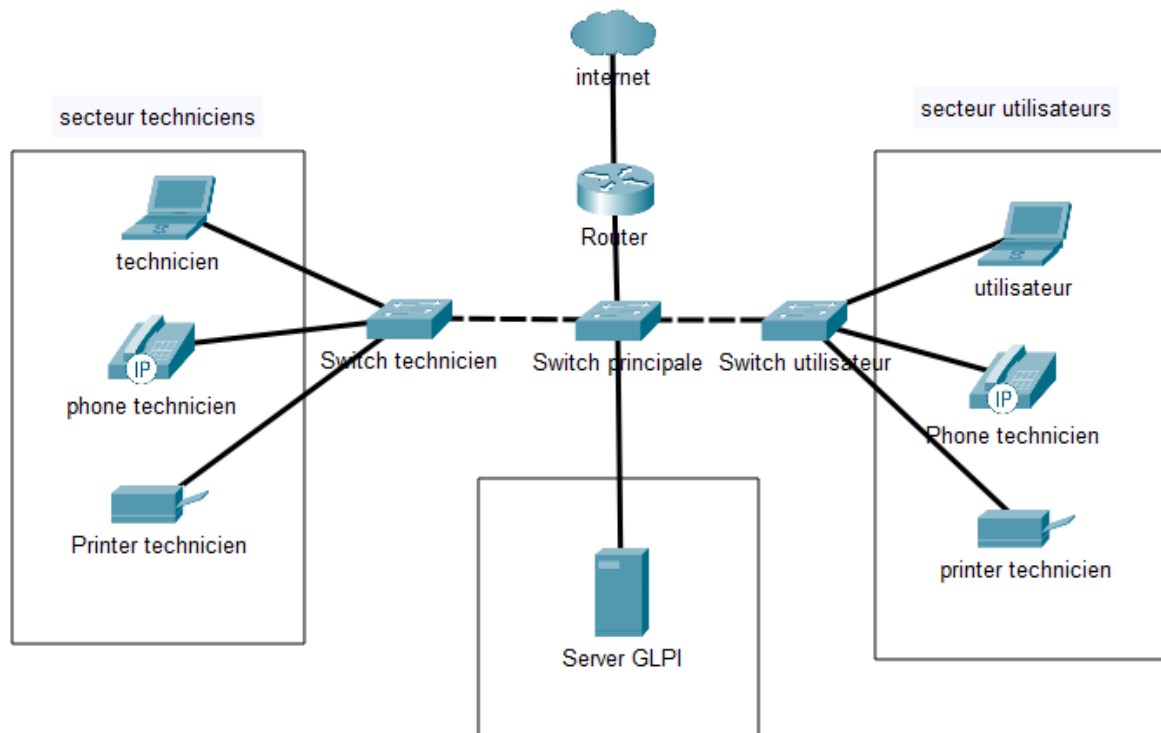
Français / Anglais



GLPINETWORK by teclib'

Topologie Numérique

Exemple de Topologie Numérique d'une infrastructure accueillant GLPI



Ainsi dans cette topologie Numérique nous pouvons trouver plusieurs appareils :

-  - Un serveur ou est héberger GLPI
-  - Un premier utilisateur (personne faisant la création de ticket)
-  - Un Technicien (personne s'occupent de résoudre le ticket)
-  - Un téléphone
-  - Imprimante

De plus, afin de pouvoir faire communiquer les différents appareils nous utiliserons :

-  - Un switch (Communication LAN)
-  - Un routeur Wireless (pour les utilisateur distant)
-  - Internet

Procédure d'installation GLPI sous Linux



Sommaire

1.	Préparation du serveur avant installation.....	11
a.	Installation du socle LAMP.....	11
b.	Préparation d'une base de données pour GLPI.....	11
2.	Installation GLPI.....	14
a.	Répertoire /etc/glpi.....	14
b.	Répertoire /var/lib/glpi.....	15
c.	Répertoire /var/log/glpi.....	15
d.	Création des fichiers de configurations.....	15
e.	Configuration Apache2.....	16
f.	Activation du site.....	17
g.	Utilisation de PHP8.2-FPM avec Apache2.....	18
h.	Installation de GLPI.....	19
3.	Installation du plugin GLPI inventory.....	24

1. Préparation du serveur avant installation

Afin de préparer notre serveur GLPI avant l'installation de celui-ci nous devons dans un premierement faire une mise à jour des paquets sur la machine linux.

```
sudo apt-get update && sudo apt-get upgrade
```

a. Installation du socle LAMP

Notre première grande étape consiste à installer les paquets du socle LAMP (Linux Apache2 MariaDB PHP) ainsi ces différents éléments nous permettrons de lancer correctement notre serveur GLPI.

```
sudo apt-get install apache2 php mariadb-server
```

Ensuite nous allons installer toutes les extensions nécessaires au bon fonctionnement de GLPI

```
sudo apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl  
php-zip php-bz2 php-imap php-apcu
```

Ces commandes vont permettre de récupérer les versions de ces extensions pour PHP 8.2

b. Préparation d'une base de données pour GLPI

Nous allons préparer MariaDB pour qu'il puisse héberger la base de données de GLPI. Nous devons donc exécuter la commande suivante :

```
sudo mysql_secure_installation
```

Vous serez invité à changer le mot de passe root, mais aussi à supprimer les utilisateurs anonymes, désactiver l'accès root à distance, etc...

```

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!

```

Nous allons donc ensuite créer une base de données dédiée pour GLPI pour un utilisateur qui lui sera dédié.

Connectez-vous à votre instance MariaDB :

```
sudo mysql -u root -p
```

Saisissez le mot de passe root de MariaDB, que vous venez de définir à l'étape précédente.

Nous continuerons par la création d'une Base de données « glpi-db » avec ainsi l'utilisateur « glpi_adm » et un mot de passe de votre choix :

```
CREATE DATABASE glpi-db ;
GRANT ALL PRIVILEGES ON glpi-db .* TO glpi_adm@localhost IDENTIFIED BY "MotDePasseRobuste";
FLUSH PRIVILEGES;
EXIT
```

Ce qui nous donne :

```
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.11.3-MariaDB-1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE glpi-db
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON glpi-db .* TO glpi_adm@localhost IDENTIFIED BY
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT
Bye
glpi_adm@SRV-GLPI:~$
```

2. Installation GLPI

Pour l'installation de GLPI, nous devons aller sur le site de GLPI et télécharger une version au choix de GLPI. Il est téléchargeable à cette adresse :

<http://glpi-project.org/?article3&lang=fr>

La version de GLPI utilisé pour le téléchargement dans cette procédure est la 10.0.15.

Ainsi pour la télécharger nous devons exécuter cette commande :

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.15/glpi-10.0.15.tgz
```

Puis, nous allons exécuter la commande ci-dessous pour décompresser l'archive .tgz dans le répertoire "/var/www/", ce qui donnera le chemin d'accès "/var/www/glpi" pour GLPI.

```
sudo tar -xzf glpi-10.0.15.tgz -C /var/www/
```

Nous allons donc définir l'utilisateur "www-data" correspondant à Apache2, en tant que propriétaire sur les fichiers GLPI.

```
sudo chown www-data /var/www/glpi/ -R
```

Ensuite, nous allons devoir créer plusieurs dossiers et sortir des données de la racine Web (/var/www/glpi) de manière à les stocker dans les nouveaux dossiers que nous allons créer. Ceci va permettre de faire une installation sécurisée de GLPI, qui suit les recommandations de l'éditeur.

a. Répertoire /etc/glpi

Pour commencer nous allons créer le répertoire « /etc/glpi » qui va recevoir les fichiers de configuration de GLPI et donner les autorisations à www-data

```
sudo mkdir /etc/glpi  
sudo chown www-data /etc/glpi/
```

Puis déplacer le répertoire "config" de GLPI vers ce nouveau dossier :

```
sudo mv /var/www/glpi/config /etc/glpi
```

b. Répertoire /var/lib/glpi

Répetons la même opération avec la création du répertoire « /var/lib/glpi »

```
sudo mkdir /var/lib/glpi  
sudo chown www-data /var/lib/glpi/
```

Ainsi nous déplacerons dans celui-ci le dossier « files » qui contient la majorité des fichiers de GLPI (css, pluging,etc)

```
sudo mv /var/www/glpi/files /var/lib/glpi
```

c. Répertoire /var/log/glpi

Terminons par la création du répertoire "/var/log/glpi" destiné à stocker les journaux de GLPI.

```
sudo mkdir /var/log/glpi  
sudo chown www-data /var/log/glpi
```

d. Création des fichiers de configuration

Nous devons configurer GLPI pour qu'il sache où aller chercher les données.

Premier fichier :

Exécuter cette commande

```
sudo nano /var/www/glpi/inc/downstream.php
```

Puis écrivez :

```
<?php  
define('GLPI_CONFIG_DIR', '/etc/glpi/');  
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {  
    require_once GLPI_CONFIG_DIR . '/local_define.php';  
}
```

Deuxième fichier :

Exécuter cette commande :

```
sudo nano /etc/glpi/local_define.php
```

Puis écrivez :

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi/files');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

e. Configuration Apache2

Nous allons créer un nouveau fichier de configuration qui va permettre de configurer le VirtualHost dédié à GLPI. Dans mon cas, le fichier s'appelle "assumer.local.conf" en référence au nom de domaine choisi pour accéder à GLPI.

Veuillez exécuter cette commande :

```
sudo nano /etc/apache2/sites-available/support.it-connect.tech.conf
```

Puis écrivez :

```
<VirtualHost *:80>
    ServerName assumer.local

    DocumentRoot /var/www/glpi/public

    # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving
multiple applications),
    # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the
GLPI directory itself.
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On

        # Redirect all requests to GLPI router, unless file exists.
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
</VirtualHost>
```

Résultat :

```
GNU nano 7.2 /etc/apache2
<VirtualHost *:80>
  ServerName assurmer.local

  DocumentRoot /var/www/glpi/public

  # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is se
  # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT
  # Alias "/glpi" "/var/www/glpi/public"

  <Directory /var/www/glpi/public>
    Require all granted

    RewriteEngine On

    # Redirect all requests to GLPI router, unless file exists.
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^(.*)$ index.php [QSA,L]
  </Directory>
</VirtualHost>
```

Une fois la configuration terminée, enregistrez le fichier

f. Activation du site

Pour activer notre site dans Apache2 il nous suffit d'exécuter cette commande :

```
sudo a2ensite assurmer.local.conf
```

Afin de rendre notre configuration parfaite nous devons désactiver le site par défaut puisque celui-ci est inutile :

```
sudo a2dissite 000-default.conf
```

Veuillez activer le module « rewrite » pour les règles de réécriture utilisé précédemment dans le fichier de configuration du VirtualHost :

```
sudo a2enmod rewrite
```

Enfin, il ne nous reste plus qu'à redémarrer le service Apache2 en utilisant la commande suivante :

```
sudo systemctl restart apache2
```

g. Utilisation de PHP8.2-FPM avec Apache2

Il est recommandé d'utiliser PHP-FPM car il est plus performant et se présente comme un service indépendant.

Pour cela nous commencerons par l'installation de PHP8.2-FPM avec la commande suivante :

```
sudo apt-get install php8.2-fpm
```

Ensuite nous activerons deux modules présents dans Apache2 suivie de l'activation de la configuration de PHP-FPM avant de redémarrer Apache2, utilisez donc la commande suivante :

```
sudo a2enmod proxy_fcgi setenvif  
sudo a2enconf php8.2-fpm  
sudo systemctl reload apache2
```

Pour configurer PHP-FPM pour Apache2, nous n'allons pas éditer le fichier "/etc/php/8.2/apache2/php.ini" mais plutôt ce fichier :

```
sudo nano /etc/php/8.2/fpm/php.ini
```

Dans ce fichier, recherchez l'option "session.cookie_httponly" et indiquez la valeur "on" pour l'activer, afin de protéger les cookies de GLPI.

```
; Whether or not to add the httpOnly flag to the cookie, which  
makes it  
; inaccessible to browser scripting languages such as  
JavaScript.  
; https://php.net/session.cookie-httponly  
session.cookie_httponly = on
```

Enregistrer et appliquer les modifications en redémarrant PHP-FPM :

```
sudo systemctl restart php8.2-fpm.service
```

Pour finir, nous devons modifier notre VirtualHost pour préciser à Apache2 que PHP-FPM doit être utilisé pour les fichiers PHP

Pour cela utiliser la commande suivante :

```
<FilesMatch \.php$>  
    SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"  
</FilesMatch>
```

Voici un exemple :

```
GNU nano 7.2 /etc/apache2
<VirtualHost *:80>
    ServerName assurmer.local

    DocumentRoot /var/www/glpi/public

    # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is se
    # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On

        # Redirect all requests to GLPI router, unless file exists.
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>

    <FilesMatch \.php$>
        SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
    </FilesMatch>
</VirtualHost>
```

Une fois effectué, relancer Apache2 avec cette commande :

```
sudo systemctl restart apache2
```

h. Installation de GLPI

Pour effectuer l'installation de GLPI, veuillez-vous rendre sur votre navigateur web afin de pouvoir accéder à l'adresse GLPI, l'adresse utilisé est déclarer dans le fichier de configuration Apache2

Dans notre cas, l'adresse à utiliser est : « assurmer.local »

Une fois sur la page web, nous devons choisir la langue de notre choix, bien sur tout l'installation s'effectue par interface graphique.



Une fois la langue choisie appuyez sur « ok »

C'est une installation, nous devons donc choisir « installer »



Nous avons un état des extensions et paramétrage nécessaire pour l'installation de GLPI. Continuez

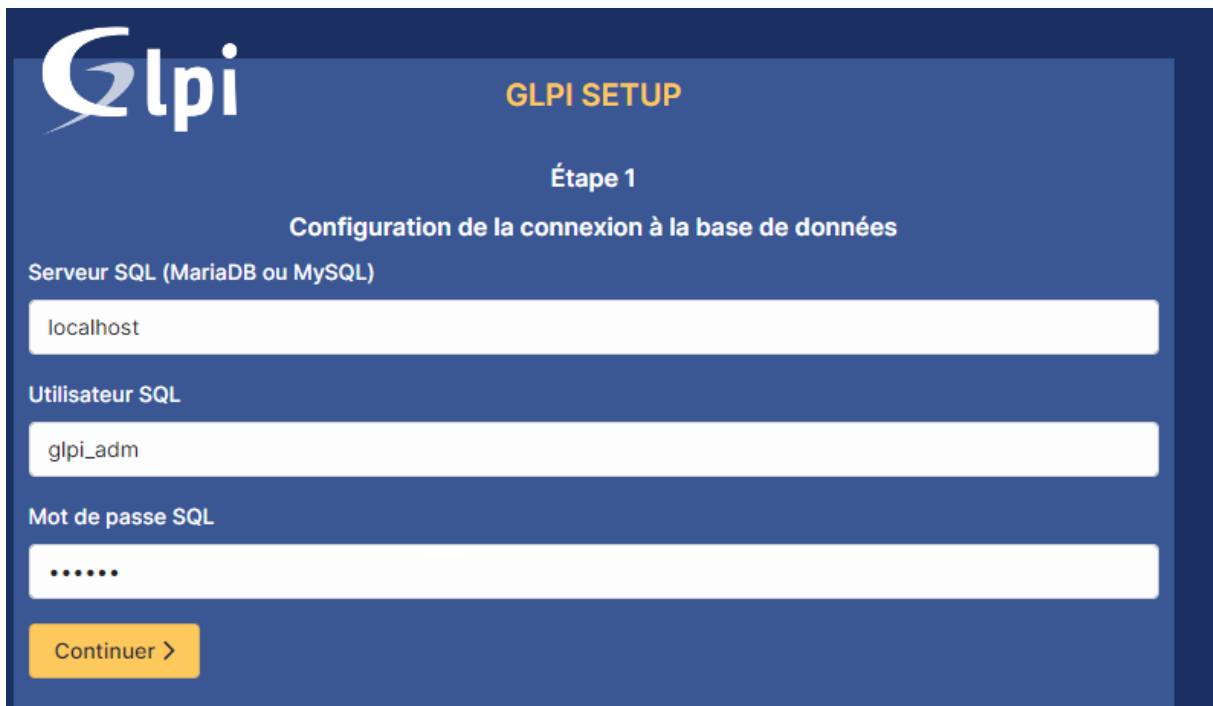
GLPI SETUP

Étape 0

Vérification de la compatibilité de votre environnement avec l'exécution de GLPI

TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysqli extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
Requis gd extension <i>Requis pour le traitement des images.</i>	✓
Requis intl extension <i>Requis pour l'internationalisation.</i>	✓
Requis zlib extension <i>Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.</i>	✓
Requis Libsodium ChaCha20-Poly1305 constante de taille <i>Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.</i>	✓
Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓
Suggéré Version de PHP supportée <i>Une version officiellement supportée de PHP devrait être utiliser pour bénéficier des correctifs de sécurité et de bogues.</i>	✓
Suggéré Configuration sécurisée du dossier racine du serveur web <i>La configuration du dossier racine du serveur web devrait être '/var/www/glpi/public' pour s'assurer que les fichiers non publics ne peuvent être accessibles.</i>	✓
Suggéré Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.</i>	✓

Toutes les informations étant enregistrer dans GLPI, il faut donc saisir l'adresse du serveur MySQL, ainsi qu'un utilisateur et un mot de passe, afin de se connecter à celle-ci.



The screenshot shows the GLPI Setup interface. At the top left is the GLPI logo. To the right, it says "GLPI SETUP". Below that, "Étape 1" (Step 1) is centered. The main heading is "Configuration de la connexion à la base de données". There are three input fields: "Serveur SQL (MariaDB ou MySQL)" with "localhost" entered, "Utilisateur SQL" with "glpi_adm" entered, and "Mot de passe SQL" with masked characters "*****". At the bottom left is a yellow button labeled "Continuer >".

Nous devons choisir la base de données "**glpi-db**" que nous avons créer



The screenshot shows the GLPI Setup interface for Step 2. At the top left is the GLPI logo. To the right, it says "GLPI SETUP". Below that, "Étape 2" (Step 2) is centered. The main heading is "Test de connexion à la base de données". A green checkmark icon is followed by the text "Connexion à la base de données réussie". Below this, the text "Veuillez sélectionner une base de données :" is centered. There is a section titled "Créer une nouvelle base ou utiliser une base existante :" with a radio button and an empty input field. Below that, the option "glpi-db" is selected, indicated by a yellow radio button and a red arrow pointing to it. At the bottom left is a yellow button labeled "Continuer >".

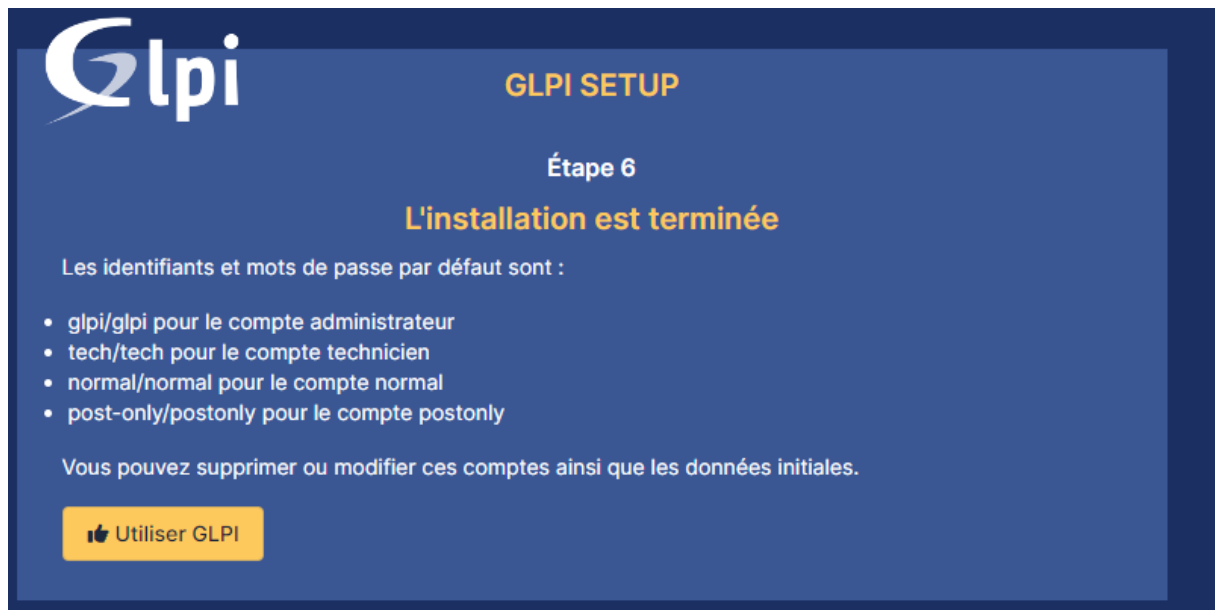
Appuyer sur « continuer » pour poursuivre



Poursuivez en appuyant sur « continuer »

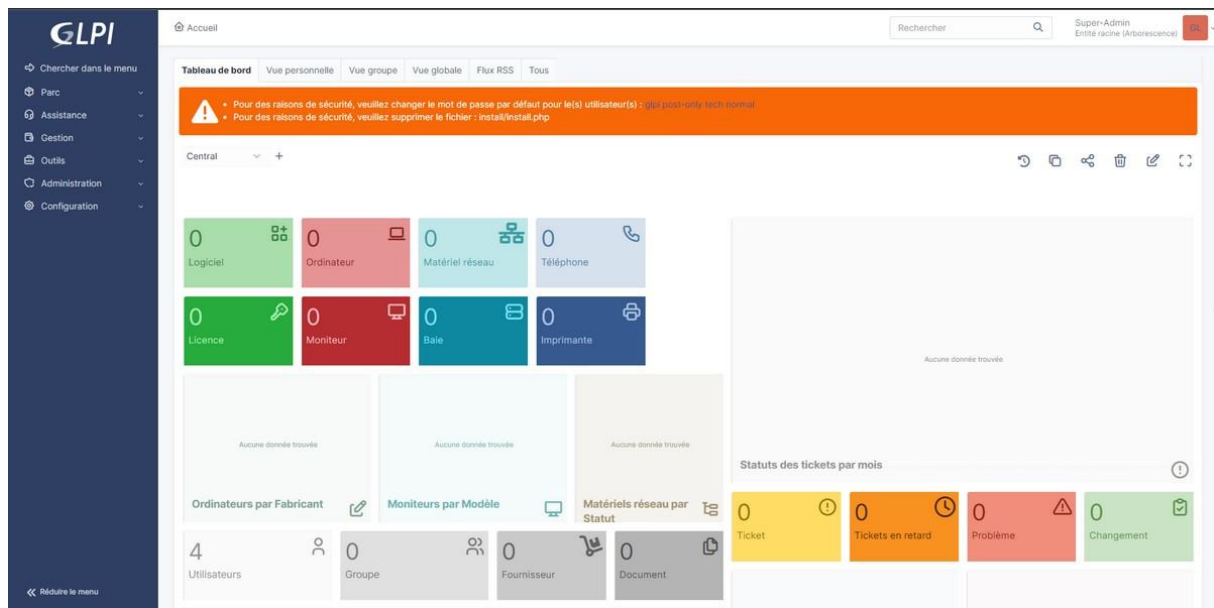


Félicitation, vous venez d'installer GLPI, poursuivez en appuyant sur « Utiliser GLPI »



Comme le précise la dernière étape, le compte **administrateur** par défaut est "glpi/glpi" !

Nous allons donc nous connecter avec le compte "glpi" et le mot de passe "glpi".



Bienvenue sur votre nouveau serveur GLPI !

3. Installation du plugin GLPI inventory

GLPI Inventory est un projet libre dont les fonctionnalités principales sont l'inventaire du matériel, le télédéploiement et la découverte réseau et complète la gestion de parc et l'helpdesk de l'outil GLPI.

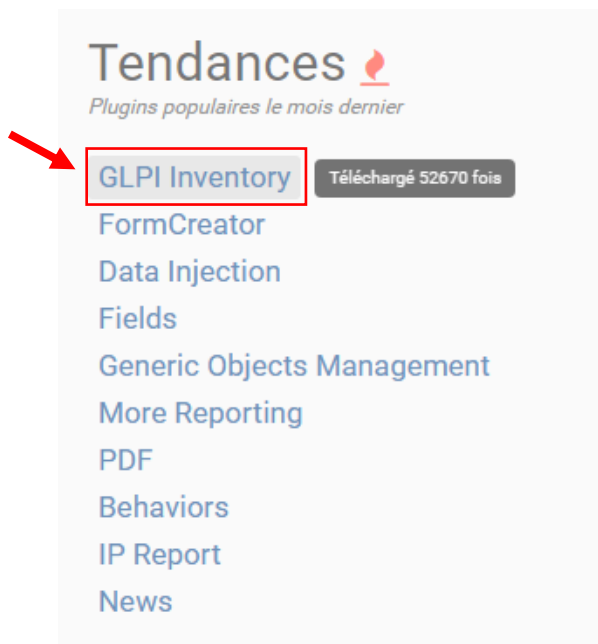
Il apporte différentes fonctionnalités à GLPI tel que :

1. Communication avec les agents d'inventaire et de découverte.
2. Gestion et planifications des tâches.
3. Règles centralisées pour ces plugins d'import de matériel.
4. Gestion du matériel inconnu

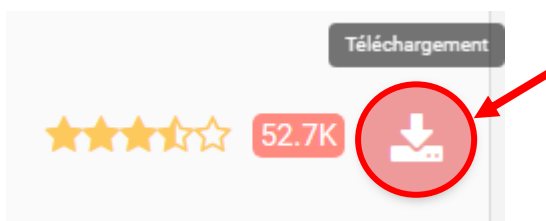
Pour installer le plugin GLPI inventory, veuillez-vous rendre sur ce lien :

<https://plugins.glpi-project.org/#/>

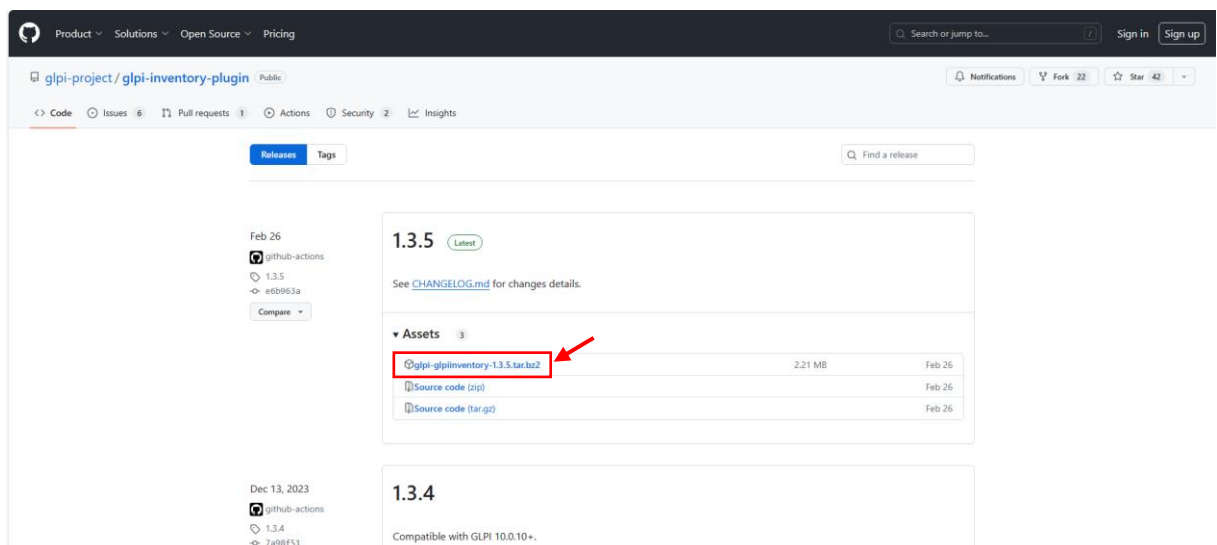
Une fois sur la page GLPI, veuillez sélectionner « GLPI Inventory »



Appuyer ensuite sur le bouton « Télécharger »



Une fois le bouton de téléchargement cliqué, une réorientation vers une page GitHub va être effectuée



Sélectionner la version de votre choix puis télécharger là, dans le cas de la procédure nous installerons la version 1.3.5 du plugin.

Une fois le téléchargement terminé, décompresser-le avec la commande :

```
tar -xvzf glpi-glpiinventory-1.3.5.tar.bz2
```

Puis Déplacer le dans le dossier « plugin » via le chemin suivant :

```
sudo mv glpiinventory/ /var/www/glpi/plugins
```

Ainsi il nous suffit ensuite de regagner notre page GLPI et de naviguer vers l'onglet « configuration » puis « plugins »



GLPI

Chercher dans le menu

Parc

Assistance

Gestion

Outils

Administration

1

Configuration

Intitulés

Composants

Notifications

Niveaux de services

Générale

Unicité des champs

Actions automatiques

Authentification

Collecteurs

Liens externes

2

Plugins

Réduire le menu

Filterer la liste des plugins

GI

GLPI Inventory

AGPLv3+

Teclib'

1.3.5

Installer

Votre plugin ici ? Contactez-nous. ✉

Nous pouvons donc retrouver notre plugin dans la liste des plugins installer, or il ne trouve pas encore télécharger, nous devons donc le télécharger dans GLPI.

Pour ce faire il suffit juste de cliquer sur le petit dossier en fin de case

→

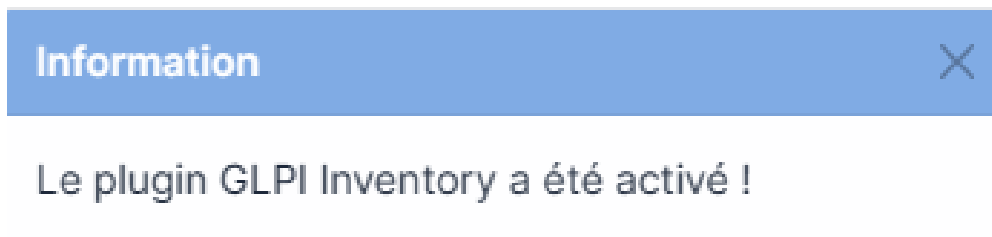
→

Information

Le plugin GLPI Inventory a été installé !

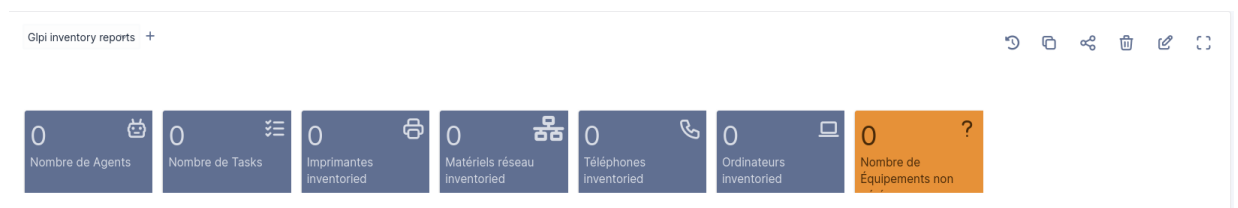
Souhaitez-vous l'activer ?

Il vous est maintenant demandé si vous voulez l'activer, nous le souhaitons, veuillez donc appuyez sur activer



Félicitation, vous venez de terminer l'installation du plugin GLPI inventory, vous pouvez maintenant créer des modules, ajouter des appareils, créer des tâches, vérifier les Plages adresse mais avant tout, effectuer un inventaire.

En effet en voyageant dans l'onglet « GLPI Inventory » incluse dans « Administration » vous pourrais y trouvez un rapport complet de vos appareils :



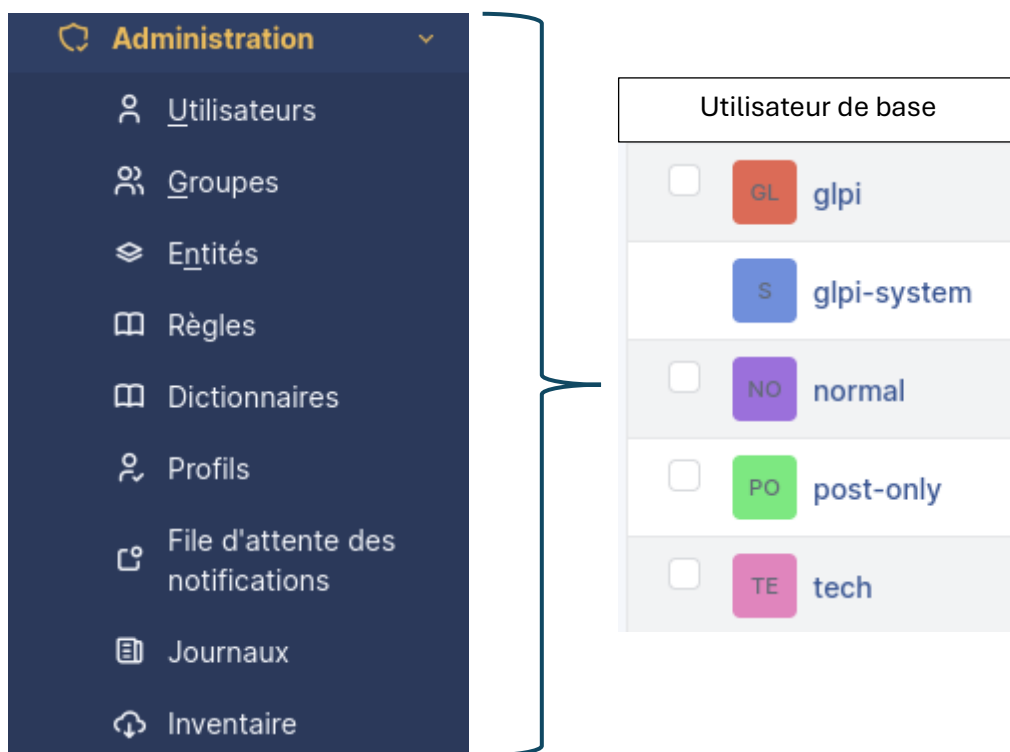
Il suffit d'ajouter vos appareil et tous est enfin près à son utilisation !

Tests et création de tickets

Afin de promouvoir la bonne expérience utilisateur, un test et création de ticket est nécessaire, pour ce faire nous utiliserons un compte « utilisateur » et un compte « technicien » ainsi « l'utilisateur » aura la charge de la création du ticket et le « technicien » en charge de la résolution de celui-ci.

Nous allons donc créer les utilisateurs « Tech » et « Utilisateur »

Pour ce faire il vous suffit d'aller dans l'onglet « Administration » puis « Utilisateurs »



En haut de page nous devons trouver un bouton « ajouter » [+ Ajouter](#)

Il nous suffit d'insérer les différentes informations relatives au compte, c'est à dire son (nom, prénom, mot de passe et habilitations).

Dans notre cas nous allons créer le compte « utilisateur »

1. Création du compte « Utilisateur »

Identifiant	utilisateur
Nom de famille	utilisateur
Prénom	utilisateur
Mot de passe	
Confirmation mot de passe	

Nous attribuons l'habilitation « Self-Service » a l'utilisateur, puisque celui-ci est limité, il pourra ainsi effectuer seulement l'envoi de demande et la création de ticket

Profil par défaut Self-Service ▼

Afin de sauvegarder notre utilisateur nous devons appuyer sur le bouton « sauvegarder » en bas de page

 **Mettre à la corbeille**

 **Sauvegarder**

Nous pouvons donc vérifier sa création dans l'annuaire utilisateur et nous connecter :

☐ GL glpi	Connexion à votre compte Identifiant utilisateur Mot de passe •••••••••• Source de connexion Base interne GLPI ▼ ☒ Se souvenir de moi Se connecter
☐ S glpi-system	
☐ NO normal	
☐ PO post-only	
☐ TE tech	
☐ UU utilisateur	

1. Création du compte « technicien »

Il existe déjà un compte « tech » de base sur GLPI or nous allons en recréer un nouveau.

Identifiant	technicien
Nom de famille	technicien
Prénom	technicien
Mot de passe	
Confirmation mot de passe	

Nous attribuons l'habilitation « Technicien » au technicien puisque celui-ci est dédié à un utilisateur qui gère les tickets, c'est un profil avec pouvoir

Profil par défaut

Technician ▼

Afin de sauvegarder notre technicien tout comme l'utilisateur nous devons appuyer sur le bouton « sauvegarder » en bas de page

 Mettre à la corbeille

 Sauvegarder

Nous pouvons donc vérifier sa création dans l'annuaire utilisateur et nous connecter :

☐		glpi
		glpi-system
☐		normal
☐		post-only
☐		technicien
☐		utilisateur

Connexion à votre compte

Identifiant

Mot de passe

Source de connexion

☒ Se souvenir de moi

Se connecter

En tant qu'utilisateur j'ai l'accès à la création de ticket pour signaler un problème ou effectuer une demande, pour ce faire je vais donc dans l'onglet « Créer un ticket »

[+ Créer un ticket](#)

Ainsi il suffit à l'utilisateur d'effectuer sa demande, dans le cas de notre test nous avons rédigé un ticket en « incident » signalant un problème d'ordinateur

Interface simplifiée - GLPI

Non sécurisé | 192.168.25.100/glpi/front/tracking.injector.php

Accueil

UT

GLPI

Accueil

+ Créer un ticket

Tickets

Réservations

Foire aux questions

« Réduire le menu »

Description de la demande ou de l'incident

Type: Incident

Catégorie: -----

Urgence: Haute

Éléments associés: +

Observateurs:

Titre: Problème ordinateur

Description: Paragraphe a l'aide

Fichier(s) (40 Mio maximum)

Il nous suffit simplement de soumettre la demande en cliquant sur le bouton « Soumettre la demande »

[+ Soumettre la demande](#)

Nous pouvons voir que la création du ticket a belle et bien été prise en compte sur le serveur GLPI

ID	TITRE	STATUT	DERNIÈRE MODIFICATION ▼	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE	TTR
4	Problème ordinateur	● Nouveau	2024-05-02 21:14	2024-05-02 21:14	Haute	utilisateur			

15 ▼ lignes / page De 1 à 1 sur 1 lignes

Maintenant nous passons technicien sur un autre ordinateur en charge de la gestion et résolution de tickets, nous pouvons donc constater que le ticket créer précédemment apparais dans la liste des tickets

GLPI

Home / Assistance / Tickets

Search...

Technician
Entité racine (tree structure)

----- Characteristics - Status - Is - Not solved -

rule global rule group Search

Actions

ID	TITRE	STATUS	LAST UPDATE	OPENING DATE	PRIORITY	REQUESTER - REQUESTER	ASSIGNED TO - TECHNICIAN	CATEGORY	TIME TO RESOLVE
4	Problème ordinateur	New	2024-05-02 21:14	2024-05-02 21:14	High	utilisateur			

20 rows / page Showing 1 to 1 of 1 rows

192.168.25.100/glpi/front/central.php

Taper ici pour rechercher

21:30 02/05/2024

Nous pouvons donc clôturer le ticket effectuer par l'utilisateur

The screenshot shows a ticket management interface. On the left is a sidebar with a 'Ticket' section and a list of categories: Statistics, Approvals, Knowledge base, Items, Costs, Projects, Project tasks, Problems, Changes, and All. The main area displays two tickets. The first ticket, 'Problème ordinateur', is created 9 minutes ago by 'utilisateur' and last updated 'Just now' by 'tech'. It has a status of 'Solved' and a priority of 'High'. The second ticket, 'problème résolue', is created 'Just now' by 'tech' and has a status of 'Solved' and a priority of 'High'. The right sidebar shows the 'Ticket' details, including 'Opening date' (2024-05-02 21:14:15), 'Type' (Incident), 'Category' (-----), 'Status' (Solved), 'Request source' (Helpdesk), 'Urgency' (High), 'Impact' (Medium), and 'Priority' (High). The 'Actors' section shows the 'Requester' as 'utilisateur' and the 'Observer' as 'tech'. The bottom of the interface has an 'Answer' button and a 'Save' button.

Enfin, il se retrouve dans la section des ticket « solved » ce qui désigne qu'il a bien été résolu

ID	TITLE	STATUS	LAST UPDATE	OPENING DATE	PRIORITY	REQUESTER - REQUESTER	ASSIGNED TO - TECHNICIAN	CATEGORY	TIME TO RESOLVE
4	Problème ordinateur	Solved	2024-05-02 21:25	2024-05-02 21:14	High	utilisateur i			

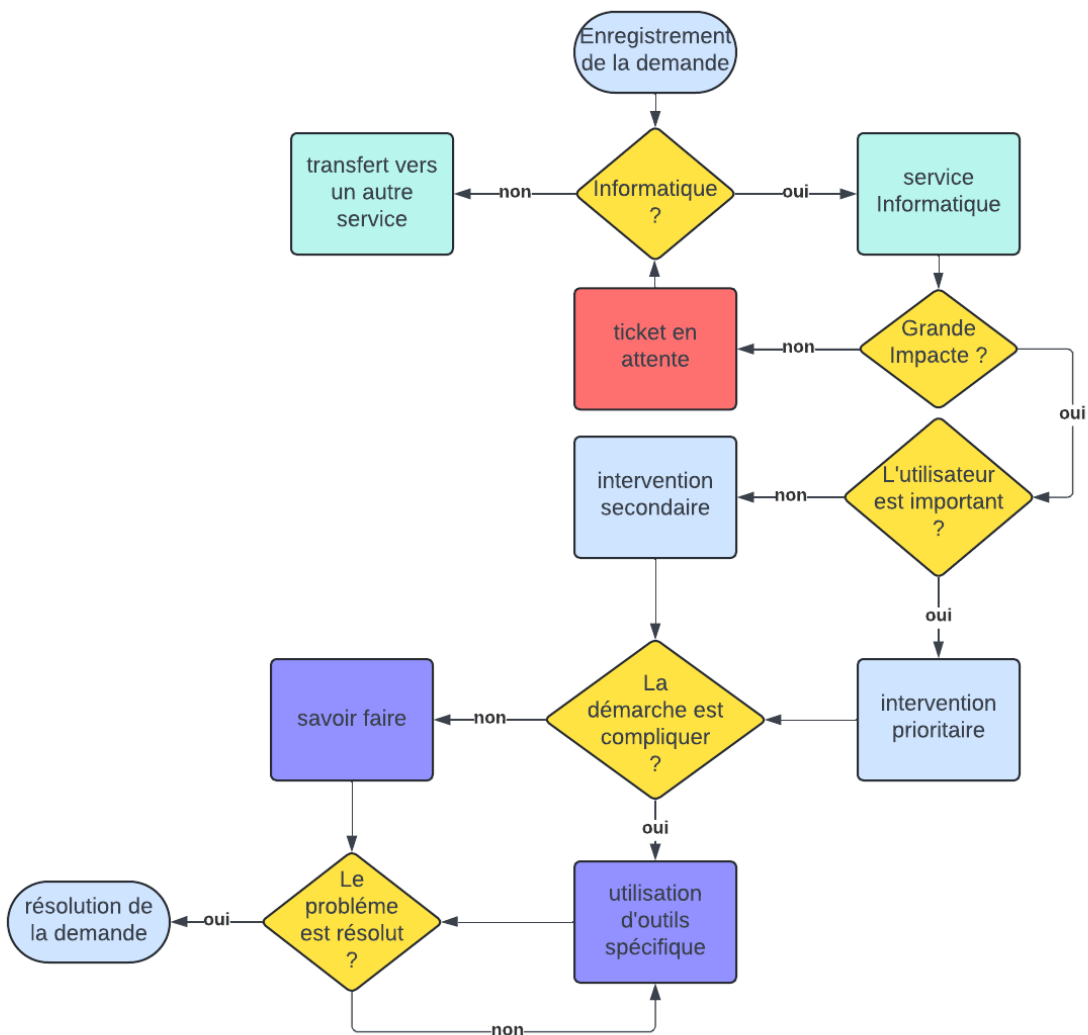
Showing 1 to 1 of 1 rows

Félicitation, Le Test et une réussite, l'échange entre « utilisateur » et « technicien » est fonctionnel !

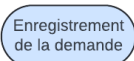


« Nombre de ticket effectuer sur une période déterminé »

Logigramme du cycle de vie d'un ticket



Etape 1 : Enregistrement de la demande :



Etape 2 : Catégorisation de la demande :



Etape 3 : Hiérarchisation de la demande :



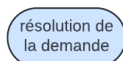
Etape 4 : Affectation de la demande :



Etape 5 : Résolution ou réalisation :



Etape 6 : Fermeture de la demande :



Resolution / demande



Différents Services



Question théorique



Mise en attente



Types D'intervention



Methodes d'utilisation

Etape 1 : Enregistrement de la demande

- Le client soumet sa demande sur le service d'assistance GLPI
- La demande est enregistrée dans le système de ticket

Etape 2 : Catégorisation de la demande

- Affectation du ticket au services correspondant
- Si le ticket ne relève pas des compétences du service visé, il sera transféré vers le service compétant.

Etape 3 : Hiérarchisation de la demande

- L'impact du ticket est important, la réalisation du ticket est prioritaire :
 - L'utilisateur est important, la demande devient une priorité
 - L'utilisation n'est pas importante, la demande est secondaire
- L'impact du ticket est léger :
 - Mise en attente temporaire du ticket

Etape 4 : Affectation de la demande

- La démarche est simple, Les compétences nécessaires dans la résolution sont acquises :
 - Utilisation du savoir-faire du technicien
- La démarche est compliquée, les compétences nécessaires dans la résolution ne sont pas suffisantes :
 - Utilisation d'outils spécifique par le technicien dans la résolution du ticket

Etape 5 : Résolution ou réalisation

- La résolution du problème c'est effectué sans difficulté :
 - Le ticket est résolu
- La résolution du ticket n'a pas abouti correctement :
 - Utilisation d'outils spécifique par le technicien dans la résolution du ticket

Etape 6 : Fermeture de la demande

- Fermeture de la demande utilisateur
- Résolution du ticket effectué

Procédure Utilisateur GLPI



Procédure d'utilisation de GLPI pour les utilisateurs (avec démo)

Introduction

GLPI est un outil de gestion de parc informatique open source qui permet de gérer les inventaires matériels et logiciels, les tickets d'assistance, les contrats de maintenance et bien plus encore. Ce guide a pour but de vous familiariser avec les fonctionnalités de base de GLPI en tant qu'utilisateur.

Se connecter à GLPI

1. Ouvrez votre navigateur web et accédez à l'URL de votre portail GLPI. Cette URL vous a été fournie par votre administrateur système.
2. Saisissez vos identifiants de connexion GLPI (nom d'utilisateur et mot de passe) et cliquez sur le bouton "Connexion".

Interface utilisateur

Une fois connecté, vous serez redirigé vers le tableau de bord principal de GLPI. Ce tableau de bord présente une vue d'ensemble des informations clés de votre parc informatique, telles que le nombre d'ordinateurs, de tickets d'assistance et de contrats de maintenance ouverts.

Gestion des tickets d'assistance

Les tickets d'assistance sont utilisés pour signaler et suivre les problèmes informatiques. Voici comment créer un ticket d'assistance :

1. Cliquez sur l'onglet "Assistance" dans le menu principal.
2. Cliquez sur le bouton "Créer un ticket".
3. Sélectionnez le type de ticket approprié (par exemple, problème matériel, problème logiciel, demande d'assistance).
4. Renseignez les informations requises sur le ticket, telles que le titre, la description du problème, la priorité et le demandeur.
5. Cliquez sur le bouton "Créer".

Votre ticket sera créé et attribué à un technicien approprié. Vous recevrez des notifications par e-mail concernant le statut de votre ticket.

Consultation de la base de connaissances

La base de connaissances GLPI contient des articles et des solutions aux problèmes informatiques courants. Vous pouvez consulter la base de connaissances en cliquant sur l'onglet "Base de connaissances" dans le menu principal.

Personnalisation de votre profil

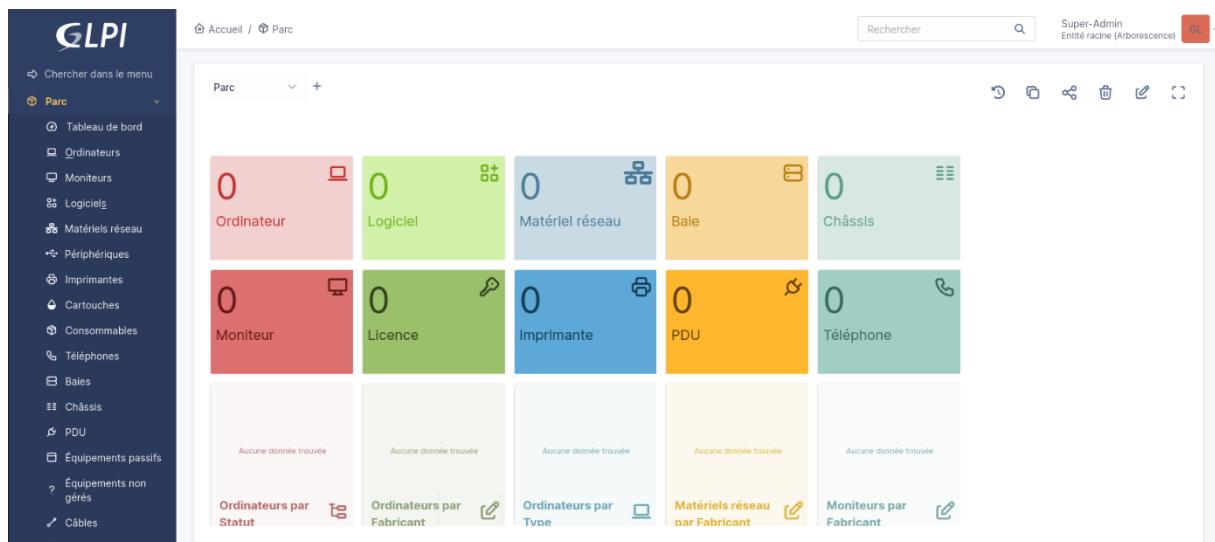
Vous pouvez personnaliser votre profil GLPI en cliquant sur votre nom d'utilisateur dans le coin supérieur droit de l'écran. Vous pouvez modifier vos informations personnelles, telles que votre nom, votre adresse e-mail et votre photo.

Conclusion

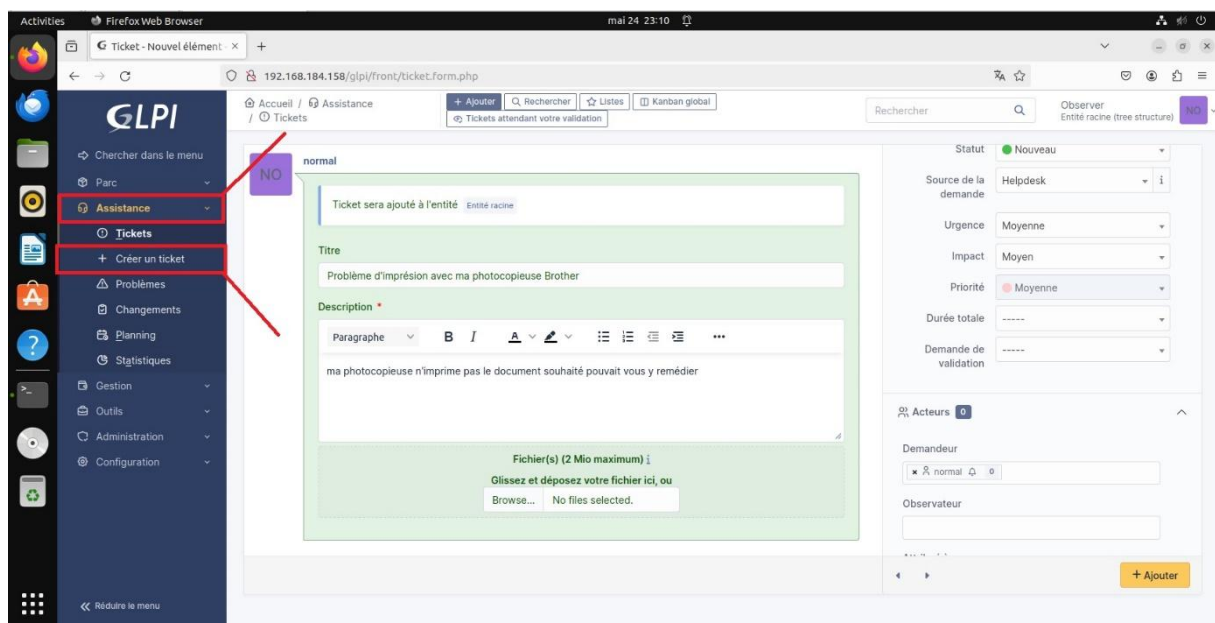
Ce guide vous a présenté les fonctionnalités de base de GLPI en tant qu'utilisateur. Pour plus d'informations, veuillez consulter la documentation officielle de GLPI <https://glpi-project.org/documentation/>.

Démonstrations :

- **Tableau de bord principal :**



- **Création d'un ticket d'assistance :**



1. Cliquez sur l'onglet "Assistance" dans le menu principal.
2. Cliquez sur le bouton "Créer un ticket".

3. Renseigner les détails du ticket : Remplissez les champs obligatoires dans le panneau Détails du ticket, en décrivant précisément le problème et sa catégorie.
4. Rédiger une description claire : Développez le problème dans la zone Description, en fournissant autant de détails que possible.

5. Renseignez les informations requises sur le ticket, telles que le titre, la description du problème, ainsi que des documents pertinent la priorité et le demandeur.

Exemple ci-dessous :

File Upload					
Name	Location	Size	Type	Accessed	
ipconfig	Documents/photocopier	92 bytes	Text	23:41	
images.jpeg	Pictures	7,8 kB	Image	23:22	
TP7	Documents			Yesterday	
TP7	Documents/TP7	7,6 kB	Program	13 mai	
tp7.sh	Downloads	6,7 kB	Program	13 mai	

Ticket

Date d'ouverture: 2024-05-24 14:30:00

Type: Demande

Catégorie: -----

Statut: ● Nouveau

Source de la demande: Helpdesk

1 Urgence: Moyenne

2 Impact: Moyen

3 Priorité: ● Moyenne

Durée totale: 0h25

Demande de validation: -----

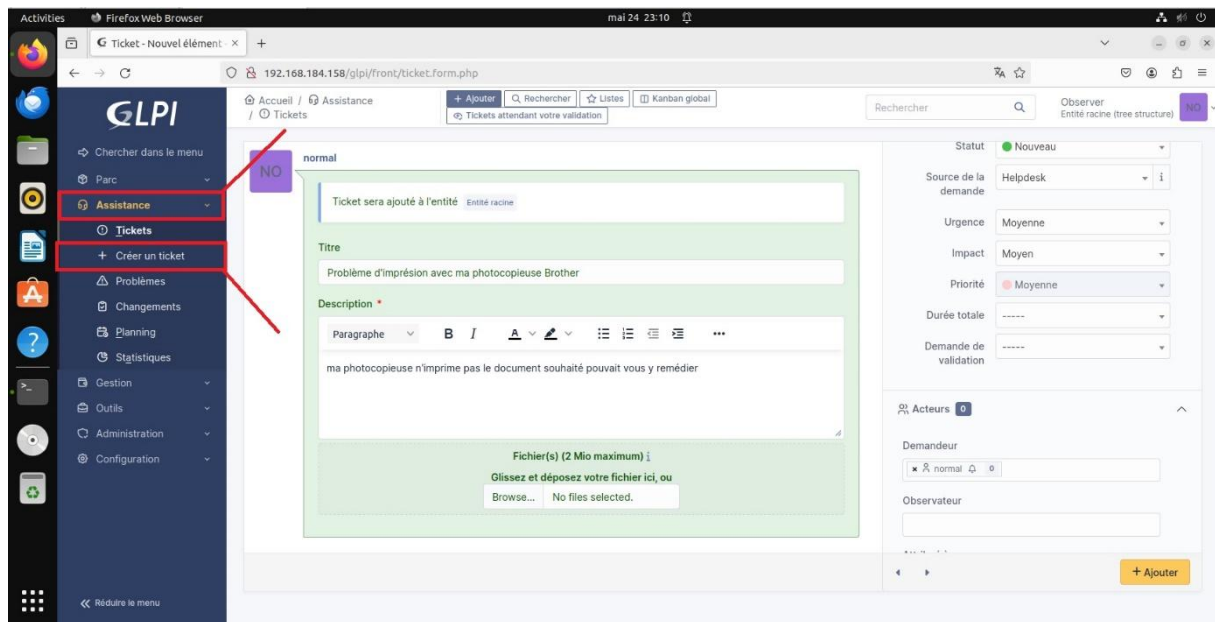
Utilisateur

Groupe

Ajouter

1. Évaluer l'urgence du problème : Évaluez la gravité et l'impact du problème que vous signalez.
2. Déterminer la priorité appropriée : Choisissez le niveau de priorité qui reflète le mieux l'urgence du problème.
3. Sélectionner le niveau de priorité : Cliquez sur le niveau de priorité correspondant dans le menu déroulant.

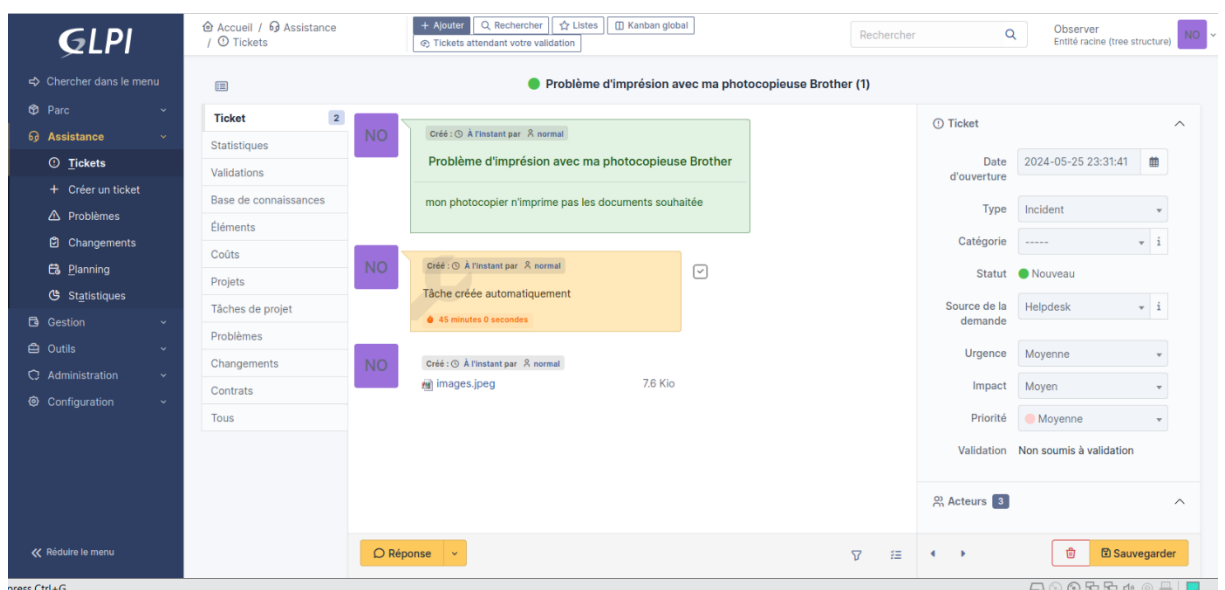
Une fois toutes les informations remplies vous pouvez cliquer sur ajouter en bas à droite pour envoyer votre demande



Facultatifs :

- Vous pouvez sélectionner une durée de temps dans laquelle devra être résolu votre problème dans un temps délimiter
- Vous pouvez aussi choisir les membres de l'équipe être observateur de votre ticket

Comme vous pouvez le voir le ticket a bien été créé pour l'utilisateur



Le technicien a bel est bien reçu le ticket

localhost/glipi/front/ticket.php

GLPI

Chercher dans le menu

Parc

Assistance

Tableau de bord

Tickets

+ Créer un ticket

Problèmes

Changements

Planning

Statistiques

Tickets récurrents

Changements récurrents

Gestion

Outils

Administration

Configuration

Réduire le menu

Accueil / Assistance / Tickets

+ Ajouter

Rechercher

Listes

Gabarits

Kanban global

Rechercher

Super-Admin
Entité racine (Arborescence)

1 Ticket

1 Tickets entrants

0 Tickets en attente

0 Tickets assignés

0 Tickets planifiés

0 Tickets résolus

0 Tickets fermés

Caractéristiques - Statut

est

Non résolu

Règle

Règle globale

(+) groupe

Rechercher

Actions

ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE	TTR
1	Problème d'impression avec ma photocopieuse Brother	Nouveau	2024-05-25 21:34	2024-05-25 23:31	Moyenne	normal			

20 lignes / page

De 1 à 1 sur 1 lignes