Alix JOURDAN
BTS SIO - SISR
Lycée Geoffroy Saint Hilaire
Académie de Versailles

Mairie de Arles

Synthèse du stage effectué du 06 janvier 2025 au 14 février 2025

SOMMAIRE :

INTRODUCTION :

Contexte Professionnel – Présentation Générale :

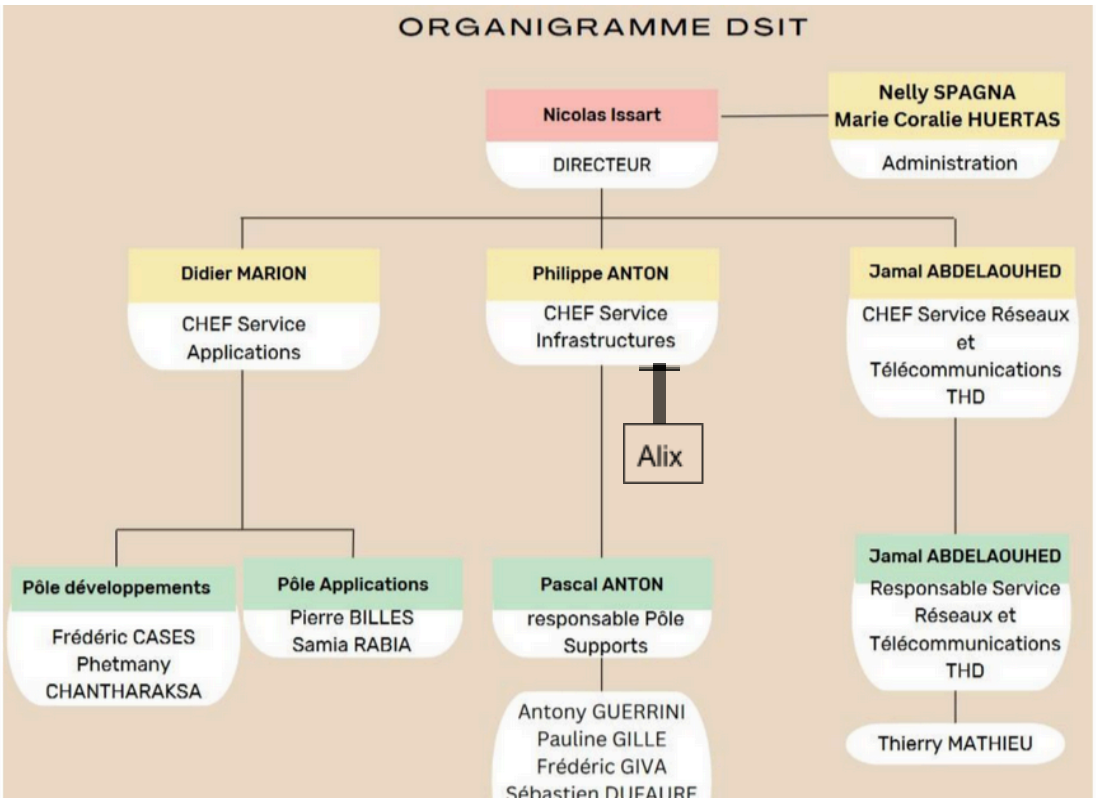
1/ Présentation de l'entreprise :

L'entreprise qui m'accueille est une mairie sous une collectivité territoriale de la région. Elle a un service qui est la Direction des Systèmes d'Information et de Télécommunications (DSIT) de la ville d'Arles. La DSIT joue un rôle central au sein de l'administration municipale. Elle est responsable de la gestion et de la supervision des technologies de l'information et des communications au sein de la municipalité. À ce titre, elle régule le trafic réseau de plusieurs communes et mairies avoisinantes. De plus, elle a déployé la gestion du réseau et l'installation de la fibre optique pour les entreprises. Son infrastructure réseau, vaste et disséminée à travers la ville, a été conçue pour renforcer la sécurité et prévenir aussi bien les cyberattaques que les menaces involontaires, tout en assurant une mise en œuvre optimale des solutions de télécommunication afin de répondre aux besoins des usagers.

ARLES
PATRIMOINE MONDIAL DE L'HUMANITÉ

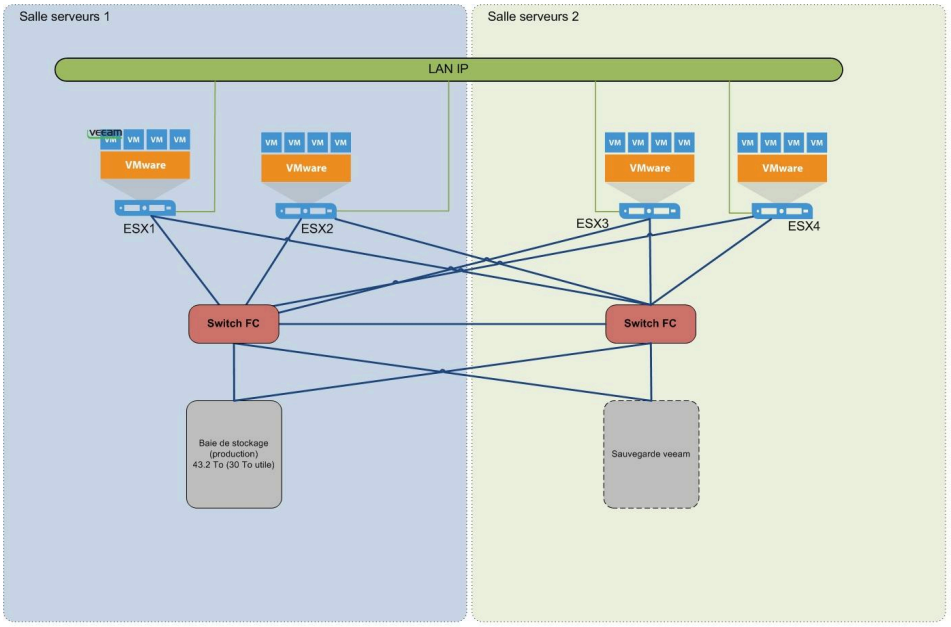
La DSIT est également chargée de maintenir et de développer l'infrastructure technologique de la ville, de mettre en place des systèmes informatiques et de communication performants, et de garantir la sécurité des données ainsi que des réseaux. Elle a également embauché un sous-traitant en tant que DPO, qui traite les données à caractère personnel, les références ainsi que toutes les données traitées par la mairie. De plus, la DSIT a mis en place une charte informatique et organise des formations pour sensibiliser les utilisateurs aux règles à respecter, conformément aux directives du DPO et au respect du RGPD.

Organigramme du service informatique :

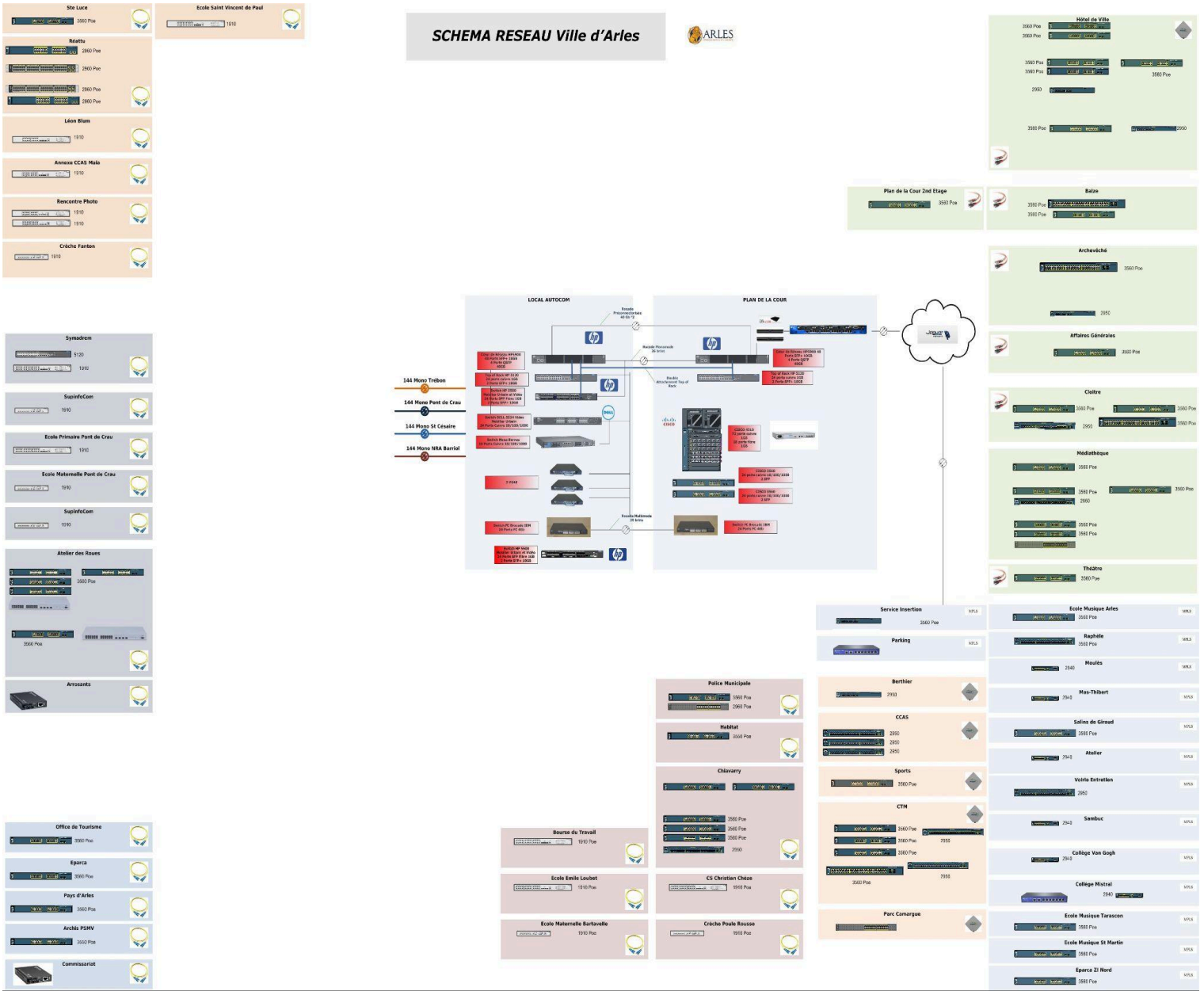


Architecture réseaux :

Voici les ESXi de la mairie d'Arles, répartis sur le switch et connectés au biais de stockage. Les ESXi sont directement connectés au proxy du domaine et redirigés vers le vSphere Client.



Architecture complète de la Mairie de Arles



1 / Contexte et présentation des missions du stage

Le stage s'est déroulé dans le cadre de ma deuxième année d'études supérieures au sein du BTS SIO (Services Informatiques aux Organisations), formation dispensée au Lycée Geoffroy-Saint-Hilaire à Étampes. D'une durée de 1 mois et 2 semaines, cette deuxième expérience de stage avait pour objectif de mettre en pratique les connaissances acquises au cours de l'année.

Dans le cadre de mes études, je me spécialise dans la cybersécurité des infrastructures réseau, des systèmes et des services informatiques, une spécialisation nommée SISR (Solutions d'Infrastructures, Systèmes et Réseaux). C'est pourquoi j'ai choisi un stage en lien avec cette spécialisation, afin de renforcer mes connaissances et de mettre en application la base théorique étudiée en cours.

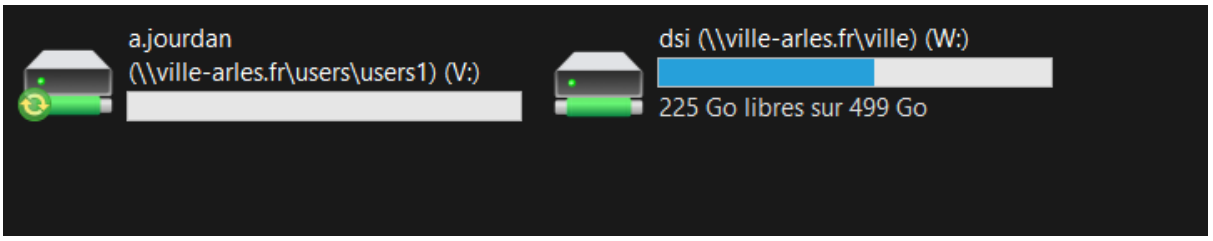
L'entreprise qui m'a accueillie est la Mairie d'Arles. Elle m'a confié plusieurs missions au cours de ma période de stage, telles que la gestion des supports avec le logiciel GLPI pour le suivi des tickets et la gestion des utilisateurs dans l'infrastructure réseau. J'ai également participé à la mise en place d'une segmentation dans l'infrastructure réseau, ainsi qu'au paramétrage du proxy pour la gestion des droits d'accès. Enfin, j'ai pris part à l'installation du matériel physique réseau dans la région.

2/ Environnement de Travail :

Je travaille sous Windows 11 Professionnel sur un PC portable.

Plusieurs sessions ont été créées pour moi :
une en tant qu'utilisateur et deux autres en tant qu'administrateurs. La première session administrateur est dédiée à la gestion de l'Active Directory et des serveurs, tandis que la deuxième est utilisée pour des tâches administratives spécifiques, telle que l'installation d'applications sur les machines.

Sur la session, on m'a connecté le lecteur réseau personnel qui est le V et celui du service DSIT qui est le W.

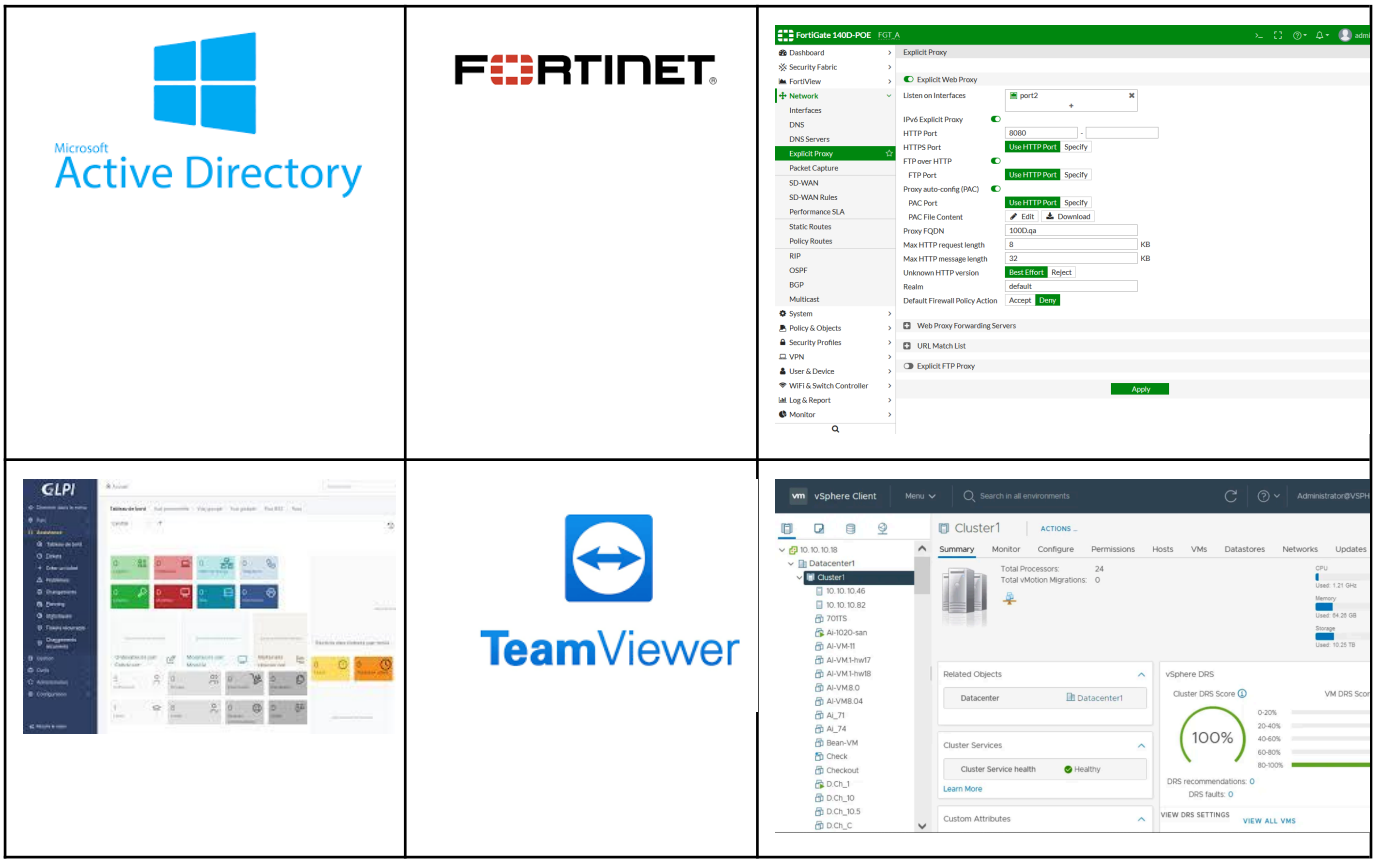


Matériels et applications utilisés dans l'entreprise :

Dans cette partie, j'explique le matériel utilisé par la mairie d'Arles et les applications employées pour la gestion.

Le service infrastructure a sécurisé le système réseau de la mairie. Le service support gère les tickets et les interventions :

- **Active Directory** : Référence les utilisateurs et machines du domaine de la mairie. Connecté à GLPI et Office 365 pour la gestion des licences et droits des utilisateurs.

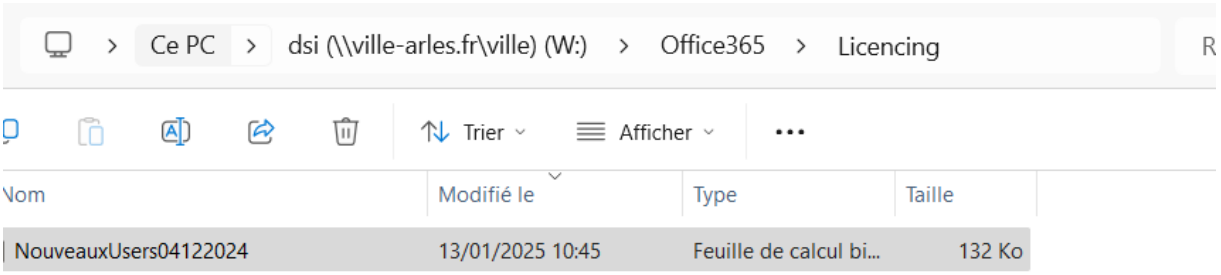


- **Fortinet** : Utilisé pour configurer les pare-feux et les VLANs, que ce soit par application ou physiquement via des switchs.
- **ESXi** : Deux solutions. Hyperviseur vSphere Client pour quelques utilisateurs, et Wallix pour configurer les paramètres des utilisateurs selon les machines qu'ils doivent voir

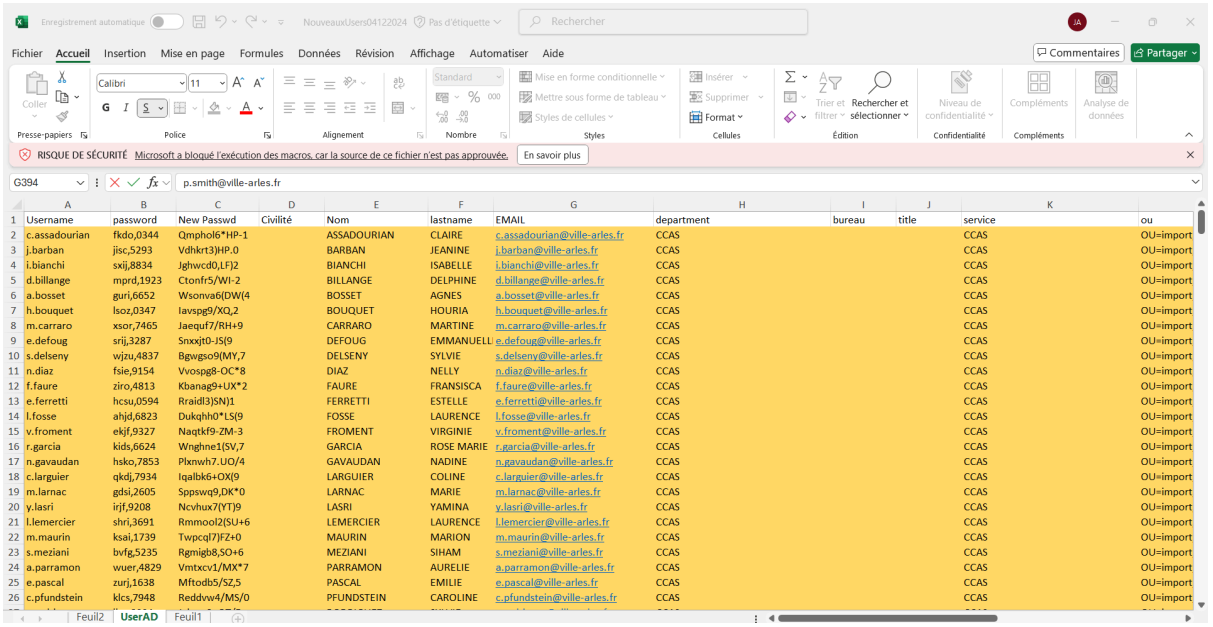
Mission 1 : Mise en place et gestion des utilisateurs dans Active Directory (AD) avec synchronisation de l'adresse email :

Comme première mission, on m'a confié l'ajout de nouveaux utilisateurs dans l'Active Directory (AD), en les plaçant dans le bon groupe d'activité et la section appropriée, puis en synchronisant leurs adresses e-mail .

Dans un premier temps, il faut ouvrir les fichiers Excel pour enregistrer les nouveaux utilisateurs.

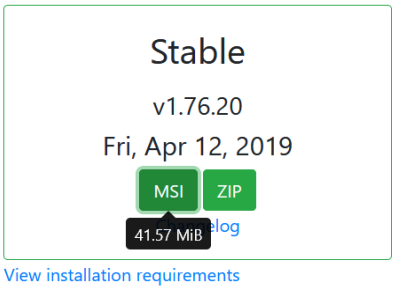


comme ceci :

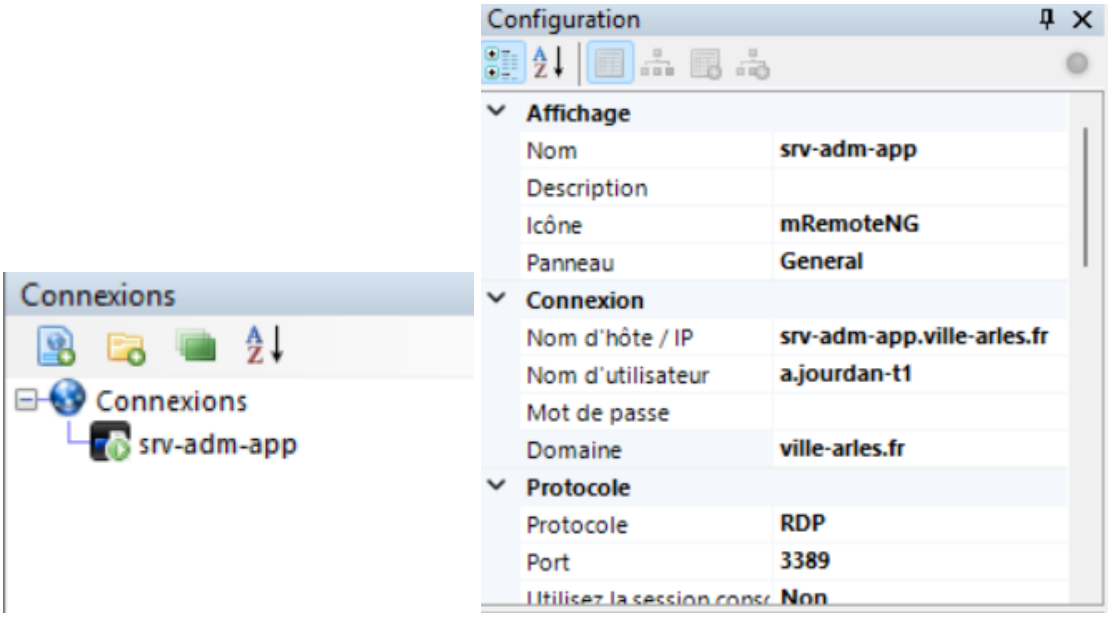


	A	B	C	D	E	F	G	H	I	J	K	
1	Username	password	New Passwd	Civilité	Nom	lastname	EMAIL	department	bureau	title	service	ou
2	c.assadourian	fkdo,0344	Qmphol6*HP-1		ASSADOURIAN	CLAIRE	c.assadourian@ville-arles.fr	CCAS			CCAS	OU=import
3	j.barban	jisc,5293	Vdhkrt3)HP.0		BARBAN	JEANINE	j.barban@ville-arles.fr	CCAS			CCAS	OU=import
4	i.bianchi	sxij,8834	Jghwcd0,LF)2		BIANCHI	ISABELLE	i.bianchi@ville-arles.fr	CCAS			CCAS	OU=import
5	d.billange	mprd,1923	Ctonfr5/WI-2		BILLANGE	DELPHINE	d.billange@ville-arles.fr	CCAS			CCAS	OU=import
6	a.bosset	guri,6652	Wsonva6(DW(4		BOSSET	AGNES	a.bosset@ville-arles.fr	CCAS			CCAS	OU=import
7	h.bouquet	lsoz,0347	Iavspg9/XQ,2		BOUQUET	HOURIA	h.bouquet@ville-arles.fr	CCAS			CCAS	OU=import
8	m.carraro	xsor,7465	Jaequf7/RH+9		CARRARO	MARTINE	m.carraro@ville-arles.fr	CCAS			CCAS	OU=import
9	e.defoug	srij,3287	Snxxjt0-JS(9		DEFOUG	EMMANUELL	e.defoug@ville-arles.fr	CCAS			CCAS	OU=import
10	s.delseny	wjzu,4837	Bgwgso9(MY,7		DELSENY	SYLVIE	s.delseny@ville-arles.fr	CCAS			CCAS	OU=import
11	n.diaz	fsie,9154	Vvospg8-OC*8		DIAZ	NELLY	n.diaz@ville-arles.fr	CCAS			CCAS	OU=import
12	f.faure	ziro,4813	Kbanag9+UX*2		FAURE	FRANSISCA	f.faure@ville-arles.fr	CCAS			CCAS	OU=import
13	e.ferretti	hcsu,0594	Rraidl3)SN)1		FERRETTI	ESTELLE	e.ferretti@ville-arles.fr	CCAS			CCAS	OU=import
14	l.fosse	ahjd,6823	Dukqhh0*LS(9		FOSSE	LAURENCE	l.fosse@ville-arles.fr	CCAS			CCAS	OU=import
15	v.froment	ekjf,9327	Naqtkf9-ZM-3		FROMENT	VIRGINIE	v.froment@ville-arles.fr	CCAS			CCAS	OU=import
16	r.garcia	kids,6624	Wnghne1(SV,7		GARCIA	ROSE MARIE	r.garcia@ville-arles.fr	CCAS			CCAS	OU=import
17	n.gavaudan	hsko,7853	Plxnwh7.UO/4		GAVAUDAN	NADINE	n.gavaudan@ville-arles.fr	CCAS			CCAS	OU=import
18	c.larguier	qkdj,7934	Iqalbk6+OX(9		LARGUIER	COLINE	c.larguier@ville-arles.fr	CCAS			CCAS	OU=import
19	m.larnac	gdsi,2605	Sppswq9,DK*0		LARNAC	MARIE	m.larnac@ville-arles.fr	CCAS			CCAS	OU=import
20	y.lasri	irjf,9208	Ncvhux7(YT)9		LASRI	YAMINA	y.lasri@ville-arles.fr	CCAS			CCAS	OU=import
21	l.lemercier	shri,3691	Rmmool2(SU+6		LEMERCIER	LAURENCE	l.lemercier@ville-arles.fr	CCAS			CCAS	OU=import
22	m.maurin	ksai,1739	Twpcql7)FZ+0		MAURIN	MARION	m.maurin@ville-arles.fr	CCAS			CCAS	OU=import
23	s.meziani	bvfg,5235	Rgmigb8,SO+6		MEZIANI	SIHAM	s.meziani@ville-arles.fr	CCAS			CCAS	OU=import
24	a.parramon	wuer,4829	Vmtxcv1/MX*7		PARRAMON	AURELIE	a.parramon@ville-arles.fr	CCAS			CCAS	OU=import
25	e.pascal	zurj,1638	Mftodb5/SZ,5		PASCAL	EMILIE	e.pascal@ville-arles.fr	CCAS			CCAS	OU=import
26	c.pfundstein	klcs,7948	Reddvw4/MS/0		PFUNDSTEIN	CAROLINE	c.pfundstein@ville-arles.fr	CCAS			CCAS	OU=import

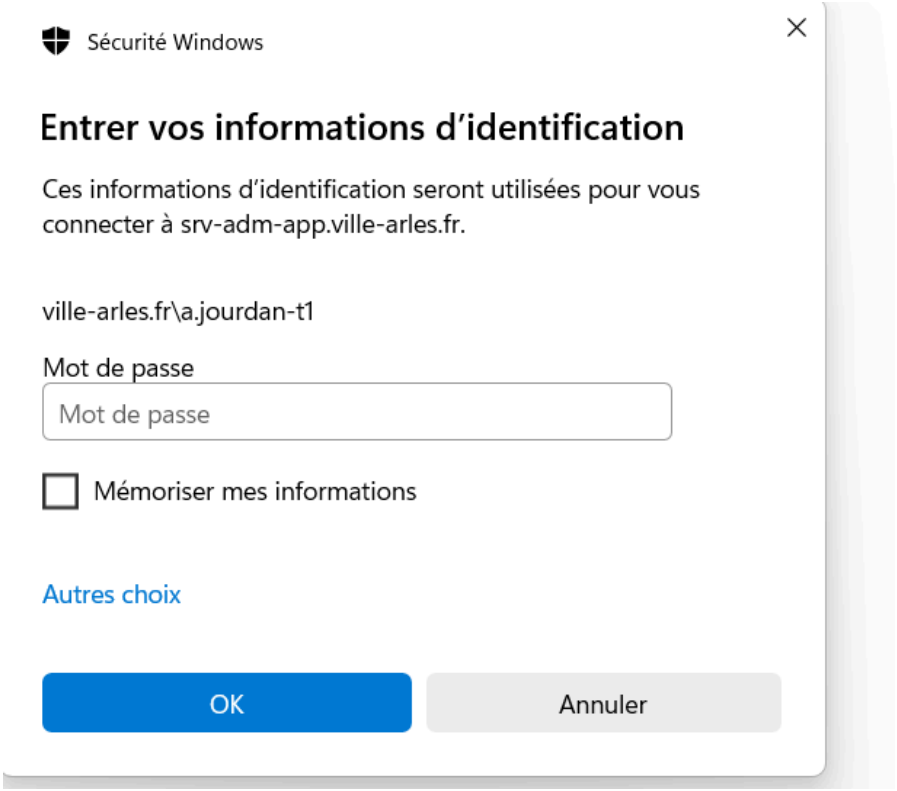
Ensuite, il faut installer l'application mRemoteNG, qui permet de réaliser des connexions à distance sur une machine. Cette application permet de centraliser et de gérer différentes connexions à des serveurs ou ordinateurs distants, en utilisant plusieurs protocoles comme RDP, SSH



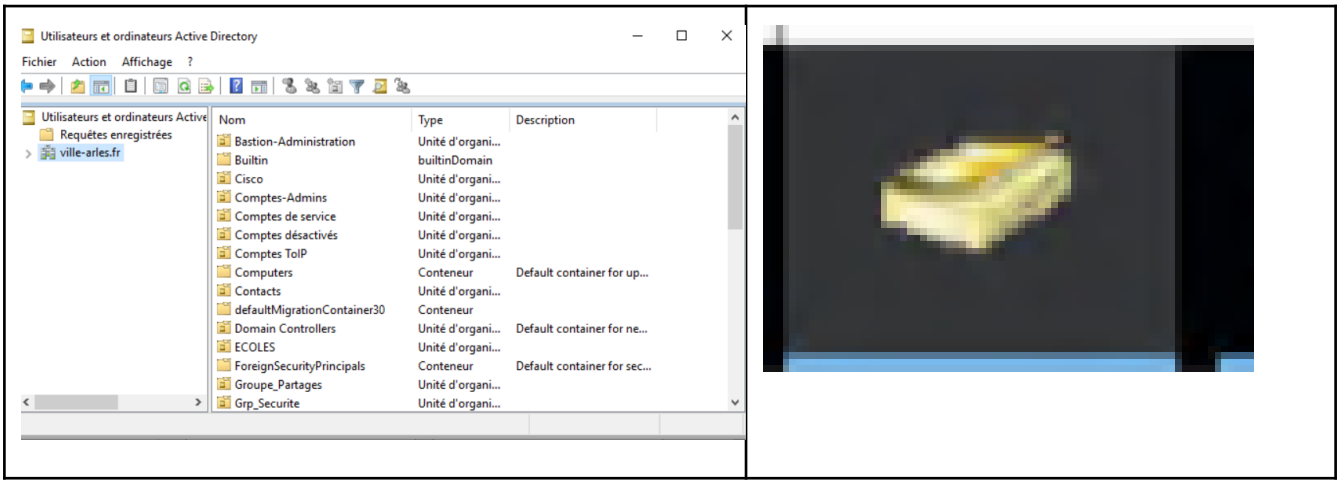
Une fois l'application installée, il faut la configurer en renseignant le nom de domaine et les identifiants nécessaires pour établir la connexion à distance sur le serveur AD.



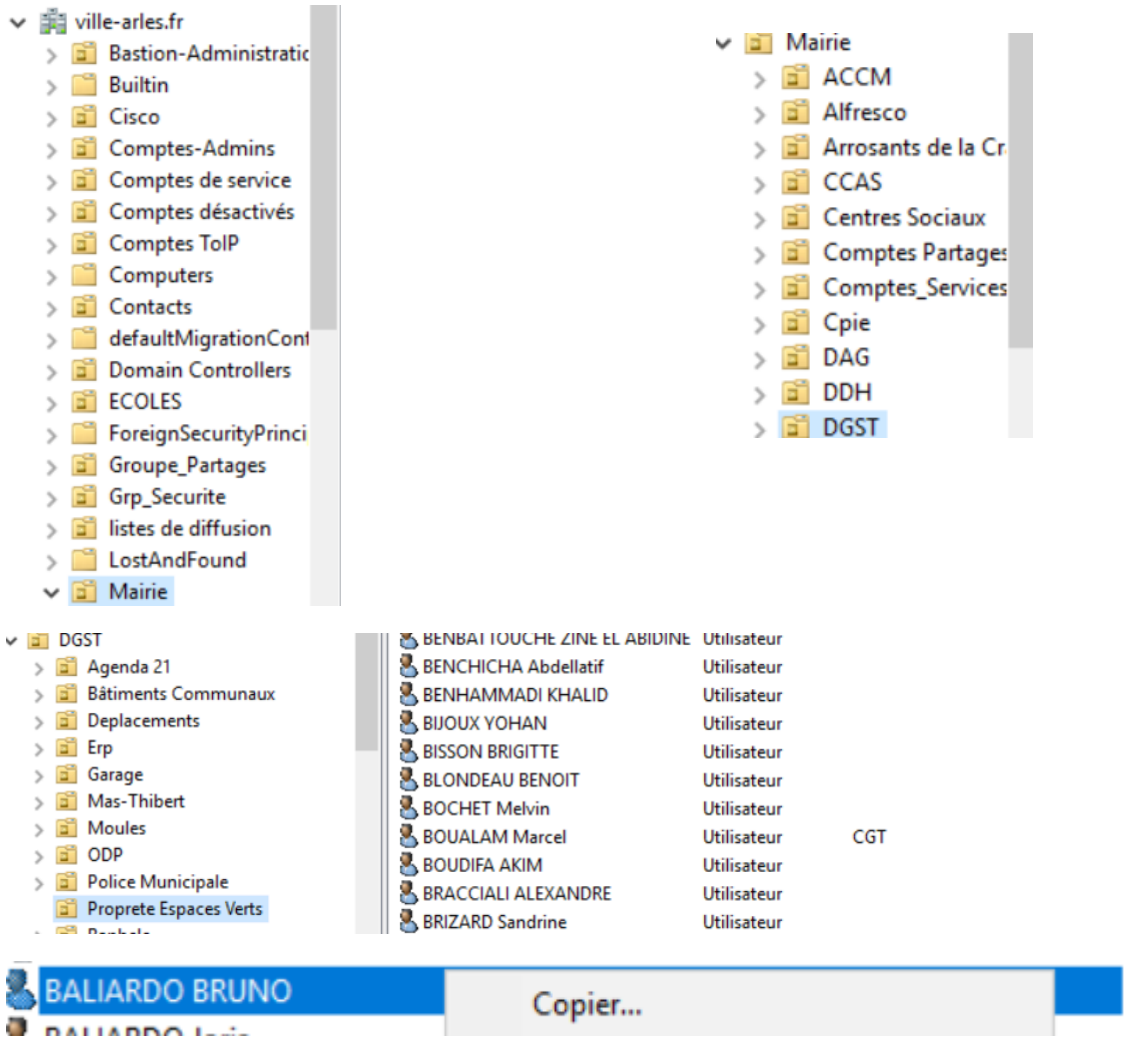
Cette identification correspond à l'identifiant administrateur, qui permet d'accéder et de faire des modifications sur l'Active Directory.



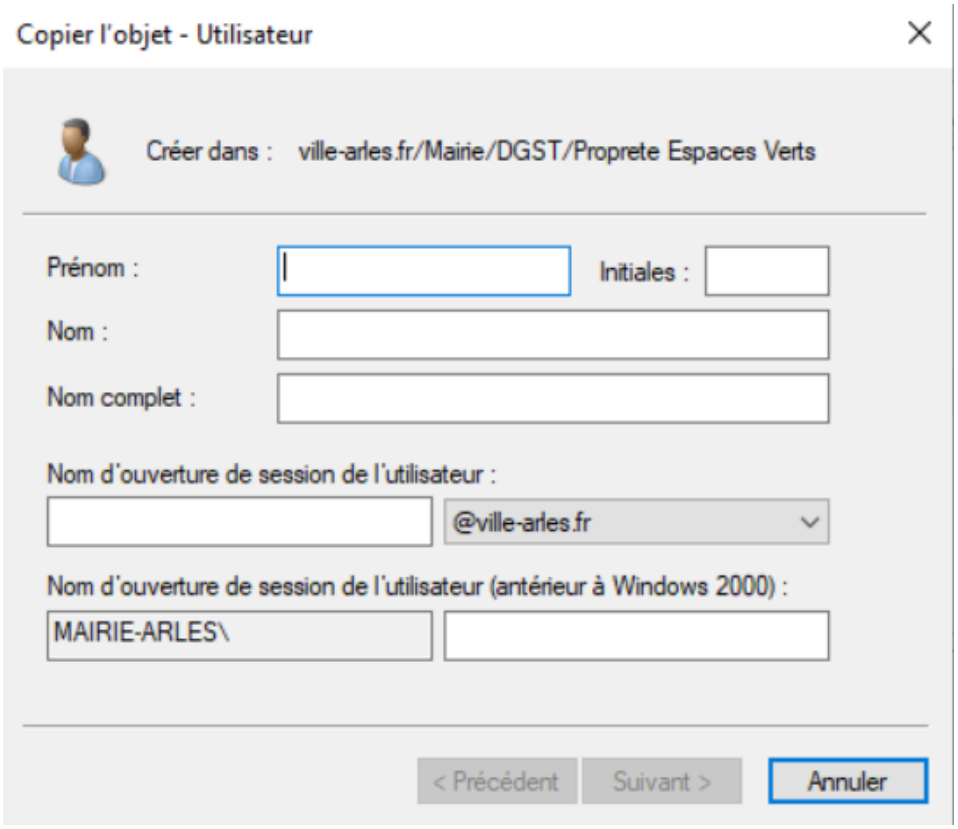
Ensuite, une fois connecté au serveur, il faut ouvrir les services liés aux utilisateurs de l'AD .

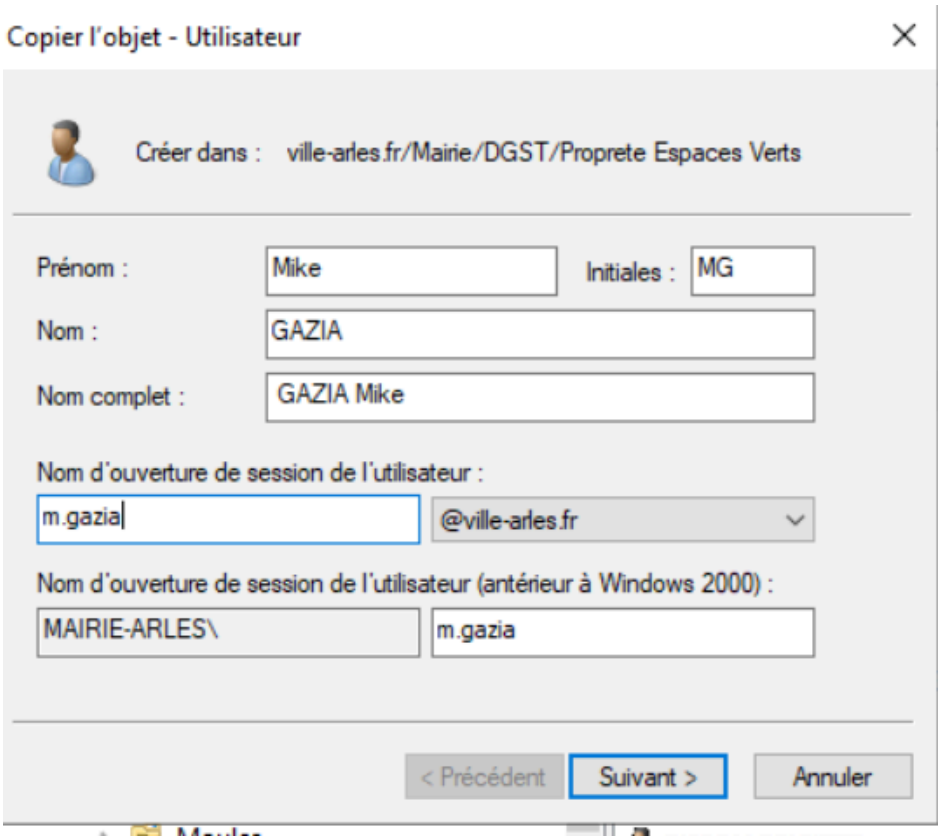


Une fois dans l'arbre du domaine, dans l'abornement de la mairie, puis ensuite dans la DGST et la propreté des espaces verts, c'est là que l'on va ajouter les nouveaux utilisateurs en prenant exemple sur un utilisateur existant pour effectuer la création des futurs clients.

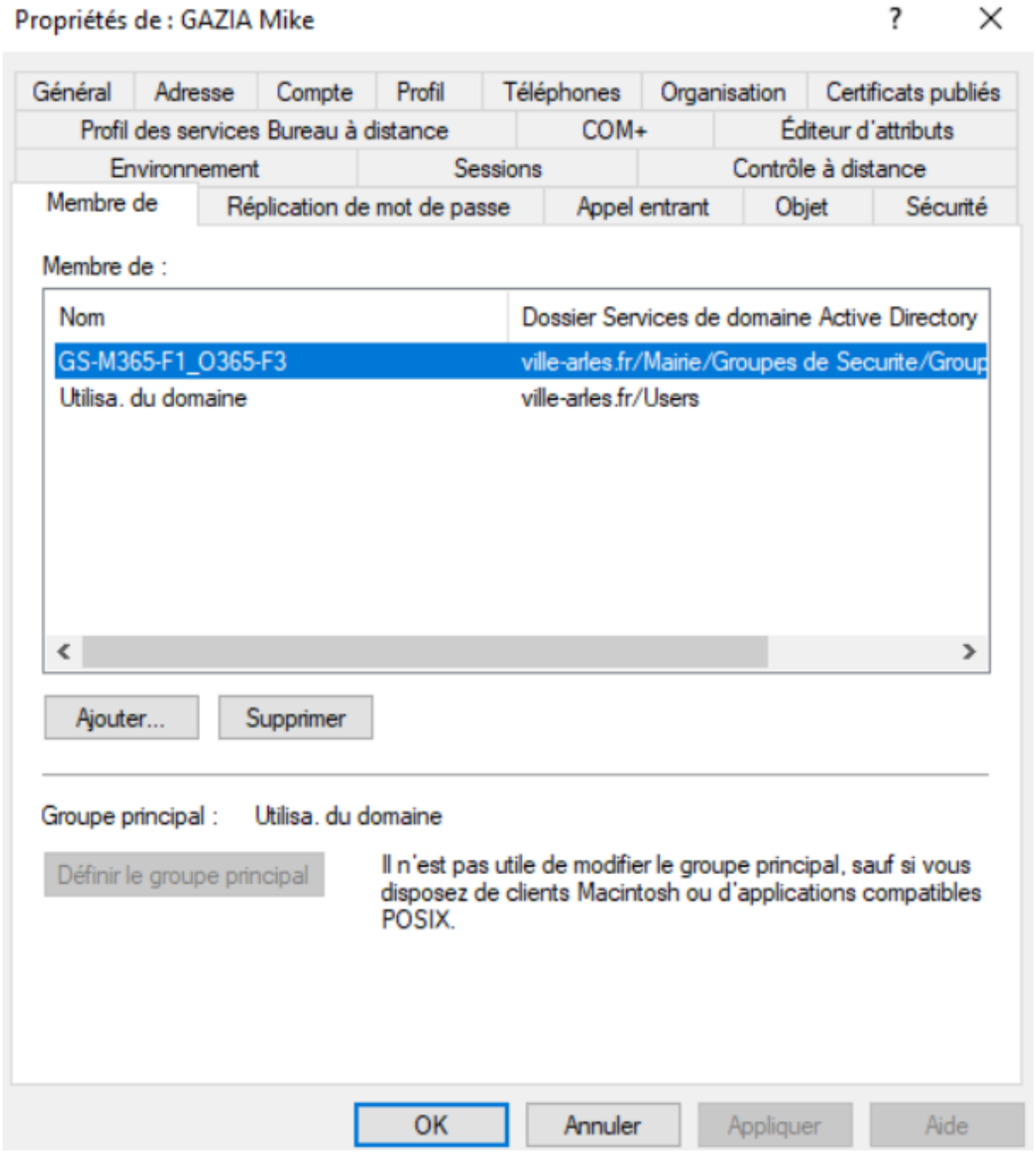


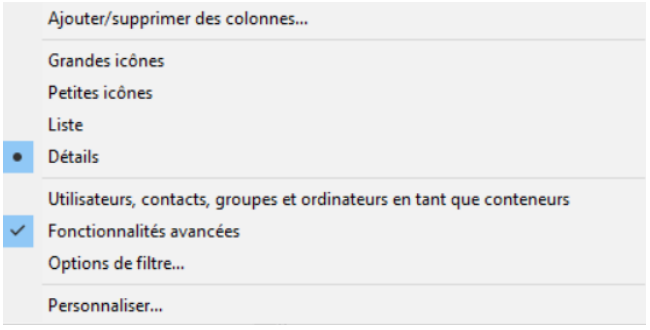
Et là, on crée un nouveau utilisateur dans le domaine :



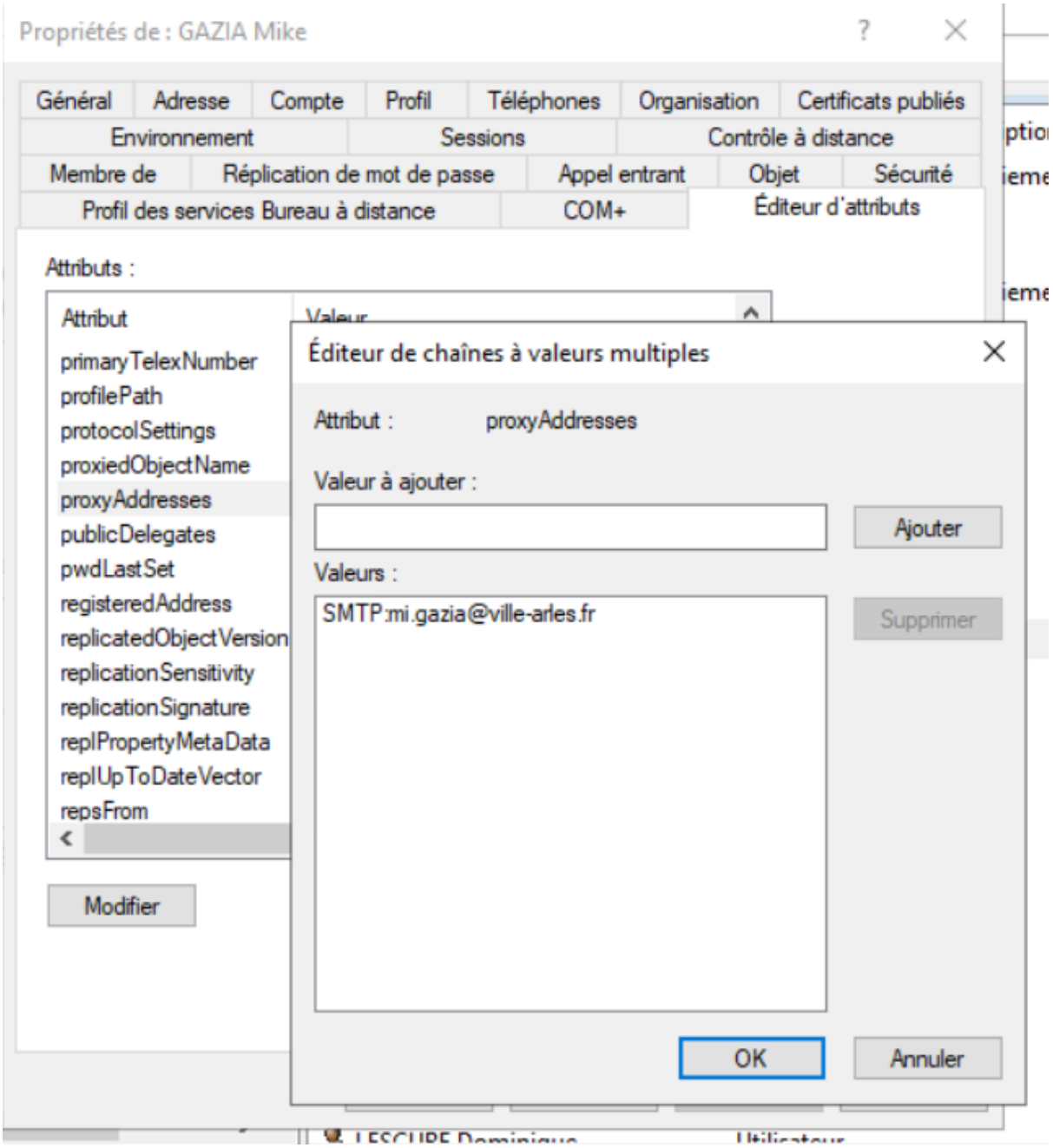


Dans cette partie, j'ai vérifié s'il avait bien accès au groupe utilisateur et au groupe où se trouvent les licences.





Ensuite, je vais lui ajouter ses adresses dans le champ proxyAddresses, qui sert à différencier et associer plusieurs adresses e-mail à un même utilisateur.Lorsqu'un utilisateur se connecte à un réseau utilisant **Active Directory (AD)**, son compte est d'abord créé dans AD avec des informations comme son nom et sa licence, si nécessaire. Le poste de travail de l'utilisateur doit être **joint au domaine** pour permettre la communication avec le contrôleur de domaine.Une fois connecté, le poste détecte automatiquement le domaine via le **DNS** et lance un processus d'authentification, souvent via un script PowerShell. Ce processus crée la **session utilisateur** et applique les **droits d'accès** définis dans AD, permettant l'accès aux **dossiers personnels** et aux **partages réseau**.Enfin, les **licences** nécessaires sont attribuées à l'utilisateur, lui permettant d'accéder aux services et applications requis pour son travail. **Active Directory** centralise ainsi la gestion des utilisateurs et des ressources, simplifiant l'authentification et l'accès aux ressources de la **mairie**.

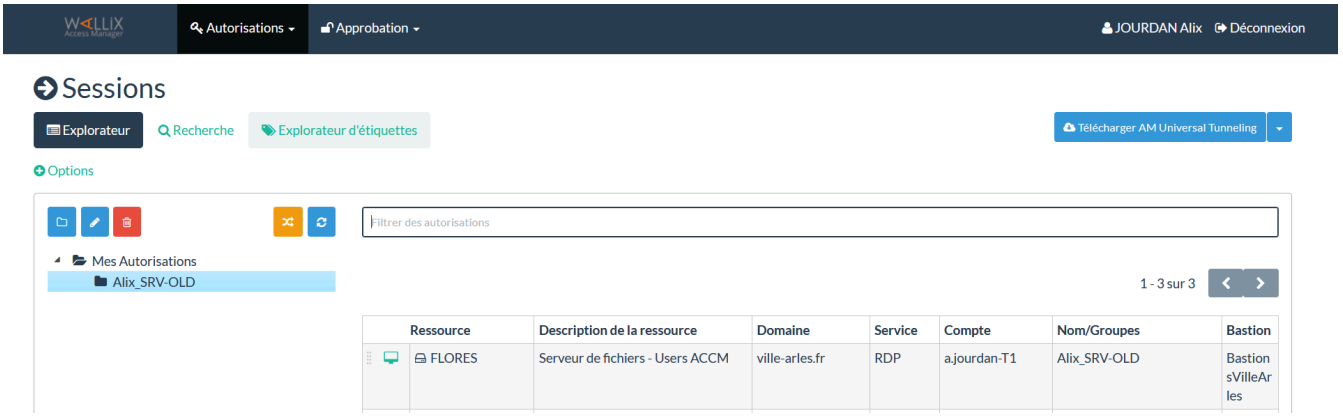


Mission 2 : Identifier les utilisateurs toujours présents dans l'Active Directory sur un ancien serveur qui va être remplacé, car il n'est plus aux normes, et les déplacer vers un nouveau serveur créé :

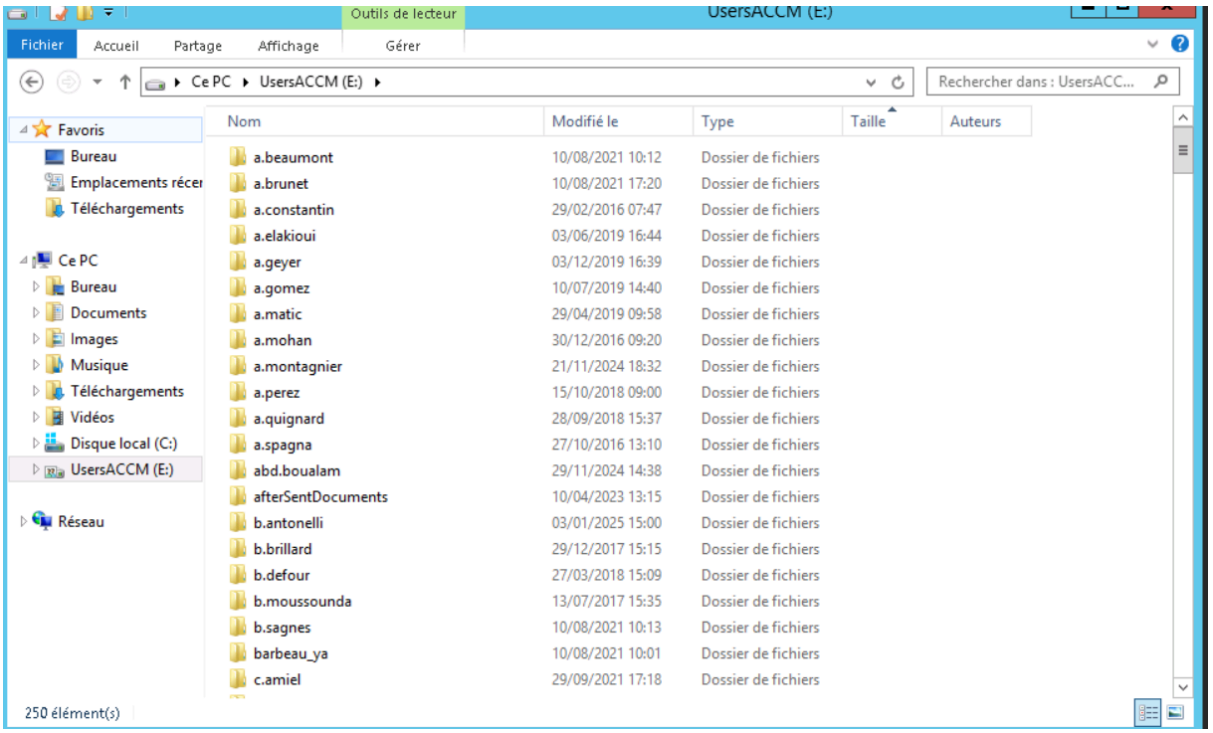
Dans cette deuxième situation, on m'a demandé de répertorier les utilisateurs sur un ancien serveur datant de 2012, de vérifier s'ils sont toujours présents dans l'Active Directory (AD) et de les lister dans un fichier Excel. L'objectif final étant de supprimer ce serveur et de transférer toutes les données vers leur OneDrive, afin de mettre en place une redirection.

Username	Nom	Prénom	Toujours présent dans l'AD	EMAIL	service	Bureau	Taille de fichier
a.beaumont	BEAUMONT	A	NON	/	/	/	/
a.constantin	CONSTANTIN	A	NON	/	/	/	/
a.elakioui	ELAKIOUI	A	NON	/	/	/	/
a.geyer	GEYER	A	NON	/	/	/	/
a.gomez	GOMEZ	A	NON	/	/	/	/
a.matic	MATIC	A	NON	/	/	/	/
a.mohan	MOHAN	A	NON	/	/	/	/
a.montagnier	MONTAGNIER	André	OUI	a.montagnier@agglo-accm.fr		00183	
a.perez	PEREZ	A	NON	/	/	/	/
a.quignard	QUIGNARD	A	NON	/	/	/	/
a.spagna	SPAGNA	A	NON	/	/	/	/
abd.boualam	BOUALAM	Abdelkader	OUI	abd.boualam@agglo-accm.fr	Services techniques ACCM	00496	
b.antonelli	ANTONELLI	Barbara	OUI	b.antonelli@agglo-accm.fr	Politique de la Ville ACCM	00644	
b.brillard	BRILLARD	Brigitte	OUI	b.brillard@agglo-accm.fr	Communication ACCM	/	
b.defour	DEFOUR	B	NON	/	/	/	/
b.sagnes	SAGNES	B	NON	/	/	/	/

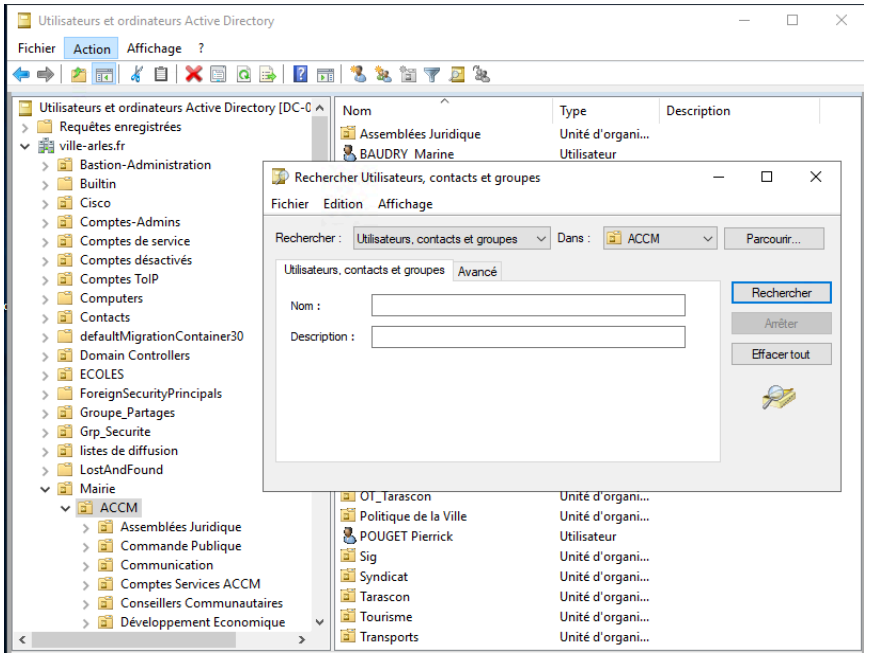
Pour que je puisse accéder au serveur, une connexion d'assistance m'a été mise en place via le service Wallix Bastion. Wallix est une solution de gestion des accès privilégiés (PAM) qui permet de sécuriser, de contrôler et d'auditer les accès aux systèmes, ainsi que de définir des paramètres spécifiques pour chaque utilisateur. Ces derniers ne peuvent voir que les machines auxquelles ils ont accès. Lorsque l'on lance une machine virtuelle à distance, un message indique 'Vous êtes surveillé'.



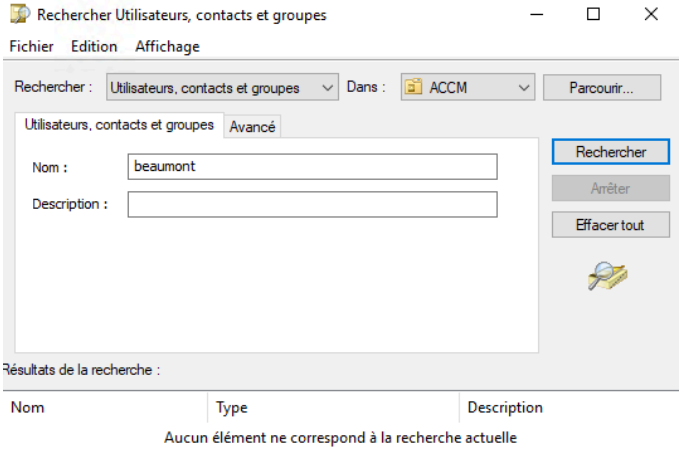
Voici leurs V personnelles qui se trouvent actuellement sur le serveur et qui seront transférées sur OneDrive. À partir de là, je devrai vérifier, sur Active Directory, si elles sont toujours présentes dans la Mairie.

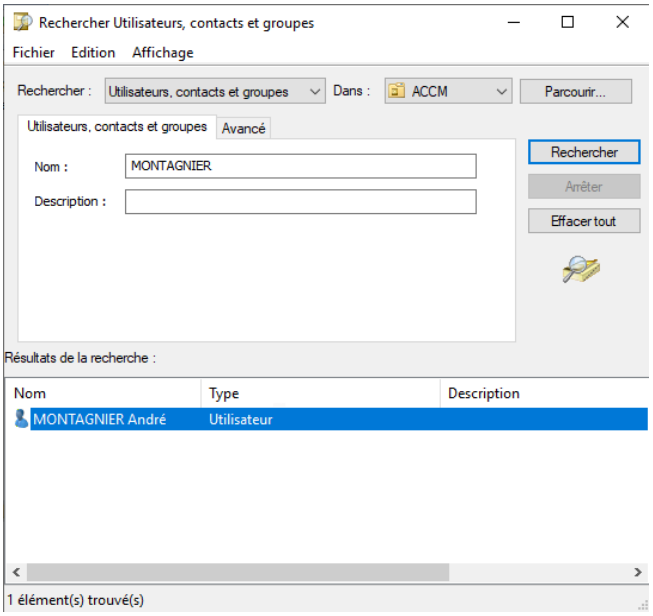


Ensuite, dans un second temps, je me connecterai à l'Active Directory pour commencer mes recherches. Les utilisateurs présents sur le serveur de Flores appartiennent au service AACM. Je devrai sélectionner le domaine de la ville, puis les groupes **Mairie** et à l'intérieur de ce groupe, le service **AACM**. À partir de là, je sélectionne l'option **Action**, puis je lance la recherche à partir du groupe **AACM**.



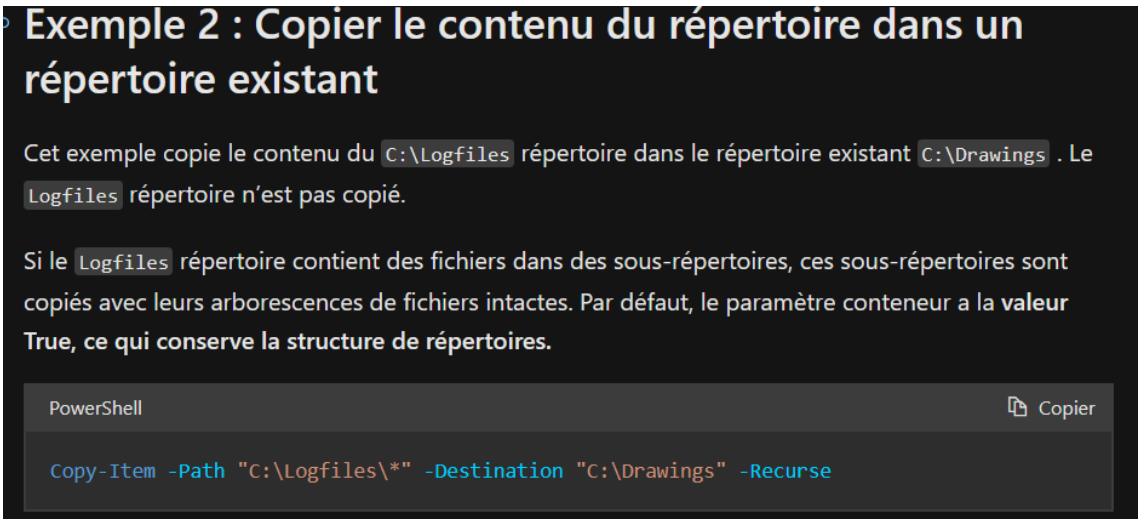
Dans ce cas, on peut observer deux situations : l'une montre que l'utilisateur n'est plus présent dans l'Active Directory, tandis que l'autre indique qu'il y est toujours.



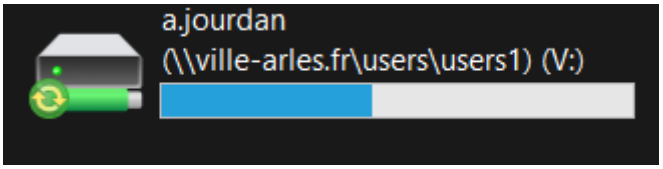


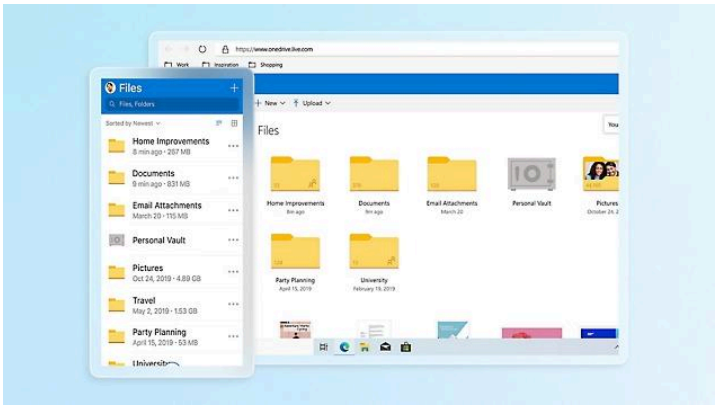
J'ai rencontré des difficultés pour accéder aux informations des dossiers en raison de droits insuffisants. Avec mon maître de stage, nous avons décidé de déplacer les fichiers personnels des utilisateurs d'un lecteur réseau vers leur OneDrive, afin de les rendre accessibles virtuellement.

Avec mon collègue Anthony, nous avons réfléchi à la meilleure façon de transférer les répertoires personnels vers OneDrive. Nous avons envisagé l'utilisation de commandes shell,



mais cela nécessiterait une intervention manuelle. Nous avons également considéré l'option de déplacer directement les répertoires, mais des questions de sécurité se sont posées en raison de la gestion des répertoires personnels différents pour chaque utilisateur. Pour l'instant, la solution manuelle semble plus adaptée.





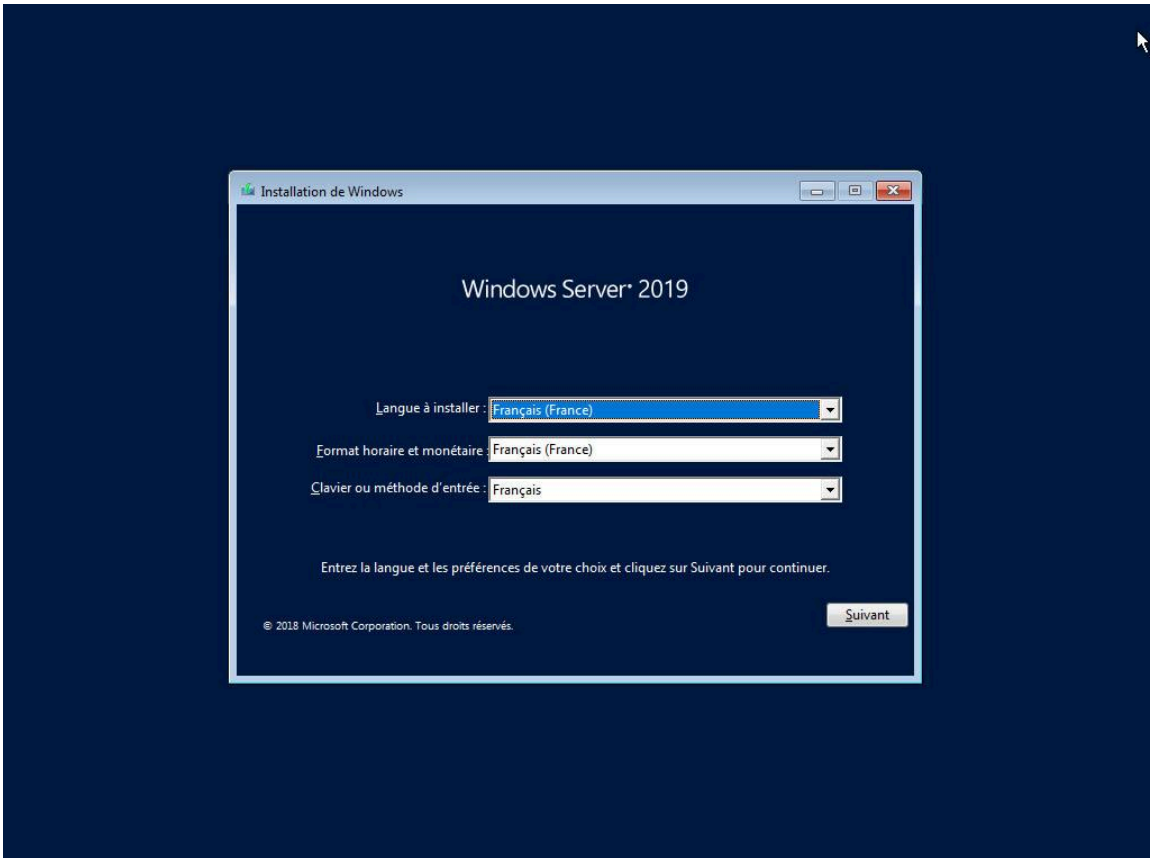
Malheureusement, je n'ai pas pu terminer cette mission. Il ne me reste plus qu'à contacter les utilisateurs pour finaliser le transfert de leurs fichiers vers OneDrive.

Mission 3 : Intégration de l'Active Directory avec GLPI pour une gestion centralisée :

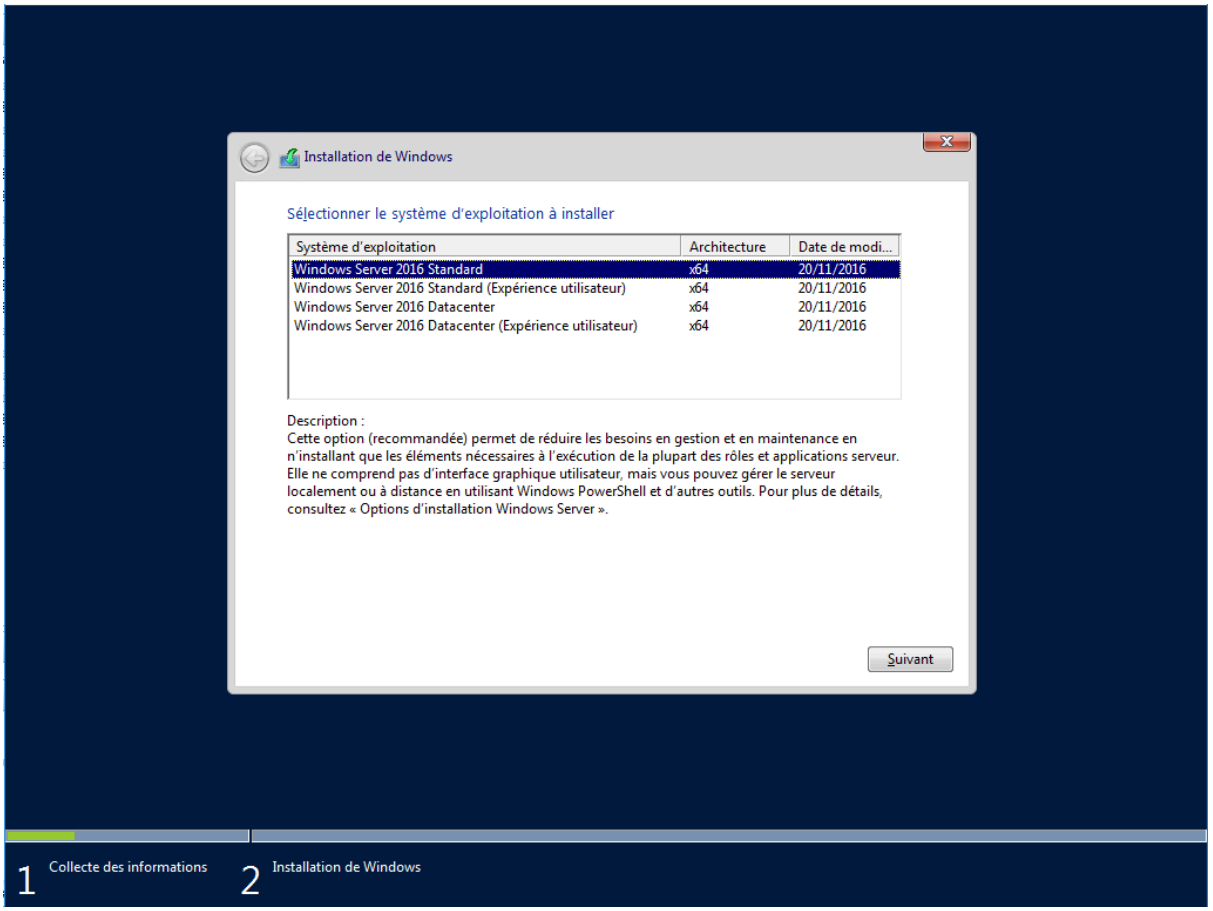
Pour cette troisième mission, mon tuteur de stage a souhaité voir les deux projets que je devais présenter lors de l'épreuve de l'E5. Ensemble, nous avons décidé de perfectionner une activité et de réfléchir à la manière de la réaliser. Nous avons choisi de travailler sur la situation 2, qui concerne la synchronisation d'Active Directory avec GLPI. Quand j'ai réalisé l'activité, j'aurais dû en parler avec mon maître de stage pour lui expliquer ce que j'avais fait ou ce que j'allais mettre en place, afin de vérifier si cela ne risquait pas de perturber le réseau.

Serveur GLPI 2019 avec IIS, configuré sous un environnement de sous-tiering

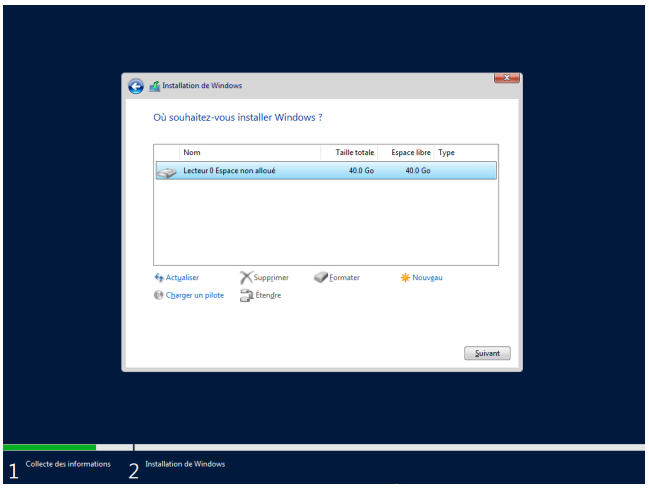
Dans cette section, nous allons voir la configuration de la machine :



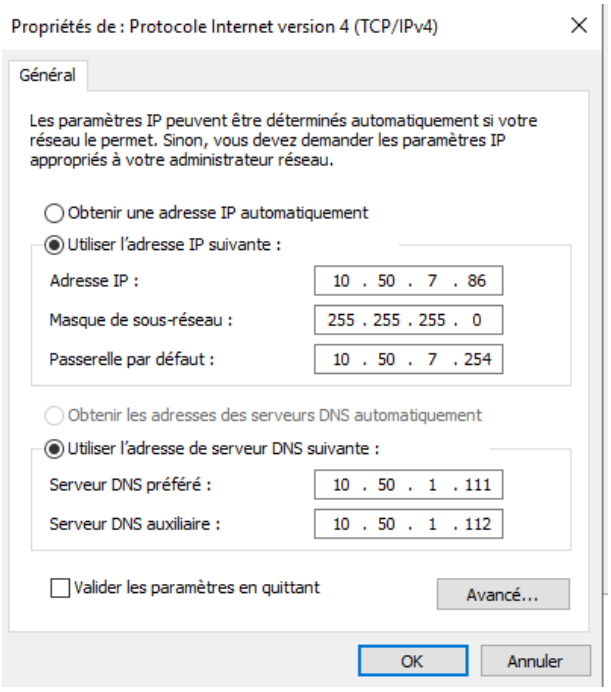
Dans cette section, il faudra sélectionner le datacenter, car la mairie dispose d'une licence spécifique. Cette licence permet d'héberger des données sensibles et d'accéder à des services cloud sécurisés, tout en garantissant la conformité aux normes de sécurité et de confidentialité, comme le RGPD.



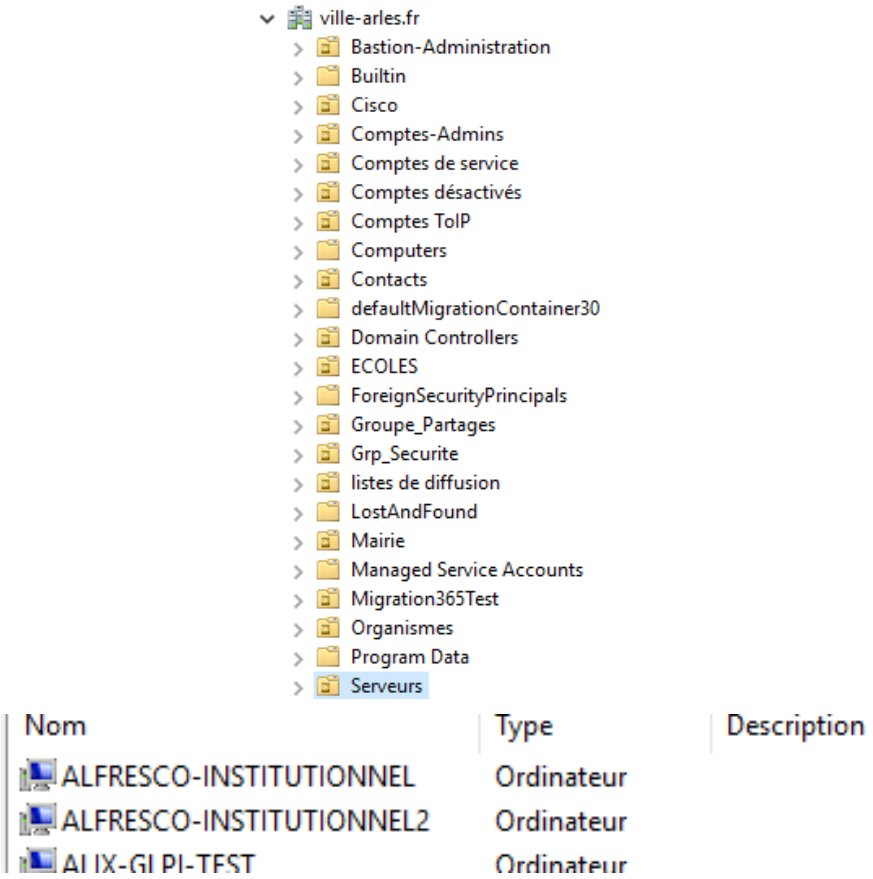
Dans cette section, nous allons répartir les disques de la machine et terminer l'installation. Il est important d'installer VMware Tools, car il permet d'améliorer les performances de la machine virtuelle, d'activer des fonctionnalités comme le redimensionnement de l'écran et le partage de fichiers entre l'hôte et la machine virtuelle, ainsi que d'optimiser les drivers pour une meilleure gestion des périphériques.

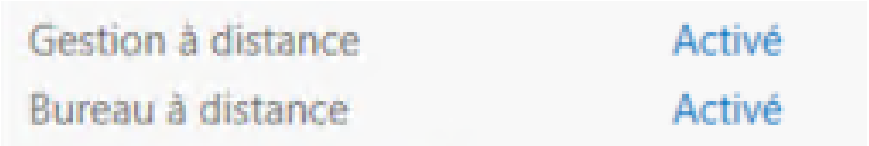


Dans cette section, nous allons configurer l'ordinateur en lui attribuant un nom pour faciliter son identification dans l'Active Directory (AD). Ensuite, nous allons configurer des adresses IP fixes, en entrant l'adresse IP du PC ainsi que les serveurs DNS.

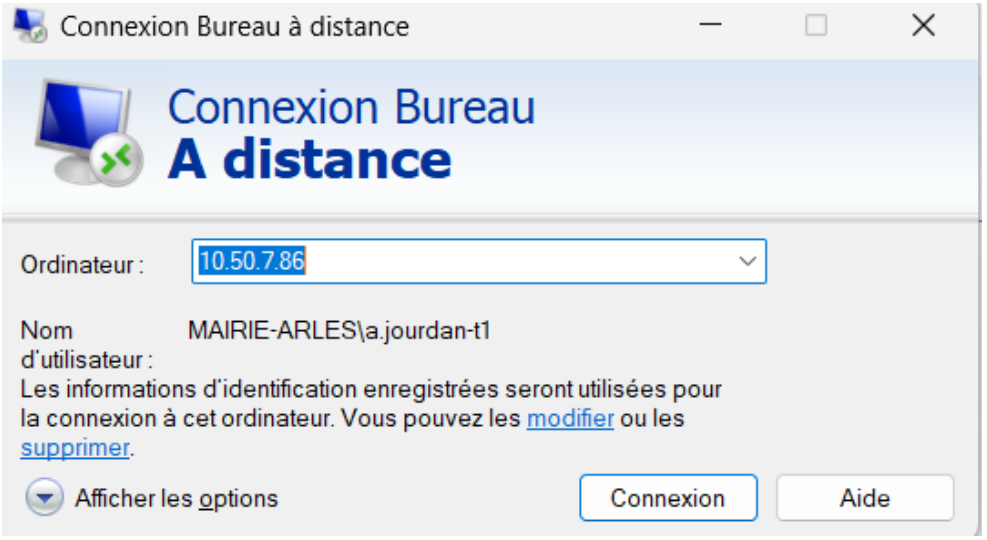


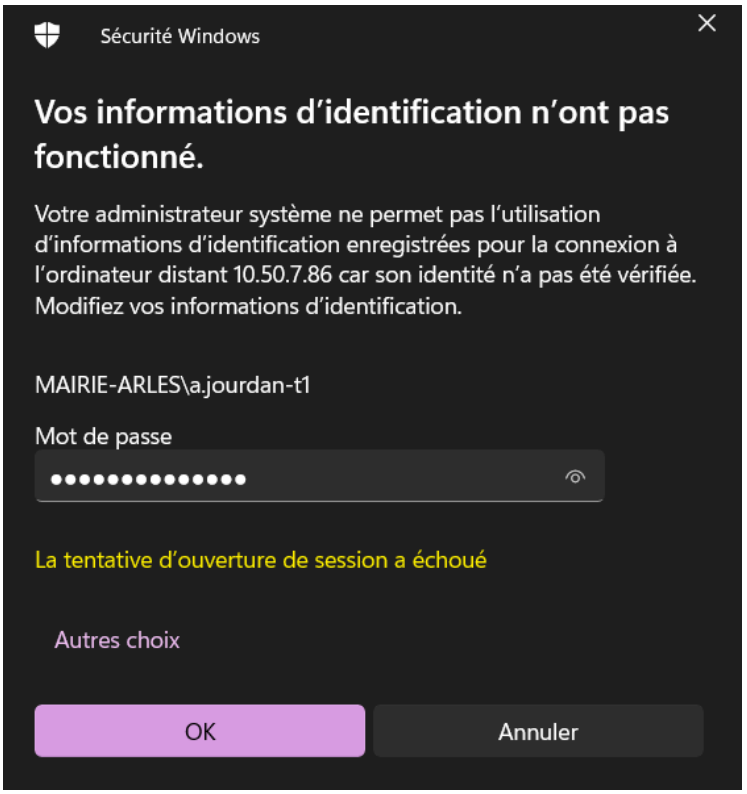
Ensuite, dans cette section, je vérifierai si le PC est bien affiché dans l'Active Directory (AD). Puis, directement sur le serveur, j'active le bureau à distance avec l'authentification.

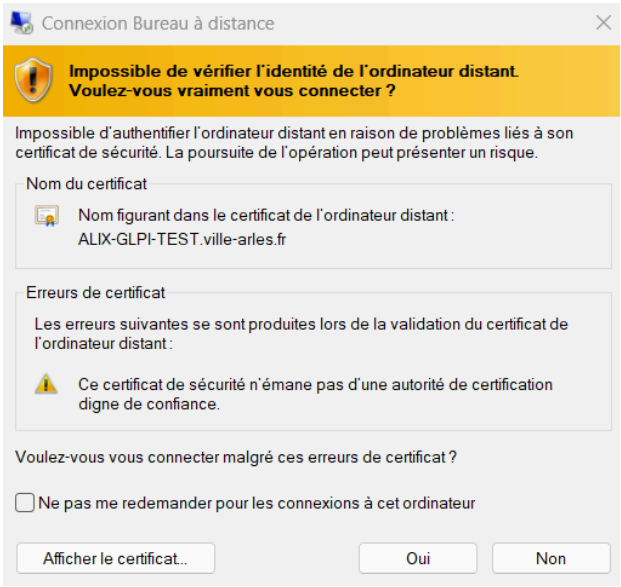




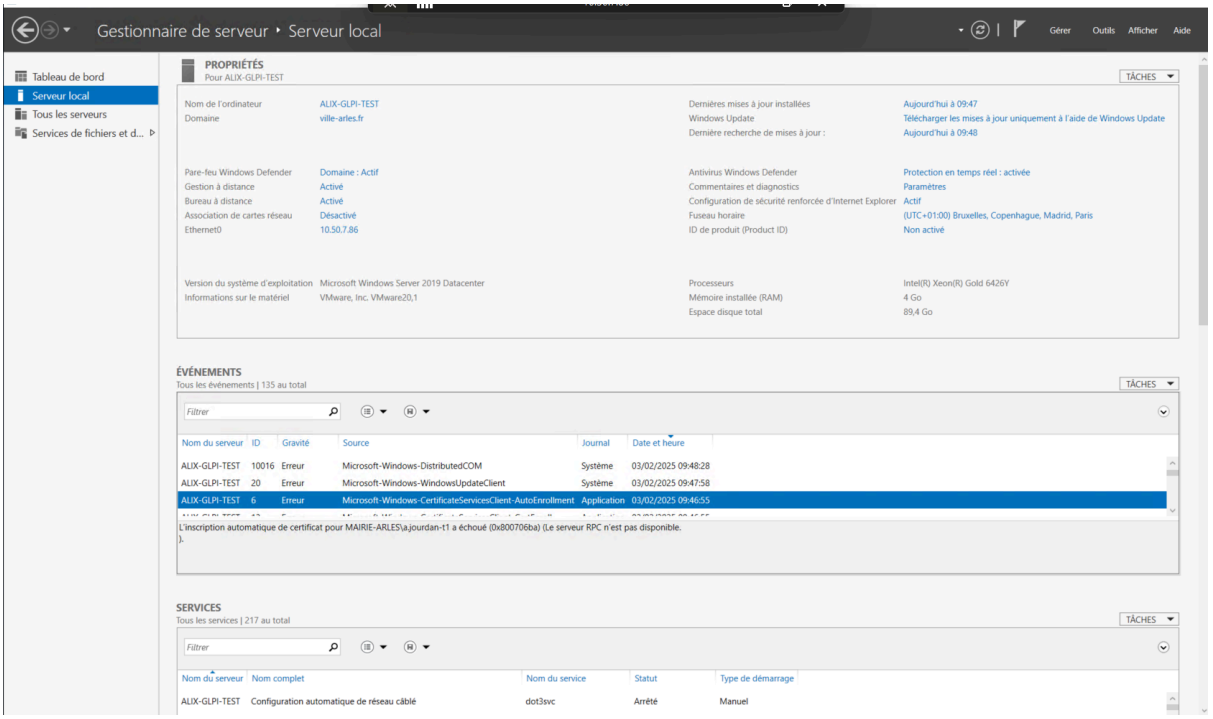
Ensuite, sur mon PC de travail, je me connecte à mon bureau à distance avec mon compte T1 pour accéder au serveur. Seuls les comptes T1 permettent d'accéder au serveur, d'y installer des logiciels ou d'y apporter des modifications. Les comptes T2 sont réservés aux machines locales ou aux PC.

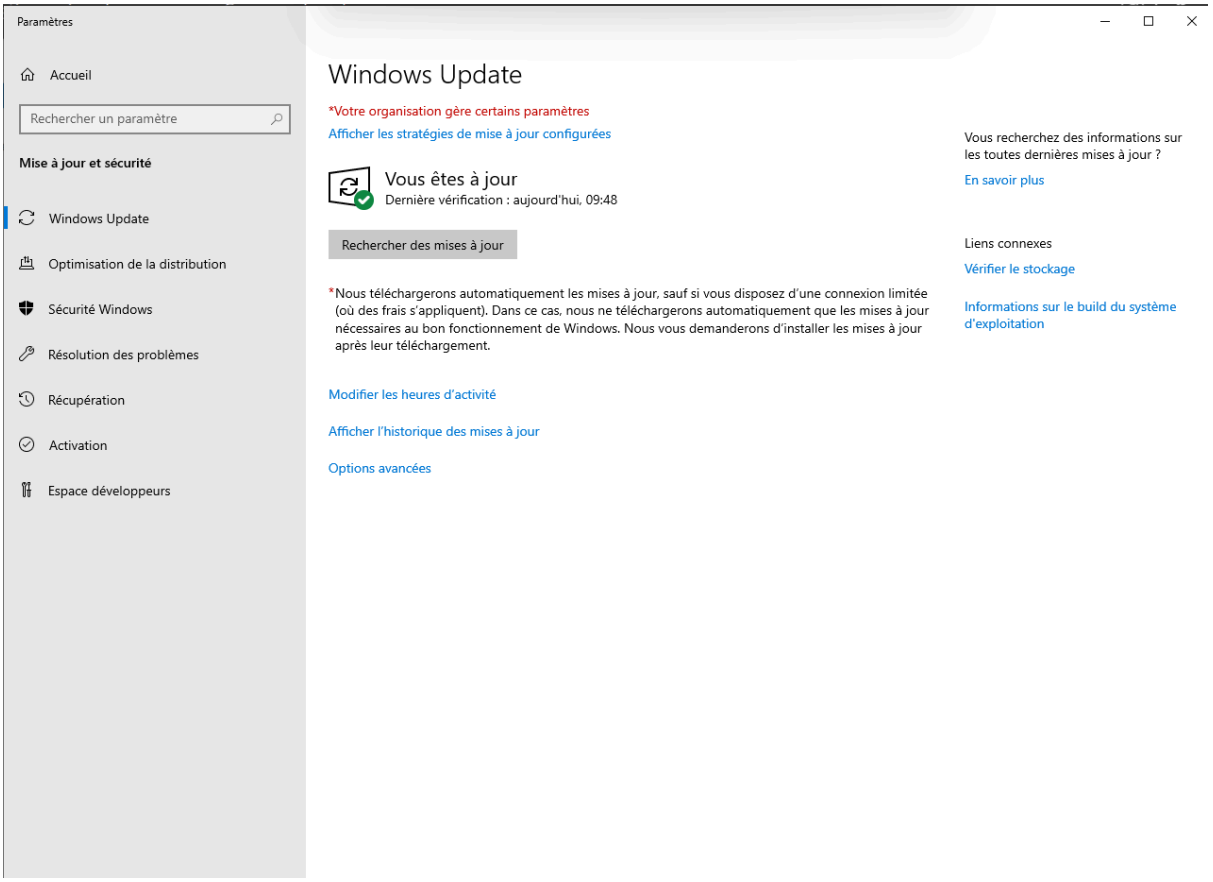




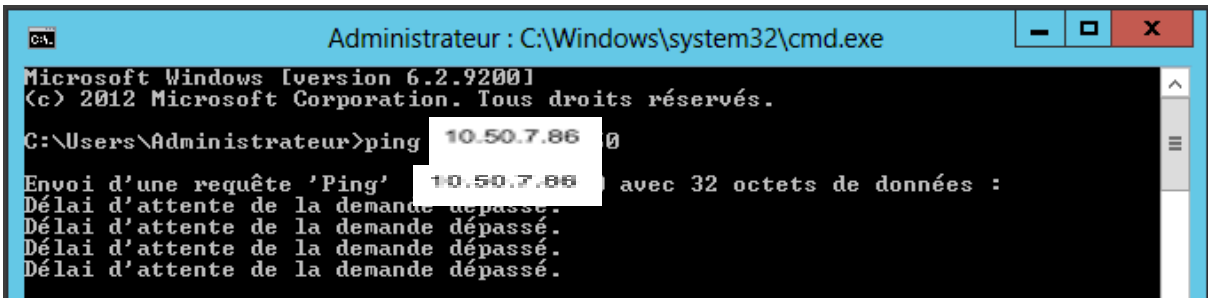


Ensuite, une fois connecté, je dois effectuer toutes les dernières mises à jour pour être à jour et éviter toute défaillance avec certains logiciels qui ne sont pas encore à jour.

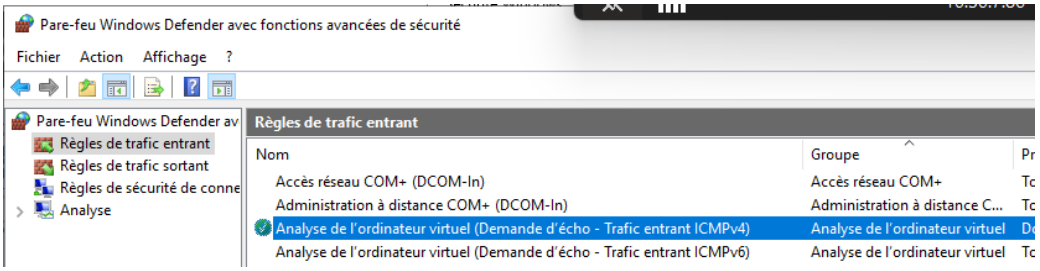


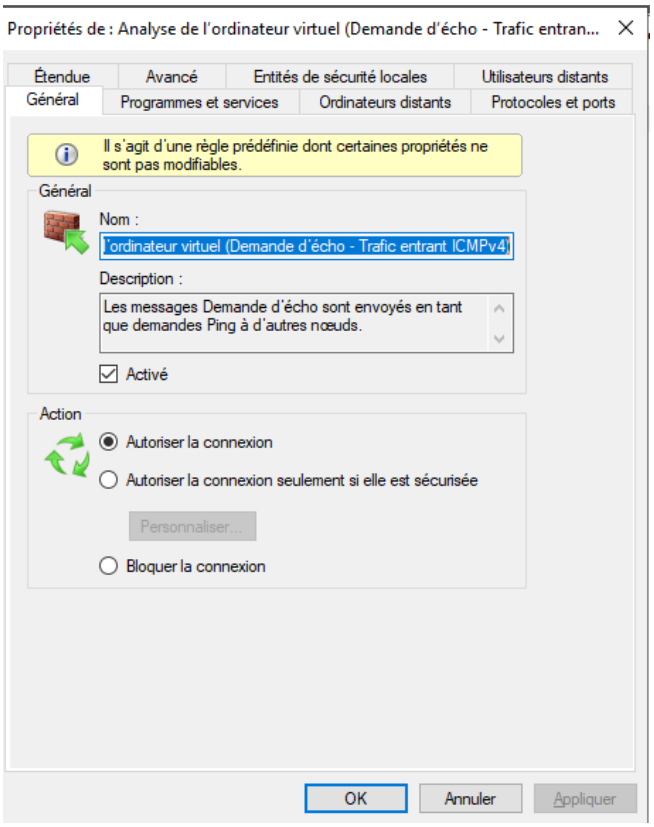


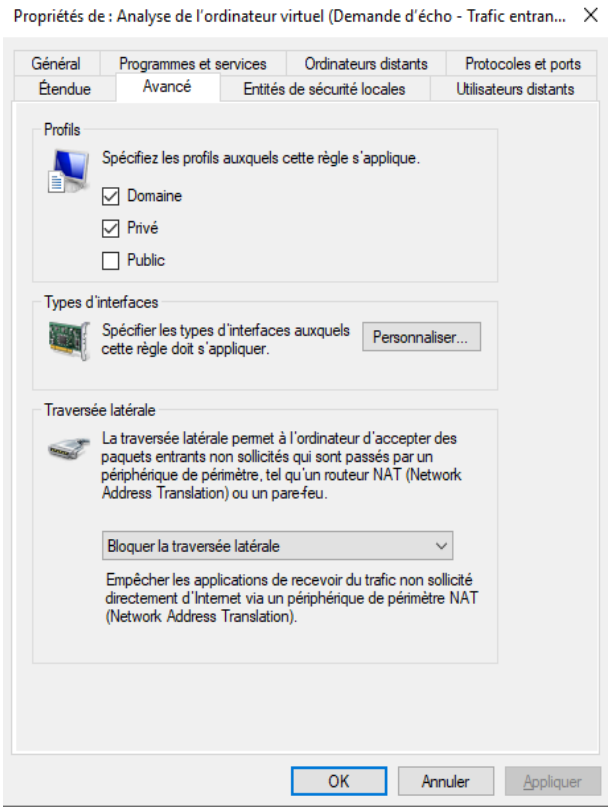
Mon maître de stage et moi avons remarqué que nous n'arrivons pas à ping la machine, car sur le serveur, le pare-feu IPv4 bloquait la liaison avec l'extérieur. Nous avons donc activé cette option pour résoudre le problème.



Dans cette partie, je vous présente la configuration du pare-feu pour activer l'accès et autoriser la communication avec l'extérieur de la machine.



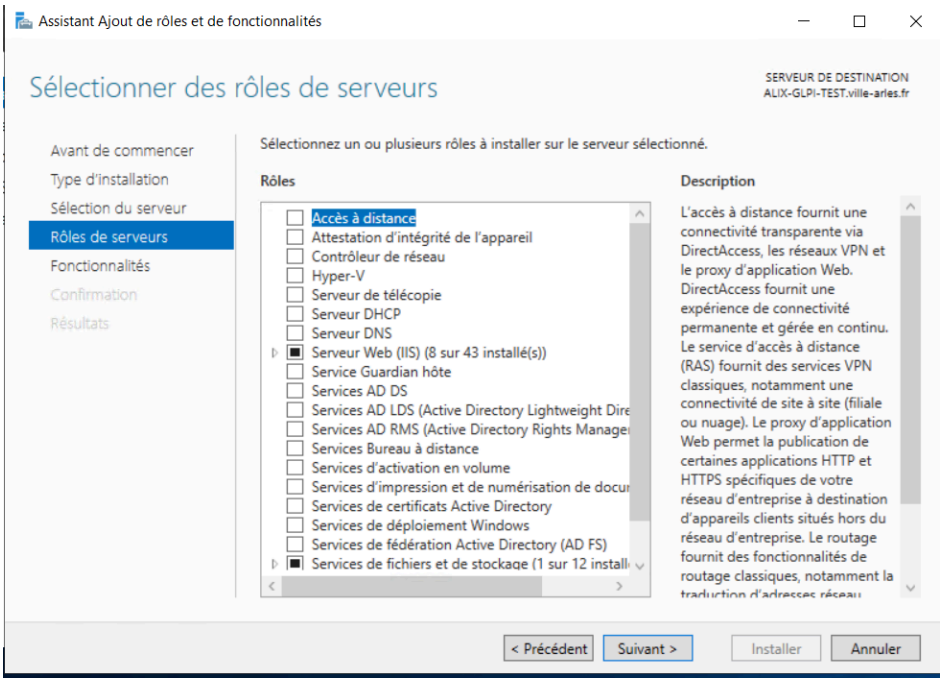




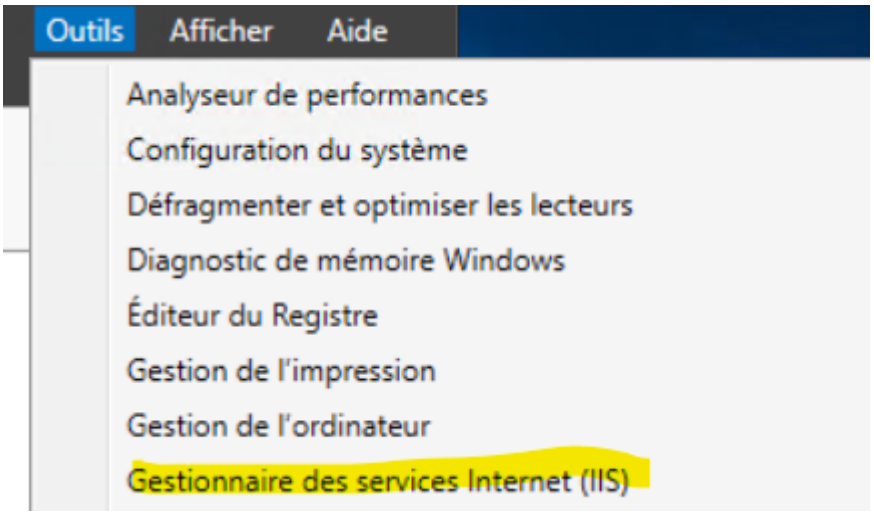
Ping a réussi :

```
Microsoft Windows [version 10.0.26100.2894]
(c) Microsoft Corporation. Tous droits réservés.

V:\>ping 10.50.7.86

Envoi d'une requête 'Ping'  10.50.7.86 avec 32 octets de données :
Réponse de 10.50.7.86 : octets=32 temps<1ms TTL=127
Réponse de 10.50.7.86 : octets=32 temps<1ms TTL=127
Réponse de 10.50.7.86 : octets=32 temps<1ms TTL=127
Réponse de 10.50.7.86 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 10.50.7.86:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

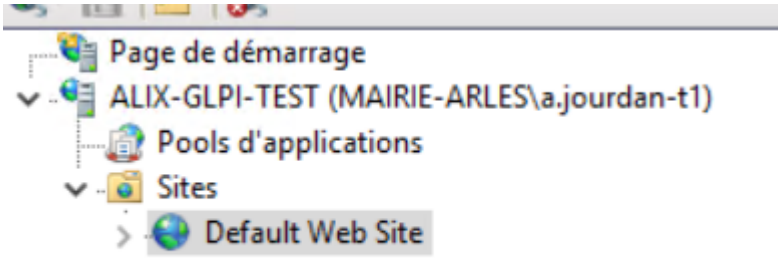
Dans cette section, je vais commencer l'installation de GLPI sur le Windows Server 2019. Dans un premier temps, il faut installer le service IIS, qui va gérer la partie web, comme le ferait Apache2.



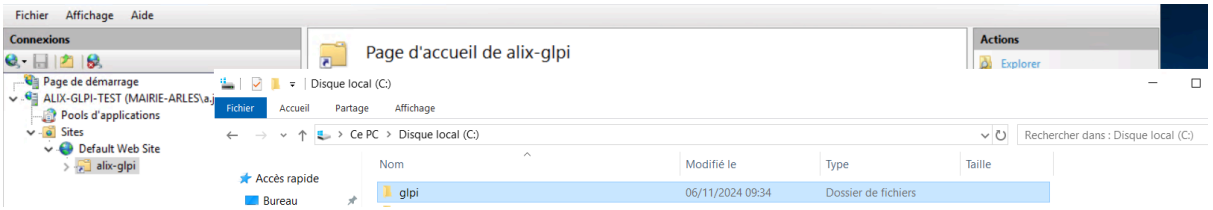
Pour accéder au service IIS :



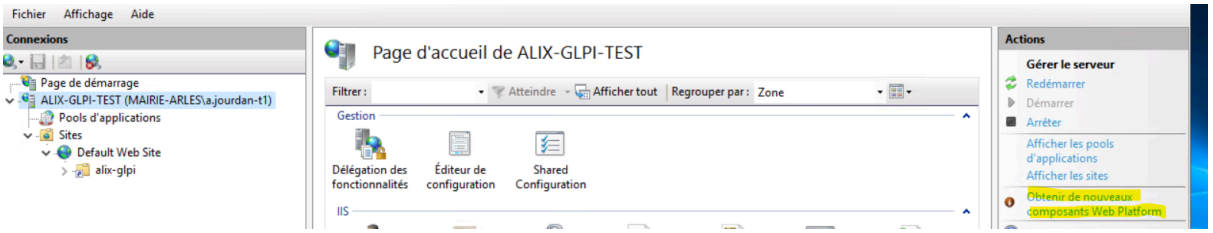
Donc, sur le service IIS, allez dans l'onglet 'Default Web Site', faites un clic droit et sélectionnez 'Ajouter un site Web'. Il faut d'abord installer la dernière version de GLPI et la placer sur le disque C.

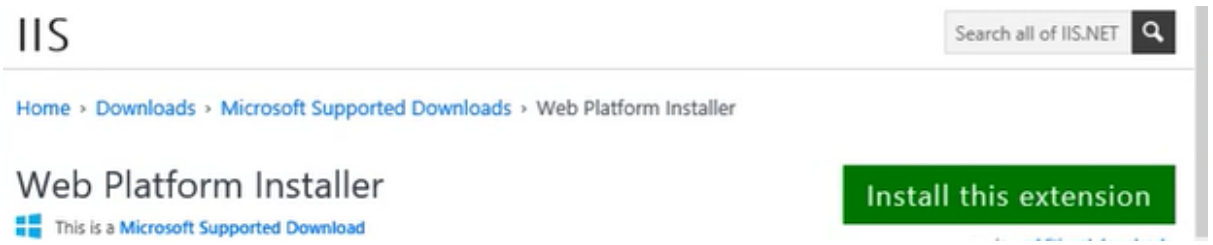


Ensuite, sélectionnez le chemin d'installation de GLPI pour le configurer correctement dans IIS.

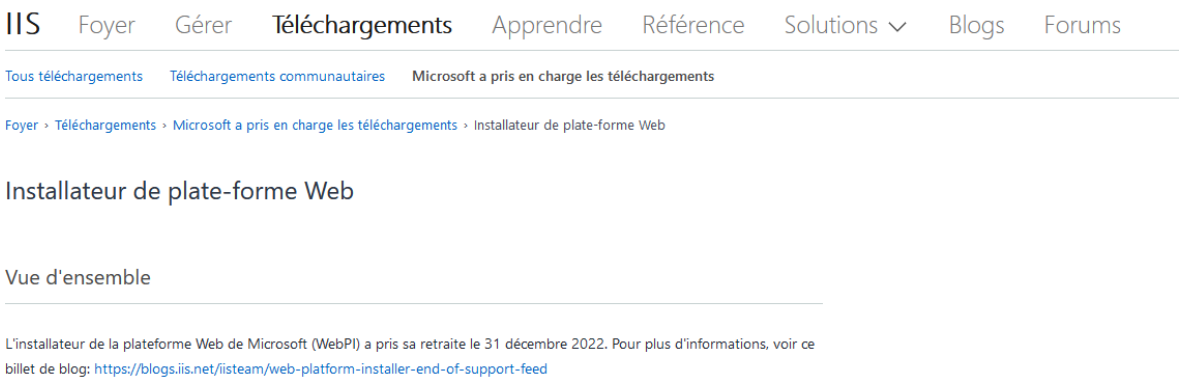


Auparavant, il fallait installer le module Web Platform pour intégrer plus facilement le service PHP ainsi que le gestionnaire PHP (PHP Manager), mais ce service a été abandonné car il est désormais obsolète

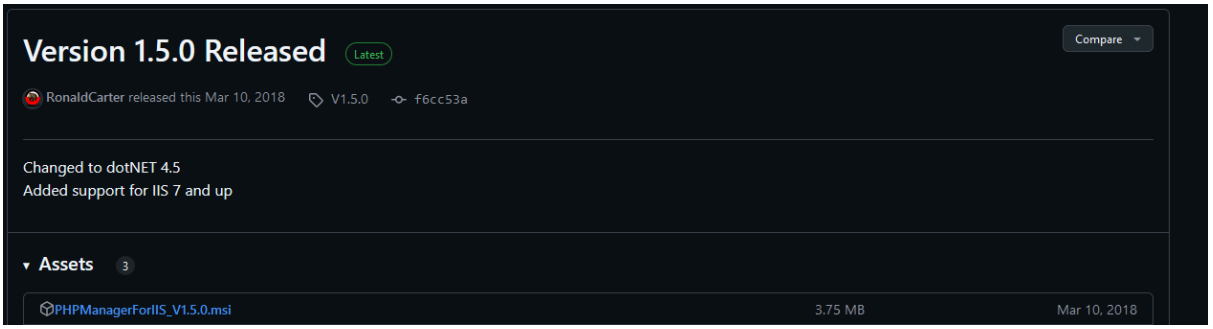




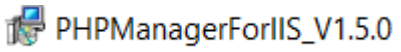
Donc, ici, je suis directement sur le serveur car je voulais installer, comme je l'ai indiqué précédemment, mais cela ne fonctionne plus car la plateforme est devenue obsolète .

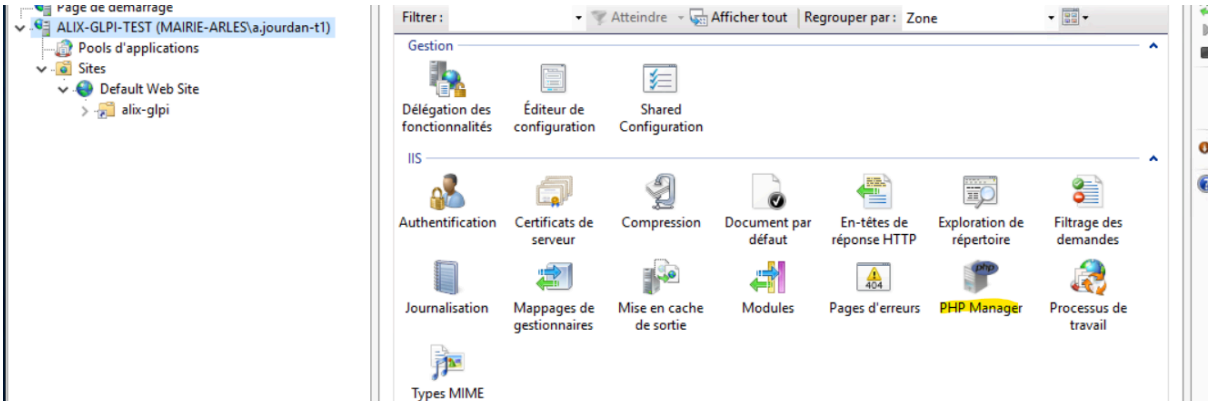


J'ai dû trouver une autre alternative pour télécharger PHP Manager et l'intégrer manuellement dans IIS. J'ai trouvé une installation adaptée à ma version sur un forum

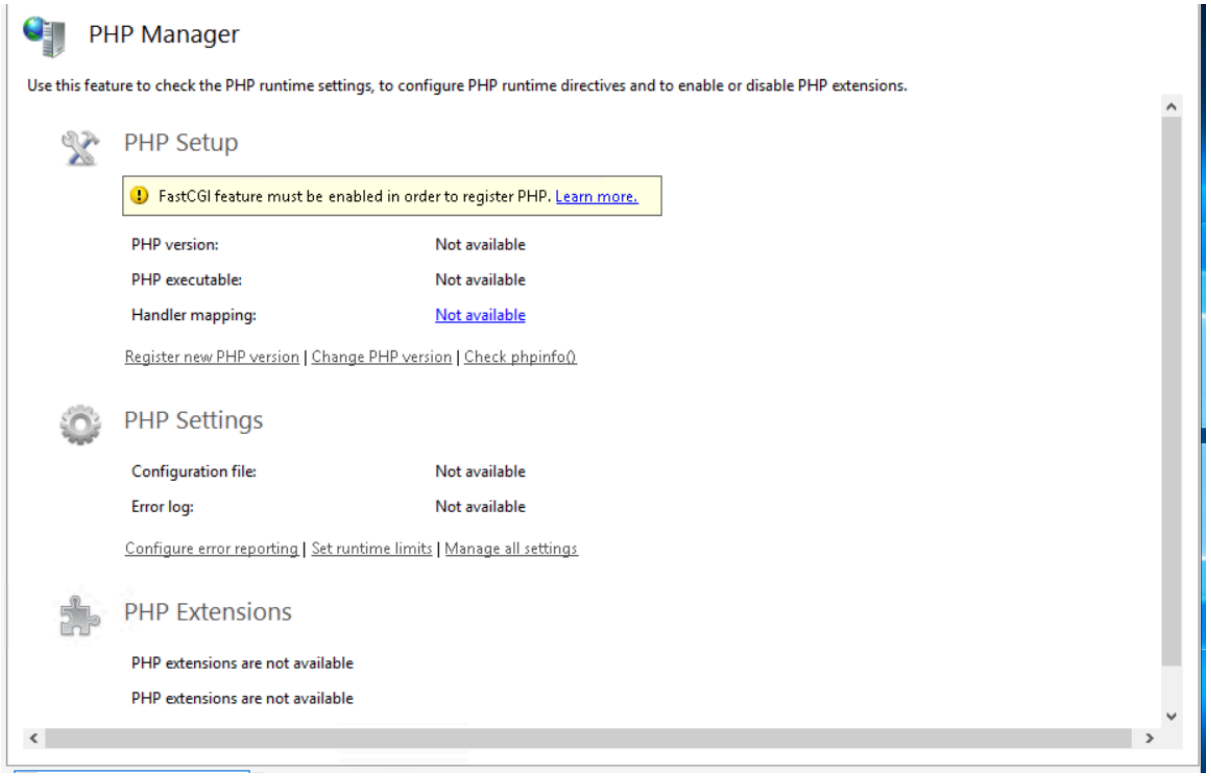


Dans cette section, je vais vous montrer qu'il n'y a rien de préconfiguré, donc je vais devoir chercher un tutoriel pour intégrer PHP moi-même.

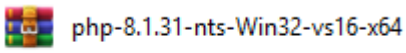


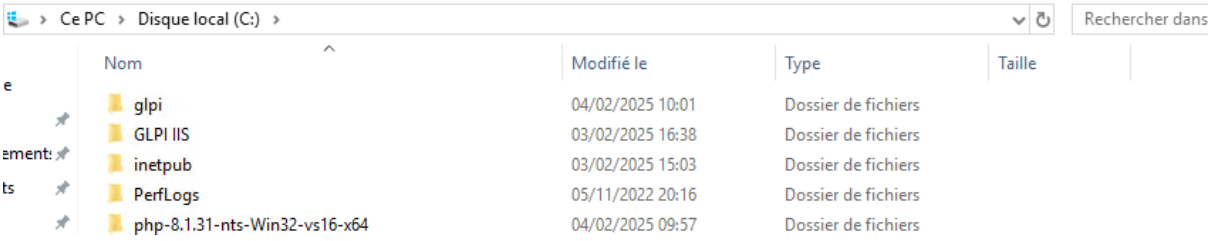


Donc, ici, on voit bien que rien n'est intégré ni configuré :

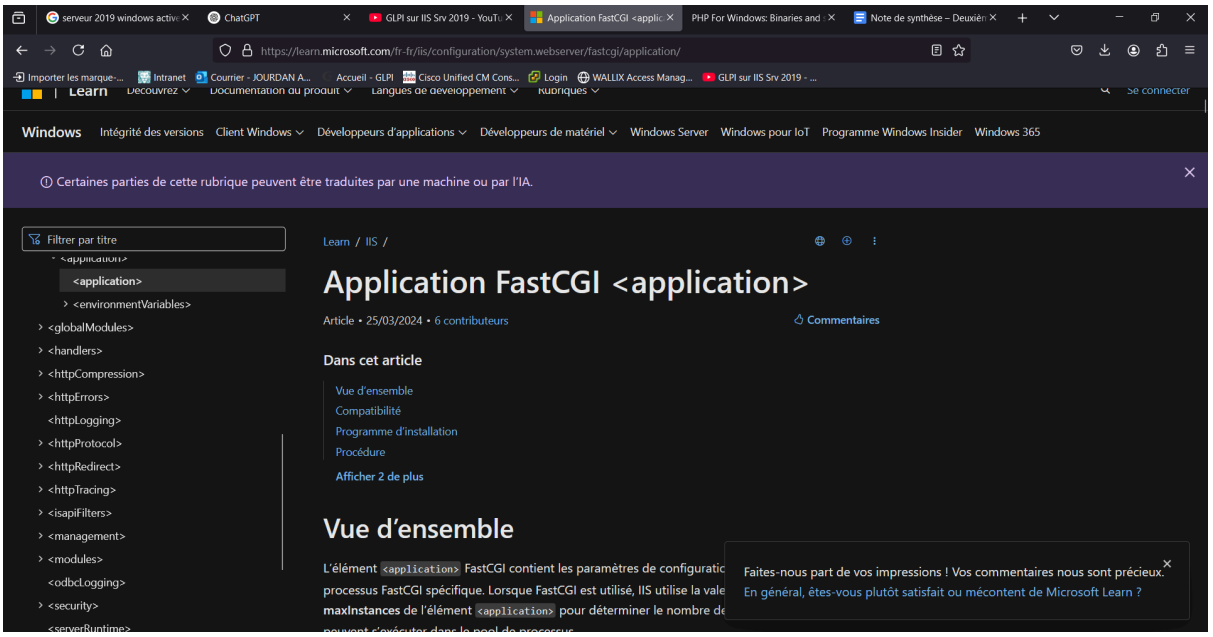


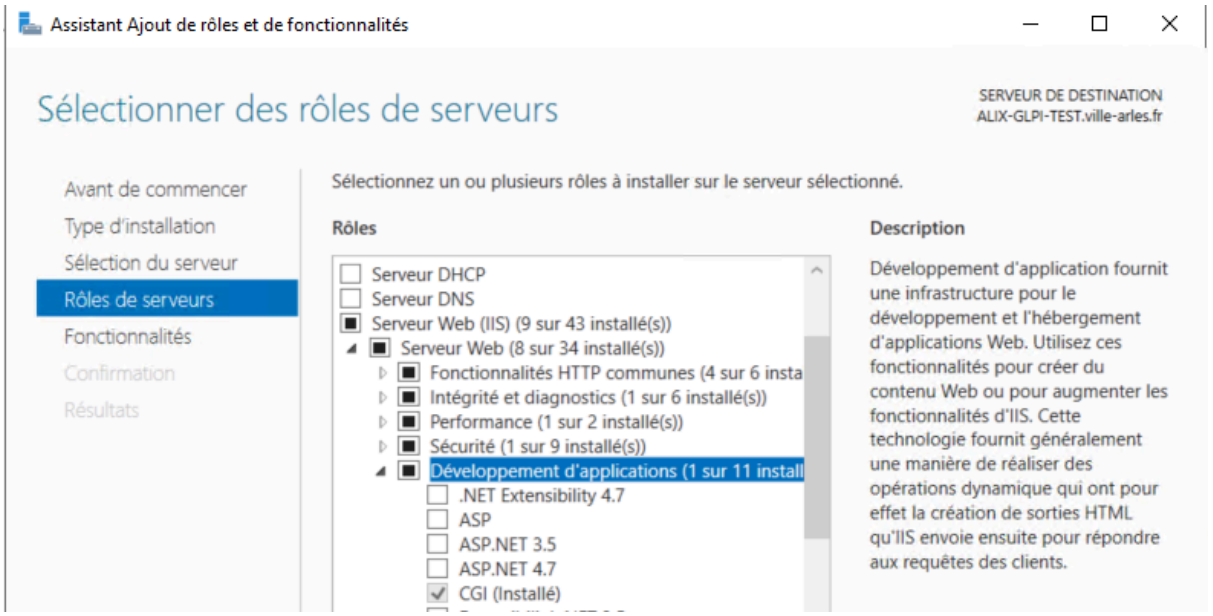
Donc, ici, j'installe PHP et je l'intègre sur le disque C.



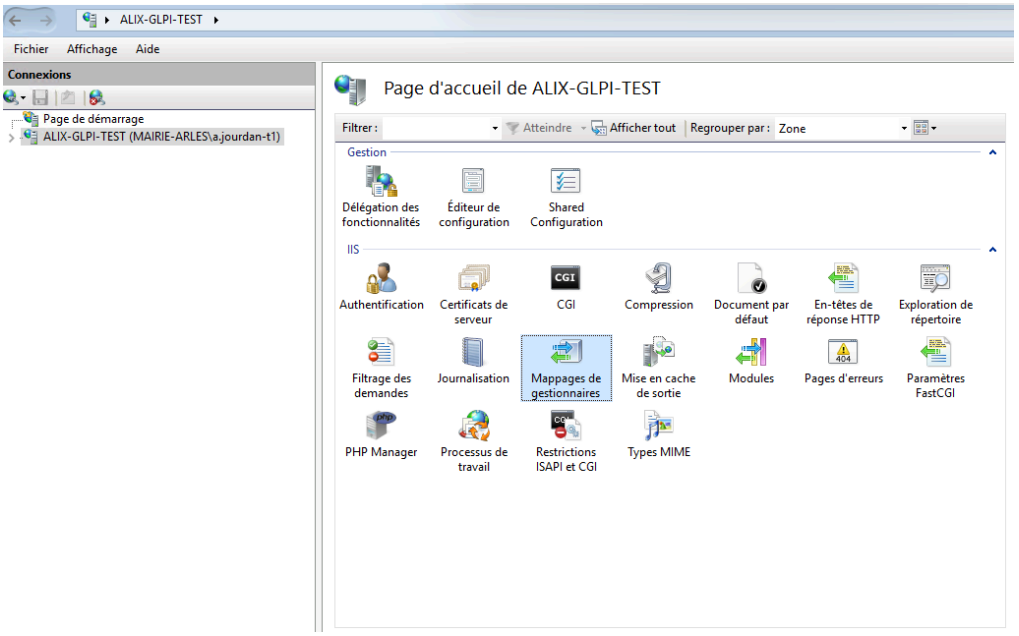


Du coup, j'ai installé l'application FastCGI pour améliorer la performance et assurer une meilleure compatibilité dans l'intégration de PHP.

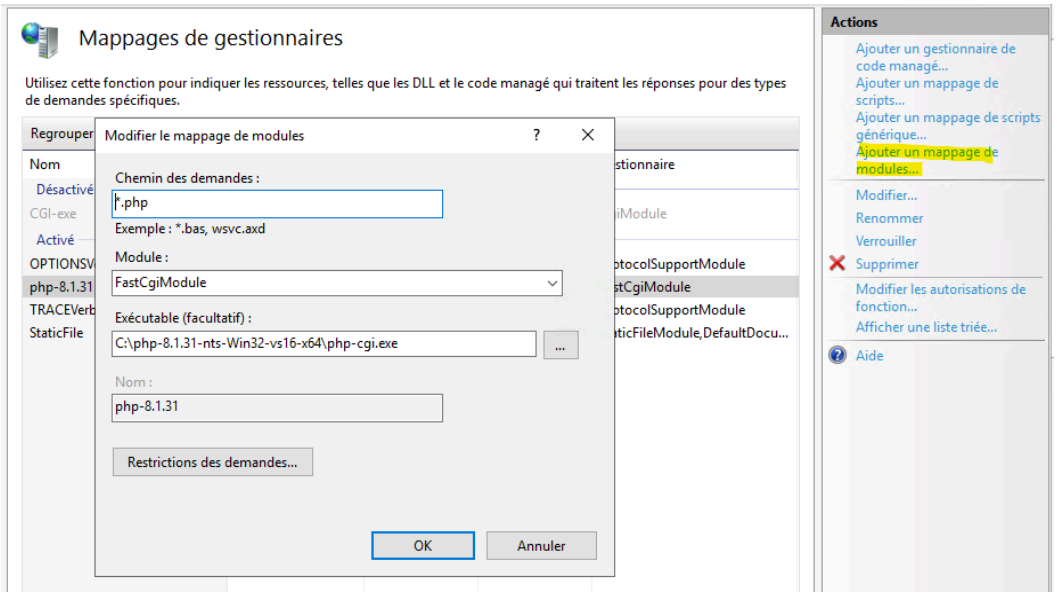




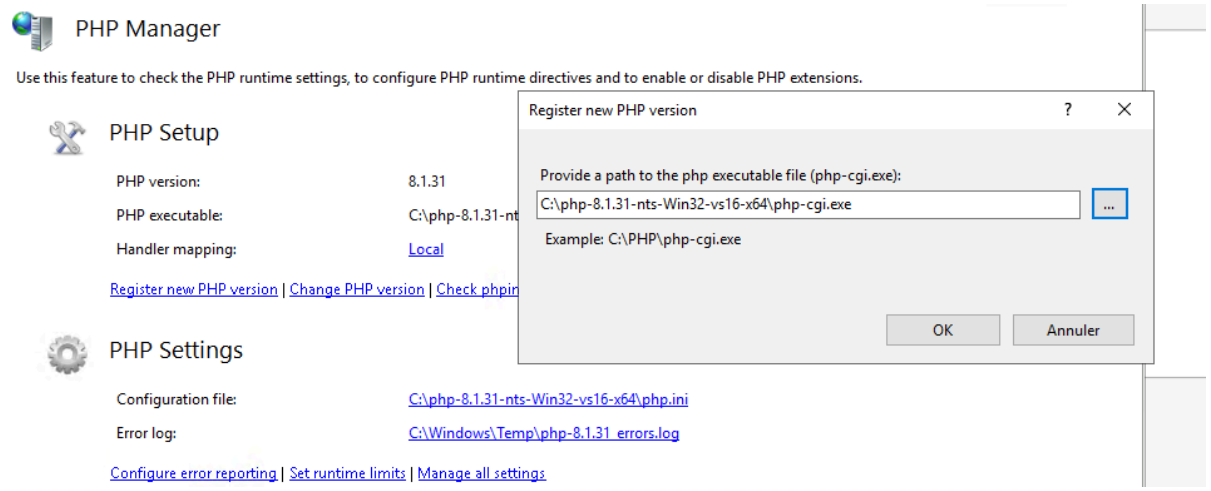
J'ai accédé au **Gestionnaire des fonctionnalités** d'IIS et sélectionné **Mappages de gestionnaires**, puis j'ai cliqué sur **Ajouter un mappage de gestionnaire**. Ce mappage est nécessaire car IIS, par défaut, ne sait pas exécuter les fichiers PHP. En l'ajoutant, j'ai configuré IIS pour utiliser **FastCGI** lors du traitement des fichiers `.php`, ce qui optimise l'exécution des scripts PHP et améliore les performances du serveur.



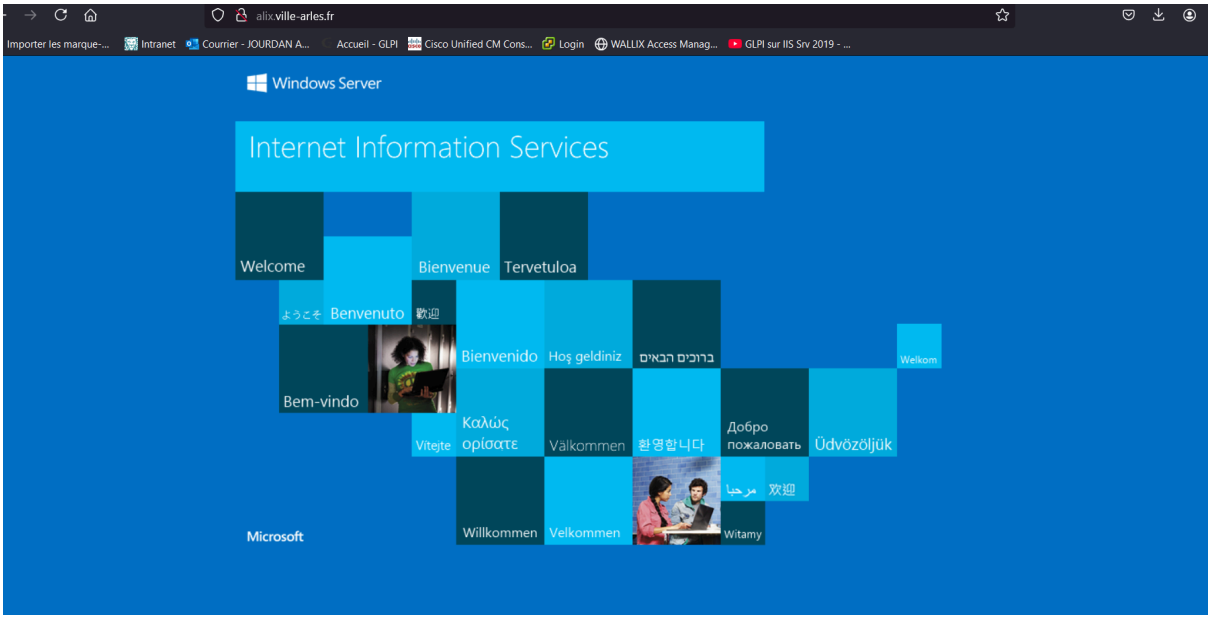
Donc, ici, je vais ajouter le module comme indiqué dans le tutoriel. Je sélectionne le chemin où se trouve l'endroit où j'ai installé PHP.



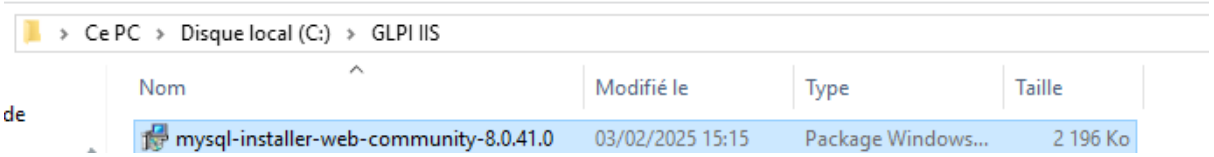
il faut appliquer ça sur tout les service sur la machine ainsi que sur mon serveur pour que ça marche :



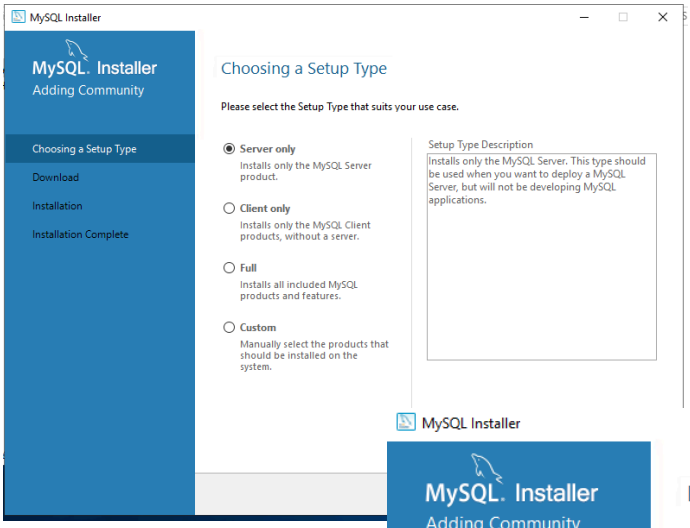
Pendant mon stage, mon maître de stage m'a montré comment utiliser des alias DNS (Domain Name System) pour mieux protéger un site internet contre les attaques. Un alias permet de créer un nom de domaine supplémentaire qui redirige vers la même adresse IP, rendant ainsi plus difficile la localisation de l'adresse IP réelle du serveur. Cela ajoute une couche de sécurité supplémentaire, car bien que le nom de domaine soit public, l'IP peut être masquée par ces alias, rendant l'attaque plus complexe :

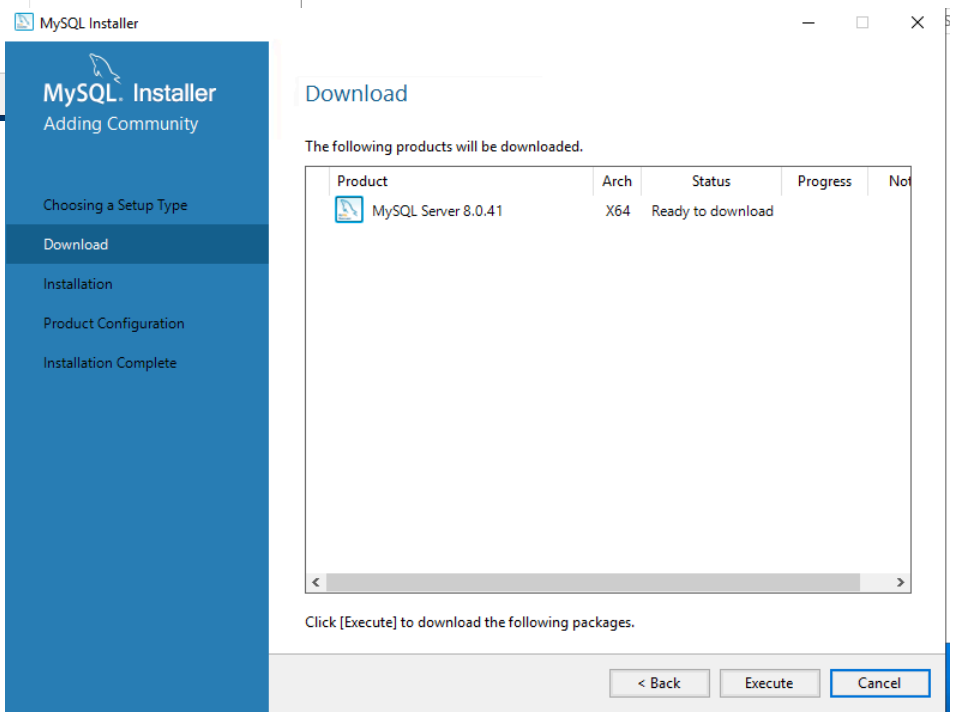


Une fois l'installation de PHP terminée et configurée, je suis passé à l'installation de MySQL. Avant cela, j'ai bien vérifié que la page de **GLPI** fonctionnait correctement, et je l'ai bien vue s'afficher.

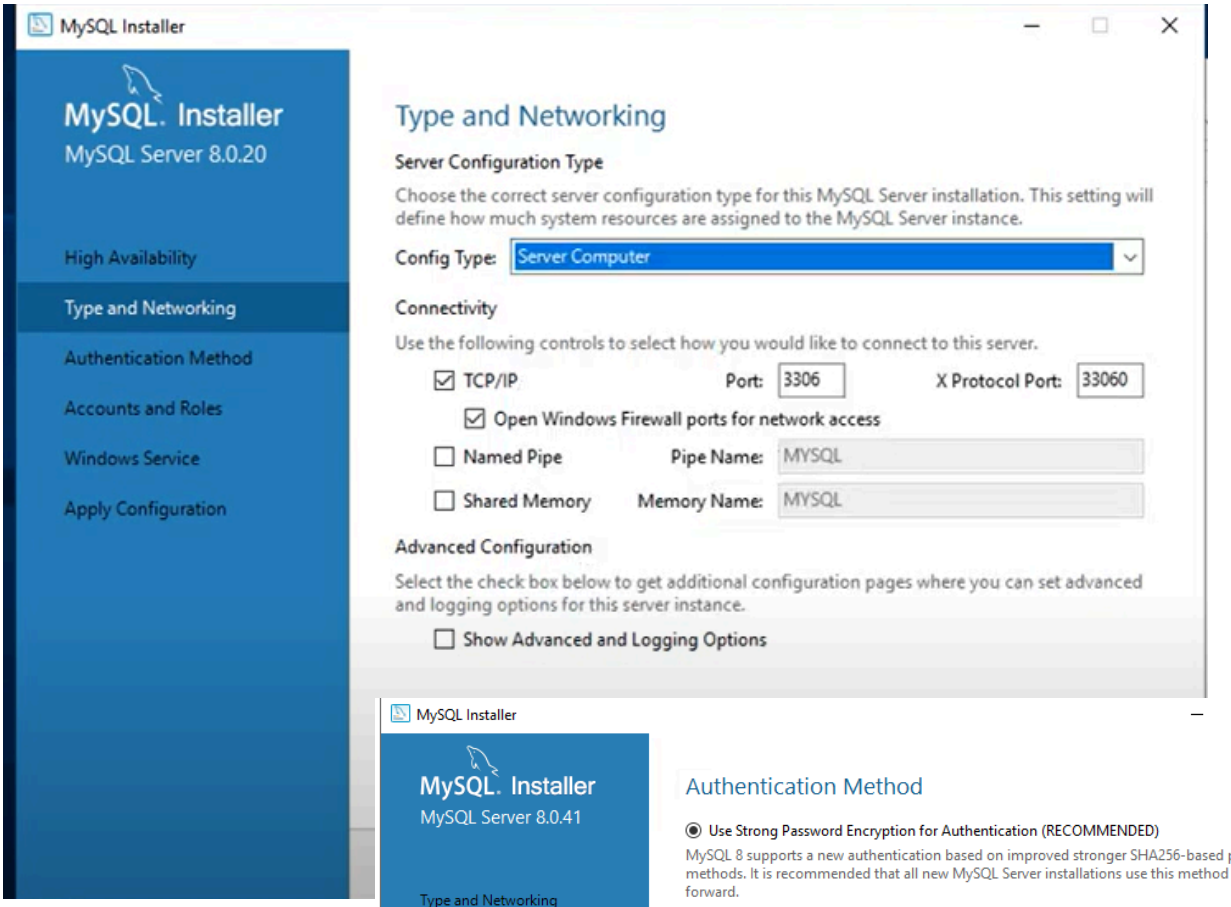


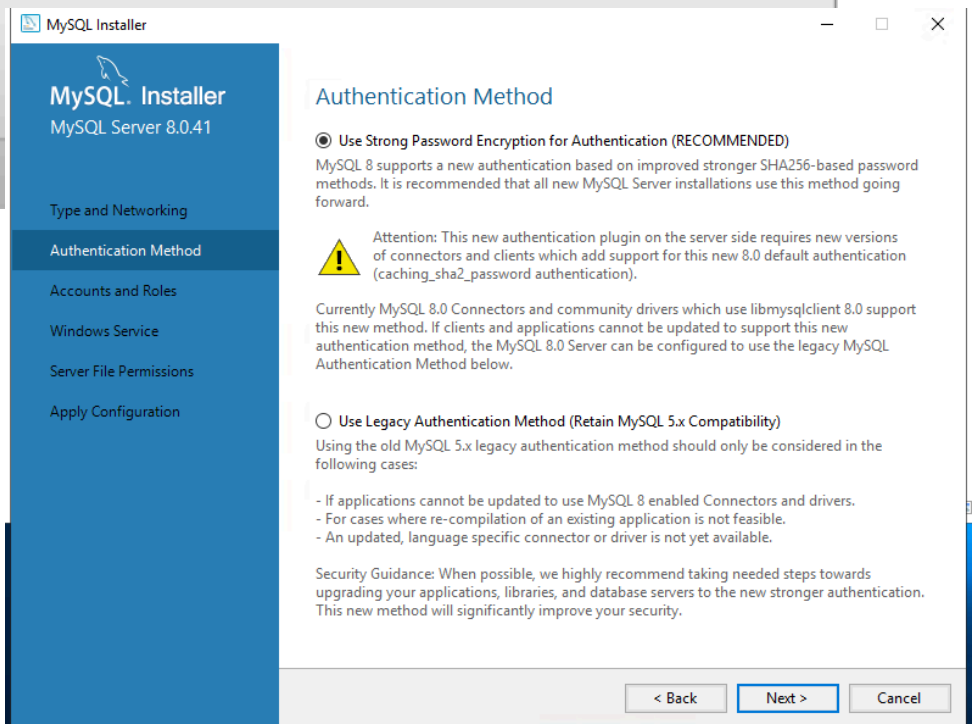
Je commence l'installation de MySQL. Tout d'abord, je choisis le type de SQL à installer ainsi que la version. Pour ma part, j'opte pour l'option Serveur unique.



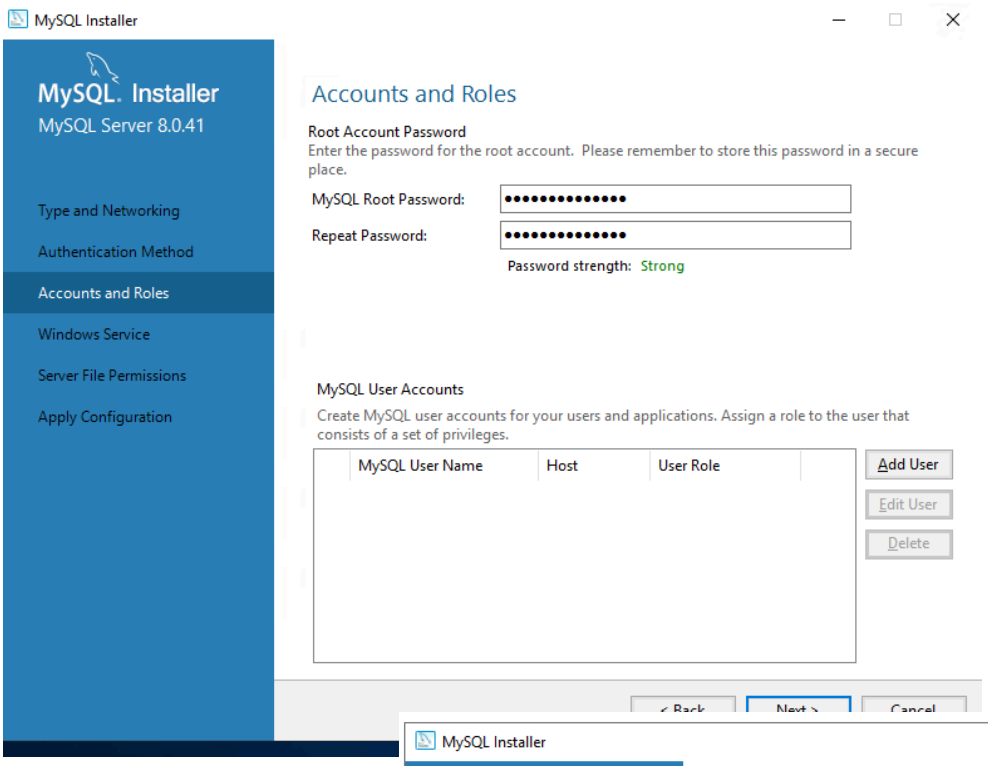


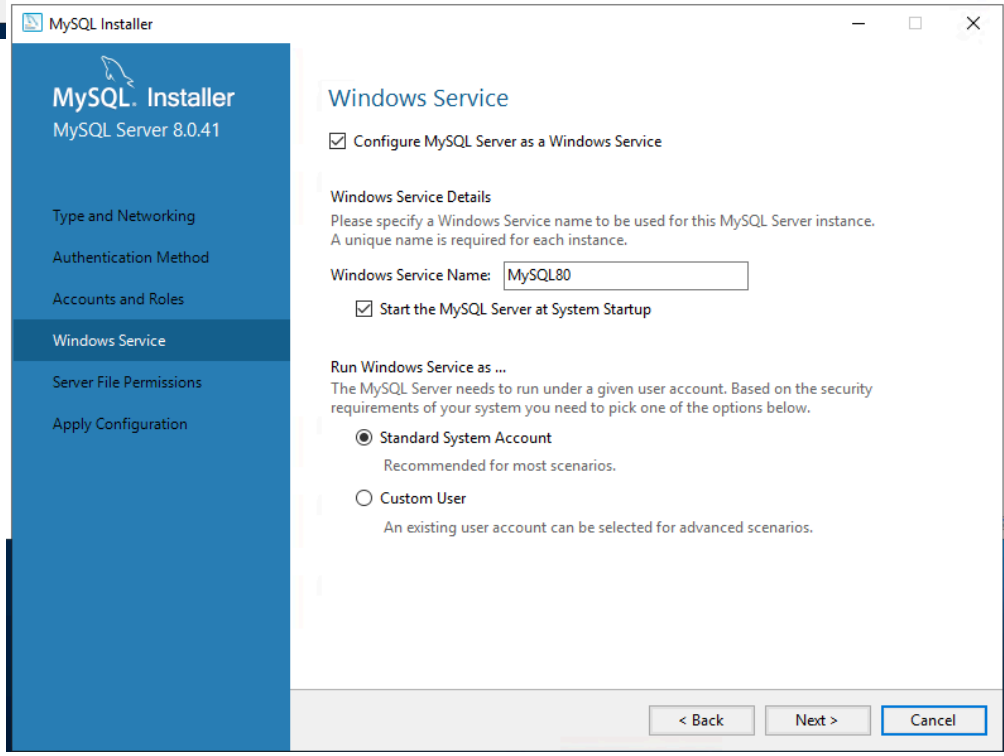
Ensuite, je choisis la configuration de type 'Server Computer' avec l'authentification cryptée.





Ensuite, je mets en place le premier compte qui va se connecter à GLPI, ainsi que la base MySQL qui sera configurée avec l'utilisateur root .



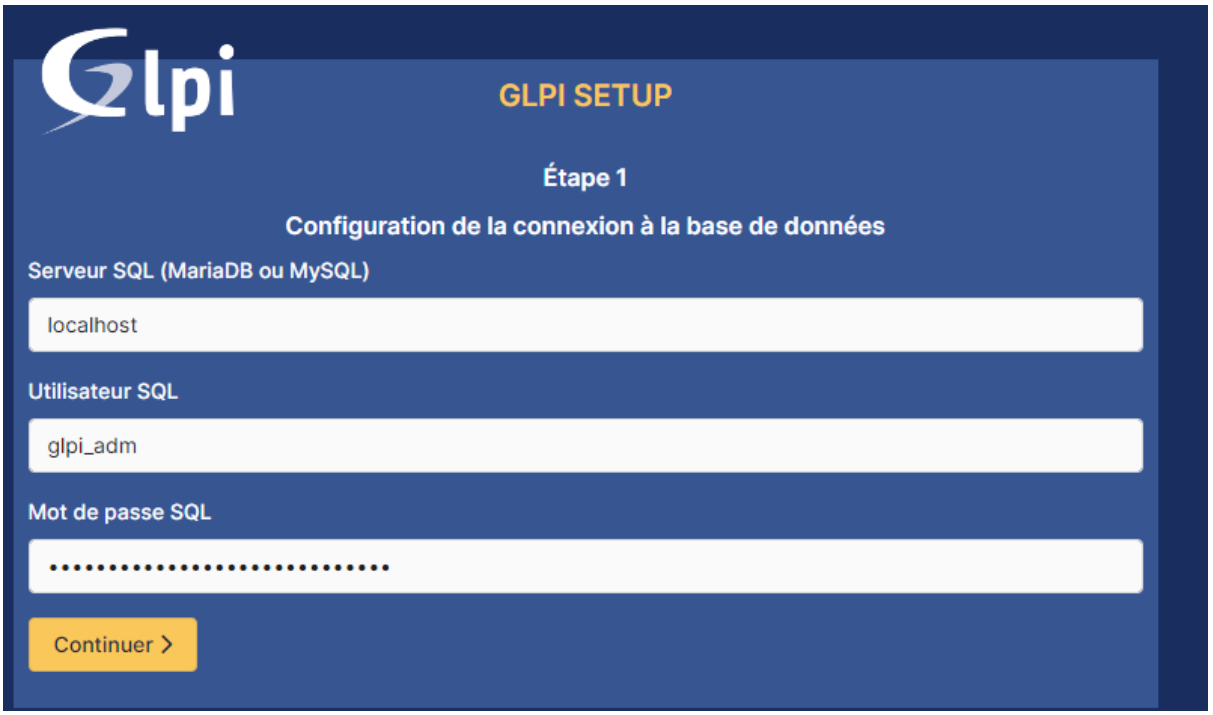


Une fois MySQL et PHP installés, je vais passer à l'installation de GLPI

donc sélectionner installer :

On voit que toutes les spécificités sur l'installation et la configuration ont bien été synchronisées donc on peut continuer l'installation .

Ensuite, sur cette partie, je vais connecter mon utilisateur root. que je viens de créer avant :

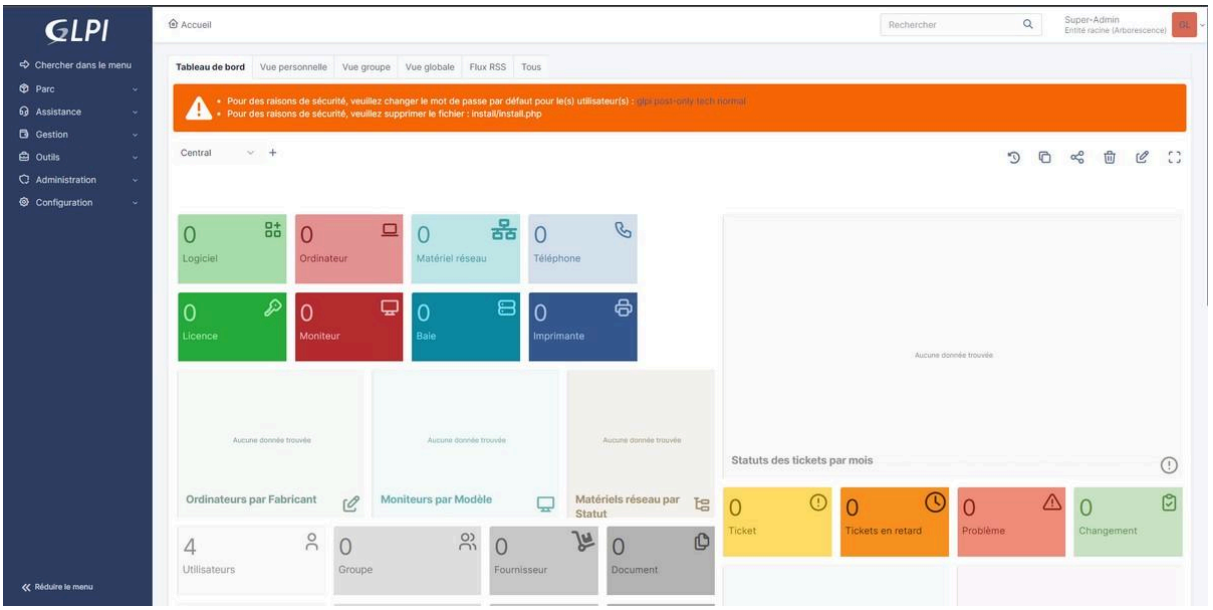


Dans cette partie, je vais créer du coup la nouvelle base de données.

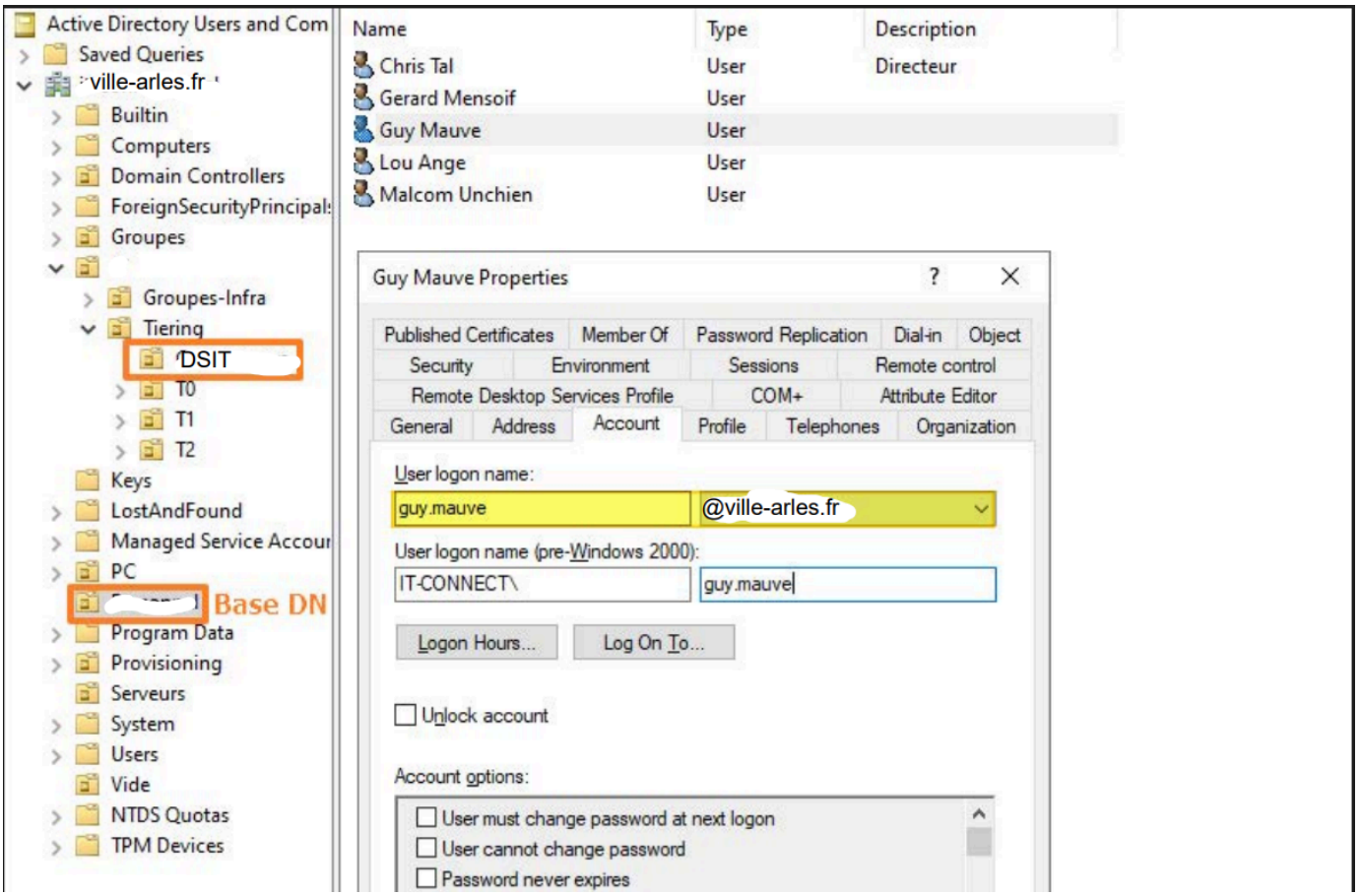
synchronisation de glpi avec l'AD :

Donc, je me connecte avec le compte root pour me connecter à GLPI

l'installation a biens réussi :

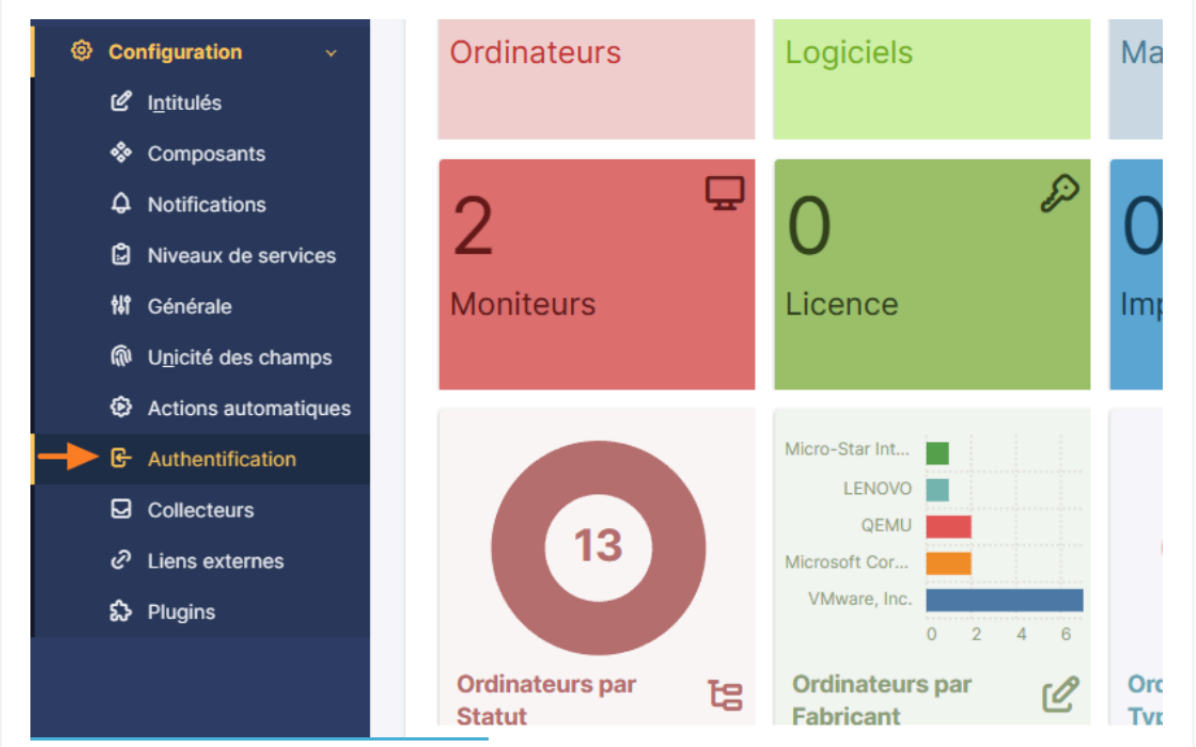


Donc, dans cette partie, je vais procéder à la synchronisation entre l'Active Directory (AD) et GLPI. Directement sur l'AD, je vais accéder au domaine et au groupe GLPI. C'est là que je vais créer les utilisateurs qui pourront se connecter à GLPI et qui appartiendront à l'AD.

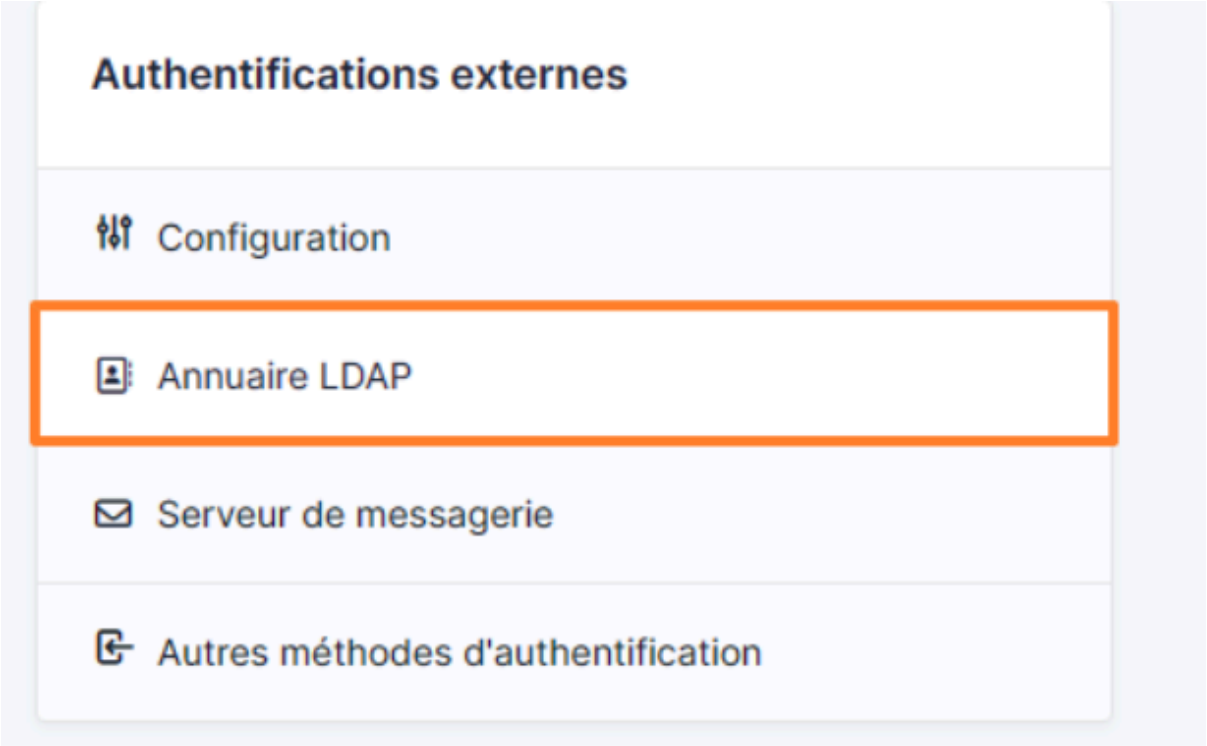


Dans cette partie je vais vous montre comment ajouter un utilisateur dans glpi qui et sur l'ad donc le relier avec LDAP :

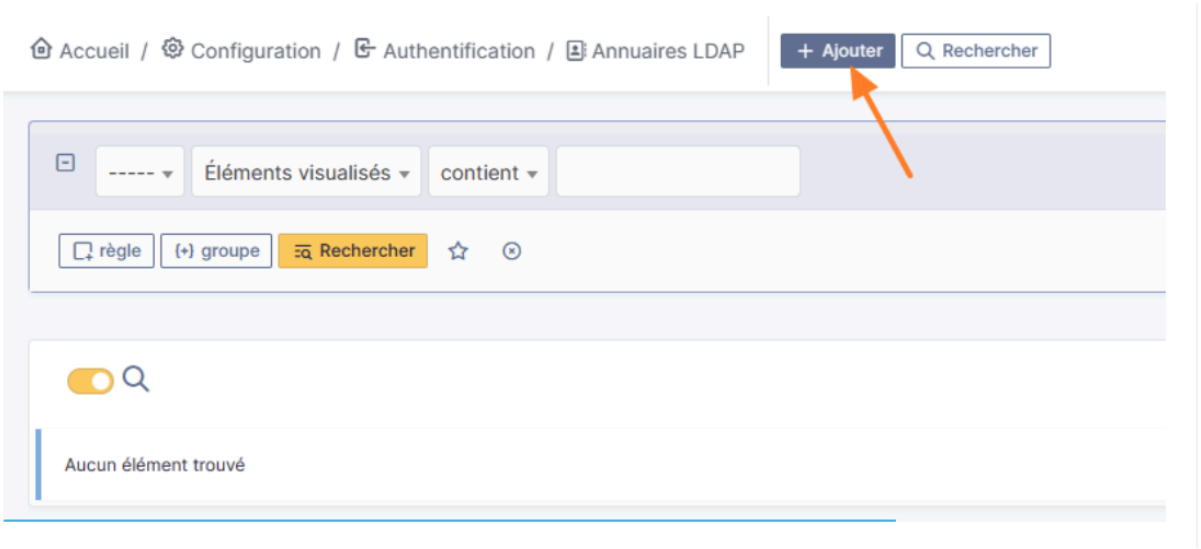
cliquez sur authentification :



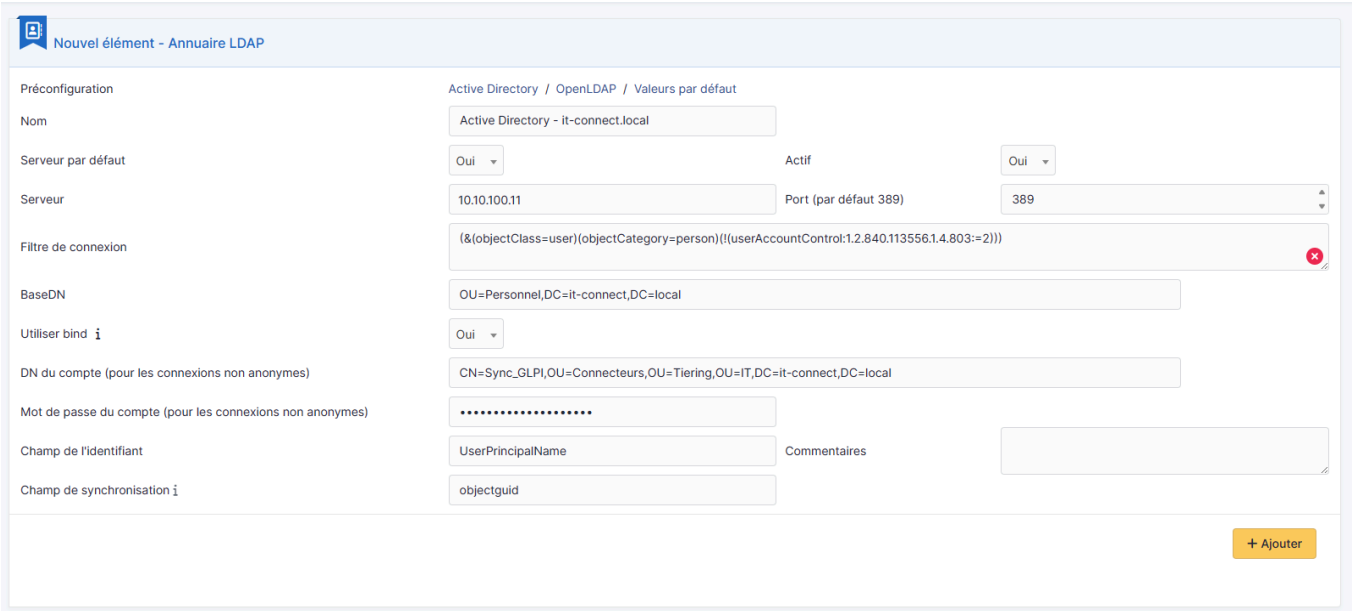
ensuite sur annuaire LDAP



et cliquez sur ajouter

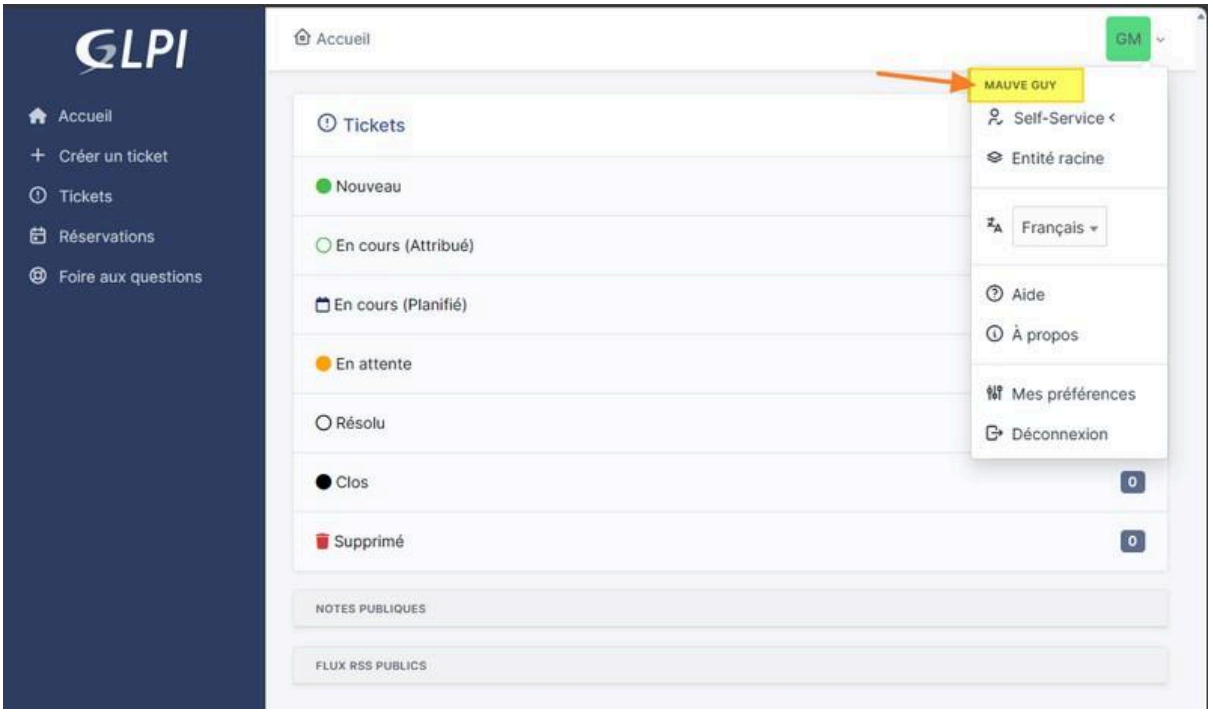


Pour connecter GLPI à Active Directory via LDAP, il est nécessaire de remplir plusieurs informations dans GLPI, notamment l'adresse du serveur Active Directory, la Base DN (qui définit le point de départ de la recherche des utilisateurs, par exemple DC=mondomaine,DC=local), et un filtre de recherche (comme (sAMAccountName=%s)) pour valider l'authentification des utilisateurs. Ces paramètres permettent à GLPI de se connecter à Active Directory, d'extraire les informations des utilisateurs et de gérer l'authentification centralisée sans avoir à créer de comptes supplémentaires dans GLPI.

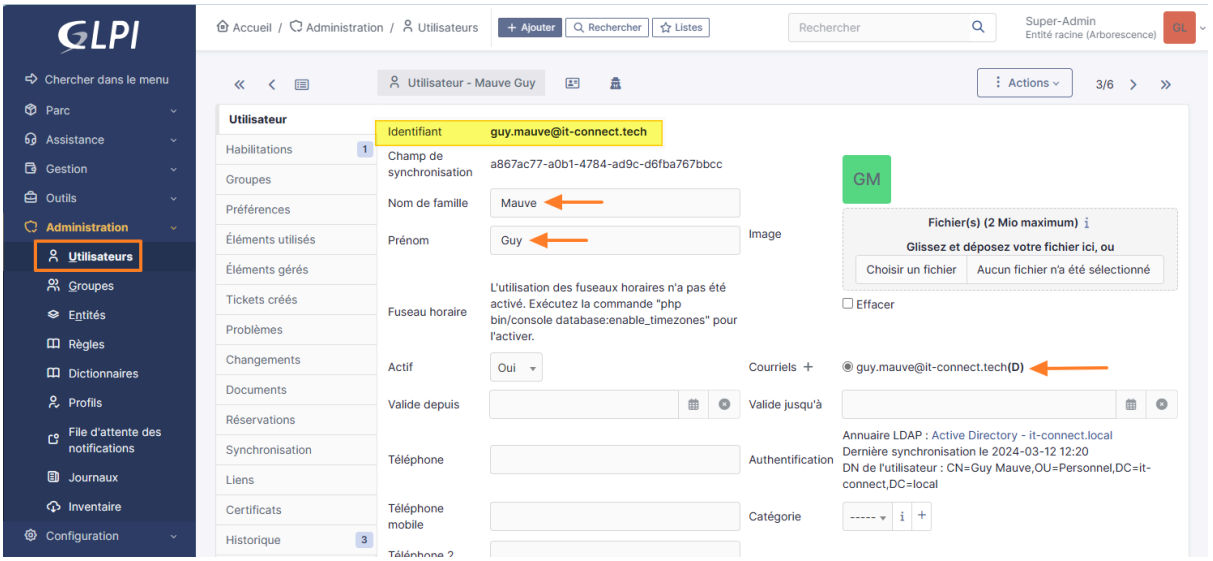


Donc là, je peux me connecter avec mon compte qui existe dans l'AD :

Donc, on voit bien sur ce screenshot que l'utilisateur que j'ai créé à bien la fonction *self-service*, c'est-à-dire que l'utilisateur va gérer les tickets.

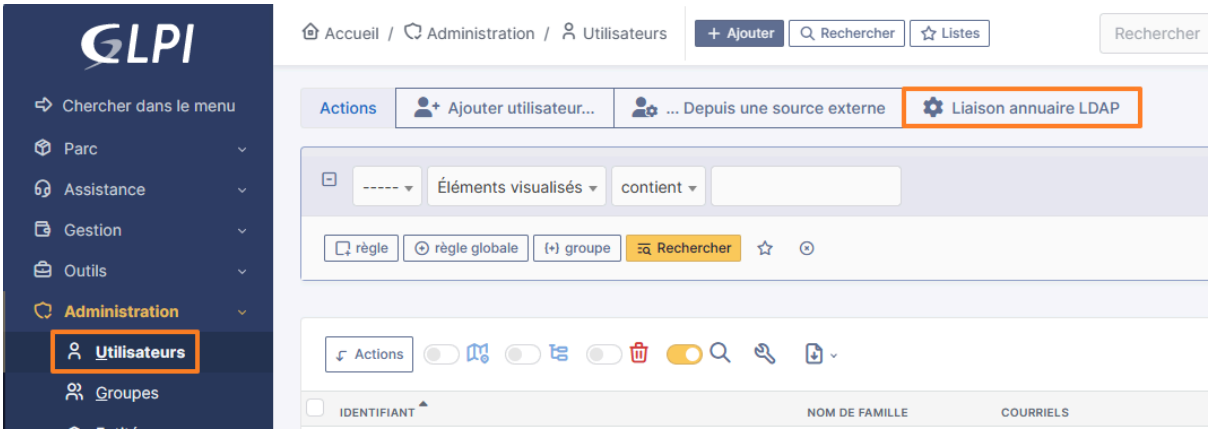


Ensuite, je retourne sur le compte administrateur et je remarque bien qu'un utilisateur a été ajouté avec son affectation de technicien.



Ensuite, dans cette deuxième partie, je vais vous montrer une synchronisation forcée ou une importation de l'AD :

Cliquez sur "**Administration**" dans le menu, puis "**Utilisateurs**". Ici, vous avez accès au bouton "**Liaison annuaire LDAP**".



Ensuite, en fonction de ce que veut faire l'administrateur, il peut soit ajouter un nouvel utilisateur, soit effectuer la synchronisation, tout dépend de ses besoins.

MISSION ANNEXE :

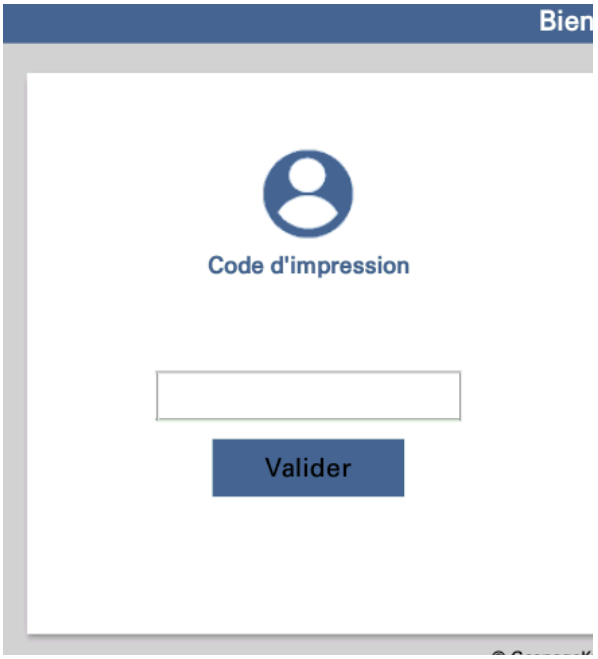
DÉPLOIEMENT COPIER :

Pendant ma période de stage à la mairie d'Arles, un contrat d'un an a été signé avec des prestataires pour installer des copieurs dans les services de la ville ainsi que dans les écoles (primaires et élémentaires). Ce contrat inclut la mise en place des nouveaux copieurs, leur gestion, ainsi que le déploiement des logiciels associés.

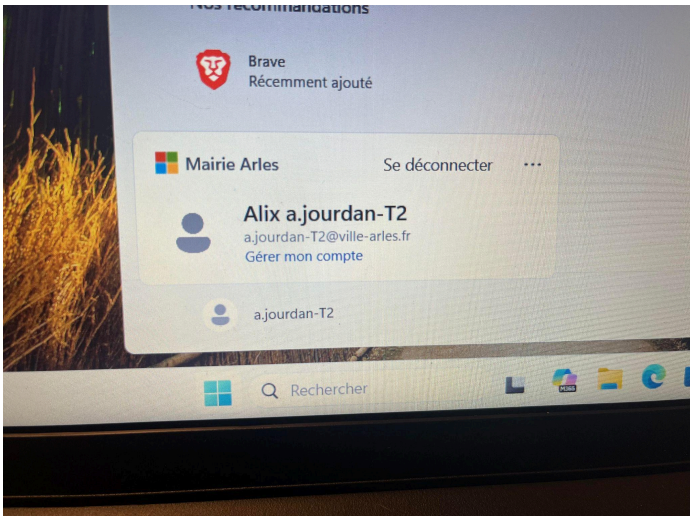
Pour le service support de la mairie, cela implique l'installation du logiciel sur chaque PC, ainsi que l'accompagnement des utilisateurs pour leur expliquer comment se connecter et imprimer. Chaque utilisateur doit se connecter à l'imprimante à l'aide d'un code PIN afin de pouvoir imprimer sur le copieur.

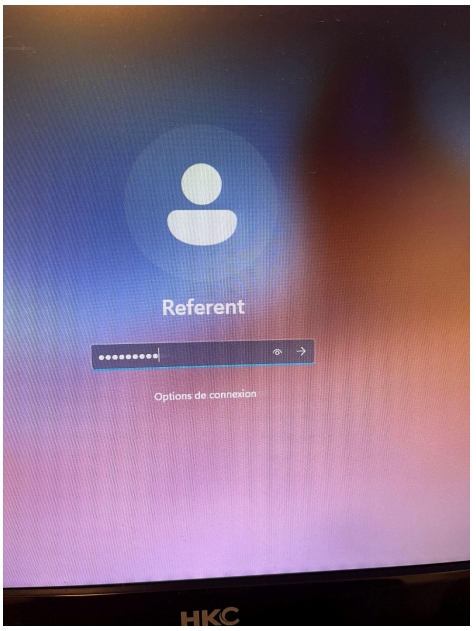
Sur cette image, nous devons installer la nouvelle imprimante, débrancher l'ancienne, et expliquer aux utilisateurs comment imprimer, car chaque connexion ou impression nécessite un code PIN

Voici le code pin

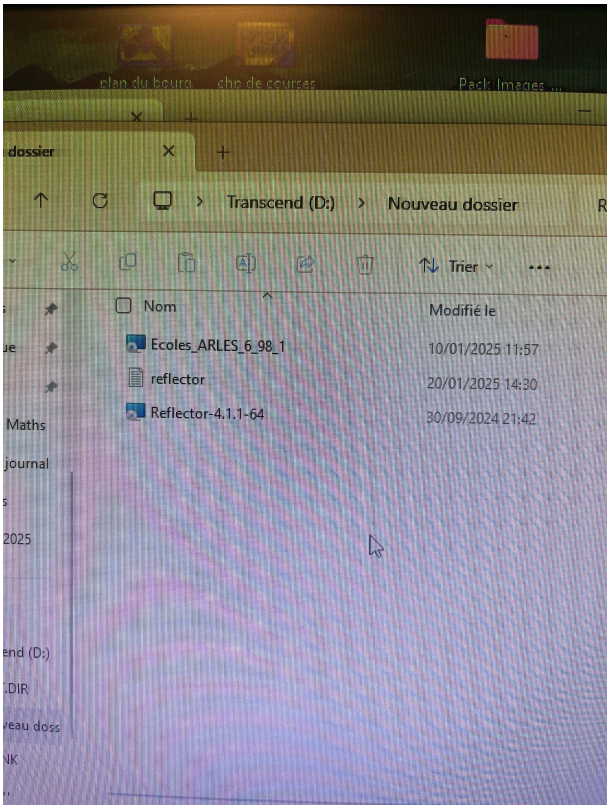


Ensuite, pour les ordinateurs des agents, je devrai me connecter soit sur le domaine avec mon compte T2, soit en local avec le compte administrateur ou référent, afin d'installer le logiciel.

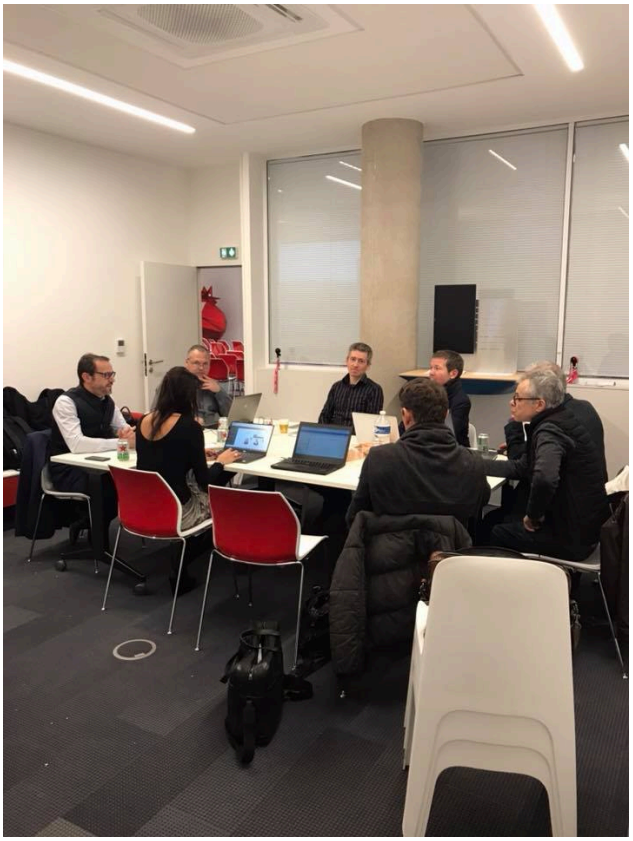




On peut ici voir les logiciels à déployer sur chaque ordinateur des agents des écoles, ainsi que le logiciel pour l'imprimante, Reflector, et celui permettant de connecter les écoles pour afficher leurs tablettes sur l'écran.



formation sur la sécurité de l'infrastructure réseaux :



formation sur la sécurité de l'infrastructure réseaux :

Lors de ma période de formation, j'ai suivi un cours sur la configuration et la mise en place de la double authentification ainsi que du protocole RADIUS avec Fortinet. J'ai également suivi une autre formation axée sur le tiering, permettant de restreindre l'accès à certains contenus, services ou serveurs avec les comptes T1,T2,T0.

Objectif de l'intervention du prestataire Pour Radius :
Le prestataire est intervenu pour nous former afin de renforcer la sécurité des accès au réseau, en mettant en place une solution de double authentification (2FA) via Fortinet et un serveur RADIUS local pour l'authentification des utilisateurs, soit par un pop-up, soit par un code délivré via l'application Fortinet Authenticator. Cette approche vise à réduire les risques d'accès malveillant et à assurer un contrôle plus strict des utilisateurs internes. La mairie d'Arles avait constaté que son système Active Directory (AD) était trop vulnérable. En effet, si un attaquant parvenait à pénétrer dans l'AD et obtenait des droits d'administration sur le proxy, les règles du pare-feu ou le VLAN, il pourrait potentiellement bloquer l'ensemble des services. C'est pour cette raison qu'ils ont fait appel à un prestataire afin de se protéger contre ce risque potentiel.

Détails de la solution proposée durant la formation :

Double authentification (2FA) sur Fortinet :

- La **double authentification** (2FA) sera mise en place sur les dispositifs Fortinet (principalement les pare-feu FortiGate et le proxy) afin de renforcer la sécurité des connexions réseau.
- **FortiAuthenticator** sera utilisé pour gérer l'authentification à deux facteurs, ajoutant une couche de sécurité supplémentaire avec un code de validation en plus du mot de passe.

Authentification via le protocole RADIUS local :

- Un serveur **RADIUS local** sera déployé pour gérer l'authentification des utilisateurs sans être lié à **Active Directory**. Cette approche permet de

garantir que, même si un utilisateur malveillant réussit à s'introduire dans l'Active Directory, il ne pourra pas accéder aux ressources protégées par le **RADIUS** (comme le proxy ou d'autres services réseau).
- Le serveur RADIUS servira à valider l'accès aux dispositifs Fortinet de manière indépendante, afin d'assurer une séparation de la gestion des accès et de minimiser les risques liés à une compromission de l'annuaire Active Directory.

Surveillance et gestion des données avec Wireshark :

- **Wireshark** sera utilisé pour analyser et surveiller les échanges de données entre le serveur RADIUS et les dispositifs Fortinet. Cet outil permettra de vérifier que les processus d'authentification fonctionnent correctement et de détecter tout dysfonctionnement ou tentative d'intrusion dans le réseau.
- L'analyse des paquets permettra également de diagnostiquer et résoudre rapidement les problèmes techniques.

Bénéfices attendus :

- **Sécurisation des accès internes** : La mise en place d'un serveur RADIUS local assure que même en cas de compromission de l'Active Directory, les accès aux services critiques (comme le proxy) restent protégés.
- **Renforcement de la sécurité** avec la 2FA pour garantir que les utilisateurs doivent prouver leur identité de manière plus rigoureuse.
- **Supervision réseau** grâce à l'utilisation de Wireshark pour analyser les flux de données et détecter toute anomalie.

Conclusion :

La solution proposée avec **RADIUS local** et **double authentification** assure une sécurité accrue pour l'accès aux ressources réseau. Elle permet de protéger les services critiques contre les risques de compromission de l'Active Directory, tout en offrant un contrôle d'accès plus rigoureux grâce à la 2FA. La surveillance du réseau avec **Wireshark** garantira une gestion optimale des données et une détection rapide des éventuels incidents.

Objectif de l'intervention du prestataire Pour tiering de l'Active Directory :

L'autre prestataire est intervenu pour nous former et renforcer la sécurité des accès au réseau, en mettant en place une solution de tiering lors des connexions à des services contenant des informations critiques. C'est dans ce cadre que la mairie d'Arles a fait appel à un prestataire et a réalisé un audit pour anticiper les risques futurs. Il a été recommandé de se référer au tiering, un protocole recommandé par l'ANSSI, qui comprend les niveaux T0, T1 et T2.

Avant cette démarche, l'ensemble des comptes administrateurs dans le service informatique de la mairie d'Arles étaient laissés ouverts, ce qui représentait un risque majeur. Si un administrateur oubliait de fermer sa session, des utilisateurs malintentionnés, en accédant au PC d'un utilisateur lambda, pouvaient exploiter cette vulnérabilité pour se connecter en tant qu'administrateur. Cela leur permettait de verrouiller l'accès ou de perturber les services. C'est pourquoi la mairie d'Arles a décidé de faire appel à un prestataire et de procéder à cet audit pour prévenir de tels risques.

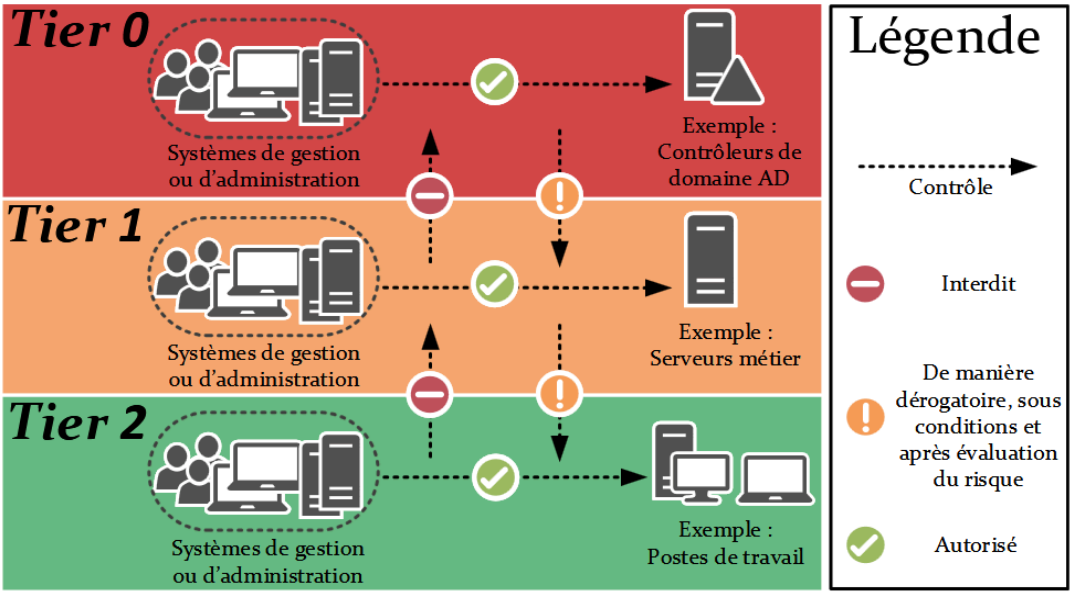
Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory

L'ANSSI fait régulièrement le constat que des compromissions de systèmes d'information (SI) reposant sur un annuaire Active Directory (AD) résultent de l'application de mauvaises pratiques d'administration et d'un cloisonnement insuffisant. Ces compromissions commencent souvent par des attaques qui ciblent les postes de travail. Les attaquants exploitent ensuite des faiblesses du SI pour opérer des déplacements, dits latéraux et élever progressivement leurs privilèges jusqu'à obtenir le contrôle total de l'AD. À ce niveau de contrôle de l'AD, un attaquant est en mesure de s'aménager des portes dérobées qui lui assurent un contrôle persistant du SI, c'est-à-dire également des processus et des données métiers de l'organisation.

Le guide d'administration sécurisée des systèmes d'information reposant sur un annuaire AD aborde les aspects spécifiques à l'administration de ces environnements et guide dans le cloisonnement du SI en zones de confiance. Il complète ainsi les *recommandations de sécurité relatives à l'administration sécurisée des systèmes d'information* qui se veulent agnostiques des technologies mises en œuvre.

Comprendre le tiering et son rôle pour chaque compte :

Le tiering est mis en place pour contrôler les accès et restreindre certaines actions. En cas d'incident malveillant, si un compte est compromis, le tiering permet de limiter les conséquences en s'assurant que l'attaque ne puisse pas atteindre des niveaux supérieurs, comme le T1 ou le T0. Ainsi, l'attaque reste confinée au niveau du T1, avec les privilèges spécifiques associés à ce niveau. Chaque groupe de niveau T1 dispose de spécifications et de restrictions appliquées via des GPO (Group Policy Objects).



- Administrateur T0 : Un administrateur T0 peut gérer uniquement les composants de la couche T0. Il peut se connecter via RDP uniquement sur des serveurs intégrés à ce niveau, tels que les contrôleurs de domaine, la PKI (Public Key Infrastructure), ADFS (Active Directory Federation Services), etc. Cet accès ne doit en aucun cas être utilisé pour se connecter à des serveurs d'une couche inférieure. De plus, les administrateurs T0 n'enregistrent pas leurs mots de passe dans la base de données ou sur les ordinateurs, car ils sont protégés par le groupe Protected Users, qui ajoute une couche de sécurité supplémentaire pour éviter le stockage local des identifiants.

- Administrateur T1 : Un administrateur T1 gère les serveurs applicatifs et autres middlewares au sein de l'infrastructure de l'entreprise. Il ne doit pas utiliser ses privilèges pour se connecter à des serveurs d'une couche supérieure ou inférieure.

- Administrateur T2 : Un administrateur T2 gère les postes de travail des utilisateurs et autres périphériques. Ce compte ne doit pas être utilisé pour accéder aux couches supérieures.

Conclusion :

Dans le cadre de la sécurisation des accès au réseau de la mairie d'Arles, l'intervention du prestataire a permis de mettre en place une solution de tiering pour protéger les services contenant des informations critiques. En réponse aux risques identifiés lors de l'audit, la mairie a choisi de renforcer la gestion des comptes administrateurs, en appliquant un protocole de tiering recommandé par l'ANSSI. Ce protocole, structuré autour des niveaux T0, T1 et T2, vise à limiter l'accès aux systèmes en fonction du rôle de chaque administrateur, garantissant ainsi que toute tentative malveillante reste confinée à un niveau limité.

Avant la mise en place de ce tiering, les comptes administrateurs étaient laissés ouverts, créant des vulnérabilités exploitées par des utilisateurs malintentionnés qui pouvaient accéder à des niveaux critiques du système. Aujourd'hui, chaque niveau d'administration est clairement défini pour assurer une meilleure séparation des responsabilités et restreindre les privilèges d'accès en fonction du rôle spécifique, que ce soit pour un administrateur T0, T1 ou T2.

En conclusion, l'introduction du tiering au sein de l'Active Directory de la mairie d'Arles contribue à réduire les risques en isolant les accès et en appliquant des restrictions de manière granulaire. Cela garantit une meilleure sécurité des systèmes et un contrôle renforcé des accès aux informations sensibles, répondant ainsi efficacement aux défis de la cybersécurité.

Référentiel sur la partie juridique du service informatique de la Mairie d'Arles :

Dans cette section, je vais aborder l'aspect juridique du service informatique de la Mairie d'Arles.

Au sein de la Mairie d'Arles, le service informatique est rattaché à la région, qui est une collectivité territoriale. Ce service a mis en place trois grands pôles pour gérer les aspects juridiques, la sécurisation, la cybersécurité et les finances.

En premier lieu, il y a le **DSI** (Directeur des Systèmes d'Information). C'est lui qui prend les décisions principales et gère l'ensemble du budget alloué à la sécurité informatique. C'est également lui qui sollicite les financements nécessaires pour mettre en œuvre ces mesures de sécurité, telles que l'achat de nouveaux outils de protection, la formation des employés, ou encore la mise en place de protocoles de sécurité renforcés. Le DSI a une responsabilité importante, car il doit veiller à ce que les investissements en matière de sécurité informatique soient effectués de manière à protéger efficacement les données sensibles de la mairie.

Ensuite, il y a le **RSSI** (Responsable de la Sécurité des Systèmes d'Information). Ce rôle est essentiel pour garantir la sécurité du parc informatique, la cybersécurité et la protection des données personnelles. Le RSSI prend les décisions relatives à la sécurisation des systèmes, ainsi qu'à la mise en place de mesures préventives et réactives en cas de cyberattaque. Il est également responsable de la gestion des incidents de sécurité. En cas de violation de données, le RSSI doit rédiger des rapports détaillant les événements survenus et les actions mises en place pour résoudre la situation et éviter que cela ne se reproduise. Ces rapports sont ensuite envoyés aux autorités compétentes, telles que la CNIL, et doivent être conservés pour démontrer que les actions nécessaires ont été entreprises.

Le **DPO** (Délégué à la Protection des Données) a pour mission de garantir que la Mairie d'Arles respecte les exigences du **Règlement Général sur la Protection des Données** (RGPD). Il est chargé de sensibiliser les employés à la notion de données personnelles, d'assurer leur formation et de vérifier que la collecte et le traitement des données respectent la législation en vigueur. Le DPO est également responsable de la mise en place des procédures en cas de fuite ou de violation de données personnelles, en plus de leur notification à la CNIL. Si un incident se produit, il doit rédiger des rapports pour documenter les actions entreprises et garantir que la Mairie a pris toutes les mesures possibles pour protéger les données personnelles.

Les relations contractuelles avec les prestataires externes :

Lorsqu'une **Mairie** ou toute autre entité publique passe un contrat avec un prestataire externe pour des services informatiques, ce contrat doit impérativement comporter des **clauses spécifiques** pour garantir la **confidentialité**, le respect du **RGPD** et la sécurité des **infrastructures**. Ces clauses ont pour objectif de protéger les données sensibles et d'assurer la conformité avec les obligations légales.

1. **Clause de confidentialité** :
   Les prestataires doivent s'engager à respecter la confidentialité des informations auxquelles ils auront accès dans le cadre de l'exécution du contrat. Cette clause de confidentialité garantit que le prestataire ne divulguera aucune information sensible sans autorisation préalable. Elle est essentielle pour protéger les données personnelles des citoyens et des employés de la Mairie.
2. **Respect du RGPD** :
   Le contrat doit explicitement indiquer que le prestataire s'engage à respecter les exigences du **Règlement Général sur la Protection des Données** (RGPD). Cela inclut des engagements concernant la **sécurisation des données personnelles**, la **transparence** sur leur traitement, et l'assurance que toutes les mesures nécessaires sont prises pour protéger ces données contre tout accès non autorisé, perte ou destruction.
   Le prestataire doit également être informé de ses **obligations** de notifier rapidement à la Mairie en cas de violation de données, conformément à l'article 33 du RGPD qui impose une notification sous 72 heures. En outre, des **audits réguliers** doivent être réalisés pour garantir la conformité avec les règles de protection des données.
3. **Sécurisation des infrastructures et des réseaux** :
   Il est crucial que le prestataire mette en place des mesures de sécurité techniques et organisationnelles adaptées à la nature des données traitées. Cela peut inclure des solutions telles que :
   - **Chiffrement des données**
   - **Contrôles d'accès rigoureux**
   - **Mises à jour régulières des systèmes de sécurité**
   - **Tests de vulnérabilité et audits de sécurité**
4. Le contrat doit préciser que le prestataire a l'obligation de maintenir une **infrastructure sécurisée** et de garantir la sécurité des **réseaux**. En cas d'incident de sécurité (par exemple, une cyberattaque ou une fuite de données), il est essentiel que le prestataire mette en œuvre des plans de réponse et de reprise après sinistre, et qu'il fournisse des rapports détaillés sur les événements. Cela permet à la Mairie de prendre les mesures nécessaires et de se conformer à ses obligations de notification auprès de la CNIL, si nécessaire.

Sanctions en cas de non-respect des obligations du RGPD :

Si le prestataire ne respecte pas les obligations prévues dans le contrat, la Mairie d'Arles peut appliquer des sanctions, notamment :

- **Des amendes** : Jusqu'à **4 % du chiffre d'affaires annuel mondial** du prestataire ou **20 millions d'euros**, en fonction du montant le plus élevé.
- **Des peines de prison** : En cas de non-respect grave des obligations de confidentialité et de sécurité, des peines de prison pouvant aller jusqu'à **5 ans** peuvent être prononcées à l'encontre des responsables.

Gestion des projets :

Dans le cadre de mon stage, j'ai été impliqué dans trois projets majeurs qui ont contribué à la gestion et à l'optimisation de l'infrastructure informatique de la Mairie d'Arles. Chaque projet m'a permis de mettre en œuvre des solutions techniques et d'approfondir mes compétences en gestion de l'Active Directory, de la sécurité des données, ainsi qu'en intégration de nouveaux outils au sein du système informatique. Voici un aperçu de la gestion de ces projets :

Projet 1 : Gestion des utilisateurs dans l'Active Directory (AD)

Pour la première mission, j'ai été chargé de l'ajout de nouveaux utilisateurs dans l'Active Directory (AD) et de la gestion de leurs comptes en fonction des groupes et des sections appropriées. Le projet visait à centraliser l'administration des utilisateurs en facilitant l'intégration de nouveaux employés dans l'écosystème informatique de la mairie.

Actions réalisées :

- Création de nouveaux utilisateurs dans AD et gestion de leurs adresses e-mail via le champ **proxyAddresses**.
- Utilisation de l'outil mRemoteNG pour établir des connexions à distance avec les serveurs AD et effectuer les modifications nécessaires.
- Vérification des groupes et des licences des utilisateurs pour assurer un accès approprié aux ressources de la mairie.
- Synchronisation des informations des utilisateurs dans les différents systèmes de la Mairie, garantissant ainsi une gestion centralisée.

Difficultés rencontrées :

- L'intégration manuelle de certains utilisateurs dans les groupes d'AD a nécessité une attention particulière pour éviter des erreurs de placement.
- La gestion de la sécurité a également été un point crucial, car toute mauvaise attribution des groupes pouvait compromettre l'accès à des données sensibles.

Projet 2 : Migration des utilisateurs d’un ancien serveur vers un nouveau serveur

Lors de ma deuxième mission, j'ai été impliqué dans l'identification et la migration des utilisateurs d'un ancien serveur (version 2012) vers un serveur plus moderne. L’objectif principal était de déplacer les utilisateurs présents dans l'Active Directory et de sécuriser leurs données personnelles sur **OneDrive** avant la mise hors service du serveur.

Actions réalisées :

- Connexion au serveur via **Wallix Bastion** pour assurer une gestion sécurisée des accès.
- Répertorier les utilisateurs actifs sur le serveur, vérifier leur présence dans l'Active Directory et préparer le transfert de leurs données.

- Collaboration avec mes collègues pour explorer différentes options de transfert de données, en utilisant **OneDrive** pour centraliser les répertoires personnels.
- Planification de la suppression du serveur obsolète une fois la migration terminée et les données sécurisées.

Difficultés rencontrées :

- L'accès limité aux répertoires utilisateurs en raison des droits insuffisants a nécessité une intervention avec mon maître de stage pour résoudre cette contrainte.
- Le transfert des données a été un processus lent et nécessitait une approche manuelle, en raison de questions de sécurité liées aux répertoires personnels spécifiques à chaque utilisateur.

Projet 3 : Intégration de l'Active Directory avec GLPI pour une gestion centralisée des utilisateurs

Le dernier projet a consisté à intégrer **Active Directory** avec **GLPI**, un outil de gestion des services informatiques et de gestion des tickets. L'objectif était de centraliser l'authentification des utilisateurs à travers l'Active Directory pour simplifier l'accès aux services et garantir une gestion efficace des utilisateurs dans GLPI.

Actions réalisées :

- Configuration de l'environnement serveur avec **Windows Server 2019** et installation des services nécessaires, tels que **IIS** et **PHP**, pour faire fonctionner GLPI.
- Installation de **MySQL** pour gérer les bases de données nécessaires à GLPI.
- Synchronisation entre l'Active Directory et GLPI via LDAP, permettant une gestion centralisée des utilisateurs et de leurs droits d'accès.
- Ajout d'un utilisateur à GLPI en lien avec son compte dans l'Active Directory, garantissant ainsi un processus d'authentification centralisé.

Difficultés rencontrées :

- L'installation et la configuration de PHP dans IIS ont présenté des défis techniques, nécessitant une solution alternative après l'abandon de certains outils obsolètes.
- La configuration de l'annuaire LDAP pour la synchronisation entre AD et GLPI a demandé une attention particulière pour s'assurer que l'intégration se fasse de manière fluide, sans perte de données.

Conclusion sur la gestion des projets

Ces trois projets m'ont permis de développer une expertise technique dans la gestion des utilisateurs, la migration de données et l'intégration de systèmes. En travaillant sur l'Active Directory et en explorant des solutions comme **GLPI** et **OneDrive**, j'ai appris à gérer des projets complexes, à résoudre des problèmes techniques tout en respectant les exigences de sécurité et de confidentialité des données.

Chaque projet a été l'occasion de mettre en pratique des compétences clés en gestion des systèmes et d'apporter des solutions concrètes aux défis rencontrés. La gestion de ces projets m'a non seulement permis d'acquérir des connaissances techniques, mais aussi de mieux comprendre la manière de planifier et d'exécuter des projets dans un environnement professionnel.

Bilan Personnel - Conclusion :

Mon stage à la Mairie d'Arles a été une expérience très enrichissante, tant d'un point de vue **technique** que **juridique**. En tant qu'étudiante en **BTS SIO**, j'ai eu l'opportunité de mettre en pratique mes compétences en **administration des réseaux** et **cybersécurité**, tout en me confrontant aux enjeux juridiques liés à la gestion des systèmes d'information.

Les formations sur la **double authentification** (2FA) et le **protocole RADIUS** ont été particulièrement marquantes, car elles m'ont permis de comprendre l'importance de sécuriser l'accès aux ressources et d'éviter toute compromission des systèmes critiques. L'**implémentation du tiering** dans l'Active Directory, en particulier, m'a appris à restreindre l'accès en fonction du rôle de chaque utilisateur, une démarche clé pour la sécurité mais aussi pour **respecter les normes de conformité**, comme le **RGPD**, concernant la gestion des données sensibles.

Ce stage m'a non seulement permis de renforcer mes compétences techniques, mais aussi d'intégrer les **contraintes juridiques** liées à la cybersécurité. J'ai compris l'importance de garantir une **sécurisation optimale des systèmes** tout en respectant les **régulations et normes** en vigueur. En conclusion, cette expérience a enrichi ma formation et m'a préparée à relever les défis professionnels dans le domaine de l'informatique, en conciliant efficacement aspects techniques et juridiques.