Active Directory
Projet 1
Doc technique
Loïs

TABLE DES MATIERES

Windows Server	2
Prérequis	3
Qu'est-ce que Active Directory	3
Configuration Active Directory	4
Contrôleur de domaine	10
Configuration du serveur de fichier	15
Partages SMB	19
Permission du dossier	23
Utilisateurs et ordinateurs active directory	26
Ajouter une UO (Unité d'Organisation)	26
Ajouter un utilisateur	27
Ajouter un groupe	29
Création de GPO	30
Relier une machine au domaine Active Directory	33
Déployer l'agent GLPI automatiquement	35
Installation agent GLPI avec GPO	35
Configurer l'agent GLPI avec GPO	37
Lier Active Directory et GLPI	40
Installer l'extension LDAP de PHP	40
Ajouter un annuaire LDAP dans GLPI	41
Synchronisation des utilisateurs	46

WINDOWS SERVER

Windows Server 2019 est une version de Windows basée sur Windows 10, conçue pour mettre en place et gérer des services réseau, principalement destinés aux entreprises. Il offre des fonctionnalités spécialisées, telles que :

- Active Directory (gestion des utilisateurs et des ressources)
- Serveur DHCP (attribution automatique d'adresses IP)
- Serveur de connexion TSE (bureaux à distance via RDS)
- Serveur de fichiers (stockage et partage de données)
- Serveur d'impression (gestion centralisée des imprimantes)

• Et bien d'autres services.

Comme son nom l'indique, ce système d'exploitation est conçu pour des serveurs et non pour une utilisation en tant que station de travail. L'utiliser comme OS personnel est non seulement inutile, mais également peu rentable, car son coût de licence est nettement supérieur à celui des versions Windows destinées au grand public, telles que les éditions Professionnelle ou Familiale. Windows Server 2019 fournit des services réseau avancés ainsi que des outils adaptés à une gestion optimisée des utilisateurs et des ressources dans un environnement professionnel.

PREREQUIS

Pour configurer un domaine Active Directory, les éléments suivants sont nécessaires :

- Une machine équipée de Windows Server
- Une adresse IP fixe pour le serveur
- Un réseau internet opérationnel

QU'EST-CE QUE ACTIVE DIRECTORY

Le serveur Active Directory est un annuaire LDAP propriétaire développé par Microsoft. Il joue le rôle de contrôleur de domaine et intègre deux composants essentiels :

- 1. **Serveur LDAP**: Il permet la centralisation des comptes utilisateurs, facilitant ainsi la gestion des authentifications sur l'ensemble du réseau. Grâce à cela, chaque utilisateur peut se connecter à un ordinateur faisant partie du domaine en utilisant un identifiant unique (comme un nom et prénom).
- 2. **Serveur DNS** : Indispensable pour le bon fonctionnement du domaine, il gère la résolution des noms dans le réseau.

Avec Active Directory, il est également possible de mettre en place des **GPO** (**Group Policy Objects**). Les GPO permettent de définir et d'appliquer des règles de sécurité et des configurations spécifiques à des utilisateurs ou des machines du domaine. Cela offre une gestion centralisée et sécurisée des ressources et des accès au sein du réseau.

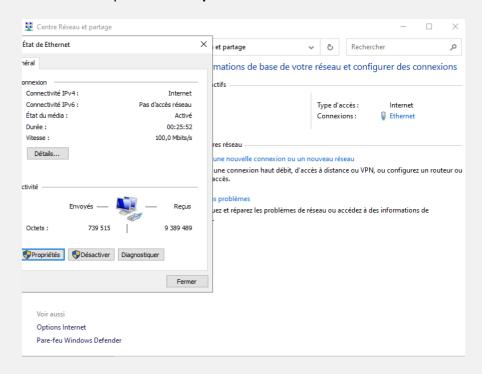
CONFIGURATION ACTIVE DIRECTORY

Nous allons dans un premier temps changer le nom du serveur, pour s'y retrouver plus facilement. Je choisis dans mon cas « **WSLOLO** ».

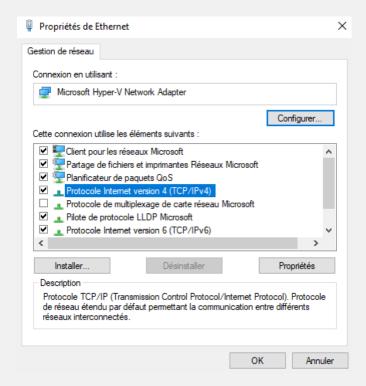


Nous allons ensuite attribuer une adresse IP fixe pour notre serveur. Pour ce faire, appuyez sur « **Windows + R** », et écrivez « **ncpa.cpl** ».

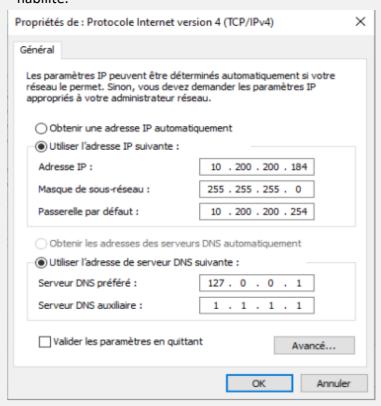
On clique sur « Ethernet » puis sur « Propriétés »



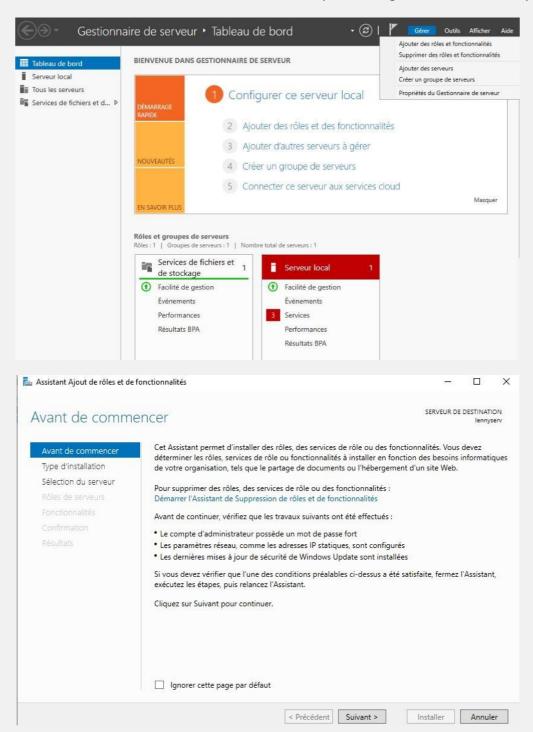
Vous allez dans « Protocole Internet version 4 TCP/IPv4 »



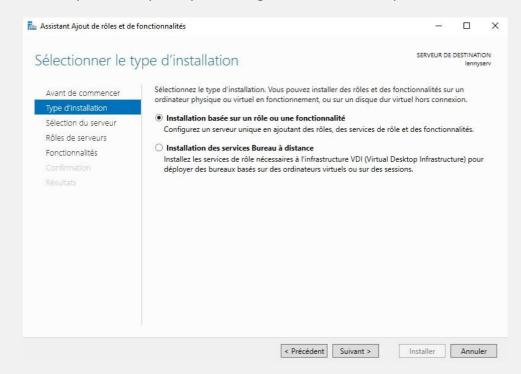
Renseignez l'adresse IP fixe, le masque de sous-réseau et la passerelle par défaut. Ensuite, configurez les serveurs DNS. Dans cet exemple, le serveur principal est celui de **Cloudflare** (1.1.1.1) et le secondaire celui de **Google** (8.8.8.8), reconnus pour leur rapidité et leur fiabilité.



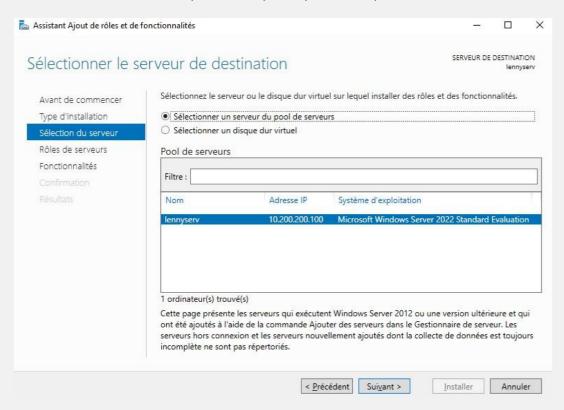
Pour installer **Active Directory**, commencez par ajouter un rôle. Pour cela, ouvrez le **Gestionnaire de serveur**, cliquez sur **Gérer**, puis sélectionnez **Ajouter des rôles et fonctionnalités**. Suivez ensuite l'assistant d'installation pour configurer Active Directory.



On sélectionne la première option, pour configurer un serveur unique.

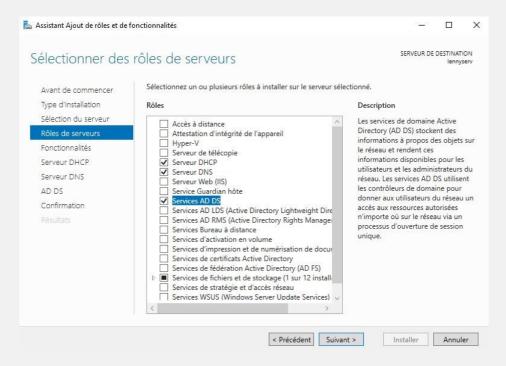


On sélectionne la première option, puis on clique sur « Suivant »

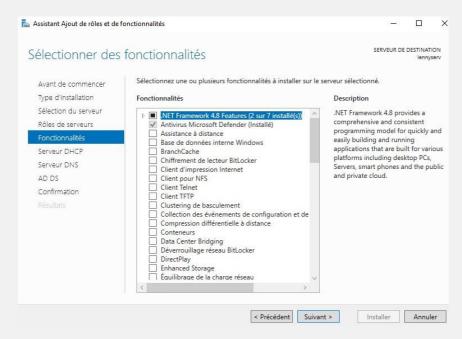


Ici nous sélectionnons le serveur **DHCP**, et le serveur **AD DS**. Le serveur **DNS** est sélectionné automatiquement.

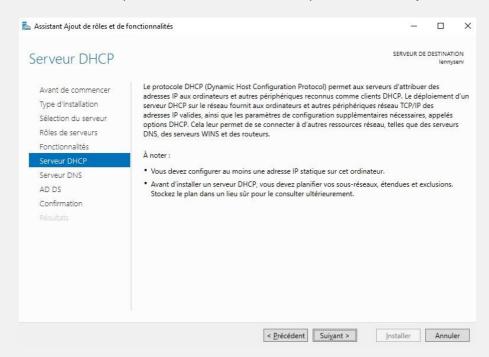
Le serveur **DHCP** permet d'attribuer automatiquement des adresses IP aux nouvelles machines se connectant sur notre serveur Active Directory, c'est donc une étape très importante pour le bon fonctionnement global et avoir une bonne communication entre les machines de notre Active Directory.



Nous n'avons pas besoin de fonctionnalités supplémentaires dans notre cas, on continue.

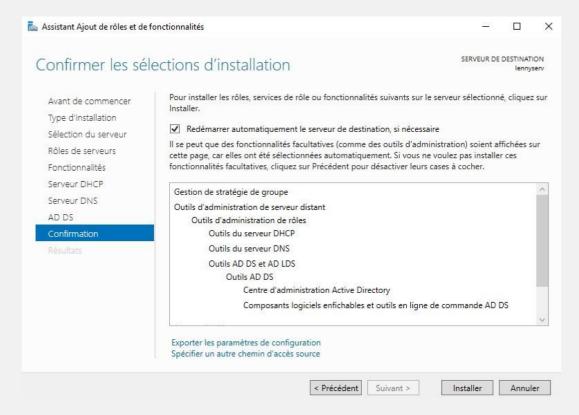


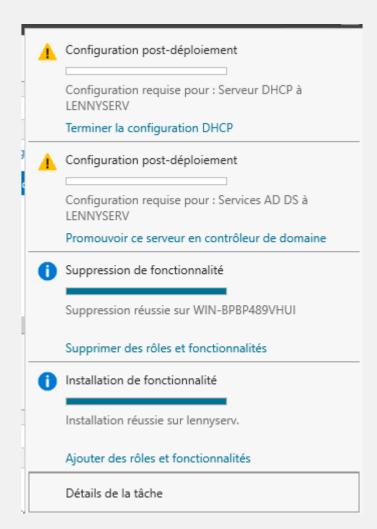
Nous avons ensuite un récapitulatif des fonctionnalités que nous avons ajoutées.



On clique sur « **Suivant** » plusieurs fois, puis on arrive à l'écran de confirmation qui nous confirme les choix effectués, et on clique sur « **Installer** ».

On a l'avancement ainsi que le statut de l'installation une fois le service installé nous pouvons cliquer sur **Fermer**.



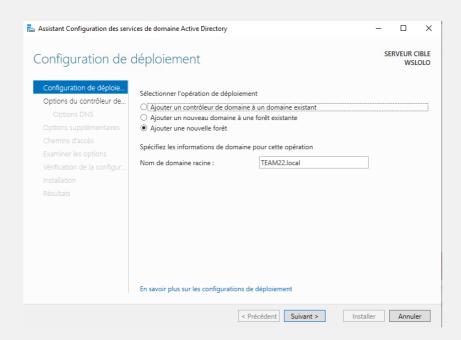


CONTROLEUR DE DOMAINE

Un **contrôleur de domaine** est un serveur qui gère l'accès centralisé aux ressources et aux utilisateurs dans un réseau Windows basé sur Active Directory. Il est responsable de l'authentification, de la gestion des comptes, et de la sécurité dans un domaine.

Promouvoir un serveur en tant que contrôleur de domaine signifie **installer et configurer Active Directory** sur ce serveur pour qu'il assume le rôle de contrôleur dans un domaine.

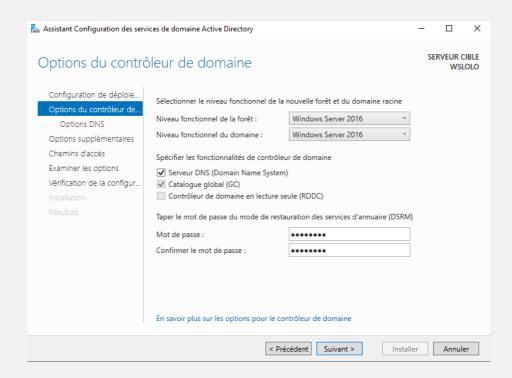
Pour ce faire on clique sur le drapeau en haut à droite. Comme il s'agit d'un nouveau domaine, dans une nouvelle forêt, choisissez "**Ajouter une nouvelle forêt**" et indiquez le nom, dans mon cas **TEAM22.local**



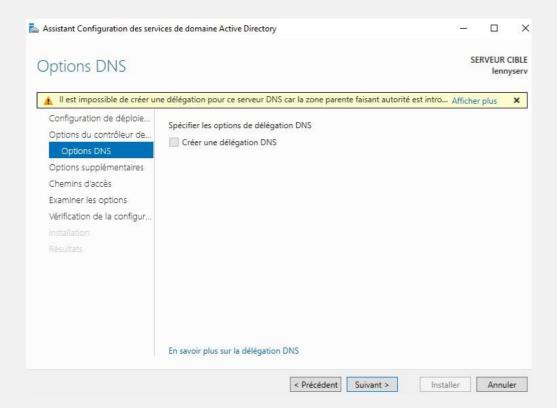
Pour définir le niveau fonctionnel de la forêt et du domaine, sélectionnez **"Windows Server 2016"**. Cela signifie que tous les contrôleurs de domaine devront obligatoirement fonctionner sous Windows Server 2016 ou une version ultérieure.

Actuellement, "Windows Server 2016" représente le niveau fonctionnel le plus élevé disponible. Cependant, ce niveau sera amené à évoluer avec la sortie de Windows Server 2025.

Configurez le serveur comme **serveur DNS** et **catalogue global**. Ensuite, définissez un mot de passe pour les services de restauration de l'annuaire. Notez que ce mot de passe est distinct de celui de l'administrateur de votre futur domaine.

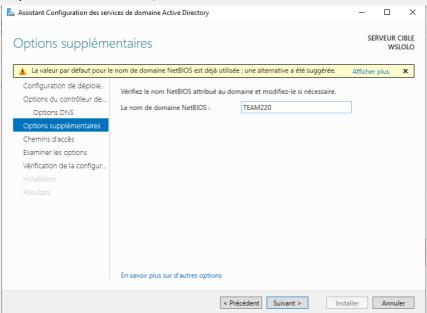


Comme il s'agit d'un nouveau serveur DNS pour une nouvelle zone, ne vous inquiétez pas pour ce message, vous pouvez poursuivre.

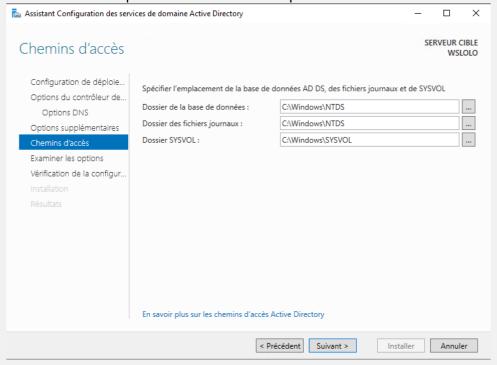


Le domaine NetBIOS est un nom court et simplifié qui identifie de manière unique un domaine dans un réseau Microsoft. Il est utilisé principalement pour assurer la rétrocompatibilité avec les anciennes applications ou protocoles basés sur NetBIOS

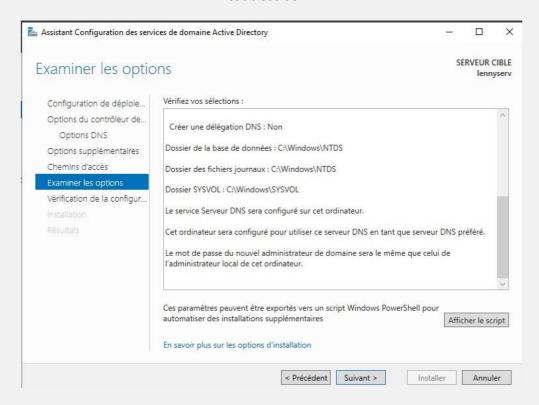
Si le nom DNS complet de votre domaine est domaine.local, le nom NetBIOS pourrait simplement être DOMAINE. Ce nom sera utilisé, par exemple, lorsque vous vous connectez à une machine en précisant DOMAINE\NomUtilisateur.



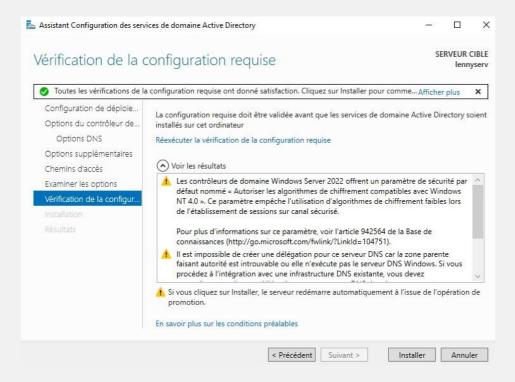
On peut laisser les chemins par défaut dans cette étape.



Nous avons ensuite un récapitulatif des options choisis précédemment, bien vérifier que tout est bon.



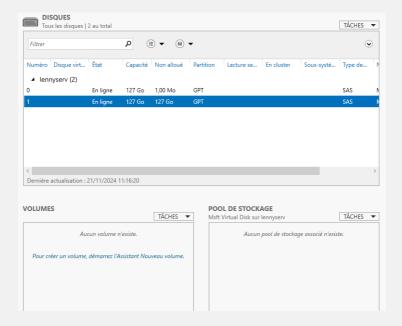
On peut cliquer finalement sur « Installer » pour finaliser l'installation. Patientez pendant l'installation. Quand ce sera terminé, le serveur va obligatoirement redémarrer, de façon automatique.



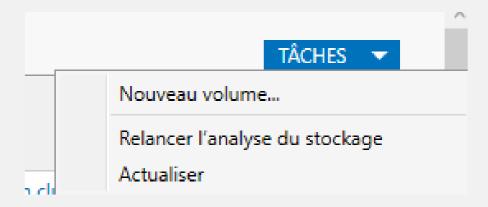
CONFIGURATION DU SERVEUR DE FICHIER

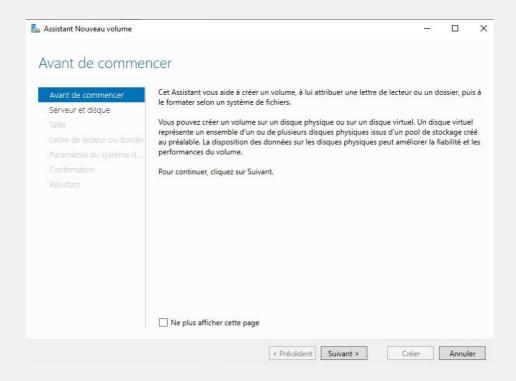
Le serveur de fichier est une ressource centralisée configurée pour partager des fichiers et des dossiers avec des utilisateurs ou des groupes définis dans le domaine Active Directory. Le service de fichiers étant déjà installer de base, nous allons directement commencer à le configurer.

On commence par vérifier si notre disque est bien affiché, dans le gestionnaire de serveur aller dans « Services de fichiers et de stockage » puis dans « Disques ».

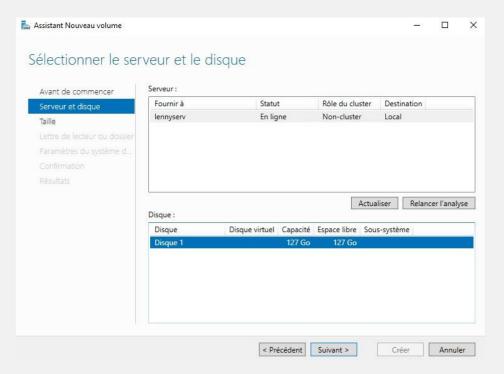


On va commencer par créer un nouveau volume, « Tâches », puis « Nouveau volume »

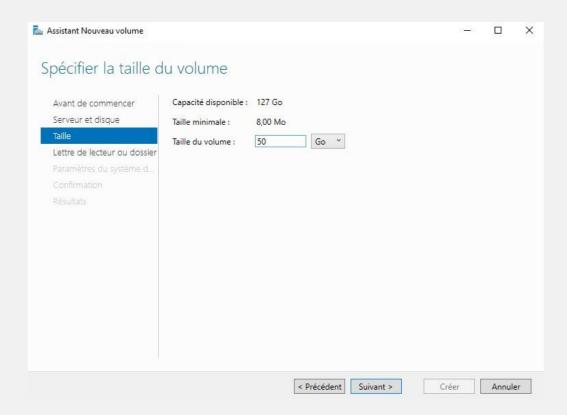




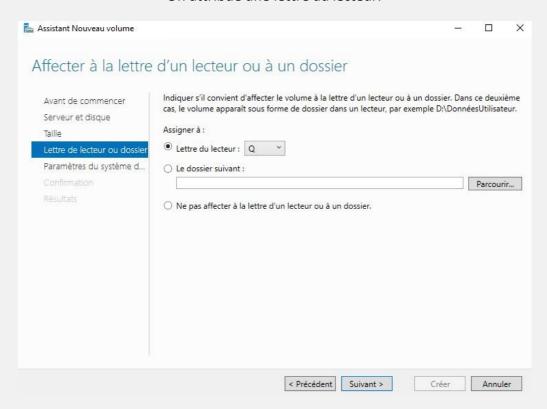
On sélectionne notre disque, ici le disque 1 (qu'il faut ajouter sur Hyper-V puis le mettre en ligne et l'initialiser dans le gestionnaire des disques), puis on clique sur « **Suivant** ».



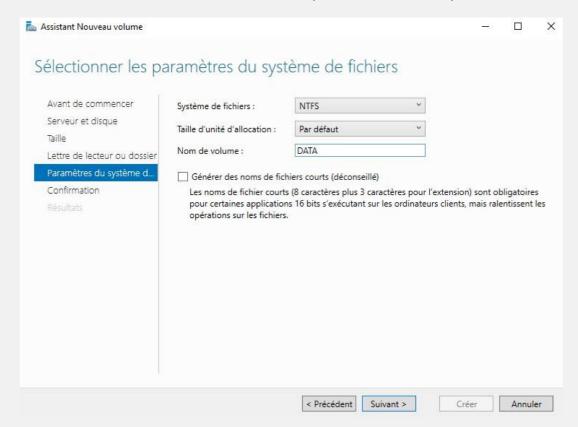
On choisit la taille de notre volume.



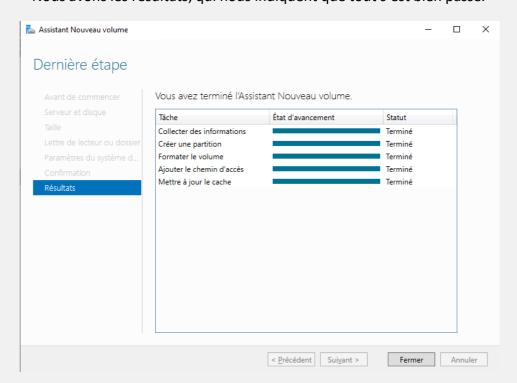
On attribue une lettre au lecteur.



On choisit le nom du volume, on laisse par défaut les autres paramètres.



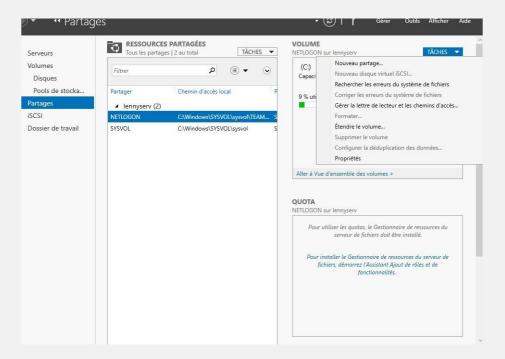
Nous avons les résultats, qui nous indiquent que tout s'est bien passé.



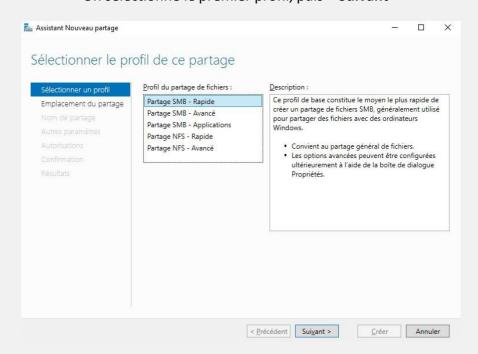
PARTAGES SMB

Le SMB est un protocole réseau qui permet aux utilisateurs et aux machines d'accéder aux fichiers, imprimantes et autres ressources partagées sur un réseau local.

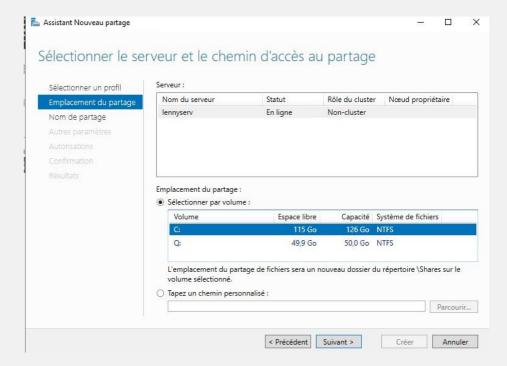
On se rend dans « **Partages** », puis on clique sur « **Nouveau partage** » en cliquant sur « **Tâches** » en haut à droite.



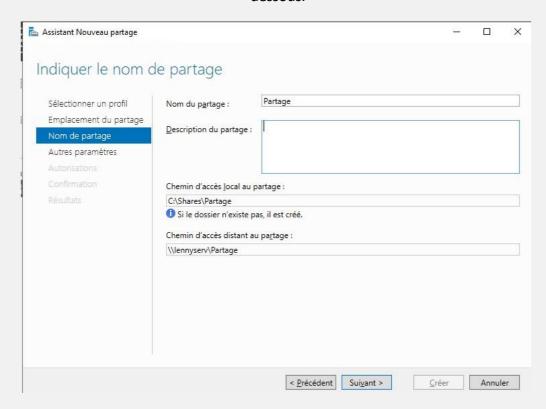
On sélectionne le premier profil, puis « Suivant »



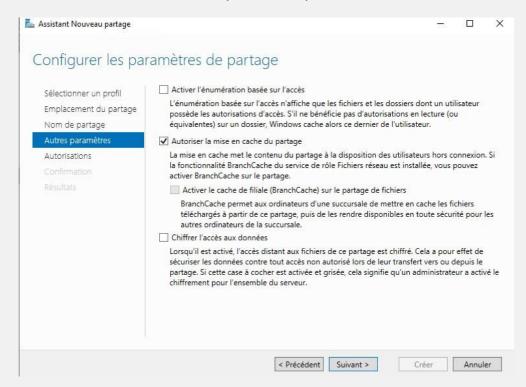
On choisit l'emplacement « **C** » qui sera l'emplacement de notre dossier partager puis « **Suivant** »



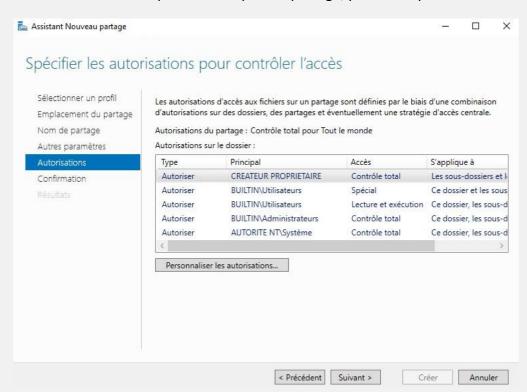
On choisit le nom du partage, puis le chemin d'accès local au partage sera affiché en dessous.



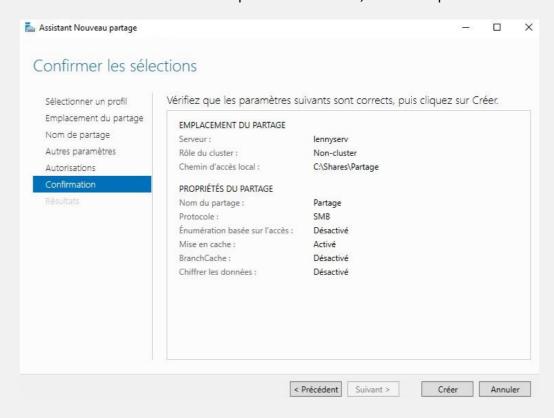
On laisse les paramètres par défaut ici.



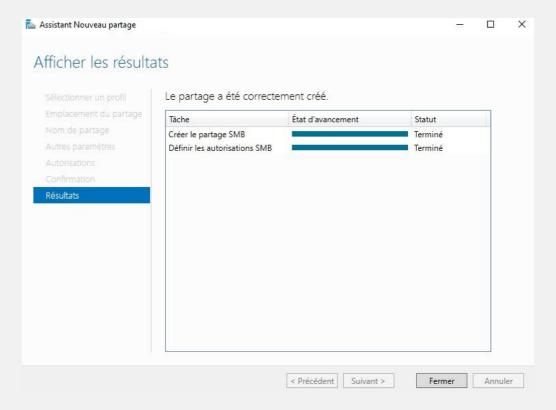
On choisit l'autorisation que l'on veut pour le partage, puis on clique sur « Suivant »



Nous avons la confirmation de ce qu'on vient de faire, on vérifie que tout est bon.

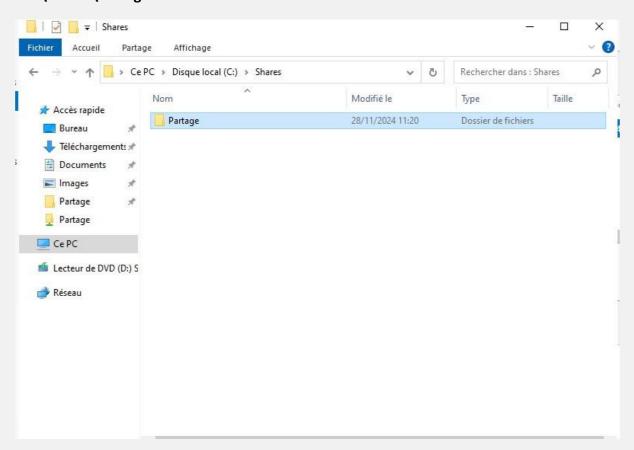


Une fois la création finie on peut cliquer sur fermer, Le partage de fichier est prêt à l'utilisation.

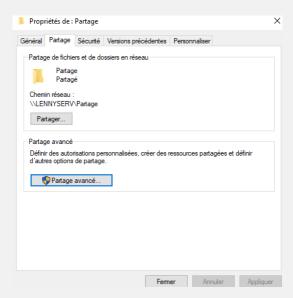


PERMISSION DU DOSSIER

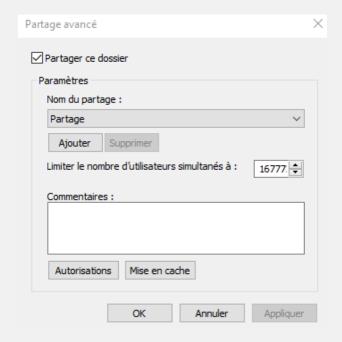
Les permissions déterminent qui peut accéder à quelles ressources et ce qu'ils peuvent faire avec ces ressources. Tout d'abord, on se rend à l'emplacement de notre dossier partagé, ici « C:\Shares\Partage »



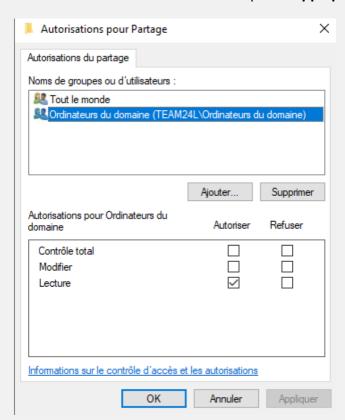
Clic droite sur le dossier, « Partage », puis « Partage avancé »



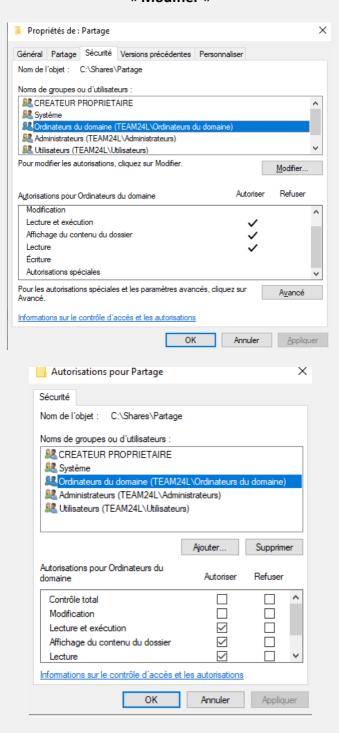
Puis « Autorisations » et « Ajouter », on rajoute « Ordinateurs du domaine »



On autorise « Ordinateurs du domaine » puis « Appliquer »



Ensuite, on fait pareil dans l'onglet « **Sécurité** ». On choisit « **Ordinateurs du domaine** », puis « **Modifier** »



Les droits de modification et de suppression sont supprimés pour les utilisateurs afin qu'ils ne puissent ni modifier ni supprimer les fichiers, mais les droits de lecture et d'exécution sont maintenus pour leur permettre de consulter et d'exécuter les fichiers.

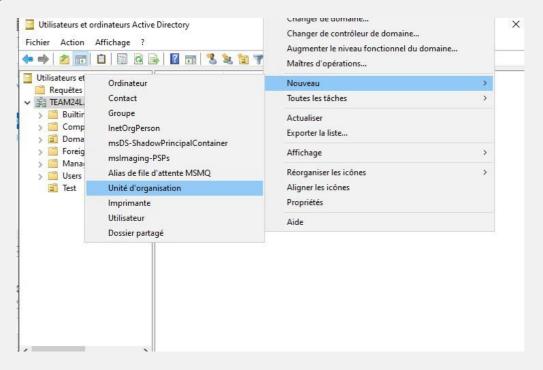
UTILISATEURS ET ORDINATEURS ACTIVE DIRECTORY

Pour gérer les utilisateurs et les ordinateurs du domaine, utilisez l'outil dédié à leur administration, nommé « **Utilisateurs et ordinateurs Active Directory** ». C'est d'ici que nous gérons les utilisateurs, les groupes les unités d'organisations de notre domaine.

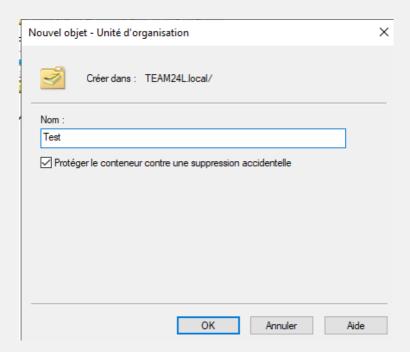
AJOUTER UNE UO (UNITE D'ORGANISATION)

Une **Unité d'Organisation (UO)** est un conteneur permettant de structurer et d'organiser votre domaine de manière hiérarchique. Elle facilite le tri et la gestion des utilisateurs, des ordinateurs, et des ressources partagées au sein du domaine.

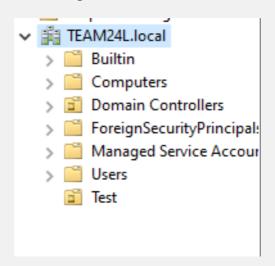
Clique droite à la racine de notre domaine, puis "Nouveau" et pour finir « Unité d'organisation »



On choisit ensuite le nom de notre **UO**, nous laissons cocher la protection de la suppression accidentelle. On clique sur « **OK** » pour la créer.



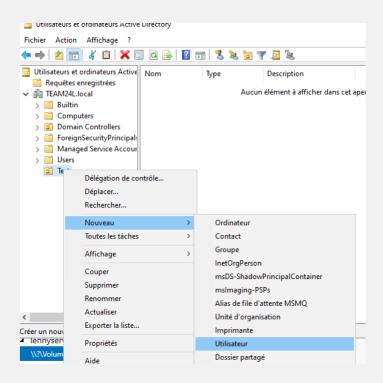
On peut voir notre UO qui s'affiche à gauche.



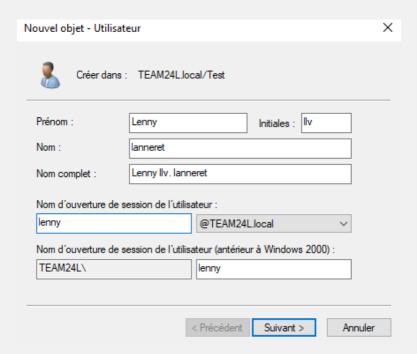
AJOUTER UN UTILISATEUR

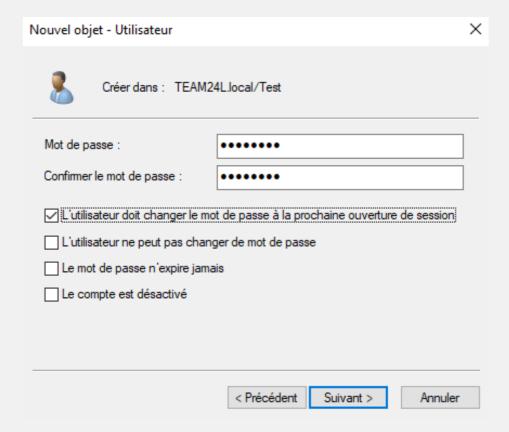
Un utilisateur correspond à un **compte utilisateur** permettant de se connecter à tout ordinateur intégré au domaine. Grâce à ce compte centralisé, les utilisateurs peuvent retrouver une session identique sur chaque poste du domaine. Il n'est pas nécessaire de créer manuellement un compte sur chaque ordinateur : le contrôleur de domaine gère l'authentification et synchronise automatiquement les modifications de session.

On choisit l'UO que l'on veut, dans mon cas celle que je viens de créer, puis clique droit et « **Nouveau** » puis « **Utilisateur** »



On rentre ensuite les identifiants de notre utilisateur, telles que le nom d'utilisateur et le mot de passe.

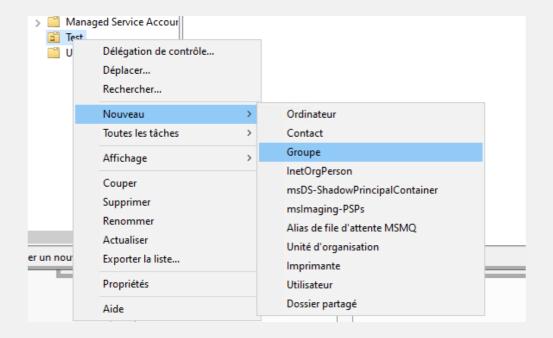




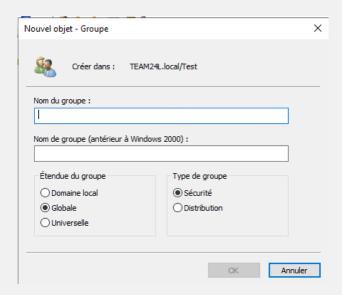
AJOUTER UN GROUPE

Nous allons créer un **groupe**, qui est une collection d'utilisateurs regroupés pour faciliter la gestion des permissions et des droits. Ce groupe pourra ensuite être utilisé pour :

- **Appliquer des GPO**: les politiques de sécurité ou de configuration pourront être appliquées à l'ensemble des membres du groupe.
- Attribuer des droits spécifiques : par exemple, des droits d'écriture ou d'accès sur des ressources comme le système de fichiers distribué DFS (Distributed File System).



Clique droite sur l'UO que l'on veut, puis « Nouveau » et « Groupe ».



On choisit le **nom du groupe** puis on laisse les paramètres par défaut et « **OK** ».

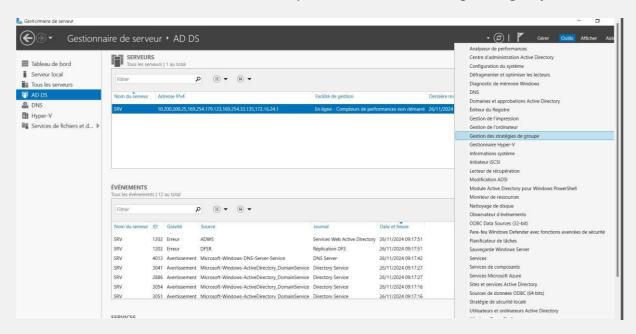
CREATION DE GPO

Une **GPO (Group Policy Object)** dans Active Directory sert à appliquer des règles et des configurations spécifiques sur les utilisateurs et les ordinateurs d'un domaine.

Par exemple, avec une GPO, on peut:

- **Configurer la sécurité** : imposer des mots de passe complexes, verrouiller les comptes après plusieurs échecs de connexion.
- **Restreindre l'accès** : bloquer certains logiciels ou empêcher l'accès à des paramètres système.
- **Automatiser des paramètres** : définir le fond d'écran, mapper des lecteurs réseau, ou installer des applications automatiquement.

Pour créer et gérer les GPO, on se rend dans le Gestionnaire de serveur, puis dans l'onglet « AD DS », dans « Outils » en haut à droite puis « Gestion des stratégies de groupe ».

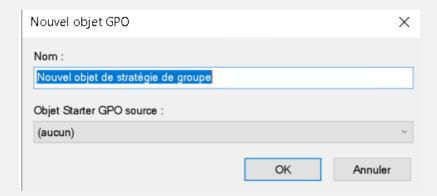


Pour créer et appliquer une GPO, effectuez un clic droit sur votre domaine, puis sélectionnez « Créer un objet GPO dans ce domaine, et le lier ici ». Cela permettra d'appliquer la GPO à tous les ordinateurs et utilisateurs du domaine.

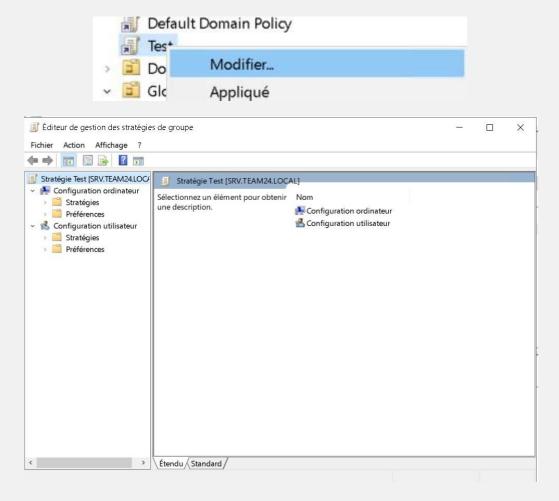
Cependant, si vous souhaitez appliquer une GPO uniquement à des groupes ou départements spécifiques, vous pouvez la lier à une **Unité d'Organisation (UO)**. Ainsi, seules les machines et utilisateurs de cette UO seront affectés.



On choisit ensuite le nom de notre GPO.



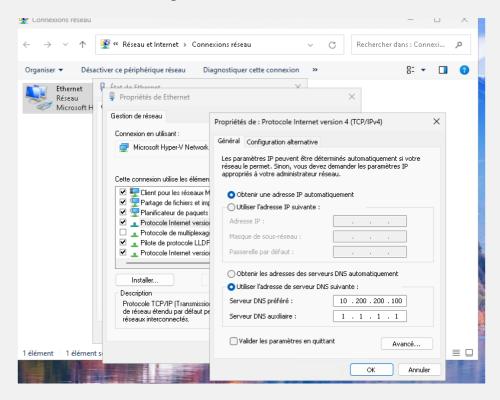
Le GPO va ensuite apparaître à gauche, on fait clique droite dessus puis « **Modifier** » pour modifier les stratégies de groupe.



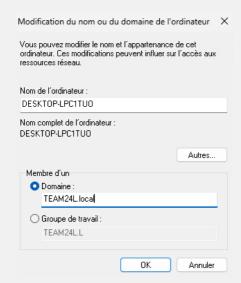
RELIER UNE MACHINE AU DOMAINE ACTIVE DIRECTORY

Nous allons commencer par modifier le paramètre DNS de la machine pour la connecter au domaine Active Directory. L'adresse IP configurée comme serveur DNS principal doit correspondre à celle du serveur Active Directory (dans mon cas : **10.200.200.100**).

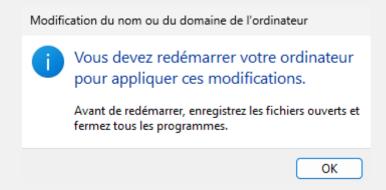
Cette étape est très importante, sinon la liaison ne se fera pas. En DNS secondaire on peut choisir celui de **Cloudflare** ou **Google.**



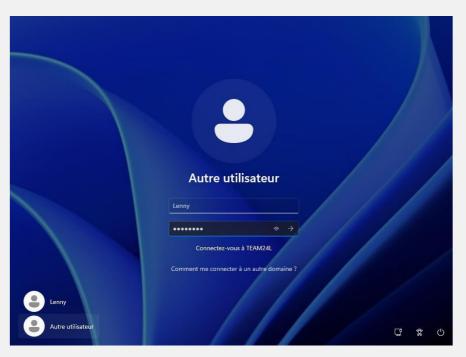
On change ensuite le domaine en se rendant dans « Systèmes », « Informations systèmes », puis « Domaine ou groupe de travail »



Il faudra par la suite entrer l'identifiant et le mot de passe d'un utilisateur du domaine Active Directory.



On redémarre le PC puis on se connecte avec un utilisateur et son mot de passe venant du Active Directory.



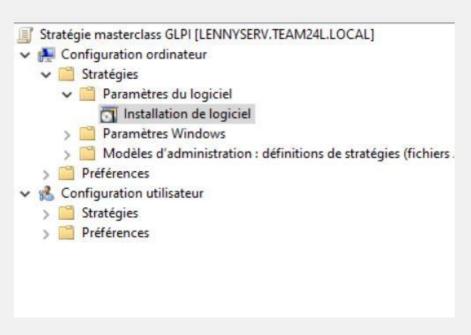
DEPLOYER L'AGENT GLPI AUTOMATIQUEMENT

Afin que les ordinateurs qui se connectent à notre domaine n'aient pas besoin d'installer l'agent GLPI et de le configurer manuellement, nous allons procéder à une automatisation de ces actions à l'aide de GPO.

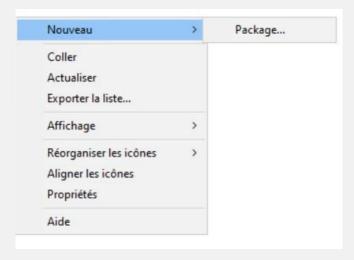
INSTALLATION AGENT GLPI AVEC GPO

Tout d'abord, nous allons créer une GPO lié à notre UO **GLPI** dans laquelle nous allons faire une règle pour exécuter l'agent GLPI automatiquement sur tous les ordinateurs qui démarrent la première fois.

On se rend dans notre GPO, puis « Configuration ordinateur », puis « Stratégies », « Paramètres du logiciel » et « Installations de logiciel »

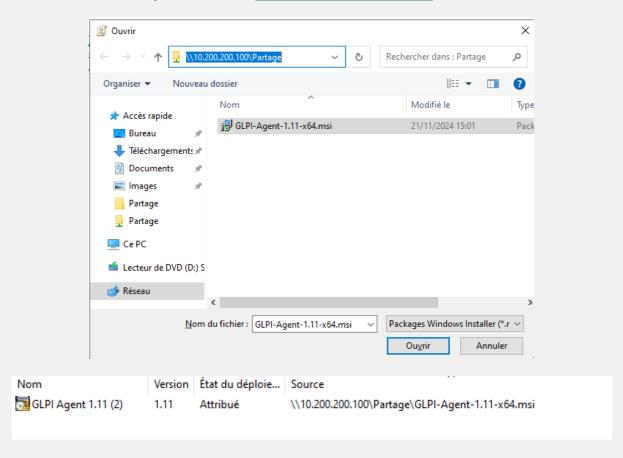


Puis à droite, on fait clic droite puis « Nouveau » et « Package »



Ensuite, on choisit l'emplacement **réseau** dans lequel on a mis le fichier **msi** de notre agent GLPI.

Le chemin est celui-ci pour mon cas : \\10.200.200.100\Partage\



CONFIGURER L'AGENT GLPI AVEC GPO

Le problème est que l'agent GLPI, lorsqu'il est déployé sans configuration, ne peut pas se synchroniser avec le serveur GLPI. En conséquence, les machines ne remonteront pas dans l'inventaire. Pour résoudre ce problème, nous allons configurer l'agent GLPI via une **GPO** en modifiant directement les valeurs situées dans la clé de registre suivante :

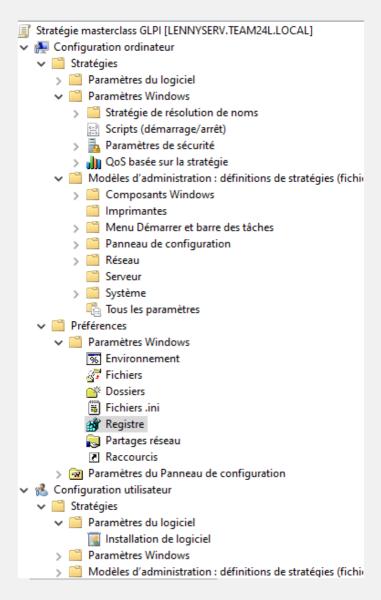
HKEY_LOCAL_MACHINE\SOFTWARE\GLPI-Agent

Nous allons configurer une valeur :

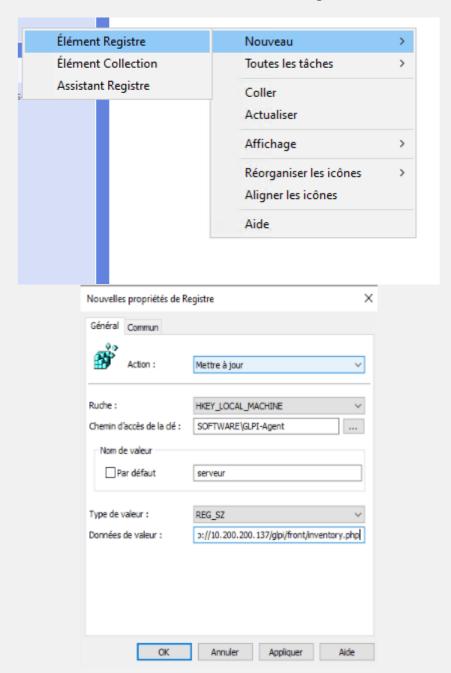
server : pour indiquer l'URL du serveur GLPI (vers une page spécifique)

On se rend dans notre GPO, puis on va dans:

Configuration ordinateur > Préférences > Paramètres Windows > Registre



Puis « Nouveau » et « Elément Registre »



Configurer la valeur "server"

Action : mettre à jour

Ruche: HKEY_LOCAL_MACHINE

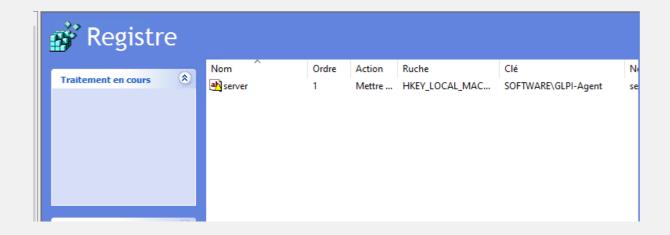
Chemin d'accès de la clé : SOFTWARE\GLPI-Agent

Loïs Perrier- CC BY-NC-ND 4.0 09/12/2024 - Page **38** sur **48**

Nom de valeur : server

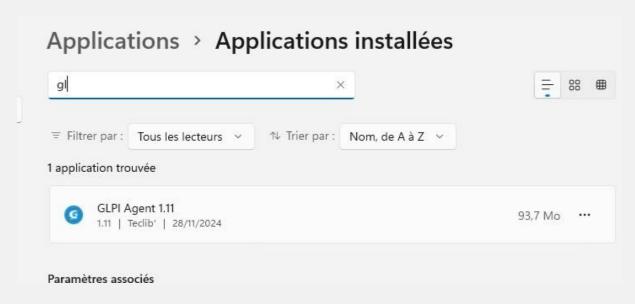
Type de valeur : REG SZ

Données de valeur : http://10.200.200.137/glpi/front/inventory.php



On peut ensuite faire **gpupdate /force** sur notre machine pour appliquer les GPO.

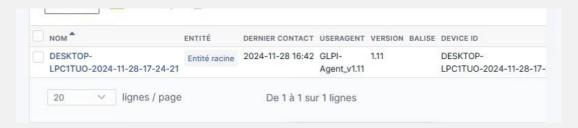
On va dans « **Applications installées** » et on peut voir que l'agent GLPI est bien installé.



Ensuite, il faut aller sur : $\underline{\text{http://127.0.0.1:62354}}$ dans le navigateur, puis cliquer sur « **Force inventory** »



On va dans notre GLPI, puis l'ordinateur devrait apparaître. Cela peut prendre quelques minutes.



LIER ACTIVE DIRECTORY ET GLPI

Nous allons configurer l'authentification LDAP dans GLPI afin de permettre la connexion à l'application GLPI en utilisant les comptes utilisateurs d'un annuaire Active Directory. Ainsi, les utilisateurs pourront accéder à GLPI avec leur nom d'utilisateur et mot de passe habituels, correspondant à leurs identifiants Active Directory.

INSTALLER L'EXTENSION LDAP DE PHP

Pour permettre à GLPI de communiquer avec votre contrôleur de domaine Active Directory, l'extension LDAP de PHP doit être installée sur votre serveur.

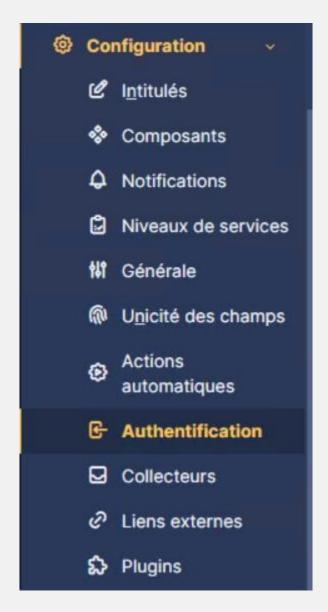
Connectez-vous à votre serveur GLPI et exécutez les commandes ci-dessous pour mettre à jour le cache des paquets, puis installer l'extension requise.

sudo apt-get update

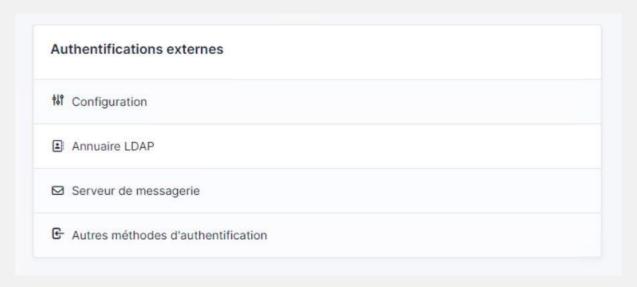
sudo apt-get install php-ldap

AJOUTER UN ANNUAIRE LDAP DANS GLPI

Désormais, nous allons ajouter notre annuaire Active Directory à GLPI. Connectez-vous à GLPI avec un compte administrateur, puis dans le menu "Configuration", cliquez sur "Authentification".

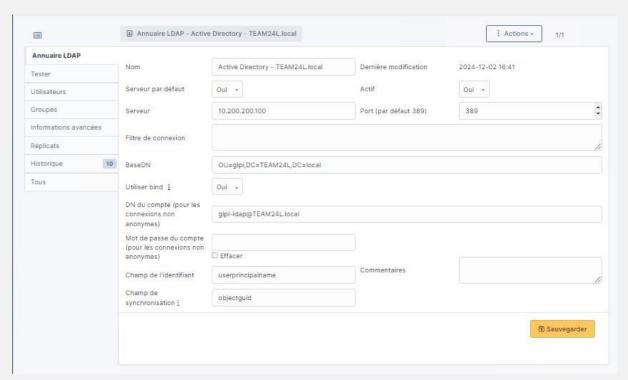


Cliquez sur "Annuaire LDAP"



Puis, cliquez sur le bouton "Ajouter" en haut à droite.





Nom: Attribuez un nom convivial à cet annuaire LDAP. Il n'est pas obligatoire d'utiliser le nom du domaine ou du serveur.

Serveur par défaut : Indiquez si ce serveur doit être utilisé par défaut pour l'authentification LDAP. Notez qu'un seul serveur LDAP peut être défini comme serveur par défaut.

Actif: Choisissez « **Oui** » pour activer ce serveur. Sinon, il sera déclaré mais non opérationnel.

Serveur : Saisissez l'adresse IP du contrôleur de domaine à interroger ici **10.200.200.184**, car l'utilisation d'un nom DNS peut ne pas fonctionner correctement.

Port: Laissez la valeur par défaut, 389, correspondant au port standard du protocole LDAP. Si vous utilisez TLS, vous devrez configurer cette option ultérieurement dans l'onglet **informations avancées** du serveur LDAP.

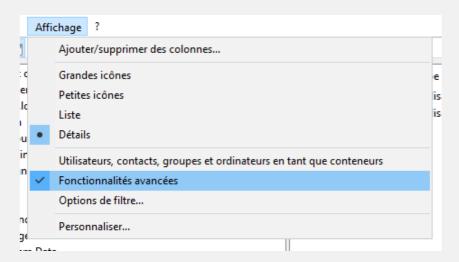
Filtre de connexion: Rédigez une requête LDAP pour cibler les objets souhaités dans l'annuaire Active Directory. En général, on récupère les objets utilisateur (objectClass=user) tout en filtrant pour inclure uniquement les utilisateurs actifs (via un filtre sur l'attribut UserAccountControl). Dans mon cas, je laisse vide.

Base DN: Spécifiez l'emplacement dans l'annuaire où effectuer les recherches utilisateur. Cela peut être la racine du domaine ou une unité organisationnelle spécifique (OU), selon l'organisation de votre annuaire et la localisation des utilisateurs à synchroniser.

Indiquez le **Distinguished Name (DN)** approprié. Le **Distinguished Name** est un nom unique qui identifie chaque objet dans l'Active Directory. C'est une chaîne de caractères qui représente la position de l'objet dans l'arborescence de l'annuaire.

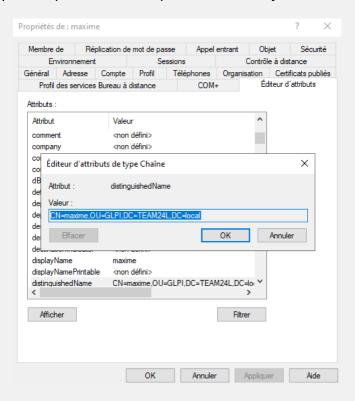
Pour voir le DN, ouvrez la console **Utilisateurs et ordinateurs Active Directory** sur votre contrôleur de domaine.

Dans le menu, cliquez sur **Affichage**, puis sélectionnez **Fonctionnalités avancées**. Cela rend l'onglet **Éditeur d'attributs** accessible dans les propriétés d'un objet.



Loïs Perrier-CC BY-NC-ND 4.0 09/12/2024 - Page 43 sur 48

Dans la liste des attributs, repérez l'attribut **distinguishedName**. Double-cliquez dessus pour ouvrir une fenêtre qui vous permettra de copier le DN de l'objet.



Utiliser bind: Sélectionnez « **Oui** » pour une connexion LDAP classique (sans TLS).

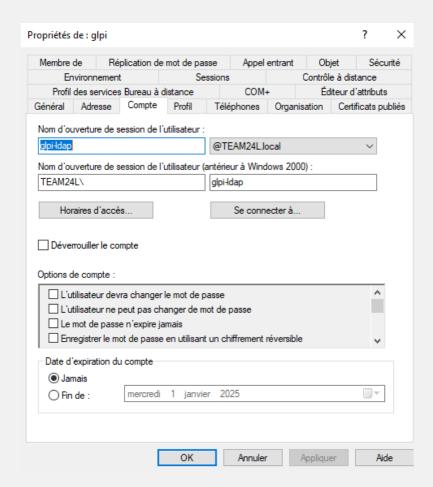
DN du compte : Nous indiquerons le compte que nous avons créé à destination de la synchronisation, ici **glpi-ldap@TEAM22.local**

Mot de passe du compte : Entrez le mot de passe associé au compte mentionné ci-dessus.

Champ de l'identifiant: Déterminez l'attribut de l'Active Directory à utiliser comme identifiant de connexion pour GLPI. Les options courantes incluent **UserPrincipalName** ou **SamAccountName**, selon vos besoins.

Champ de synchronisation: Configurez l'attribut que GLPI utilisera pour synchroniser les objets. L'attribut objectGuid est recommandé car il fournit une valeur unique et immuable pour chaque utilisateur, permettant à GLPI de suivre les modifications apportées aux comptes sans ambiguïté, sauf en cas de suppression et recréation du compte dans l'Active Directory.

On peut vérifier le compte DN que nous avons créé dans notre Active Directory, il ne faut pas oublier de décocher « l'utilisateur devra changer le mot de passe ».



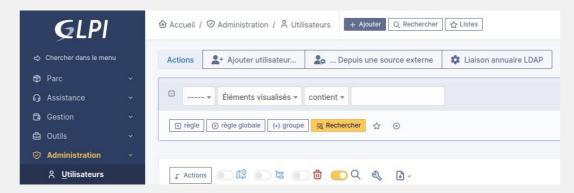
On peut ensuite tester notre lien avec notre serveur LDAP, si tout se passe bien, « **Test réussi** » devrait s'afficher.



SYNCHRONISATION DES UTILISATEURS

Pour synchroniser nos utilisateurs nous aurons deux possibilités, via l'interface graphique ou via la ligne de commande de GLPI.

Nous irons dans le menu « **Administration** », puis « **Utilisateurs** ». Nous cliquerons alors sur le bouton « **Liaison annuaire LDAP** ».

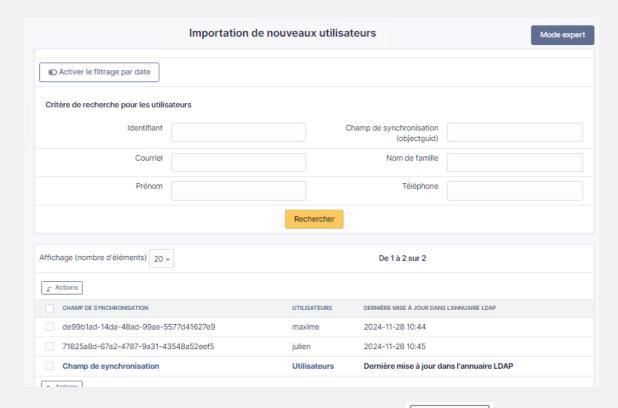


Dans la nouvelle fenêtre, le bouton « Synchronisation des utilisateurs déjà importés » permettra de synchroniser les éventuelles modifications apportées aux comptes déjà importés. Le bouton « Importation de nouveau utilisateurs » permettra d'importer les utilisateurs. Nous cliquerons sur ce dernier.

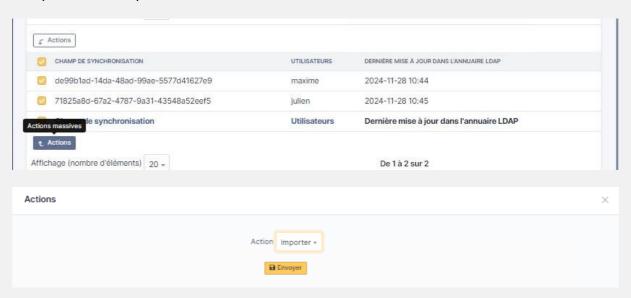


A l'étape suivante nous cliquerons sur le bouton « **Rechercher** » afin de trouver les comptes Active Directory étant dans l'UO « **glpi** » et par conséquent autoriser à disposer de GLPI.

Les comptes s'afficheront alors :



Nous les sélectionnerons tous puis dans le bouton « **Action** » nous choisirons d'importer les comptes.



Un pop-up de confirmation d'importation apparaitra.



Nos utilisateurs apparaîtront dans le menu de gestion des utilisateurs.



Détail important, un certain nombre d'informations remonterons avec les utilisateurs. Si vos utilisateurs Active Directory sont parfaitement remplis, les éléments tel que les numéros de téléphone, les adresses ou les adresses mails apparaitront (il faudra afficher les colonnes via

le bouton clé à molette (1).