

## 1.1. Présentation

## Avertissement :

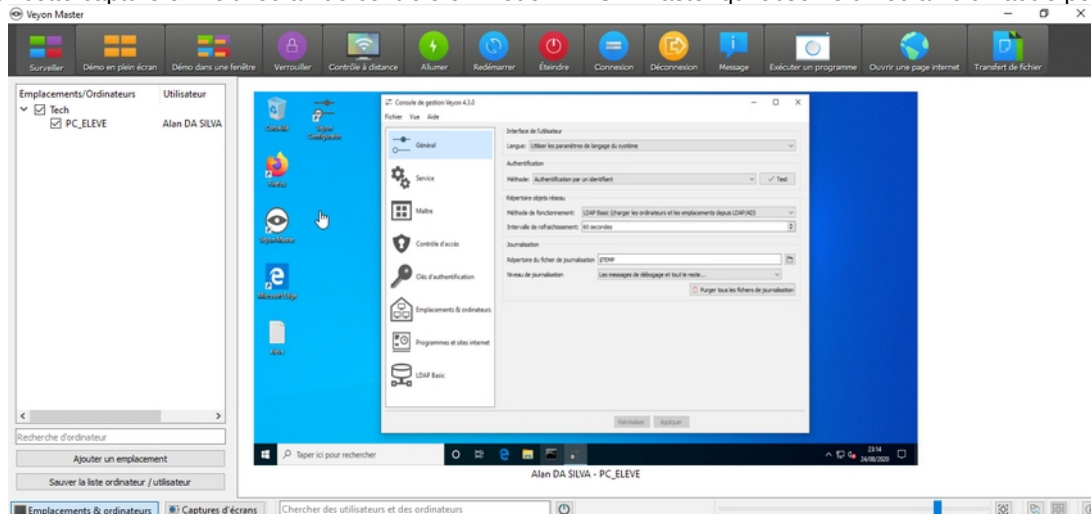
Les captures d'écrans de ce tuto ont été réalisées avec la version 4.3 de [VEYON](#) et la version 2.7 de [EOLE](#) scribe AD au collègue Carnot à Auch.

Le client EOLE basé sur SaltStack permet d'agir sur les postes clients et, en particulier d'installer et configurer le logiciel d'observation et de diffusion Veyon

Veyon (anciennement iTALC) est un logiciel libre qui permet de surveiller, contrôler et administrer les postes à distance.

Il est installé automatiquement sur le poste de travail dès qu'il est intégré au domaine via une GPO.

Sur cette capture on voit l'écran de contrôle en mode VEYON-master qui observe un écran d'un autre poste.



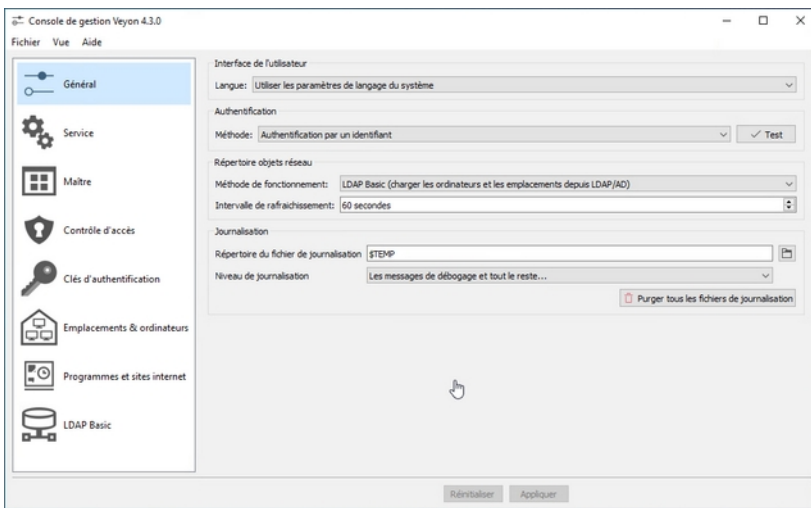
Il existe 3 exécutables pour Veyon :

- *Veyon-configurator* accessible avec un compte admin
- *Veyon-master* accessible avec un compte prof. L'icône est aussi présent sur le bureau des élèves mais ils ne peuvent pas s'y connecter (l'authentification est la même que celle du réseau Eole).
- *Veyon.cli.exe* : utilitaire pour allumer les stations à distance. Cet outil n'est pas décrit dans ce tuto.

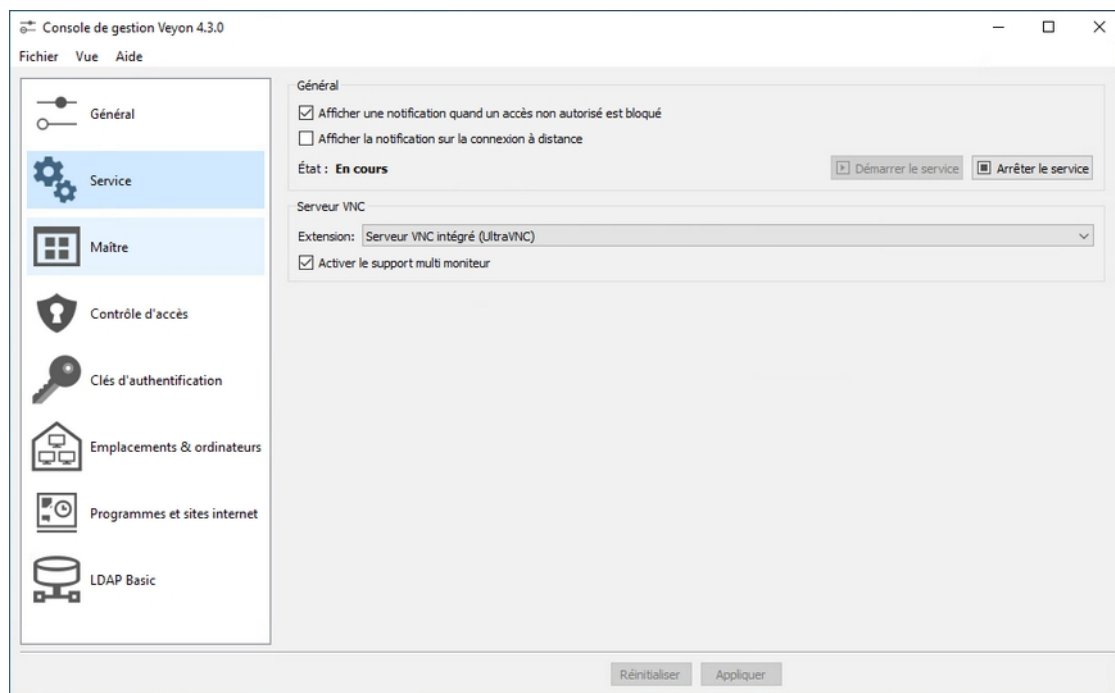
## 1.2. Configuration

Pour configurer le client Veyon, il faut lancer la **Console de gestion Veyon** (Veyon-configurator) avec le compte admin pour avoir tous les droits de modification.

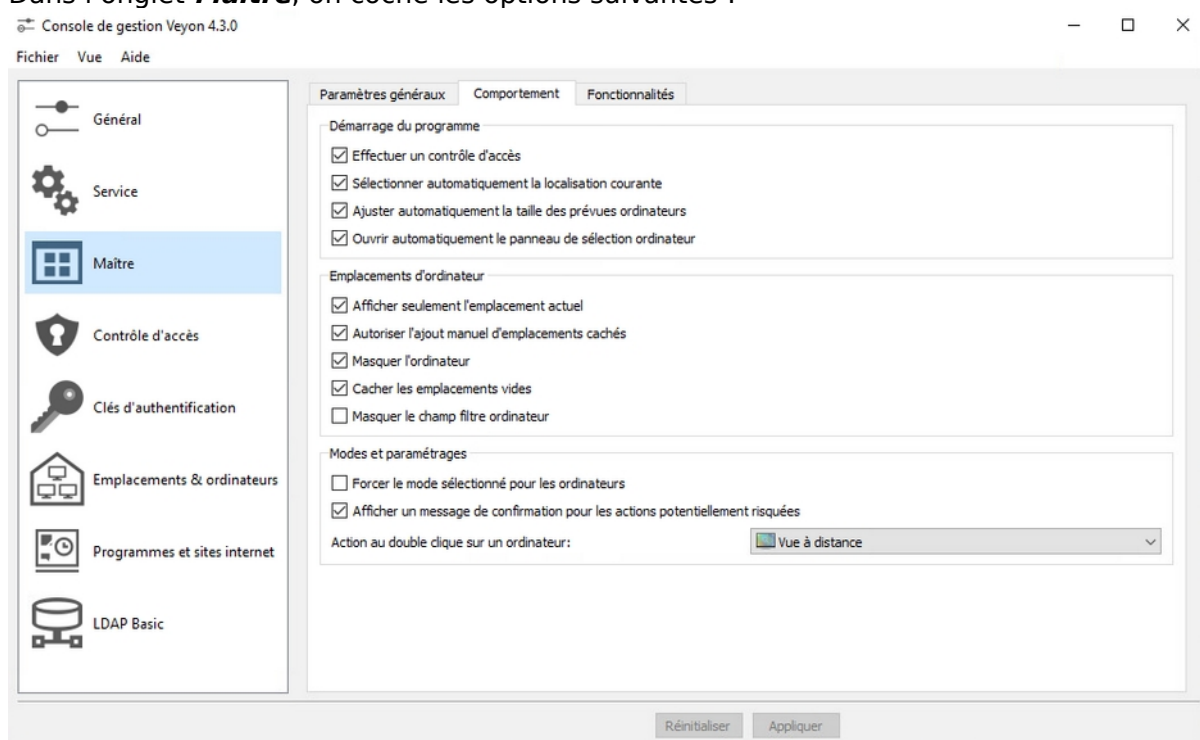
Dans l'onglet Général, on s'assure que la **Méthode d'Authentification** est bien sûr **Authentification par un identifiant**. On vérifie également que la **Méthode de fonctionnement** est bien sur **LDAP Basic** (l'annuaire du ScribeAD)



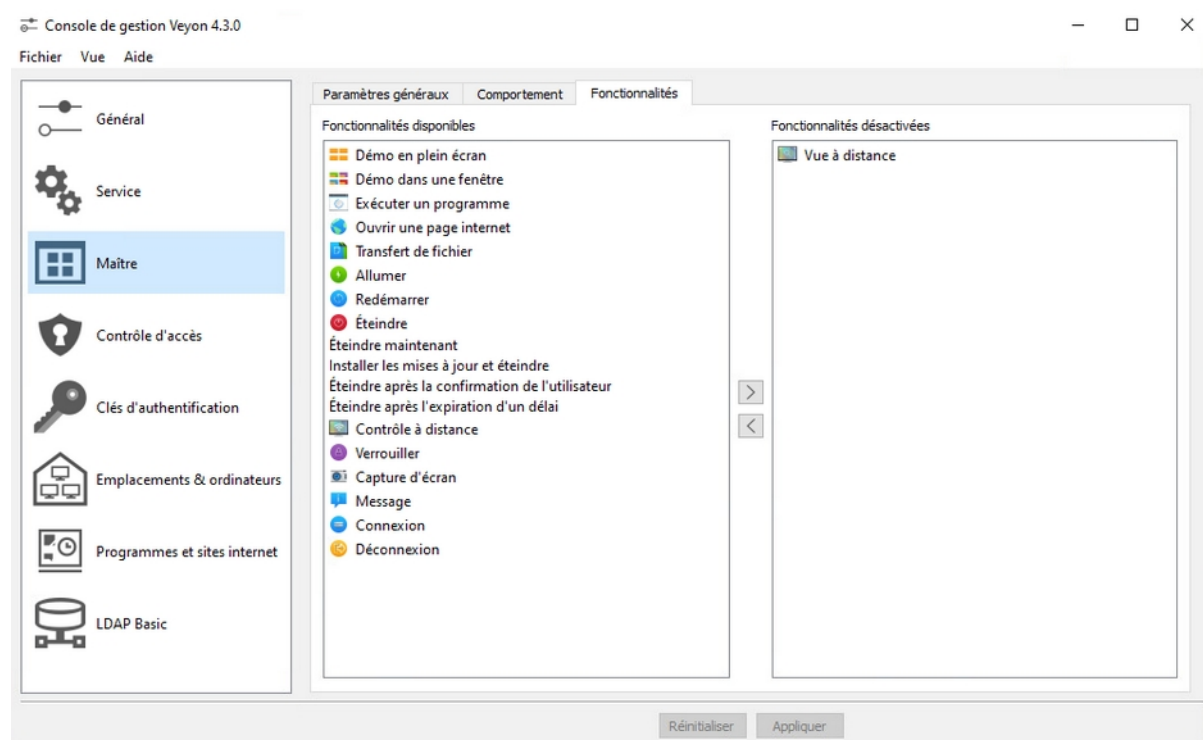
Dans l'onglet **Service**, on sélectionne le **Serveur VNC intégré** (pour la prise de main à distance) :



Dans l'onglet **Maître**, on coche les options suivantes :

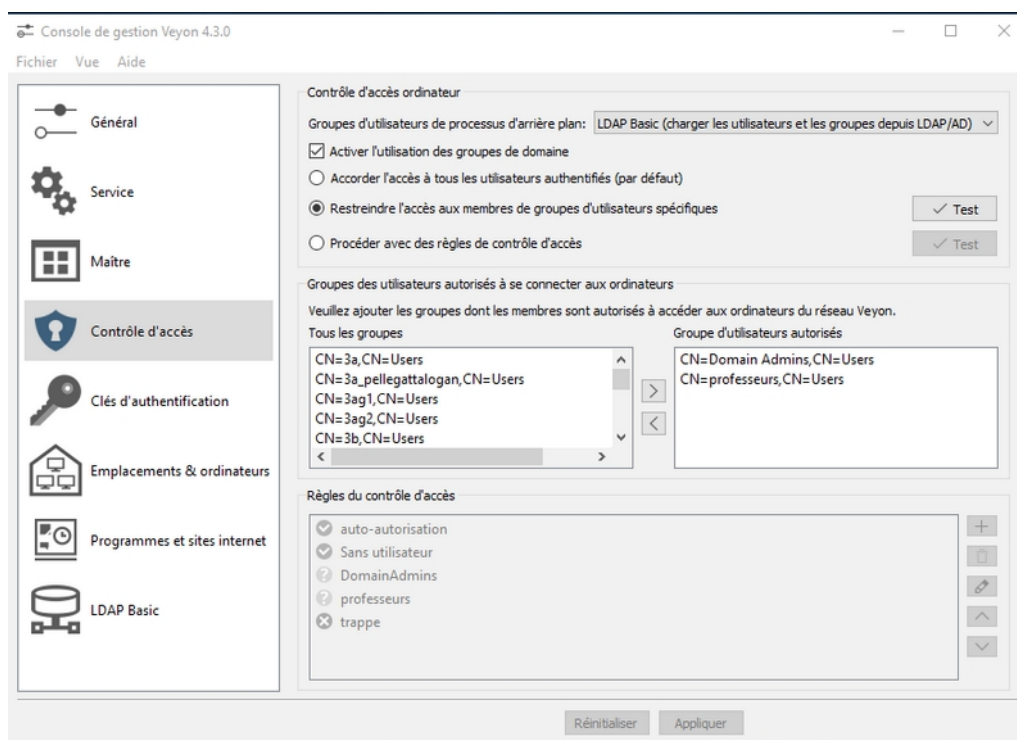


Toujours dans l'onglet **Maître** mais dans la rubrique **Fonctionnalités**, on sélectionne les outils que l'on souhaite dans l'application Veyon-master :



Dans l'onglet **Contrôle d'accès**, on coche **Activer l'utilisation des groupes de domaine** et **Restreindre l'accès aux membres de groupes spécifiques**, ce qui permet de limiter les utilisateurs à accéder aux stations implantés dans les salles. Cela évite que tout le monde accède aux stations de toutes les salles.

Pour se faire, on rajoute le groupe d'utilisateur qui est autorisé à prendre le contrôle des postes clients de la salle. Ici, on rajoute le groupe **professeurs** qui autorise à prendre le contrôle des stations des salles informatiques :

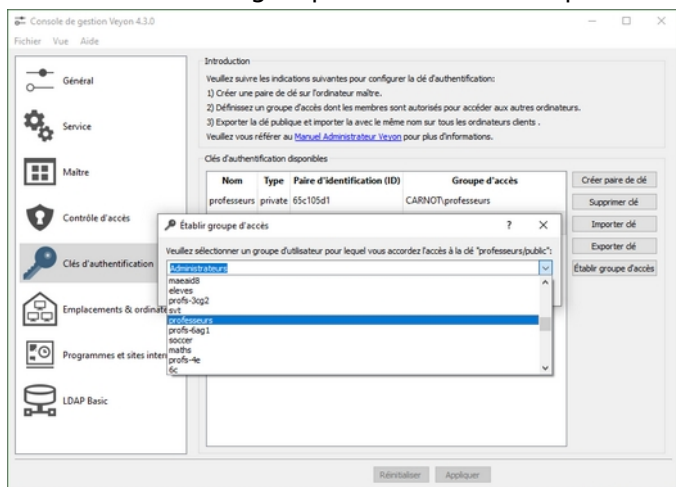


## Étapes facultatives (début)

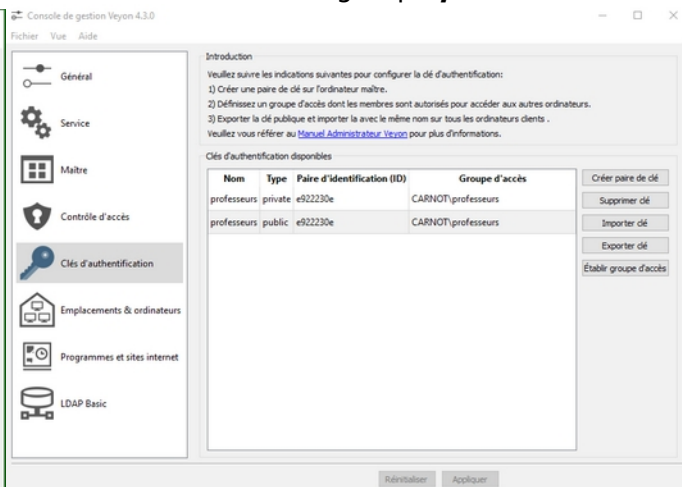
**Avertissement :** Normalement la création des clés n'est pas nécessaire avec les réglages choisis. A vérifier selon le réseau en particulier pour la fonction « Allumer » qui nécessite d'autres réglages sur le réseau (Bios, cartes réseaux, Wake on line,...) qui ne sont pas détaillés dans ce tuto.

Dans l'onglet **Clés d'authentification**, il faut créer une paire de clé qui permettra aux utilisateurs du groupe que nous avons autorisé à l'étape juste avant de pouvoir s'authentifier sur les stations des élèves.

Puis on établit un groupe d'accès à cette paire de clé, ici on sélectionne le groupe **professeurs** :

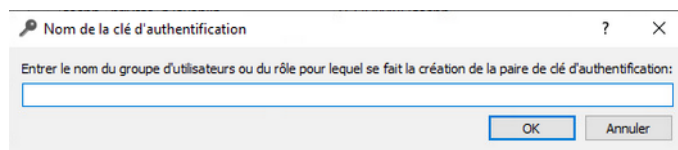


Écran pour « Établir le groupe »



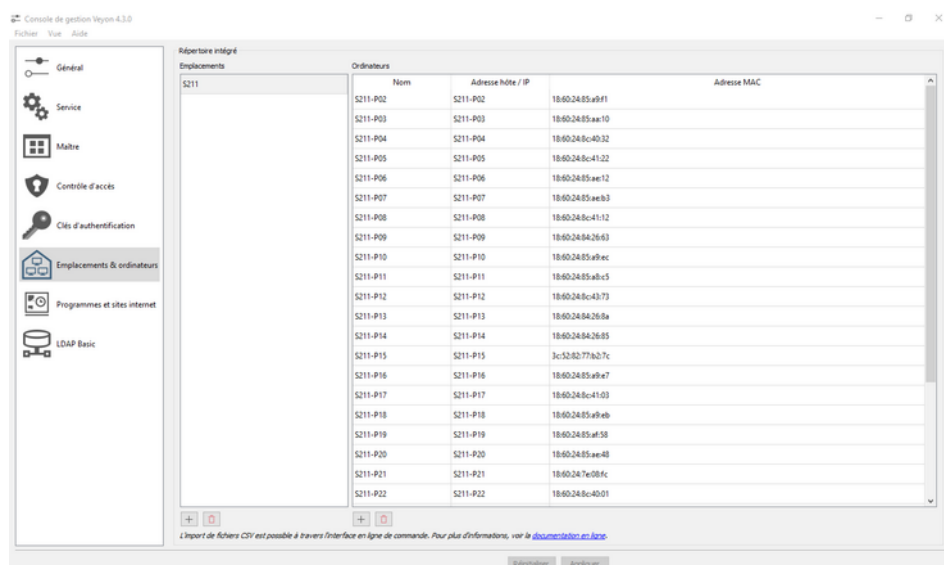
Écran final...

**Étape importante,** lors de la création, il faut donner un nom à cette paire de clé. Il faut impérativement que le nom soit le même que le nom du groupe qui a été autorisé à l'étape juste avant. Voir copie d'écran



**Avant de passer à l'étape suivante, il faut exporter la clé publique.** C'est cette clé que nous importerons sur chaque poste de la salle pour les élèves. Elle permettra d'authentifier les professeurs du groupe **professeurs** et permettra de prendre le contrôle à distance.

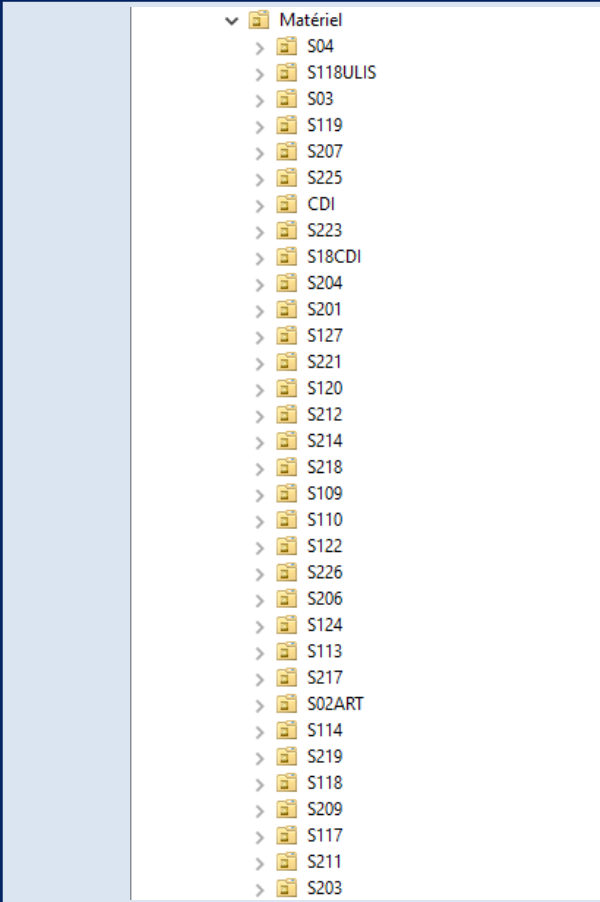
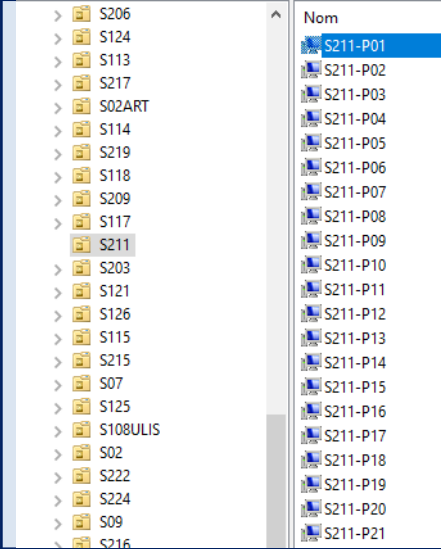
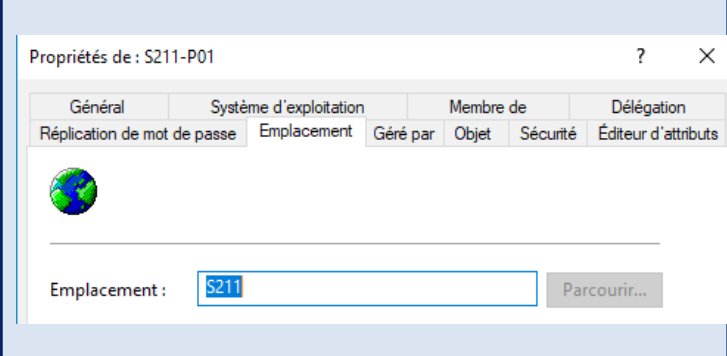
Dans l'onglet **Emplacement & ordinateurs**, il faut spécifier l'emplacement (**l'OU de la salle**) ainsi que les ordinateurs de la salle (nom, nom d'hôte et adresse MAC) :



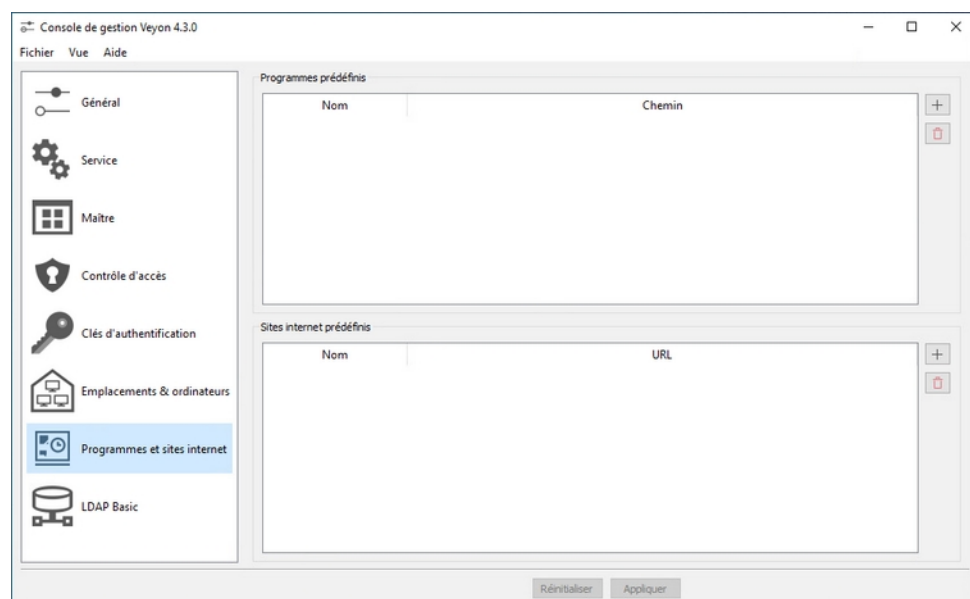
## Étapes facultatives (fin)

Dans l'onglet **Emplacement & ordinateurs**,

Pour cette étape, il faut passer par les outils **RSAT** (voir doc correspondante) qui permettent de gérer le contrôleur de domaine, notamment les **OU** des salles :

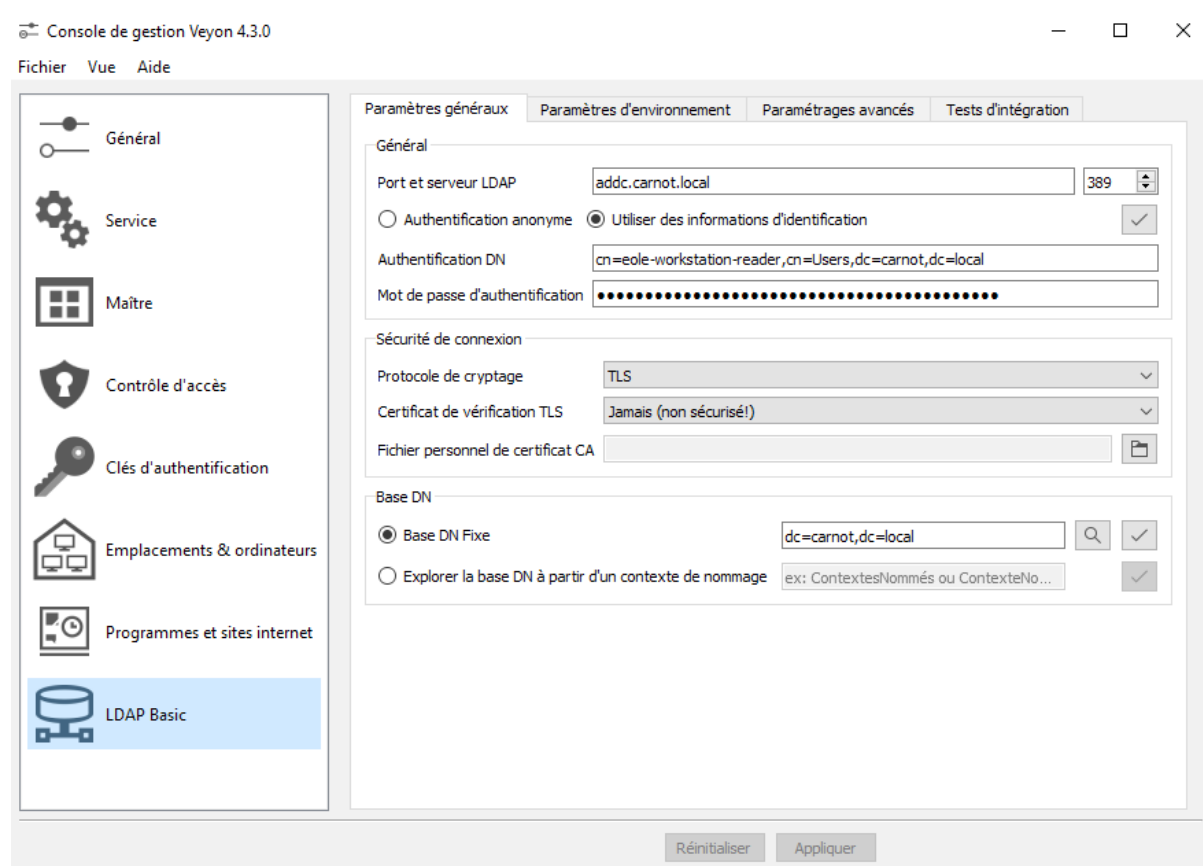
	<ul style="list-style-type: none"><li>• Dans <b>Utilisateurs et Ordinateurs Active Directory</b>, dans l'<b>OU ScribeAD</b> et la <b>sous OU Matériel</b>, nous avons un listing des <b>OU</b> par salles. Par exemple, ici nous avons l'<b>OU S211</b> qui correspond à la salle informatique S211.</li></ul>
	<ul style="list-style-type: none"><li>• Dans l'<b>OU S211</b>, nous avons à l'intérieur les stations de la salle informatique, ici ce sont <b>S211-PXX</b></li></ul>
	<ul style="list-style-type: none"><li>• Dans les propriétés de chaque poste, il faut aller dans l'onglet <b>Emplacement</b> et il faut spécifier le nom de l'<b>OU</b> de la <b>salle</b>, ici <b>S211</b>.</li><li>• Cette étape est très importante, car le client Veyon a besoin de connaître l'emplacement de chaque poste.</li></ul>

Dans l'onglet **Programmes et sites internet**, on ajoute des programmes à exécuter ainsi que des raccourcis de pages Web qui seront utilisables depuis le client **Veyon. (Facultatif)**



Dans l'onglet **LDAP Basic**, on configure l'annuaire LDAP du contrôleur de domaine. Il est utilisé pour permettre l'authentification des utilisateurs sur le client Veyon.

### **Faire exactement comme les captures d'écrans :**



Console de gestion Veyon 4.3.0

Fichier Vue Aide

Général

Service

Maître

Contrôle d'accès

Clés d'authentification

Emplacements & ordinateurs

Programmes et sites internet

**LDAP Basic**

Paramètres généraux Paramètres d'environnement Paramétrages avancés Tests d'intégration

Arborescence objet

Arborescence utilisateur OU=Utilisateurs,OU=ScribeAD

Arborescence groupe CN=Users

Arborescence ordinateur OU=Matériel,OU=ScribeAD

Arborescence groupe ordinateur (seulement si différent de l'arborescence du groupe)

☒ Effectuer des recherches récursives dans les arborescences objet

Attributs d'objet

Attribut de l'identifiant utilisateur cn

Attribut du groupe membre member

Attribut de nom d'affichage d'ordinateur cn

Attribut du nom d'hôte de l'ordinateur cn

☐ Noms d'hôtes enregistrés comme des noms de domaine pleinement nommé (FQDN, ex: monhote.exemple.org)

Attribut de l'adresse MAC de l'ordinateur ex: Adressehw

Attribut d'emplacement d'ordinateur location

Attribut de nom d'emplacement Ex: nom ou description

Réinitialiser Appliquer

Console de gestion Veyon 4.3.0

Fichier Vue Aide

Général

Service

Maître

Contrôle d'accès

Clés d'authentification

Emplacements & ordinateurs

Programmes et sites internet

**LDAP Basic**

Paramètres généraux Paramètres d'environnement Paramétrages avancés Tests d'intégration

Filtres d'objet optionnel

Filtre pour les utilisateurs (objectClass=user)

Filtre pour les groupes utilisateur (objectClass=group)

Filtre pour les ordinateurs (objectClass=computer)

Filtre pour les groupes d'ordinateurs ex: (ClasseObjet=salle) ou (ClasseObjet=Labo)

Filtre pour les conteneurs d'ordinateur ex: (ClasseObjet=container) ou (ClasseObjet=Unité d'Organisation)

Identification du groupe membre

☒ Nom distinct (Samba/AD)

☐ Attribut configuré pour l'identifiant utilisateur ou le nom d'hôte de l'ordinateur (OpenLDAP)

Identification des emplacements d'ordinateur

Identifier des emplacements ordinateur (ex salles) via:

☐ Groupe d'ordinateurs

☐ Conteneurs d'ordinateur ou bien OU

☒ Attribut d'emplacement dans les objets ordinateur

Réinitialiser Appliquer

### 1.3. tests

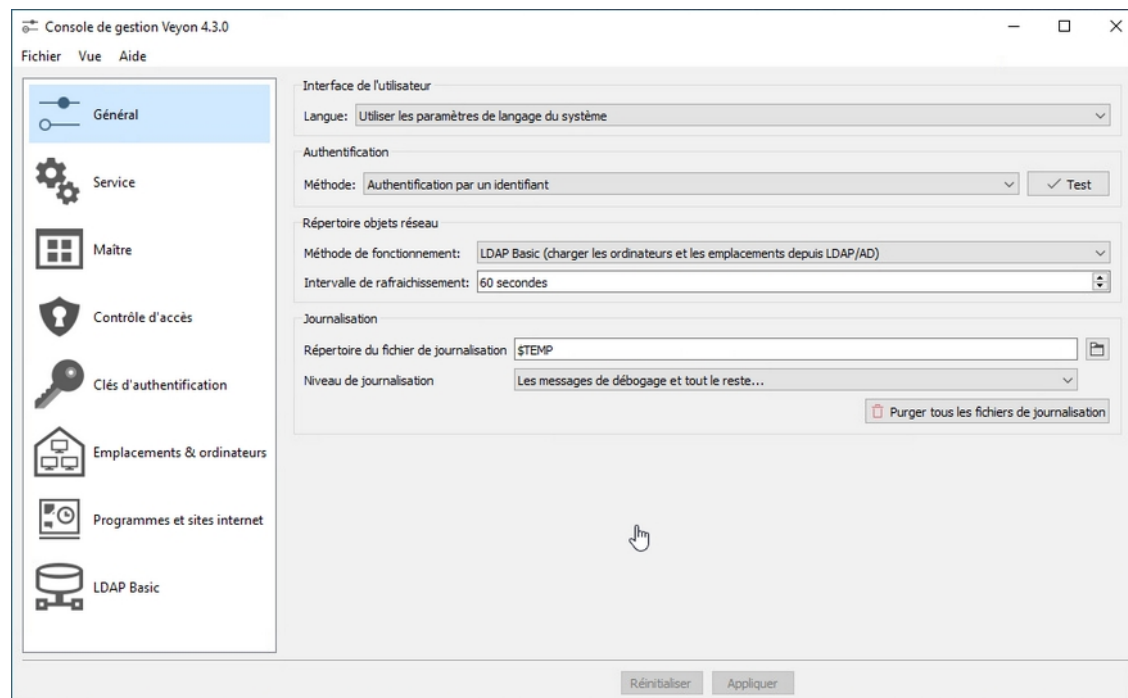
A ce stade VEYON doit marcher automatiquement, c'est à dire que sur un autre poste du réseau, il est possible de lancer VEYON-master et en se connectant avec un compte professeur de prendre en main un poste distant dans une même salle (seule la fonction « Allumer » ne marche pas). Si des problèmes subsistent, tenter de configurer les postes utilisés par les élèves comme suit :



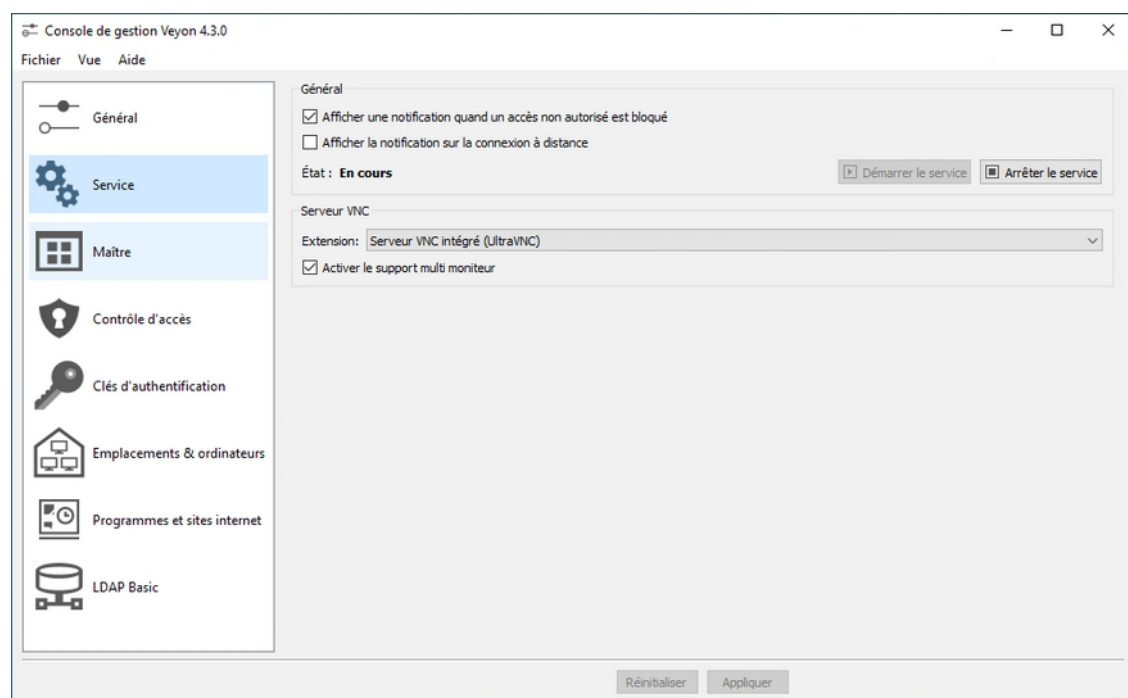
## 1.4. Configuration des postes clients (facultatif)

Pour configurer le client Veyon sur la station cliente (de l'élève), il faut lancer la **Console de gestion Veyon** (avec le compte admin pour avoir tous les droits de modification).

Dans l'onglet **Général**, on s'assure que la **Méthode d'Authentification** est bien sur **Authentification par un identifiant**. On vérifie également que la **Méthode de fonctionnement** est bien sur **LDAP Basic** (l'annuaire du ScribeAD) :



Dans l'onglet **Service**, on sélectionne le **Serveur VNC intégré** (pour la prise de main à distance) :

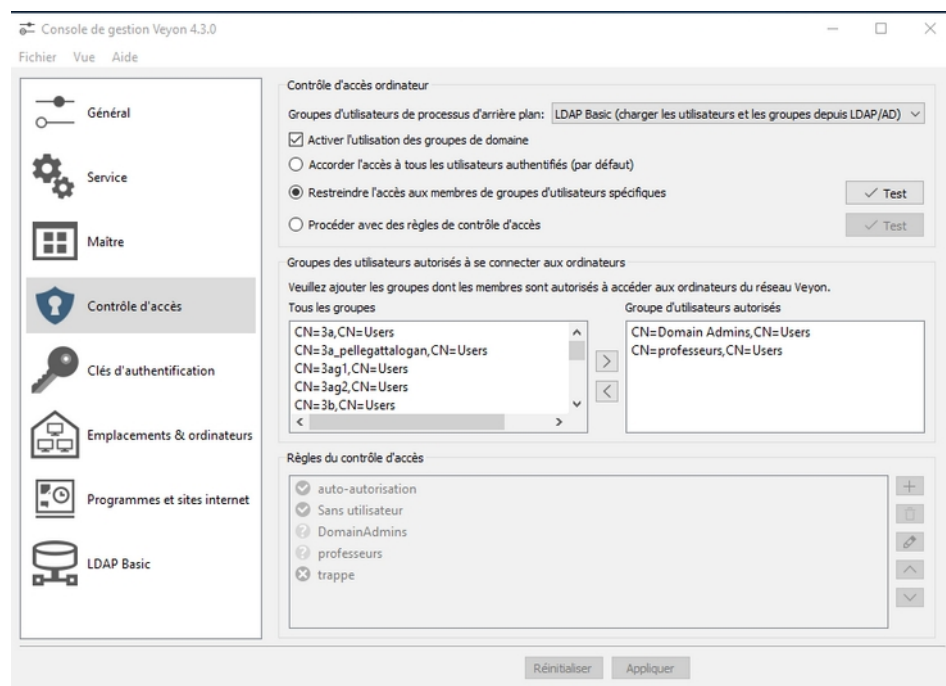


Dans l'onglet **Maître**, laissez par défaut.

Dans l'onglet **Contrôle d'accès**, on coche **Activer l'utilisation des groupes de domaine** et **Restreindre l'accès aux membres de groupes spécifiques**, ce qui permet de limiter les utilisateurs à accéder aux stations implantés dans les salles. Cela évite que tout le monde accède aux stations de toutes les salles.

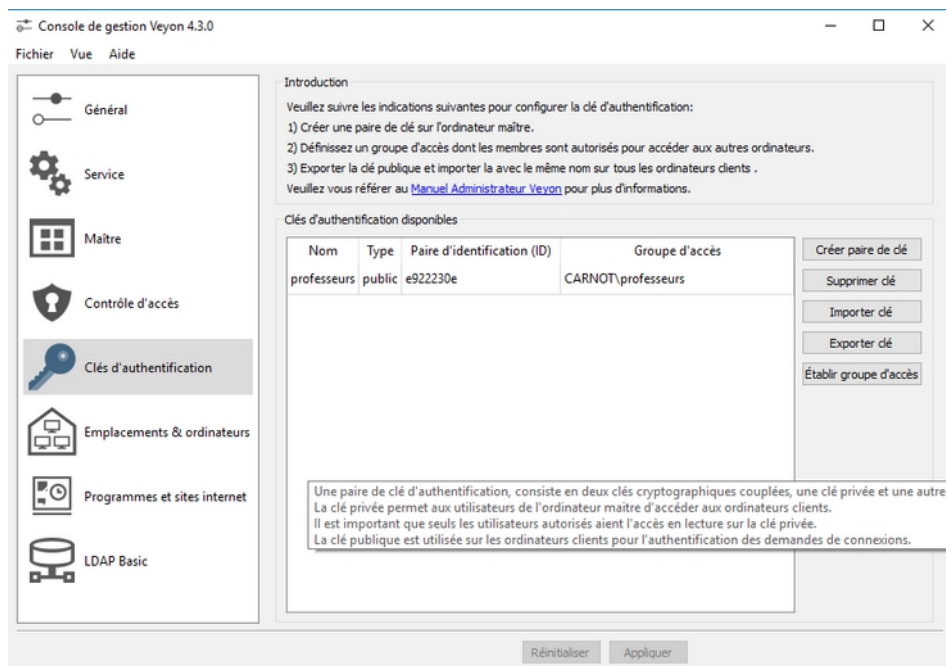


Pour se faire, on rajoute le groupe d'utilisateur qui est autorisé à prendre le contrôle des postes clients de la salle. Ici, on rajoute le groupe **professeurs** (groupe des membres des professeurs) qui autorise à prendre le contrôle des stations de la salle S211 :



Dans l'onglet **Clés d'authentification**, il faut **importer** la clé publique que nous avons exportée depuis le poste du professeur. Elle permettra aux utilisateurs du groupe que nous avons autorisé (**professeurs**) de pouvoir s'authentifier sur les stations des élèves.

On définit le groupe d'accès à cette clé publique. Ici on définit le groupe **professeurs** qui correspond au groupe de professeurs :



Dans l'onglet **Emplacement & ordinateurs**, laissez par défaut.

Dans l'onglet **Programmes et sites internet**, laissez par défaut.

Dans l'onglet **LDAP Basic**, on configure l'annuaire LDAP du contrôleur de domaine. Il est utilisé pour permettre l'authentification des utilisateurs sur le client Veyon.

**Faire exactement comme les captures d'écrans :**

