

Documentation Veyon 4.3 Windows

Sommaire

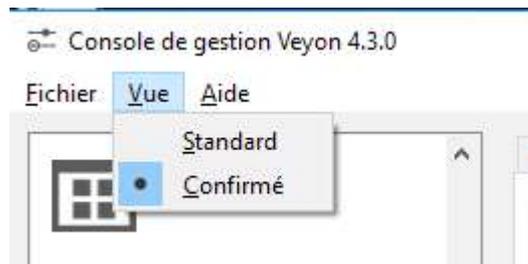
| | |
|---|----|
| 1. Installation Veyon..... | 1 |
| 2. Configuration Veyon..... | 2 |
| Général :..... | 2 |
| Services :..... | 3 |
| Maitre :..... | 6 |
| Paramètre généraux :..... | 6 |
| Comportement :..... | 7 |
| Fonctionnalités :..... | 9 |
| Contrôle d'accès :..... | 12 |
| Windows :..... | 13 |
| Clés d'authentification :..... | 16 |
| Emplacement et ordinateur :..... | 17 |
| Serveur Démo :..... | 18 |
| LDAP Basic :..... | 19 |
| Paramètres généraux :..... | 19 |
| Paramètres d'environnement :..... | 21 |
| Paramétrages avancés :..... | 24 |
| 3. Information complémentaire :..... | 26 |
| Doubleton de poste avec serveur LDAP :..... | 26 |
| Problème non référencé :..... | 26 |
| Information Veyon sur Linux :..... | 26 |

1. Installation Veyon

Exécutez le fichier du programme d'installation avec des privilèges d'administration et suivez les instructions à l'écran. Sur les ordinateurs qui n'ont pas besoin de l'application Veyon Master (par exemple, les ordinateurs des étudiants), vous pouvez désélectionner le composant Veyon Master dans la boîte de dialogue «Choisir des composants».

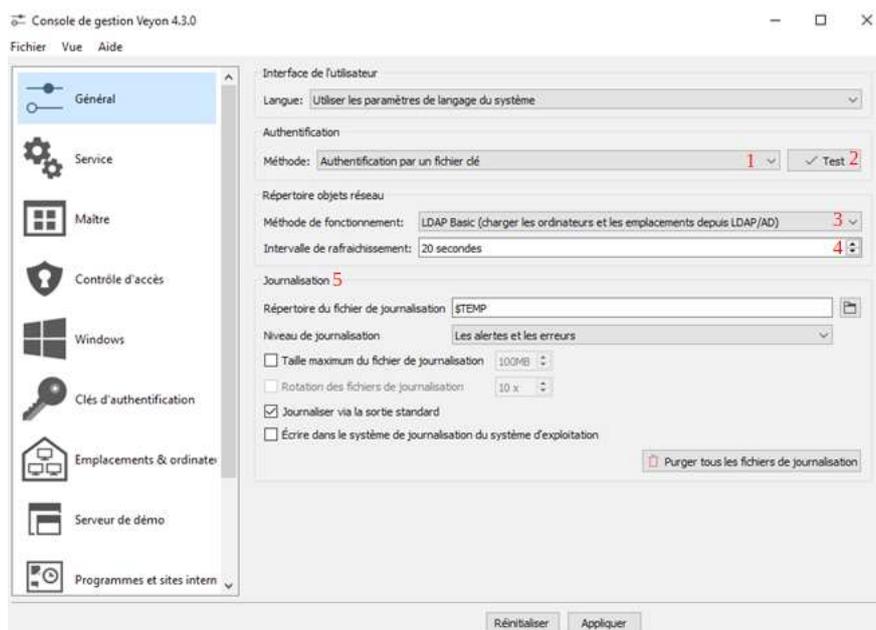
Une fois l'installation terminée, la configuration est démarrée par défaut. Ce programme permet de configurer et de personnaliser votre installation de Veyon.

2. Configuration Veyon



Pour la configuration de Veyon nous allons utiliser le mode d'affichage confirmé.

Général :



1: Cette option sert à choisir la méthode d'authentification à l'application Veyon master (Authentification par identifiant (identification via le compte du pc), Authentification par un fichier clé (consiste à s'identifier grâce à la clé privée qui est générée dans un autre menu)).

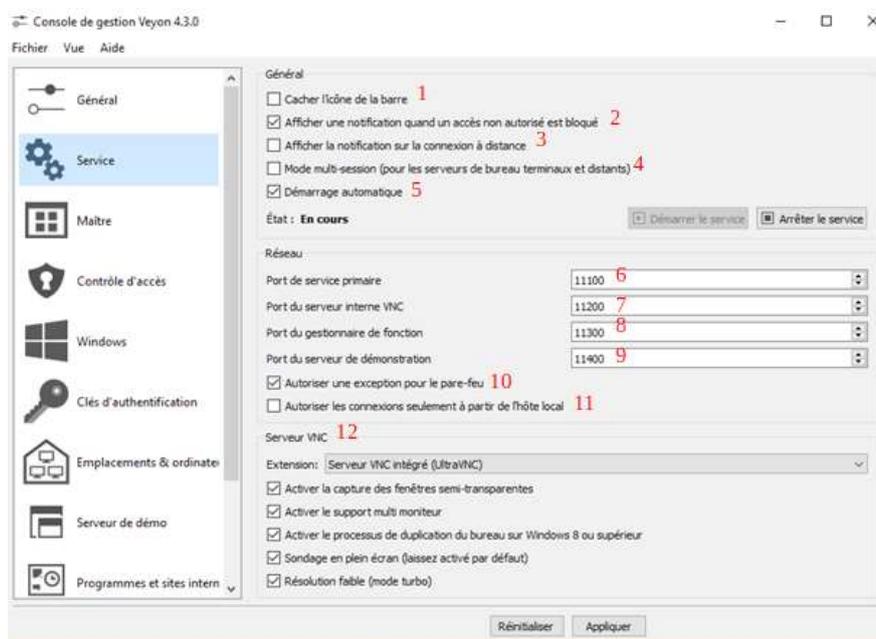
2: Le bouton test sert à tester la méthode d'authentification.

3: La méthode de fonctionnement est la façon dont Veyon va intégrer (via le menu Emplacement et ordinateur (intégration des machines manuellement), LDAP BASIC (remontée automatique des machine via la liaison avec l'annuaire LDAP configure dans le menu LDAP Basic)).

4: L'intervalle de rafraîchissement est le paramètre qui définit à quelle fréquence Veyon va interroger l'annuaire LDAP configuré dans le menu LDAP Basic ou les machines sont configurées manuellement.

5: La partie «Journalisation» est la partie de configuration des paramètres de journalisation des erreurs.

Services :



1: Cette option sert à cacher le service Veyon de la barre d'état système.

Par défaut le service Veyon affiche une icône afin d'indiquer le fonctionnement correct et de fournir des informations de base sur la version du programme.

2: Cette option spécifie si une notification doit être affichée si l'accès à l'ordinateur local a été bloqué, en raison d'un échec de l'authentification ou du contrôle de l'accès refusant l'accès.

3: Dans certains environnements, il peut être souhaitable, voire nécessaire, d'informer l'utilisateur que son ordinateur est en cours d'accès à distance. Ce comportement peut être obtenu en activant cette option. Si l'utilisateur doit demander une autorisation à la place, des règles de contrôle d'accès appropriées doivent être configurées

4: Si vous activez cette option, le service lancera un processus serveur pour chaque session interactive sur un ordinateur.

5: Lors de l'installation de Veyon, le service Veyon est enregistré en tant que service système afin de lancer automatiquement, le serveur Veyon pour les sessions utilisateur. Le démarrage du service Veyon peut être empêché en désactivant cette option. Vous devrez ensuite démarrer le serveur Veyon en session utilisateur manuellement. L'écran d'ouverture de session ne sera pas accessible dans ce cas.

6: Vous pouvez utiliser ce paramètre pour définir le port réseau principal sur lequel le serveur Veyon liste les connexions entrantes, le protocole utilisé est le protocole TCP. Port utilisé par défaut 11100.

7: Ce composant interne est une partie du serveur Veyon et permet aux processus de fournir des fonctionnalités spécifiques. Contrairement au service Veyon, ces processus doivent dans la plupart des cas s'exécuter dans le contexte de l'utilisateur enregistré et, par conséquent, pour communiquer avec le service Veyon Service via ce réseau, le protocole utilisé est le protocole TCP. Port utilisé par défaut 11200.

8: Vous pouvez utiliser ce paramètre pour définir le réseau utilisé par le gestionnaire de contenu. Ce composant interne est une partie du service Veyon Service et permet de démarrer et d'arrêter les processus pour fournir des fonctionnalités spécifiques. Contrairement au service Veyon, ces processus doivent dans la plupart des cas s'exécuter dans le contexte de l'utilisateur enregistré, par conséquent, pour communiquer avec le service Veyon Service via ce réseau, le protocole utilisé est le protocole TCP. Port utilisé par défaut 11300.

9: Vous pouvez utiliser ce paramètre pour définir le port réseau sur lequel le serveur de démonstration écoute. Le serveur de démonstration met efficacement les données d'écran d'un ordinateur sélectionné à la disposition de tous les ordinateurs participant à une démonstration, le protocole utilisé est le protocole TCP. Port utilisé par défaut 11400.

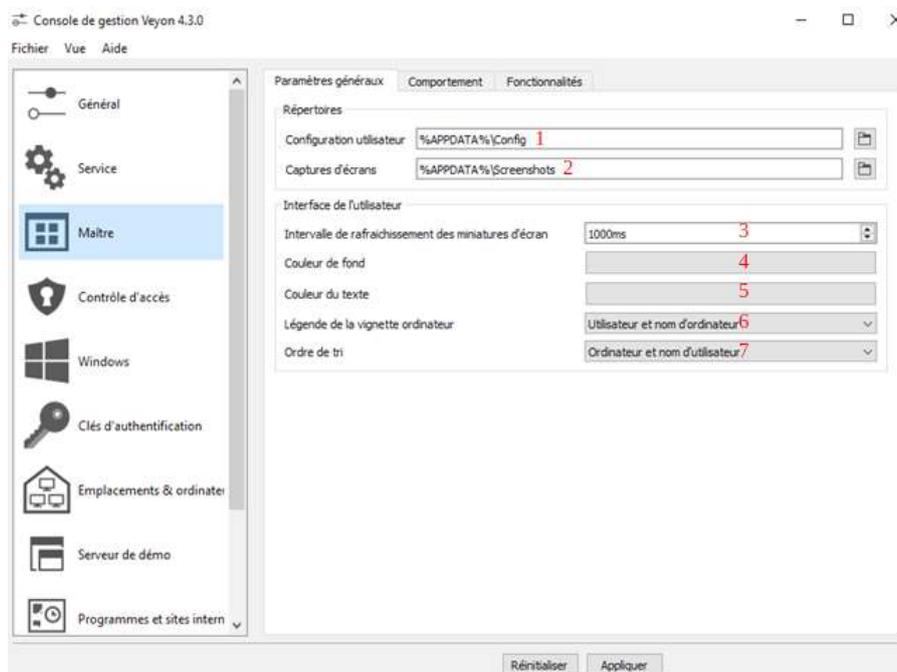
10: Selon la configuration du système, il peut être impossible d'accéder aux ports d'écoute tels que le port du serveur Veyon à partir du réseau. Sous Windows, le pare-feu Windows bloque généralement toutes les connexions entrantes. En attendant, le port de service et le port du serveur de démonstration doivent être configurés, les exceptions pour le pare-feu Windows doivent être configurées. Cette opération est effectuée automatiquement pendant le processus d'installation. Si cette configuration n'est pas désirée ni configurée manuellement, cette option est désactivée.

11: Si vous ne souhaitez pas que le serveur Veyon soit disponible pour les autres ordinateurs du réseau, vous pouvez utiliser cette option. Cette option ne doit pas être activée pour un ordinateur normal qui devrait être accessible à partir de l'application principale Veyon. Cependant, cette option peut être utilisée pour chaque ordinateur afin de garantir la sécurité au-delà de l'accès. L'accès au serveur n'est pas affecté par cette option.

12: La partie serveur VNC est la partie de configuration des options du serveur VNC.

Maitre :

Paramètre généraux :



Attention : Afin de produire une configuration générique et indépendante de l'utilisateur, vous devez utiliser des variables de substitution au lieu de chemins absolus dans les paramètres de répertoire. (Valable pour les points 1 et 2)

1: La configuration spécifique de Veyon Master est enregistrée dans ce répertoire. La configuration contient les paramètres de l'interface utilisateur ainsi que la sélection de l'ordinateur de la dernière session.

2: Tous les fichiers d'image générés à l'aide de la fonction de capture d'écran sont stockés dans ce répertoire. Si vous souhaitez collecter les fichiers dans un dossier central, vous pouvez utiliser un autre chemin que le répertoire fourni ici.

3: Ce paramètre sert à configurer la vitesse à laquelle le master Veyon actualise le retour des différents écrans des postes surveillés. Plus l'intervalle est court plus la charge processeur et réseaux sera importante.

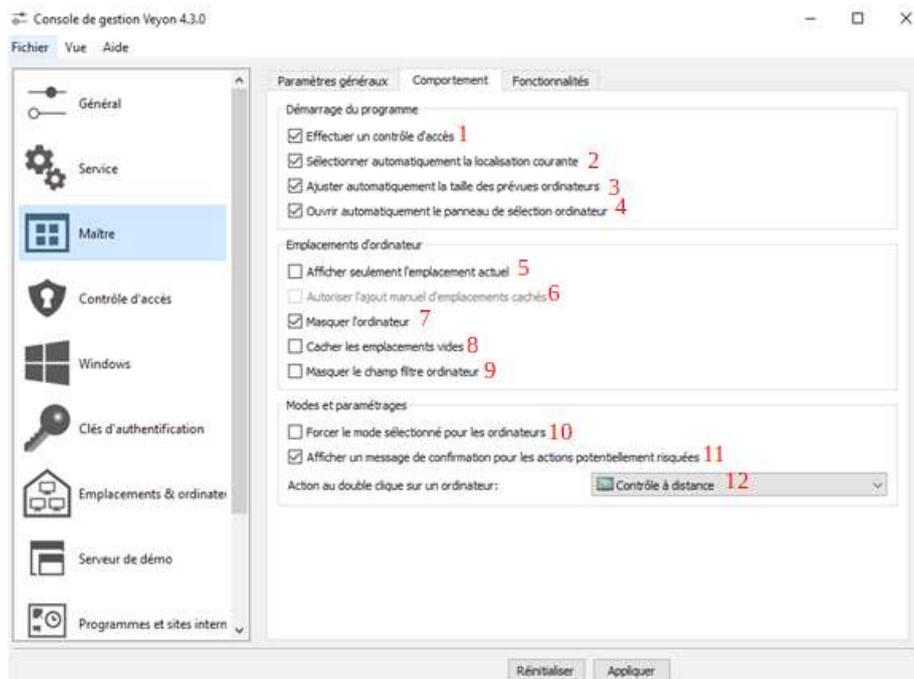
4: Ce paramètre permet de personnaliser la couleur d'arrière-plan de la vue du moniteur. Par défaut c'est noir.

5: Ce paramètre permet de personnaliser la couleur utilisée pour afficher la légende de la vignette dans la vue du moniteur. Par défaut c'est blanc.

6: Ce paramètre permet de définir la légende des vignettes d'ordinateur dans la vue du moniteur.

7: Ce paramètre permet de spécifier l'ordre de tri des ordinateurs dans la vue du moniteur.

Comportement :



1: Vous pouvez utiliser cette option pour définir si le contrôle d'accès ordinateur éventuellement configuré doit également être effectué au démarrage de l'application Veyon Master. Quand bien même le contrôle d'accès soit forcé côté

client dans tous les cas, cette option supplémentaire assure que les utilisateurs sans les droits d'accès appropriés ne peuvent même pas démarrer Veyon Master, ce qui rend la sécurité encore plus visible

2: Par défaut, tous les ordinateurs sélectionnés la fois précédente sont affichés après le démarrage de Veyon Master. Si vous souhaitez afficher tous les ordinateurs à l'emplacement de l'ordinateur maître, vous pouvez activer cette option. Veyon Master tentera ensuite de déterminer l'emplacement de l'ordinateur local à l'aide de la configuration emplacement objet et réseaux. Tous les ordinateurs situés au même endroit seront alors sélectionnés et affichés. Pour que cette fonction marche correctement, une configuration DNS convenable sur le réseau est requise pour que les deux noms d'ordinateur puissent être résolus en adresses IP et que les recherches inversées d'adresses IP renvoient des noms d'ordinateur valides.

3: Si la taille des miniatures de l'ordinateur doit être ajustée automatiquement au démarrage de Veyon Master (même effet que si vous cliquez manuellement sur le bouton *Auto*), cette option peut être activée.

4: Vous pouvez utiliser cette option pour définir le panneau de sélection de l'ordinateur est ouvert au démarrage de Veyon Master.

5: Par défaut, le panneau de sélection de l'ordinateur répertorie tous les emplacements fournis par le répertoire d'objets réseau. Si cette option est activée, seul l'emplacement de l'ordinateur Master sera sélectionné.

6: Quand l'option *Afficher seulement l'emplacement actuel* est activée, l'utilisateur peut toujours être autorisé à ajouter manuellement d'autres emplacements masqués. Si cette option est activée, un bouton supplémentaire *ajouter location* s'affiche dans le panneau de sélection de l'ordinateur. Ce bouton ouvre une boîte de dialogue avec tous les emplacements disponibles.

7: Dans les scénarios d'utilisation courante, il n'est souvent pas souhaitable d'afficher son propre ordinateur pour éviter que des fonctionnalités spécifiques n'affectent le poste Master.(verrouillage de l'écran, par exemple). Activer cette option cachera toujours l'ordinateur local pour éviter de tels problèmes.

8: Dans certaines situations, l'emplacement des objets réseau peut contenir des emplacements sans ordinateurs, par exemple en raison de filtres LDAP spécifiques. Ces emplacements vides peuvent être masqués automatiquement dans le panneau de sélection de l'ordinateur en activant cette option.

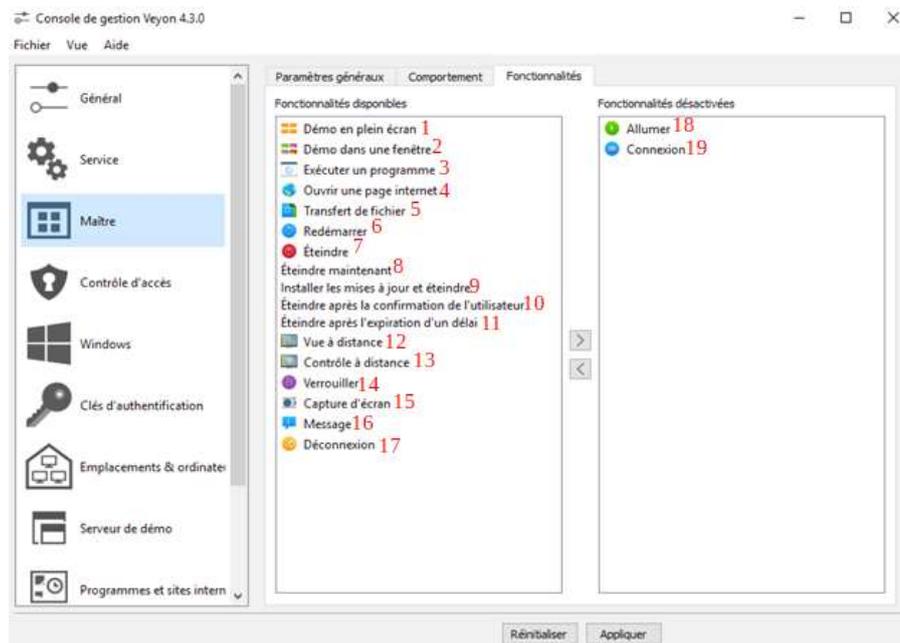
9: Le champ de filtre pour la recherche d'ordinateurs peut être caché à travers cette option. Cela permet de garder l'interface utilisateur aussi simple que possible dans les petits environnements.

10: Certaines fonctionnalités de Veyon changent le mode de fonctionnement des ordinateurs clients (mode démo, verrouillage), ces modes sont activés une fois et ne sont pas restaurés aux redémarrages. Si cette option est activée les modes seront même activés après qu'une session soit activée.

11: Cette option sert à protéger les données de l'utilisateur en cas d'activation malencontreuse de fonctionnaliser comment déconnexion, éteindre ou redémarrer

12: Cette option sert à définir l'action (vue à distance, contrôle à distance) qui sera effectuée lors du double sur un poste client.

Fonctionnalités :



Les deux listes dans les fonctionnalités permettent de définir les fonctionnalités disponibles dans Veyon Master.

1: La fonctionnalité démo plein écran sert à envoyer l'écran du poste master sur les postes clients sélectionnés en plein écran est en coupant l'utilisation des périphériques tant que l'option est activée.

2: La fonctionnalité démo dans une fenêtre sert à envoyer l'écran du poste master sur les postes clients sélectionnés dans une fenêtre.

3: La fonctionnalité « Exécuter un programme » sert à exécuter un programme installé sur le poste master sur les postes clients sélectionnés.

4: La fonctionnalité «Ouvrir une page internet» sert a ouvrir une page internet sur les postes clients sélectionnés.

5: La fonctionnalité «Transfert de fichier» sert à envoyer un fichier du poste master vers les postes clients sélectionnés dans le dossier de la session connectée.

6: La fonctionnalité «Redémarrer» sert à redémarrer un pc à distance.

7: La fonctionnalité «Eteindre »sert à éteindre un poste client a distance en fonction de l'option sélectionnée (les points de 8 a 11).

8: Cette option sert à éteindre le poste sélectionné sans délai.

9: Cette option sert à installer les mises à jour et éteindre le poste sélectionné.

10: Cette option sert à éteindre le poste client sélectionné avec l'autorisation de sont utilisateurs.

11: Cette option sert à éteindre le poste sélectionné avec un délai avant le déclenchement d'extinction

12: La fonction «Vue à distance» sert à voir l'écran d'un poste client dans une fenêtre séparée de l'application Veyon master.

13: La fonction «Contrôle à distance» sert à prendre la main sur le poste client à distance à partir du master, dans une fenêtre séparée de l'application Veyon master

14: La fonction «Verrouiller» sert à bloquer l'écran et les périphériques du poste sélectionné.

15: La fonction «Capture d'écran» sert à prendre un imprime écran du poste client sélectionné.

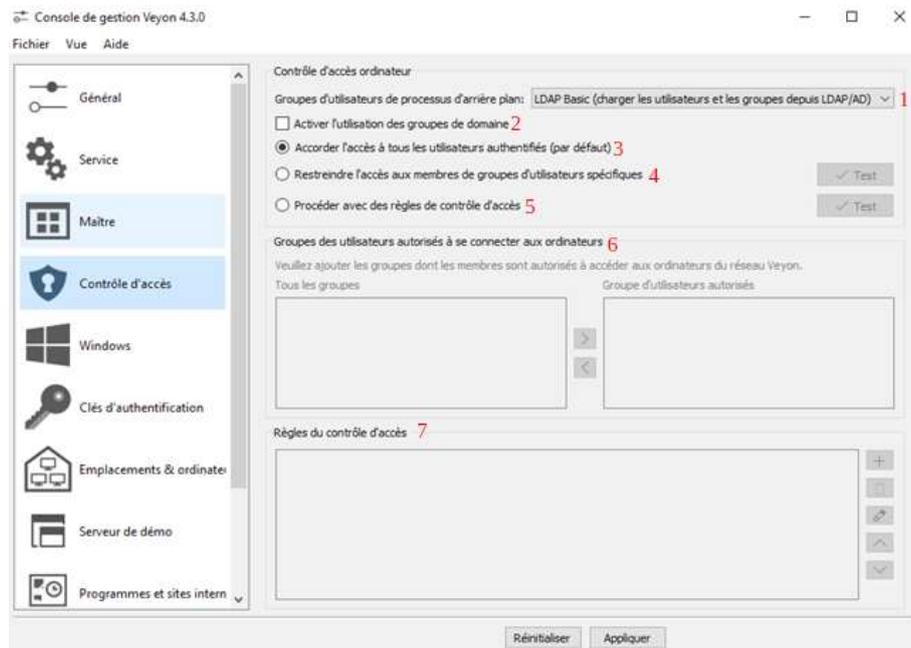
16: La fonction «Message» sert à envoyer un message aux postes sélectionnés.

17: La fonction «Déconnexion» sert a déconnecter l'utilisateur de sa session du poste sélectionné.

18: La fonction «Allumer» sert à allumer un poste client a distance, cette fonction n'est utilisable que sur les postes enregistrés dans «Emplacements objet réseaux»

19: La fonction «Connexion» permet de connecter un utilisateur particulier à distance sur tous les postes clients.

Contrôle d'accès :



1: Cette option sert à sélectionner les groupes d'utilisateur autorisés, elle définit la manière dont les groupes vont être récupérés par Veyon. Alors que le serveur principal par défaut convient aux groupes d'utilisateurs du système, les serveurs LDAP feront en sorte que les groupes d'utilisateurs LDAP / AD soient disponibles pour le contrôle d'accès.

2: Lorsque vous utilisez le contrôle d'accès combiné avec le moteur par défaut, seuls les groupes de systèmes locaux sont disponibles par défaut. En activant cette option, tous les groupes du domaine auquel appartient un ordinateur peuvent être interrogés et utilisés. Cette option n'est pas activée par défaut pour des raisons de performances. Dans les environnements avec un grand nombre de groupes de domaines, le contrôle d'accès peut prendre beaucoup de temps. Dans de tels scénarios, vous devriez envisager de configurer l'LDAP/AD intégration et d'utiliser un des services LDAP d'arrière plan.

3: Si le schéma d'authentification sélectionné est suffisant (par exemple, lors de l'utilisation d'une authentification de fichier de clé avec un accès restreint aux

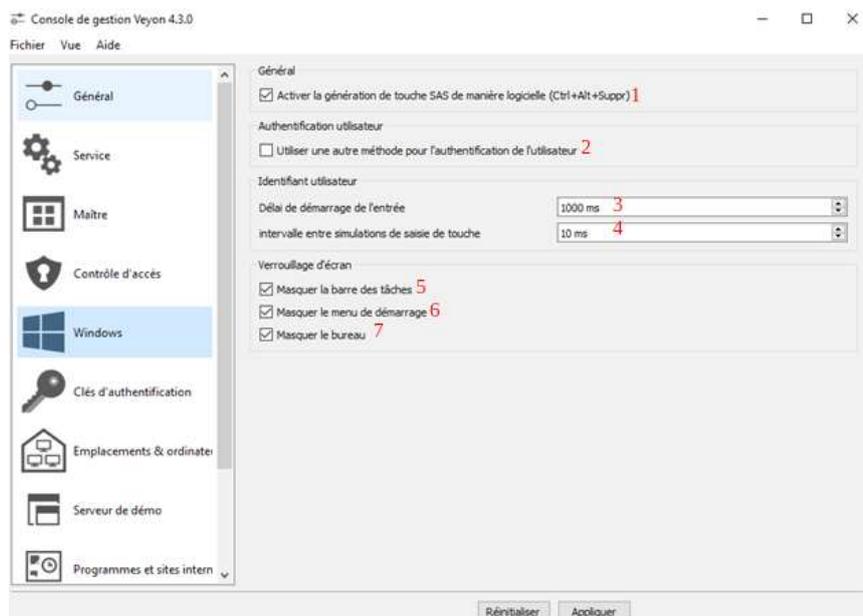
fichiers de clé), cette option peut être activée. Dans ce mode, aucun autre contrôle d'accès n'est effectué.

4: Dans ce mode, l'accès à un ordinateur est limité aux membres de groupes d'utilisateurs spécifiques. Ces groupes d'utilisateurs autorisés peuvent être configurés dans la section «Groupes des utilisateurs autorisés à se connecter aux ordinateurs».

5: Ce mode permet un contrôle d'accès détaillé basé sur les règles de contrôle d'accès définies par l'utilisateur et offre la plus grande flexibilité

7: La configuration de ce mode de contrôle d'accès est simple. La liste de gauche contient tous les groupes d'utilisateurs fournis par le processus sélectionné. Par défaut, ce sont tous des groupes d'utilisateurs locaux. Si l'LDAP/AD Basic (charger les utilisateurs et les groupes depuis LDAP/AD) est configurée, tous les groupes d'utilisateurs LDAP sont affichés. Vous pouvez alors sélectionner un ou plusieurs groupes et les déplacer vers la liste de droite en utilisant les boutons correspondants entre les deux listes. Tous les membres de chaque groupe de la liste de droite peuvent accéder à l'ordinateur. N'oubliez pas de transférer la configuration à tous les ordinateurs par la suite.

Windows :



1: Sous Windows par défaut, il est impossible pour les applications de générer la séquence d'alerte sécurisée (Ctrl+Alt+Suppr) afin de simuler l'utilisation de ces touches. Lors de l'activation de cette option, une stratégie est écrite dans le registre Windows, ce qui modifie ce comportement. Il est recommandé de laisser cette option activée afin de pouvoir envoyer Ctrl+Alt+Del lors du contrôle à distance d'un ordinateur.

Veyon implémente deux mécanismes différents pour authentifier un utilisateur (vérifier son nom d'utilisateur et son mot de passe) sur Windows lors de l'utilisation de l'authentification d'ouverture de session. Le mécanisme par défaut est utilisé avec succès depuis de nombreuses années. Il est basé sur l'interface du fournisseur de support de sécurité et fonctionne dans presque tous les environnements.

2: Si le mécanisme par défaut ne fonctionne pas dans votre environnement, vous pouvez utiliser un autre mécanisme de secours. Ce mécanisme utilise une

fonction de haut niveau dans le système d'exploitation qui effectue une connexion interne de l'utilisateur réseau à vérifier les informations d'identification de l'utilisateur. Ce processus de connexion peut être plus lent que la simple authentification effectuée par le mécanisme par défaut.

3: Cette valeur spécifie le nombre de millisecondes à attendre entre l'émission Ctrl + Alt + Suppr et l'envoi du premier caractère du nom d'utilisateur. Cette valeur peut être augmentée sur des ordinateurs lents pour s'assurer que le champ de saisie du nom d'utilisateur est prêt.

4: Cette valeur spécifie le nombre de millisecondes à attendre entre les touches individuelles simulées. Augmentez cette valeur si vous rencontrez des échecs de connexion causés par des caractères manquants ou des champs de saisie mal basculés.

La fonctionnalité de verrouillage de l'écran par défaut désactive tous les périphériques d'entrée et masque des parties de l'interface utilisateur du système d'exploitation.

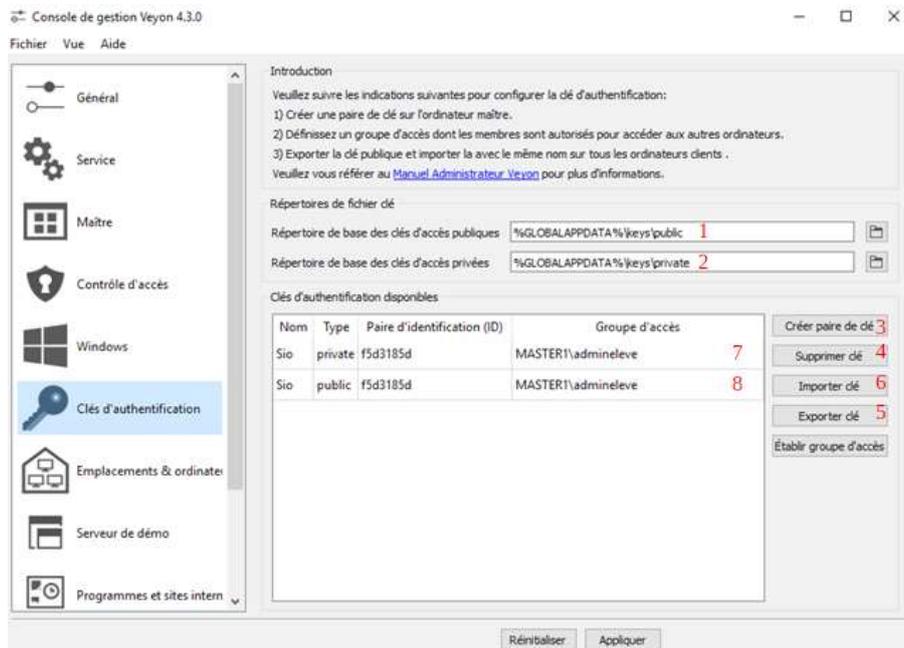
Ce comportement peut être modifié dans les cas où certaines parties de l'interface utilisateur du système d'exploitation ne fonctionnent plus correctement après le déverrouillage d'un ordinateur.

5: Cette option définit si la barre des tâches et le bouton de démarrage doivent être désactivés et masqués par la fonction de verrouillage de l'écran.

6: Cette option définit si le menu Démarrer doit être désactivé et masqué par la fonction de verrouillage de l'écran.

7: Cette option définit si le bureau doit être désactivé et masqué par l'écran fonction de verrouillage.

Clés d'authentification :



Les variables d'espace doivent être utilisées pour les deux répertoires de base. Sur Chemins d'accès Windows peut être utilisé à la place des chemins absolus.

1: Le répertoire de base spécifié contient des sous-répertoires pour chaque nom de clé dans lequel se trouve le fichier de clé publique.

2: Le répertoire de base spécifié contient des sous-répertoires pour chaque nom de clé dans lequel se trouve le fichier de clé privée. Cela permet de définir individuellement les droits d'accès aux sous-répertoires.

3: Cette option sert à créer une paire de clé (privée et publique).

4: Cette option sert à supprimer une clé (privée ou publique) sélectionnée.

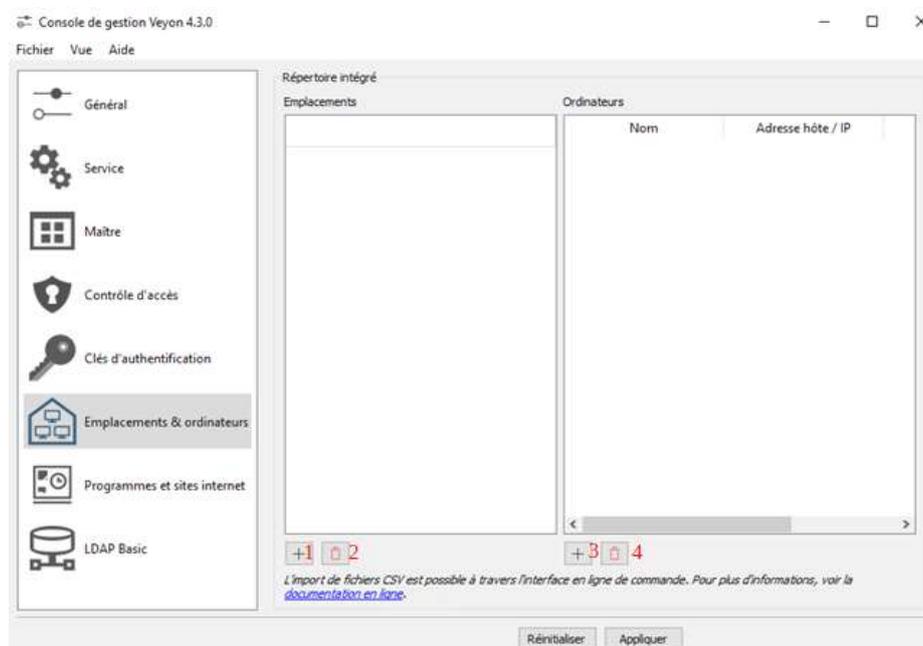
5: Cette option sert à exporter une clé (privée ou publique) sélectionnée au format PEM.

6: Cette option sert à importer une clé (privée ou Publique) aux forma PEM.

7: Veyon Master recherche les fichiers de clé privée accessibles dans ce répertoire de base et utilise les fichiers de clé privée pour s'authentifier auprès du serveur Veyon sur ordinateurs clients. Elle est aussi utile pour se connecter avec la méthode d'authentification par clé.

8: La clé publique sert à établir la liaison entre les postes clients et le poste master.

Emplacement et ordinateur :



Tout les informations entré dans cet onglet ne seront pas utilisé par l'application Veyon Master si l'option «méthode de fonctionnement» de la partie «Répertoire réseaux» dans l'onglet «Général» est configuré sur LDAP BASIC.

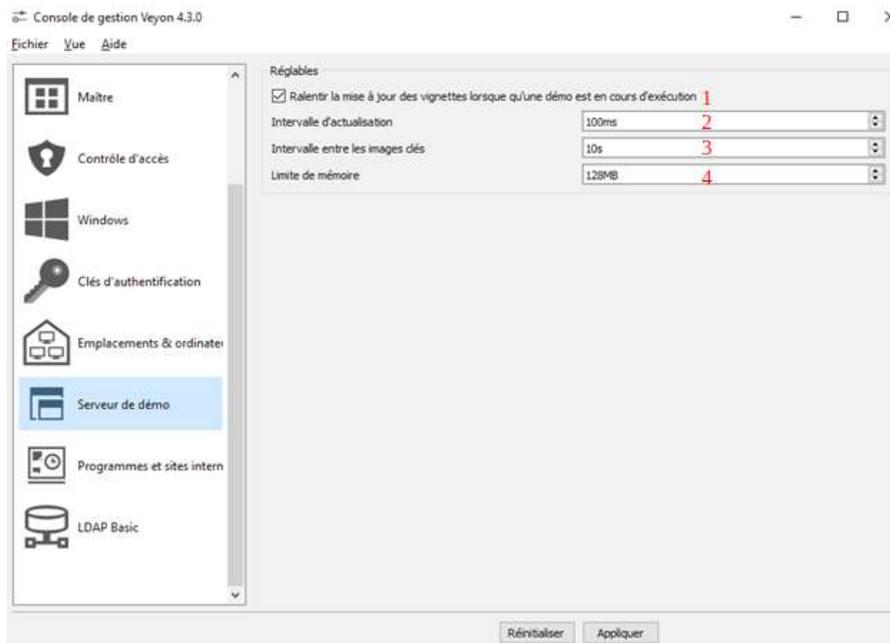
1: Ce bouton sert à crée un emplacement dans lequel pourront être ajoutés des postes clients.

2: Ce bouton sert à supprimer un emplacement.

3: Ce bouton sert à ajouter des postes clients

4: Ce bouton sert à supprimer un poste client de la liste.

Serveur Démo :



1: Cette option sert à ralentir la vitesse de mise à jour des vignettes lors que le mode démo est en cours d'exécution se réduit la charge processeur et le charge réseaux.

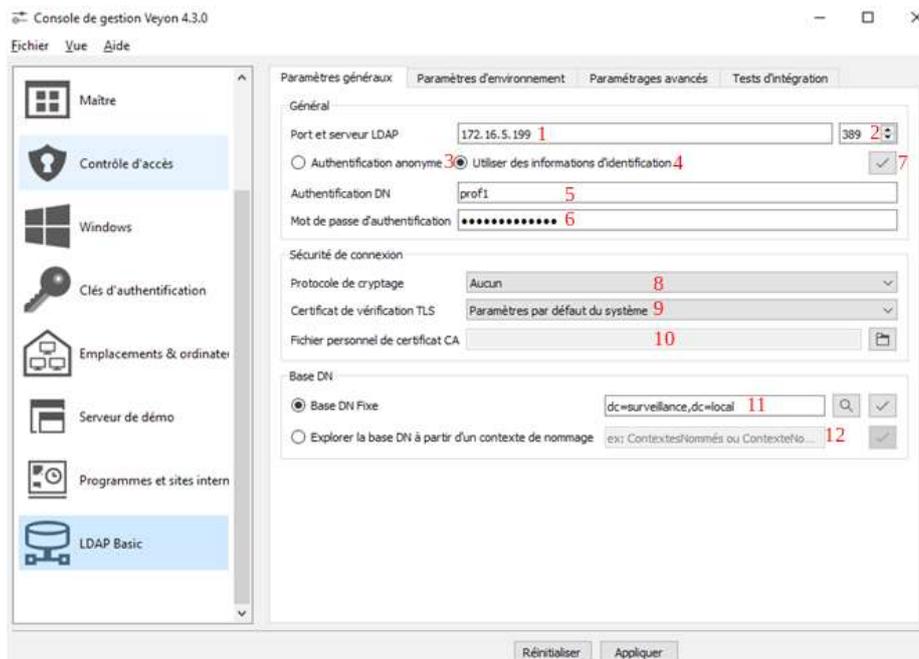
2: Cette option peut être utilisée pour définir l'intervalle entre deux mises à jour d'écran. Plus l'intervalle est petit, plus le taux de rafraîchissement est élevé et plus le transfert d'écran est fluide. Cependant, une baisse de valeur entraîne une charge de processeur plus élevée et un trafic réseau accru.

3: Pendant une diffusion d'écran, seules les zones d'écran modifiées sont envoyées au postes clients afin de minimiser le trafic réseau. Ces mises à jour sont effectuées individuellement et de manière asynchrone pour chaque client. Ainsi, après un certain temps, les clients peuvent ne plus être exécutés de manière synchrone en fonction de la bande passante et de la latence. Par conséquent, le contenu de l'écran (images clés) est transmis à intervalles réguliers, de sorte qu'une image synchrone soit affichée sur tous les clients au plus tard lorsque l'intervalle d'images clés expire. Plus la valeur n'est basse, plus le processeur et le trafic réseau sont élevés.

4: Toutes les données de mise à jour d'écran sont stockées par le serveur de démonstration dans une mémoire tampon interne, puis distribuées aux clients. Pour éviter que la mémoire tampon interne entre deux images clés n'occupe trop de mémoire en raison d'un trop grand nombre de mises à jour incrémentielles, la valeur spécifiée ici est utilisée comme limite. Cette limite est une limite souple, de sorte que si elle est dépassée, une mise à jour d'image clé est tentée, mais le tampon conserve toujours toutes les données. La mémoire tampon n'est réinitialisée que lorsque la valeur double est dépassée. S'il y a des interruptions ou des retards répétés lors de la diffusion d'un écran, cette valeur doit être augmentée.

LDAP Basic :

Paramètres généraux :



1: Entrez l'adresse du serveur LDAP (nom d'hôte ou adresse IP) ici.

2: Si un port autre que le port LDAP par défaut 389 est utilisé, le paramètre de port doit être ajusté en conséquence.

3: En fonction de l'environnement et de la configuration du LDAP sur le serveur, les requêtes LDAP peuvent être effectuées en tant qu'utilisateur anonyme ou avec des noms d'utilisateur et des mots de passe valides uniquement.

4: Si l'accès au serveur nécessite un nom d'utilisateur et un mot de passe, l'option Utiliser les informations d'identification de liaison doit être sélectionné et les informations d'identification doivent être entrées dans les champs de saisie ci-dessous.

5: Cette zone sert à définir l'identifiant ayant des droits sur le domaine qui servira à Veyon pour se connecter au serveur LDAP. ⚠ Dans certain cas il est obligatoire de pressier le nom de domaine sous la forme «identifiant@NomDeDomaine».

6: Cette zone sert à définir le mot de passe d'authentification qui servira à Veyon pour se connecter au serveur LDAP.

7: Ce bouton sert à tester si la connexion avec le serveur LDAP fonctionne bien.

8: Vous pouvez choisir entre les protocoles de cryptage *Aucun*, *TLS* et *SSL*.

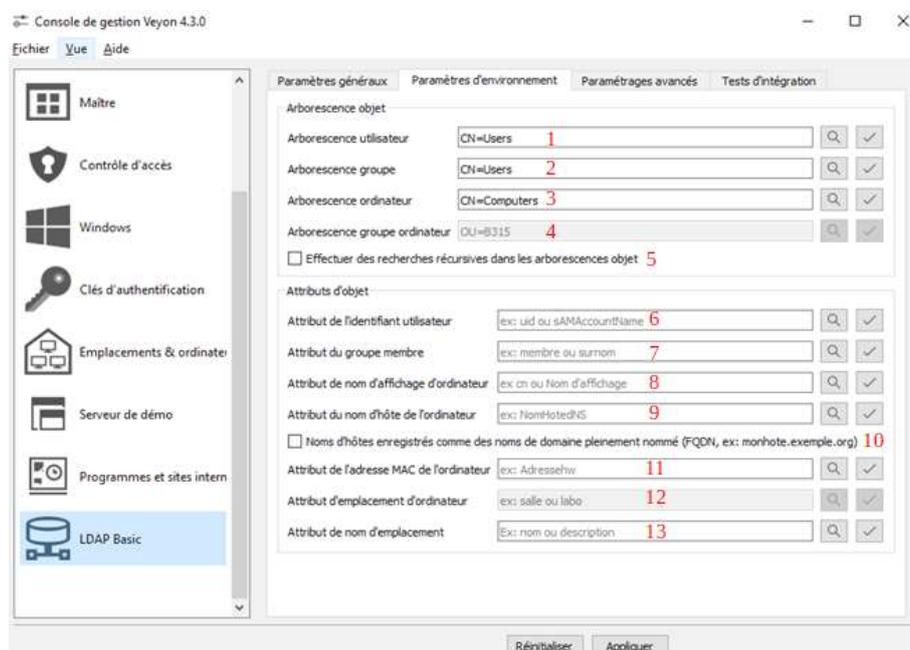
9: Ce paramètre détermine comment le certificat de sécurité du serveur LDAP doit être vérifié lorsque la connexion cryptée est établie. Avec le paramètre par défaut Système par défaut, selon le système d'exploitation utilisé, une tentative de vérification du certificat est effectuée à l'aide des certificats racine installés à l'échelle du système. Le magasin de certificats Windows n'est pas pris en compte ici, de sorte qu'une autorité de certification distincte le fichier de certificat doit éventuellement être stocké. Avec le paramètre Jamais, le certificat de serveur n'est pas du tout vérifié. Toutefois, cela autorise les attaques au cas par cas et ne devrait donc être utilisé que dans des cas exceptionnels. Le paramètre Fichier de certificat de l'autorité de certification défini par l'utilisateur garantit que la vérification du certificat est effectuée sur la base d'un fichier de certificat de l'autorité de certification spécifié.

10: Si vous utilisez votre propre autorité de certification, il peut être nécessaire pour stocker leur certificat au format de fichier PEM afin que Veyon puisse vérifier le certificat du serveur LDAP.

11: Dans la plupart des cas, un nom distinctif de base fixe est utilisé, de sorte que l'option par défaut doit être choisie. Le DN (Nom de Domaine) de base puis doit être entré dans le champ de saisie correspondant ou sélectionné sur le serveur à l'aide du bouton Parcourir. Vous pouvez utiliser le bouton Test pour vérifier si les paramètres sont corrects et si les entrées peuvent être trouvées.

12: Si une configuration Veyon générique doit être utilisée sur plusieurs sites avec des DN de base différents, Veyon peut être configuré. Afin que le DN de base soit toujours interrogé dynamiquement à l'aide de contextes de nommage LDAP. Pour que cela fonctionne la découverte du DN de base en nommant le contexte doit être choisie et l'attribut de contexte de nommage doit être adapté. Vous pouvez utiliser le bouton Test pour vérifier si un DN de base peut être déterminé.

Paramètres d'environnement :



Les arbres d'objets sont des unités organisationnelles ou structurelles dans lesquelles certains types d'objets (utilisateurs, groupes, ordinateurs) sont stockés. Les CN (noms communs) ou les OU (unités organisationnelles) respectifs doivent être entrés sans le DN de base dans le champ de saisie respectif. A côté

de chaque champ de saisie, il y a des boutons pour ouvrir les boîtes de dialogue de navigation, et pour tester le réglage individuel.

1: L'arborescence LDAP (sans DN de base) dans laquelle se trouvent les objets utilisateur doit être entrée ici, par exemple : OU=Users ou CN=Users.

2: L'arborescence LDAP (sans DN de base) dans laquelle se trouvent les objets de groupe doit être entrée ici, par exemple : OU=Groups or CN=Groups.

3: L'arborescence LDAP (sans DN de base) dans laquelle se trouvent les objets informatiques doit être entrée ici, par exemple : OU=Computers or CN=Computers.

4: Si les groupes d'ordinateurs sont situés dans une arborescence différente de celle des groupes d'utilisateurs habituels ou dans une sous-arborescence, vous pouvez spécifier ici l'arborescence LDAP correspondante. Sinon, l'arborescence des groupes est utilisée pour interroger des groupes d'ordinateurs et les filtrer avec un filtre spécifique «filtre d'objet optionnel» si nécessaire.

5: Cette option peut être utilisée pour contrôler si les objets doivent être interrogés de manière récursive. La recherche s'effectue alors non seulement dans l'arborescence spécifiée, mais également dans les sous-arborescences existantes.

Pour que Veyon puisse récupérer les informations requises à partir des objets interrogés, les noms de certains objets les attributs doivent être configurés, car ils diffèrent en fonction de l'environnement et du serveur LDAP. À côté de chaque champ de saisie, des boutons permettent de parcourir l'attribut d'un objet existant et de tester l'attribut correspondant.

6: Cet attribut doit contenir le nom de connexion d'un utilisateur. L'attribut est utilisé pour déterminer l'objet utilisateur LDAP associé à un nom d'utilisateur particulier.

7: Les membres d'un groupe sont répertoriés dans les objets de groupe via cet attribut. L'attribut est utilisé pour déterminer les groupes dont un utilisateur particulier est membre.

8: Le contenu de cet attribut facultatif est utilisé pour déterminer le nom d'un ordinateur affiché dans Veyon Master. Si laissé vide, le nom commun (CN) est utilisé à la place.

9: Cet attribut doit contenir le nom DNS de l'ordinateur. C'est utilisé pour déterminer l'objet ordinateur LDAP associé à un nom d'hôte d'ordinateur particulier.

10: Cette option spécifie si le nom de domaine pleinement qualifié FQDN (fully qualified domain name) doit être utilisé pour mapper les noms d'ordinateur sur des objets ordinateurs de l'annuaire LDAP. Si les noms d'ordinateur sont stockés sans la partie de domaine dans l'annuaire LDAP, vous devez laisser cette option désactivée, sinon elle doit être activée.

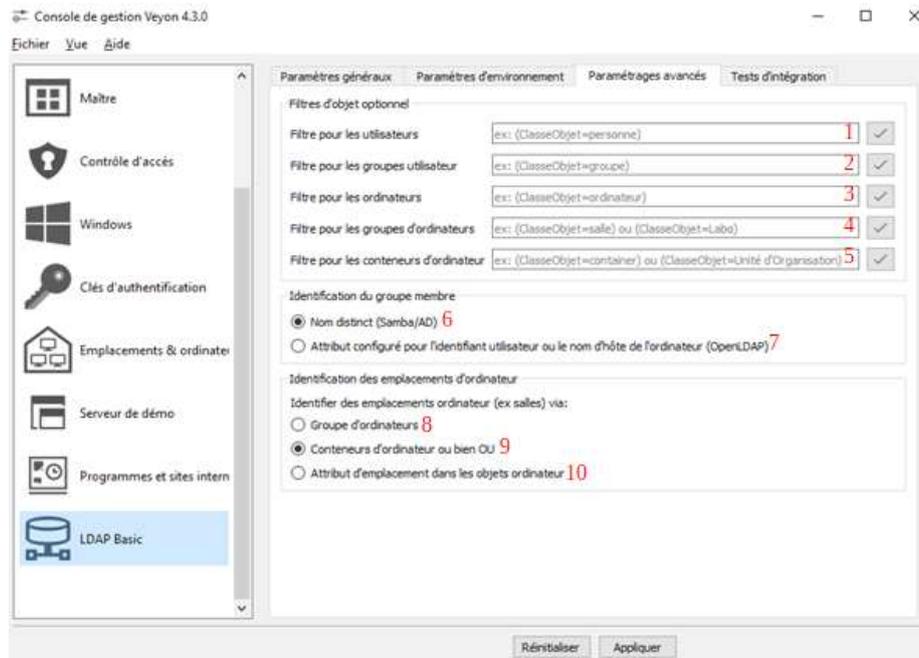
11: En complément du nom de l'ordinateur, les adresses MAC des ordinateurs sont stockées dans l'annuaire LDAP dans certains environnements, par exemple si le serveur DHCP accède également à l'annuaire LDAP. Si la fonction Veyon doit être utilisée pour allumer des ordinateurs via Allumer, le nom de l'attribut correspondant doit être entré ici, étant donné que l'adresse MAC est requise pour cette fonctionnalité. Les noms d'attributs typiques sont hwAddress ou dhcpAddress

12: Si le schéma LDAP pour les objets ordinateur fournit un attribut spécial pour le mappage vers un emplacement, vous pouvez entrer ce nom d'attribut ici. Le bouton *Test* peut être utilisé pour vérifier si les ordinateurs d'un emplacement peuvent être interrogés correctement à l'aide de l'attribut configuré.

13: Lors de l'identification d'emplacement d'ordinateur via des groupes d'ordinateurs ou des conteneurs d'ordinateurs, la valeur d'un attribut donné peut être affichée en tant que nom d'emplacement au lieu des noms communs de ces groupes ou objets. Si, par exemple, les groupes d'ordinateurs ont un attribut

appelé nom ou description, un nom d'emplacement significatif peut être stocké dans cet attribut et ce nom peut être entré ici.

Paramétrages avancés :



1: Vous pouvez définir un filtre LDAP pour les utilisateurs ici, par exemple. (object-Class = person) ou (& (objectClass = person) (objectClass = veyonUser)).

2: Vous pouvez définir un filtre LDAP pour les groupes d'utilisateurs ici, par exemple. (objet-classe = groupe) ou (| (cn = professeurs) (cn = étudiants) (cn = administrateurs)).

3: Vous pouvez définir un filtre LDAP pour les ordinateurs ici, par exemple. (classe d'objet = ordinateur) ou (& (! (cn = imprimante *)) (! (cn = scanner *)))

4: Vous pouvez définir un filtre LDAP pour les groupes d'ordinateurs ici, par exemple. (objectClass = room) ou (cn = Room *). Si des groupes d'ordinateurs sont utilisés comme emplacements, vous pouvez filtrer les emplacements affichés de cette façon

5: Vous pouvez définir un filtre LDAP pour les conteneurs d'ordinateurs ici, par exemple. (objectClass = conteneur) ou (objectClass = organizationUnit). Si les conteneurs / unités d'organisation sont utilisés comme emplacements, vous pouvez filtrer les emplacements affichés de cette façon.

Le contenu des attributs d'appartenance à un groupe varie selon les implémentations LDAP. Alors que dans Active Directory le nom distinctif (DN) d'un objet est stocké dans l'attribut membre, OpenLDAP stocke généralement le nom de connexion de l'utilisateur ou le nom de l'ordinateur. Pour que Veyon utilise la valeur correcte pour interroger les groupes d'un utilisateur ou d'un ordinateur, vous devez choisir le paramètre approprié ici.

6: Cette option doit être choisie si le nom distinctif (DN) d'un objet est stocké dans un attribut membre du groupe. Habituellement, Samba et le serveur AD utilisent ce schéma.

7: Cette option doit être choisie si le nom distinctif (DN) d'un objet est stocké dans un attribut membre du groupe. Habituellement, Samba et le serveur AD utilise Veyon propose plusieurs méthodes : pour représenter des emplacements d'ordinateur dans un annuaire LDAP. Dans le cas simple, il existe un groupe d'ordinateurs pour chaque emplacement. Tous les ordinateurs d'un emplacement spécifique sont membres du groupe correspondant. Si, à la place, les ordinateurs sont organisés en conteneurs ou en unités d'organisation, ces objets parents peuvent être utilisés comme emplacements. Les deux procédures ne nécessitent aucune adaptation du schéma LDAP. Troisièmement, le nom de l'emplacement peut également être stocké en tant qu'attribut spécial dans chaque objet ordinateur.

8: Cette option spécifie que les emplacements d'ordinateur sont identifiés par le biais de groupes d'ordinateurs. Tous les groupes d'ordinateurs sont ensuite affichés comme emplacements dans Veyon Master. Pour chaque emplacement, tous les ordinateurs membres du groupe correspondant sont affichés. Si tous les groupes LDAP ne doivent pas être affichés en tant qu'emplacements, vous devez utiliser un répertoire *computer* «group tree» doit être configuré ou les groupes d'ordinateurs doivent être restreints à l'aide d'un *computer* «group filter».

9: Cette option spécifie que les conteneurs/OU's (unités d'organisation) contenant des objets ordinateur sont utilisés comme emplacements d'ordinateur. Les conteneurs sont des objets parents d'objets informatiques dans

l'arborescence LDAP. Si tous les conteneurs ne doivent pas être affichés en tant qu'emplacements, un computer «container filter» peut être mis en place.

10: Si le schéma LDAP pour les objets ordinateur fournit un attribut spécial permettant de mapper des objets informatiques sur des emplacements, cette option peut être activée et le nom de l'attribut peut être entré. Le bouton Test peut être utilisé pour vérifier si les membres d'un emplacement d'ordinateur peuvent être interrogés correctement à l'aide de l'attribut configuré.

3.Information complémentaire :

Doublon de poste avec serveur LDAP :

Si lors de l'utilisation d'un Master Veyon liée a un serveur LDAP des doublons d'écran se font sur différent machine vérifier dans le DNS, s'il n'y a pas de doublon IP dans la correspondance entre les noms de poste et leurs IP.

Problème non référencé :

Pour tout problème lors de l'utilisation de Veyon non référencé je vous invite à vous rendre sur le site <https://docs.veyon.io/en/latest/>.

Information Veyon sur Linux :

Pour toute information sur installation ou la configuration de Veyon sur Linux je vous invite à vous rendre sur le site <https://docs.veyon.io/en/latest/>.