RÉPUBLIQUE DU SÉNÉGAL

UN PEUPLE, UN BUT, UNE FOI

MINISTERE DE L'EDUCATION NATIONALE,
DIRECTION DE L'ENSEIGNEMENT SUPERIEUR

Ecole Supérieure de Technologie et de Management de Dakar

Rapport Interne

Audit de windows serveur 2022 avec wallix

Présenter par :

KIFALA MAKELE Gerald

Supervision :

Mr Adjeoua

Année académique 2024– 2025

Audit de windows serveur 2022 avec Wallix

qu'est-ce qu'un Bastion ?

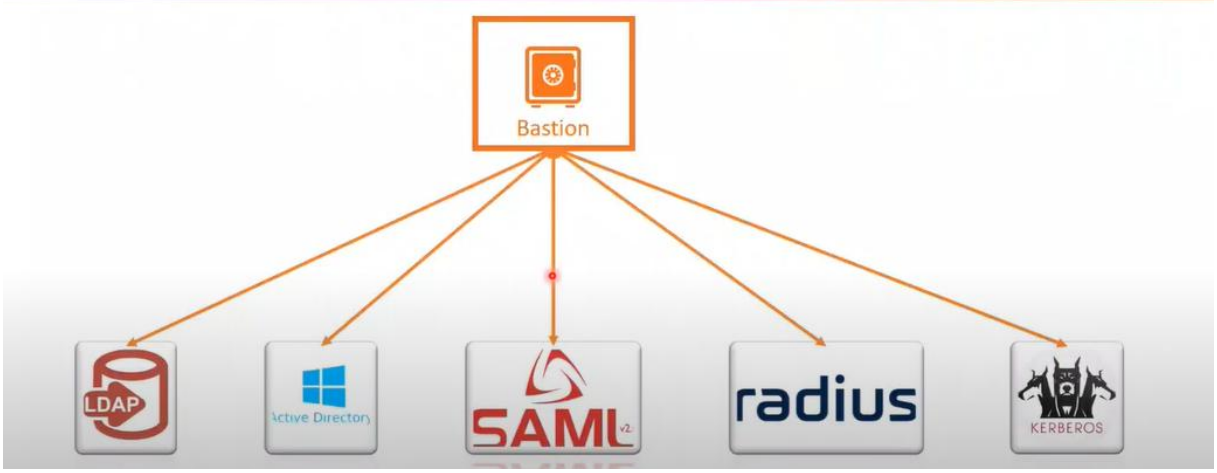
Dans le jargon de la cybersécurité, un bastion fait référence à un panneau d'administration de sécurité informatique. Celui-ci a pour but de fournir un point d'accès unique aux ressources informatiques les plus sensibles d'une société (données, CRM, logiciels SAAS, etc.). Pour protéger le patrimoine numérique d'une entreprise, ce dispositif applique divers contrôles d'accès. Il répond ainsi à des questions de l'ordre de :

- Qui a accès à quoi et quand ?
- Quels sont les actions qu'un profil a le droit d'entreprendre ?
- Quels sont les protocoles de sûreté informatique à appliquer ?

Pourquoi choisir Bastion Wallix ?

Le Bastion Wallix est reconnu depuis 2013 par l'ANSSI. Une telle reconnaissance prouve l'efficacité de cette solution, qui repose sur un module Session Manager. Grâce à ce module, toutes les sessions utilisateurs sont traçables en temps réel. Il est donc possible pour une société de savoir précisément qui s'est connecté à quoi et à quel moment. Cette dernière a donc un contrôle plus poussé de ses niveaux de sécurité et peut facilement garantir l'intégrité de ses données.

Les authentifications interne et externe



NB : le bastion à l'heure d'aujourd'hui est capable d'utiliser de l'authentification local mais également celle externes et les Auth externes peuvent être Ldap, wind server, Saml, radius, Kerb…..ect

Contexte de notre travail

« WALLIX PAM est conçu pour gérer, sécuriser et auditer l'utilisation des comptes à privilèges dans les environnements IT et OT. Ces comptes, utilisés par les administrateurs ou des applications, donnent accès à des systèmes sensibles comme les serveurs Windows.

Le bastion WALLIX se concentre sur le contrôle fin des accès, la surveillance en temps réel et l'enregistrement détaillé (audit) de toutes les actions entreprises avec ces comptes. Cela permet de vérifier la conformité des configurations d'accès, de reconstituer précisément les sessions des administrateurs sur les serveurs, et ainsi de réduire les risques d'accès non autorisé, de violation de données ou de mauvaise utilisation.

WALLIX PAM renforce la cybersécurité en garantissant que tout accès aux systèmes critiques est traçable et auditable, en réduisant les menaces internes et en fournissant les preuves nécessaires à la conformité réglementaire. »

======Etape à faire pour connecter wallix à windows serveur =====

Étapes 1 : Authentification externe

- IP ou FQDN du serveur AD
- Port LDAP/LDAPS
- DistinguishedName utilisateur qui fait partie du groupe utilisateur du domaine (le mieux est de créer un compte dédié)
- Mot de passe de l'utilisateur
- DistinguishedName du contrôleur de domaine

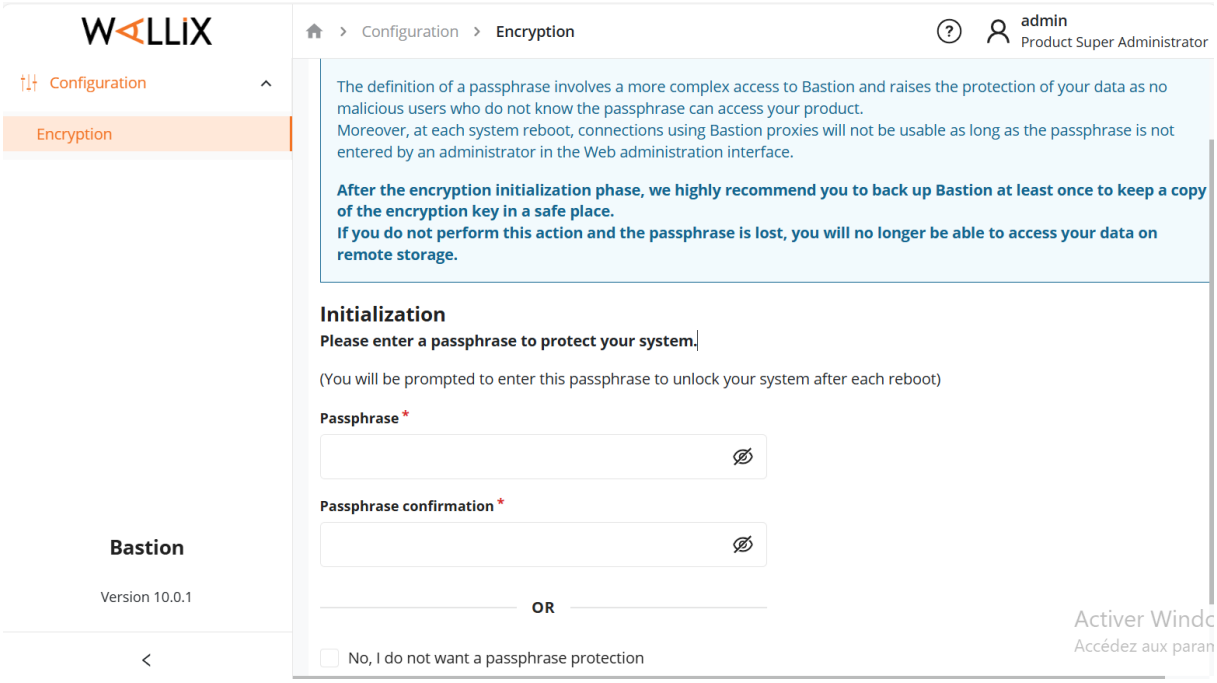
Étapes 2 : Domaine d'authentification

- Nom du domaine d'authentification
- Domaine par défaut pour les e-mails

Étapes 3 : Ajouter une correspondance

- DistinguishedName du groupe AD que l'on souhaite mapper

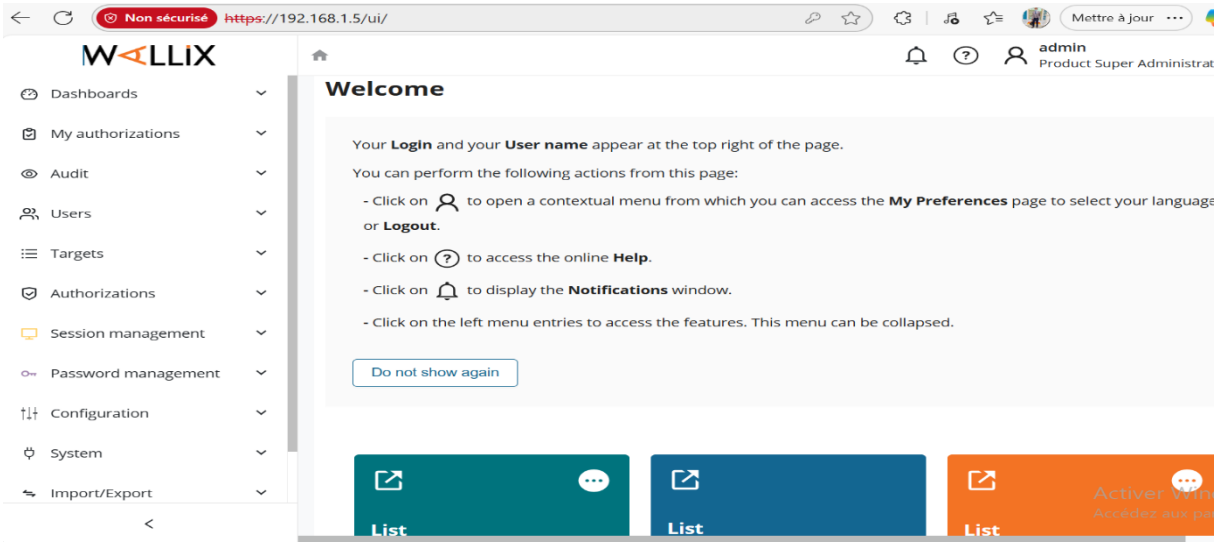
- Ici nous avons déjà installation wallix donc il ya juste les captures de connexion c'est pas difficile d'installer une machine virtuelle préconçue de wallix sur vmware voila pourquoi nous avons sauter cette partie dans nos captures mais toute fois vous pouvez toute fois faire savoir si vous avez des problèmes pour installer



NB : voici le lien pour télécharger wallix https://www.swisstransfer.com/d/c54fa541-e66b-483c-8c7d-885c29922445

Pour l'installation, il suffit juste d'importer le fichier .ova téléchargé dans l'environnement virtuel VMware Player dans notre cas. Après l'installation, les paramètres tels que le nom d'hôte, l'adresse IP, la Passerelle par défaut doivent être configurés ci-dessous quelques captures illustrant cette étape. L'Appliance est configuré par défaut avec le compte « **wabadmin** », mot de passe « **SecureWabAdmin** ». Puis dans vos configs vous allez changer ce mot de mot est modifié lors de la configuration initiale.

- Nous nous sommes connectés avec l'utilisateur admin que nous avons changer le mot de passe à la 1ère connexion

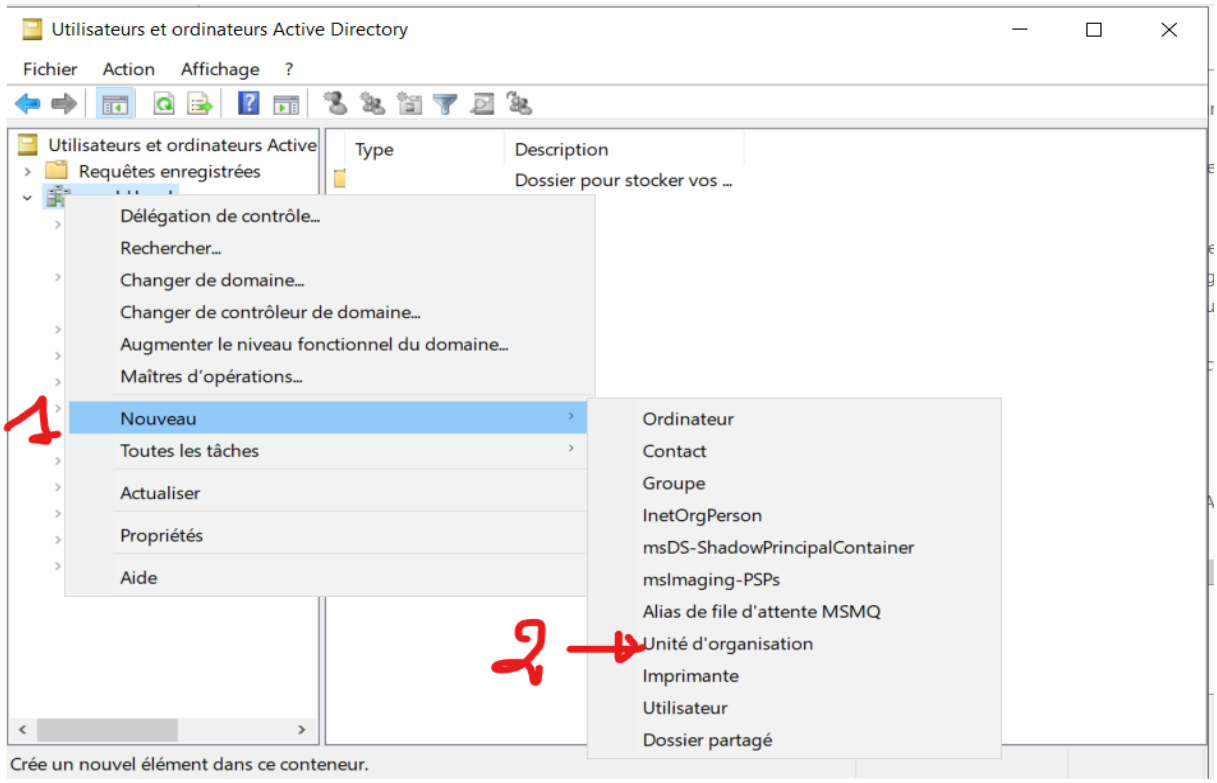


Rappel : dans les config de wallix nous avons eu à fixer l'adresse manuellement à 192.168.1.5 et la machine windows serveur est à 192.168.1.10 donc les deux machines sont dans le même réseau.

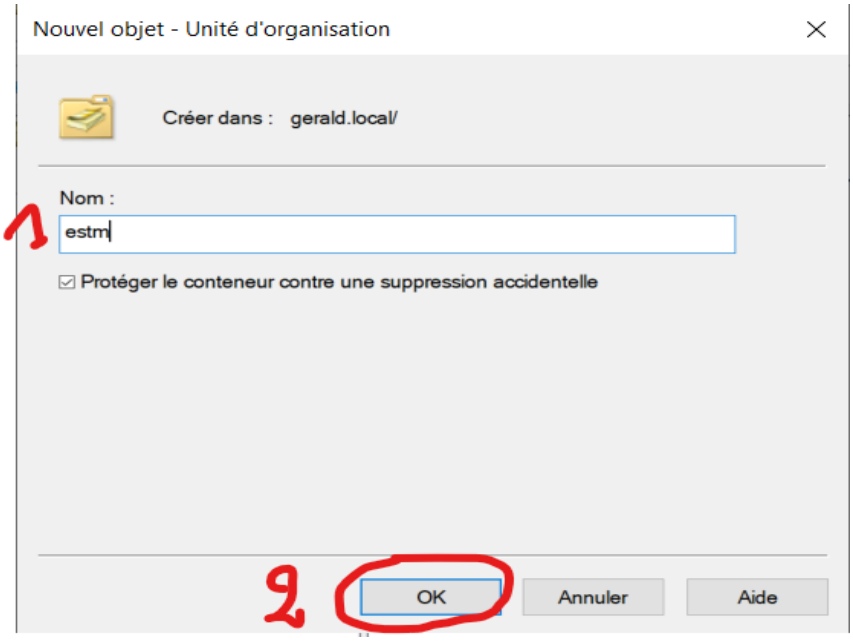
- Travail à faire sur votre windows serveur déjà operationnel je suppose

1- Après la creation de votre controleur de domaine dans mon cas : gerald.local
2- Crée une unité d'organisation dans mon cas : estm
3- Crée un groupe dans cette unité d'organisation nommé dans mon cas :groupe1
4- Puis à l'interieur du groupe1 crée deux user : alice et bob puis un autre user à l'exterieur nommé : toto
5-

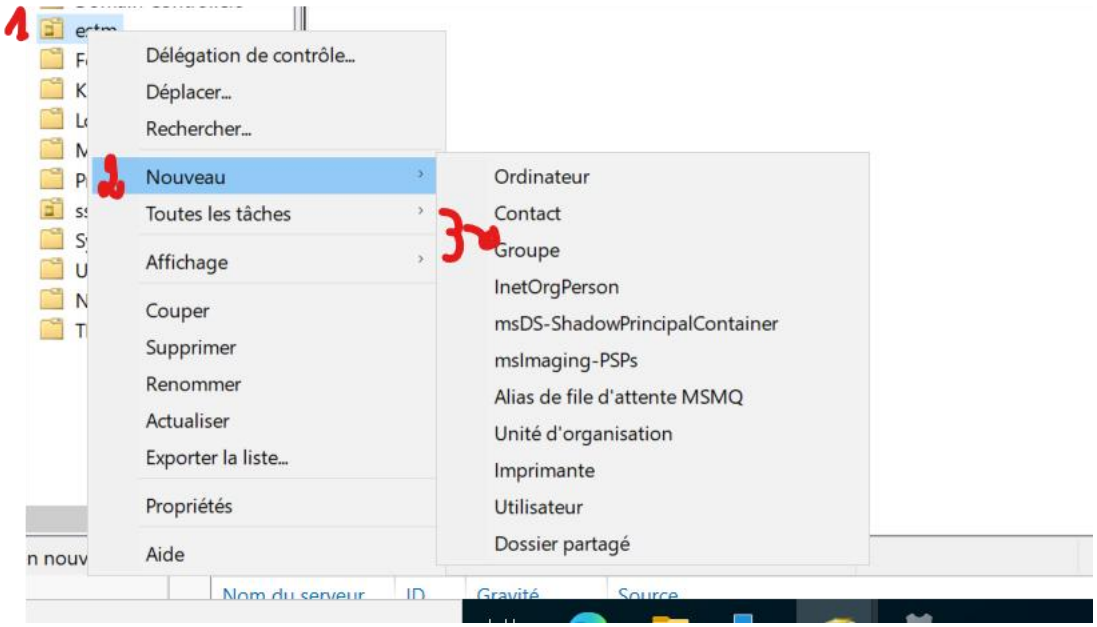
- clique droit sur le domaine **gerald.local** puis suivre la numerotation



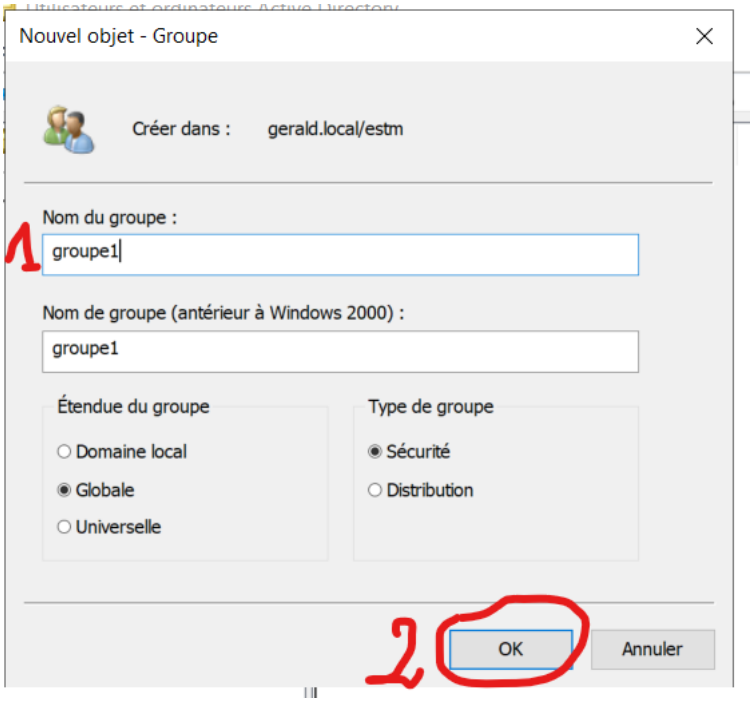
- Voici le nom de l'unité d'organisation



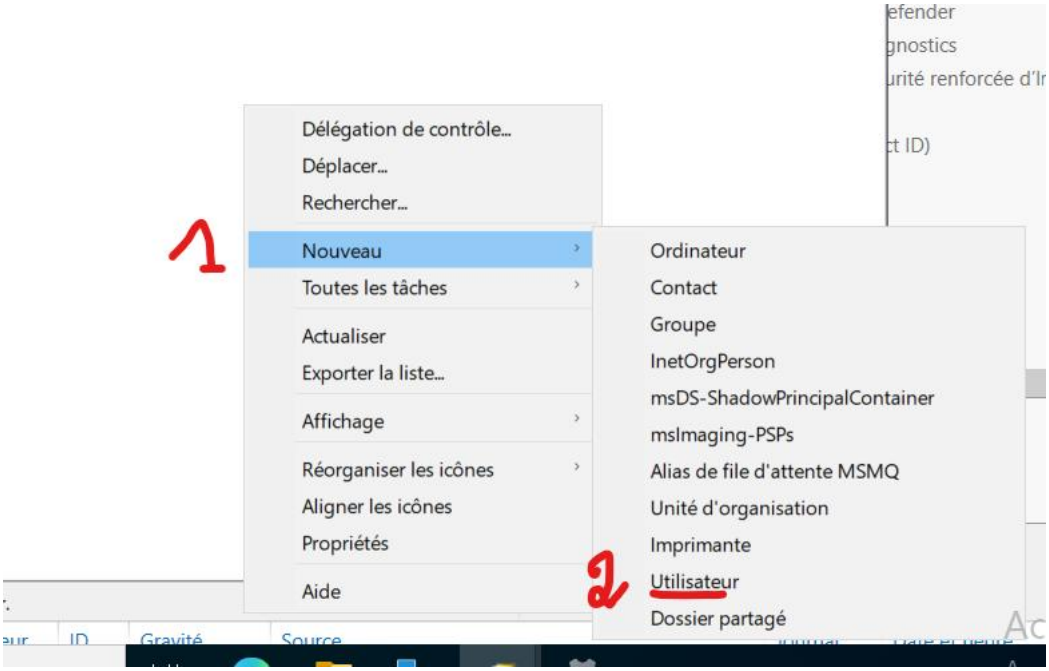
- Création du groupe dans cette u.o



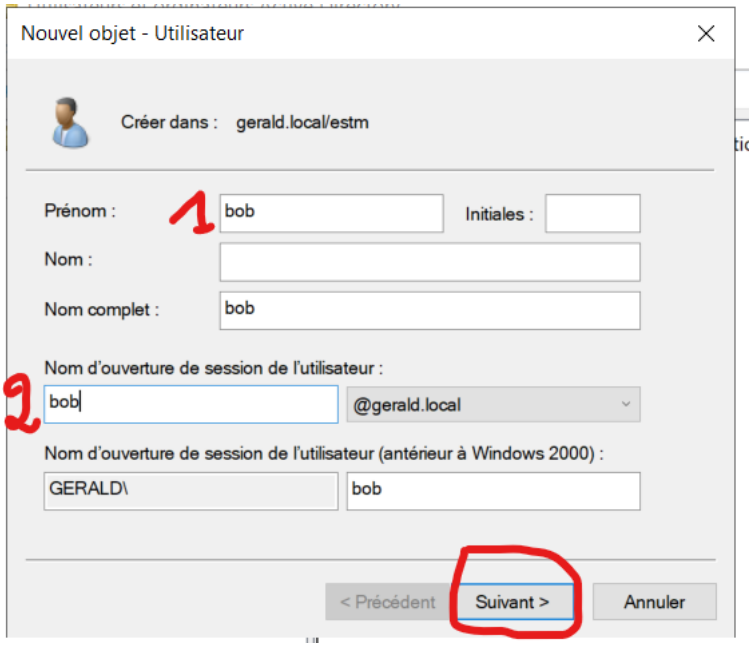
- Nommé ce groupe : groupe1



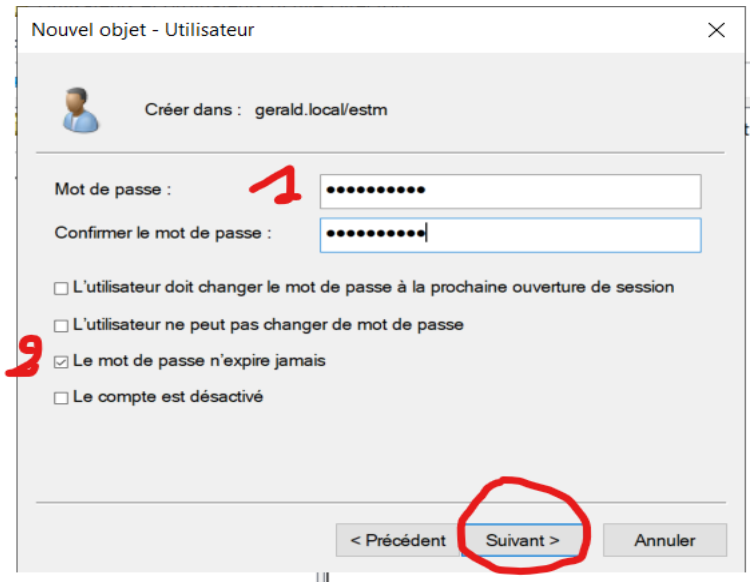
- Création des utilisateurs



- User bob

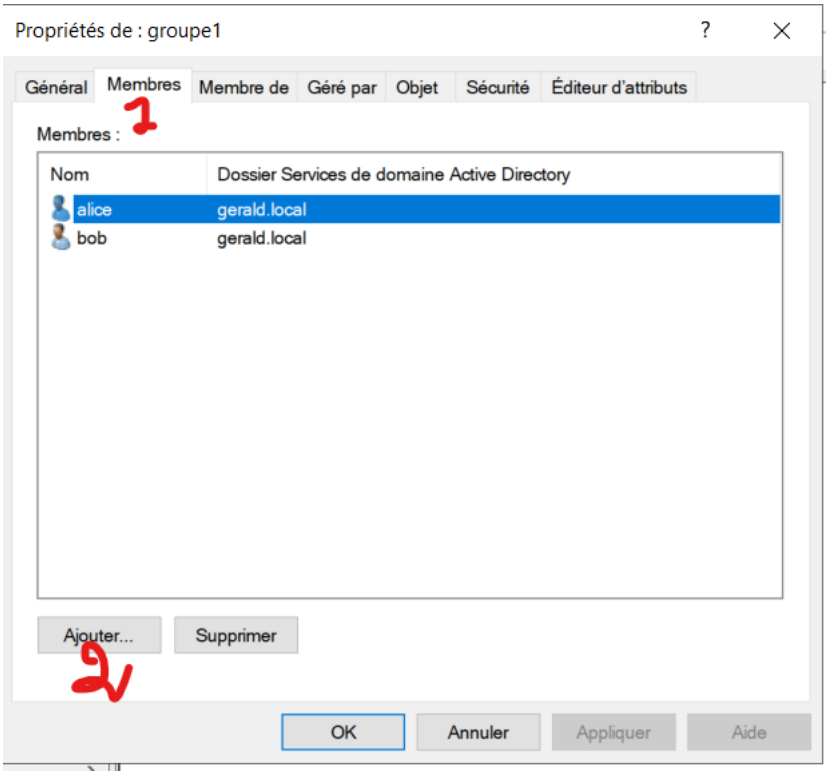


- Son mot de passe

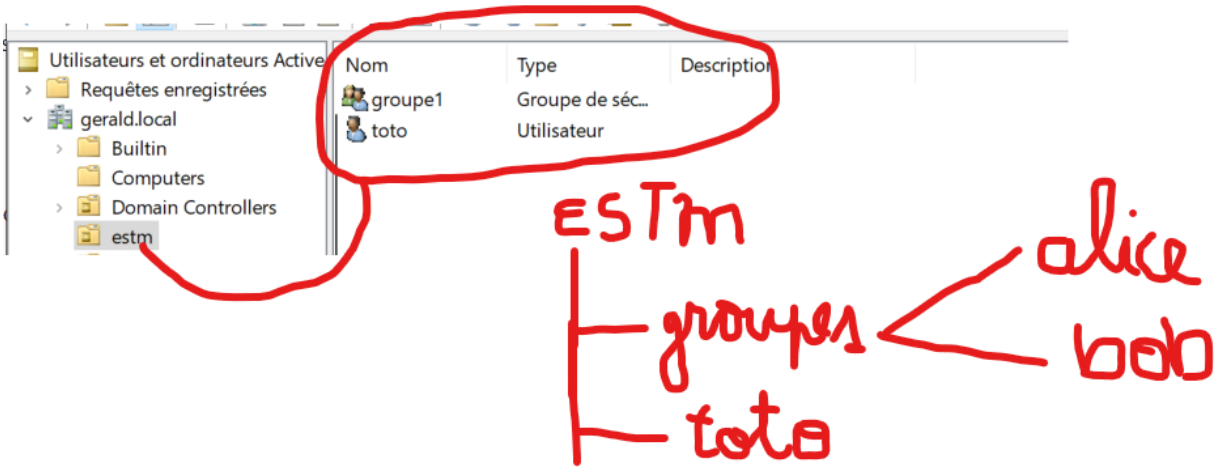


NB : Faire la même chose pour le user alice et aussi toto

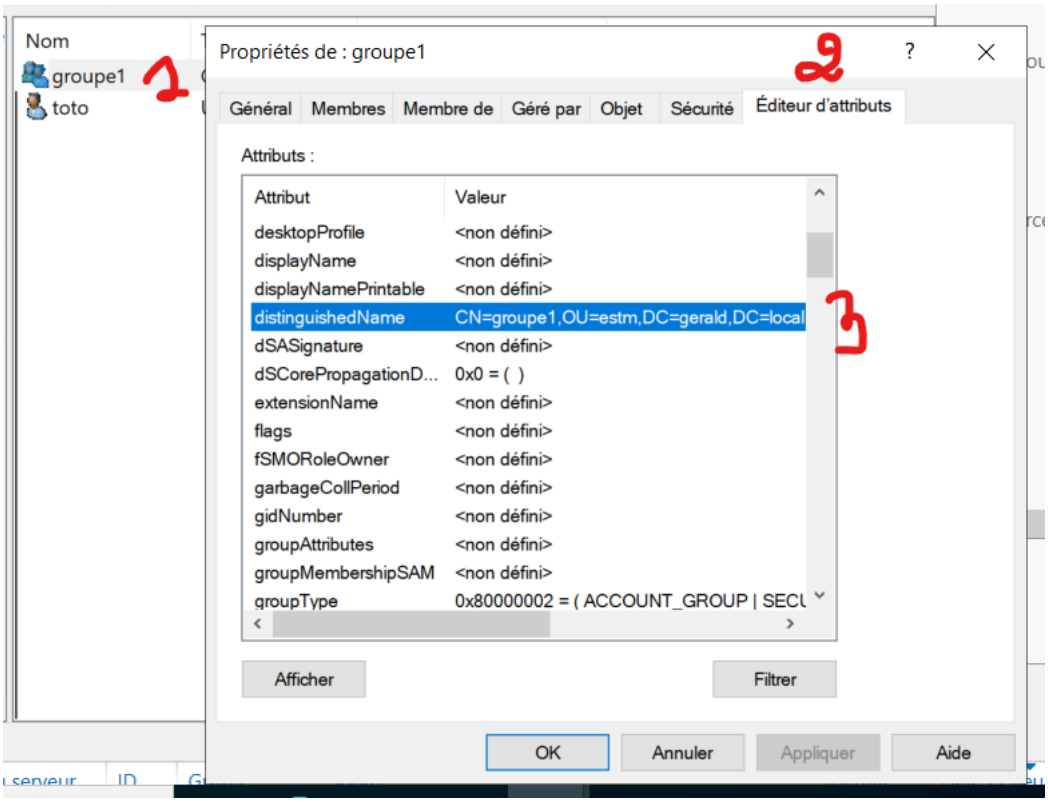
- Puis ajouter les user alice et bob dans le groupe1



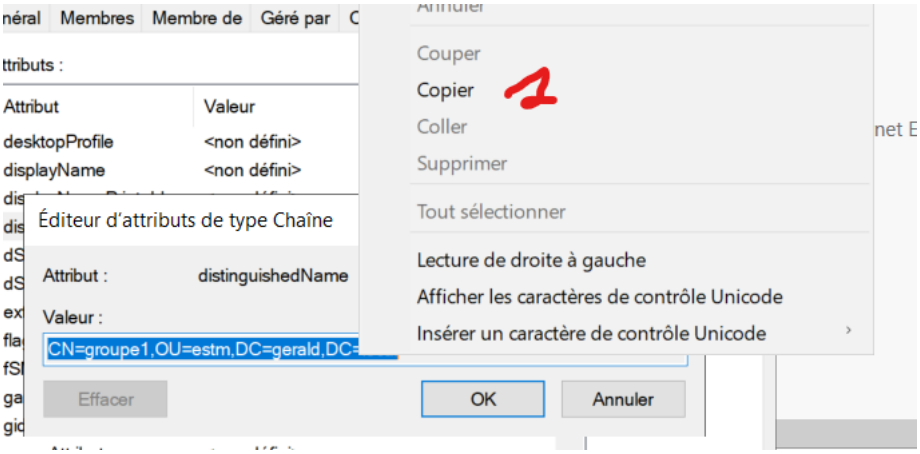
- Voici comment cela va se presenter



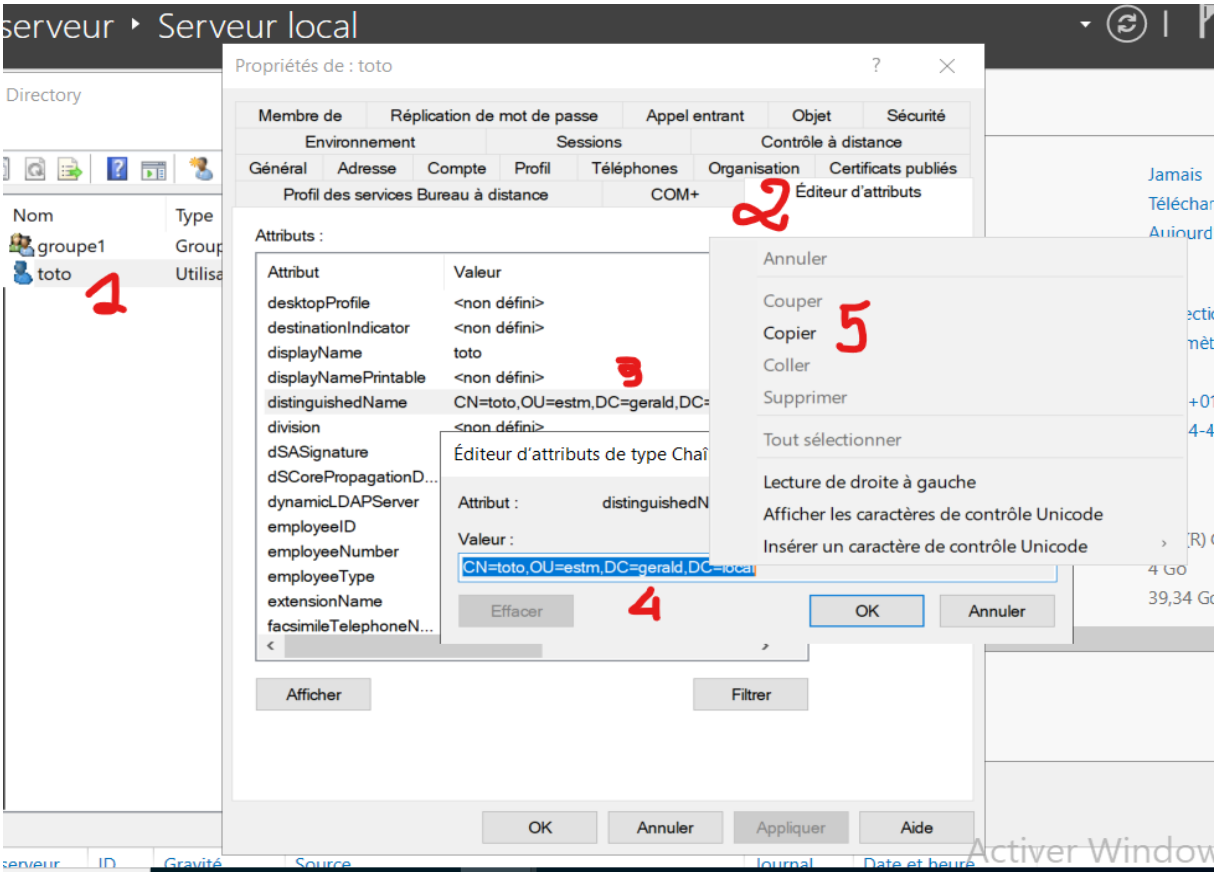
- Nous allons également se service du distinguisheName des utilisateurs toto et du groupe1 dans wallix voila comment copier cela



- Puis cliqué 2 fois sur ça et enfin copier, vous les utiliserais dans wallix donc nécessité vous oblige de connaitre comment le copier pour ne pas l'écrire aux risques des erreurs.

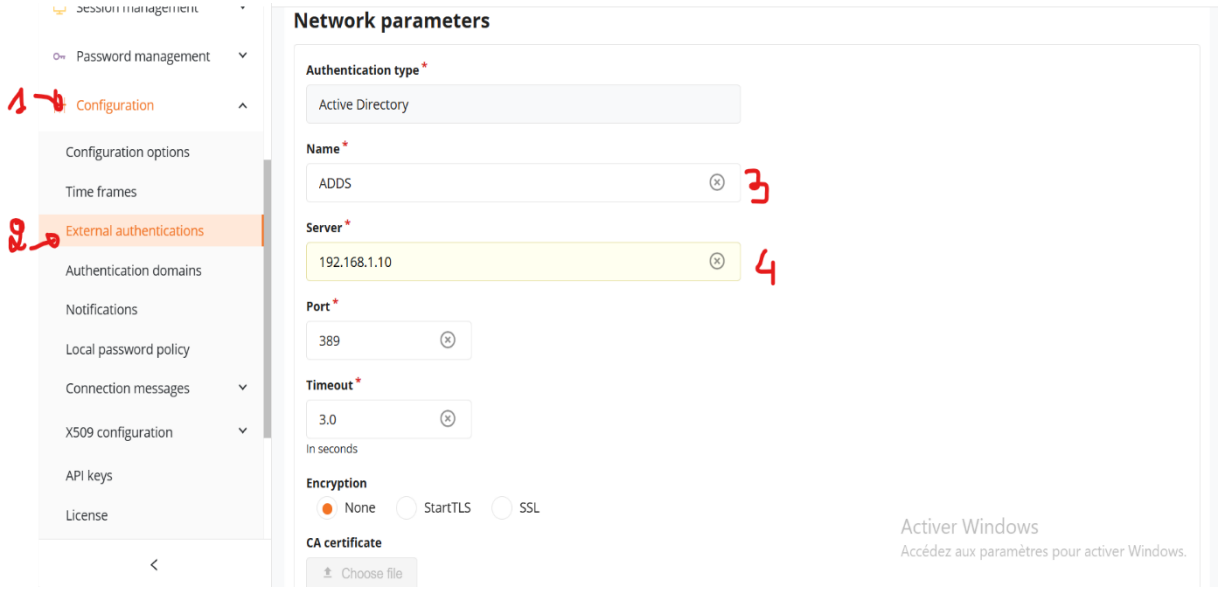


- Faire de même pour le distinguishedName de toto

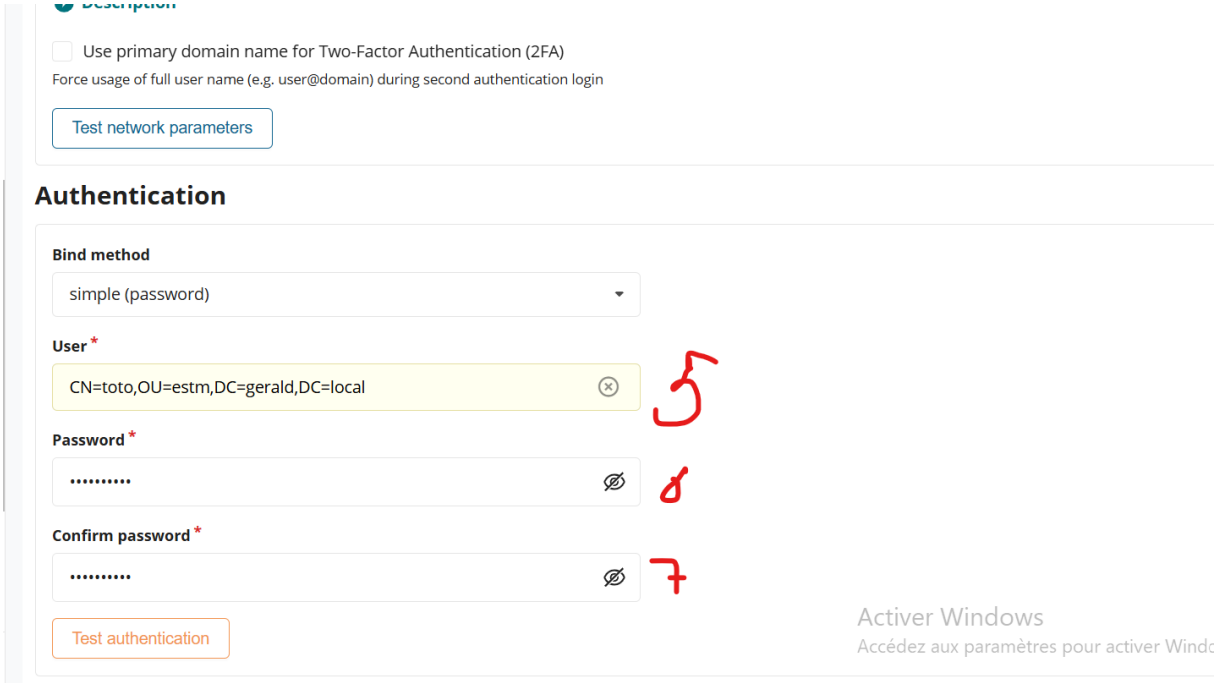


NB : ses distinguishedName permettent de

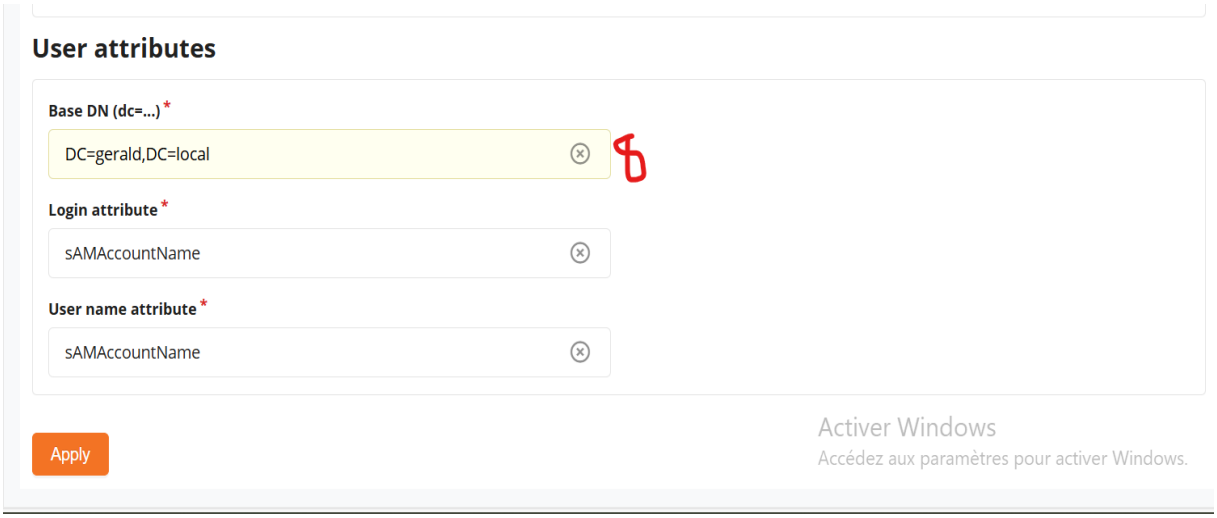
- Retournons dans Wallix, pour les différentes configurations. Dans l'onglet **Configuration** puis **Authentification externes** cliquer sur **Ajouter** puis choisir **Active Directory et dans cette authentification Active directory** renseigné toutes ses informations



- La suite en mettons ses renseignement n'oubliez pas de tester l'authentification



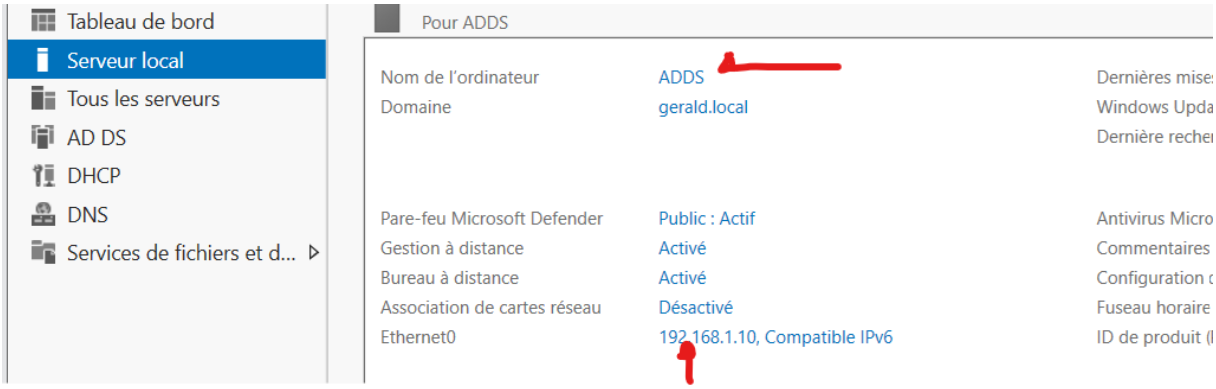
- et enfin



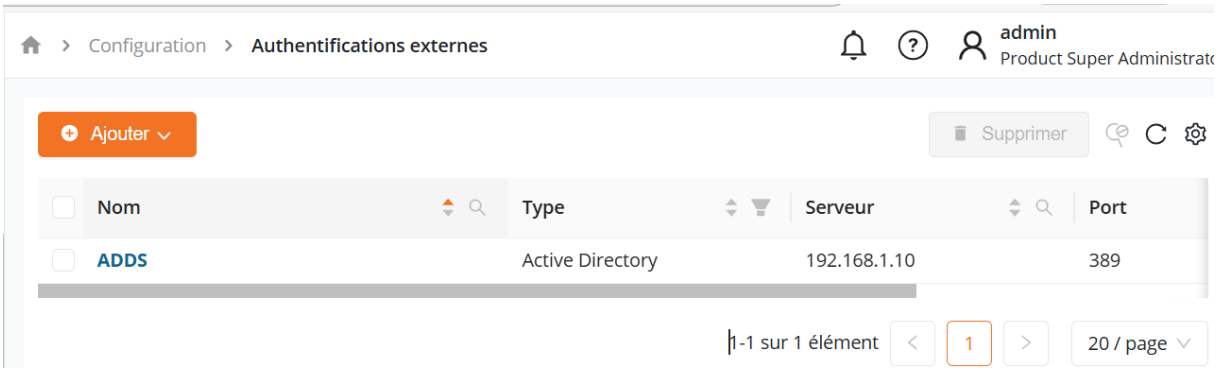
NB : toutes ses informations que nous avons rentrées doivent être configuré depuis windows serveur.

On retient ici que ADDS c'est le nom de machine Windows serveur l'adresse IP windows serv, le port c'est par défaut vous pouvez changer cela ensuite testé la connexion là ou s'est écrit test network parameters pour savoir si wallix et wind serv (le contrôleur de domaine) match bien. Dans le champ user, entré le distinguishedName du user toto comme en le copiant depuis wind serveur et le coller dans wallix au champ user et mettre le mot de passe de toto lors de sa création. Après que tout passe alors Appliqué

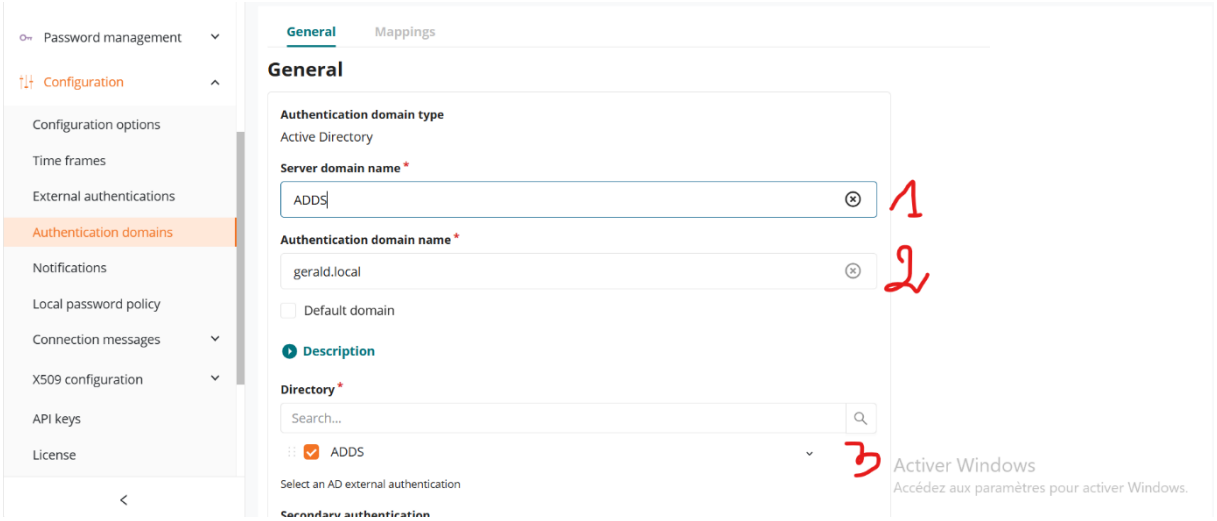
==== Pour le ADDS c'est le nom de l'ordi ou se trouve le serveur



- voici ce que ça donne



- Toujours dans l'onglet **Configuration** on vient maintenant dans **Domaine d'authentification** pour dire à notre bastion wallix que nos utilisateurs ont la possibilité de venir s'authentifier sur cette authentification externe. Donc cliquer sur Ajouter puis choisir **Active Directory** et dans cette authentification Active directory renseigné toutes ses informations suivantes

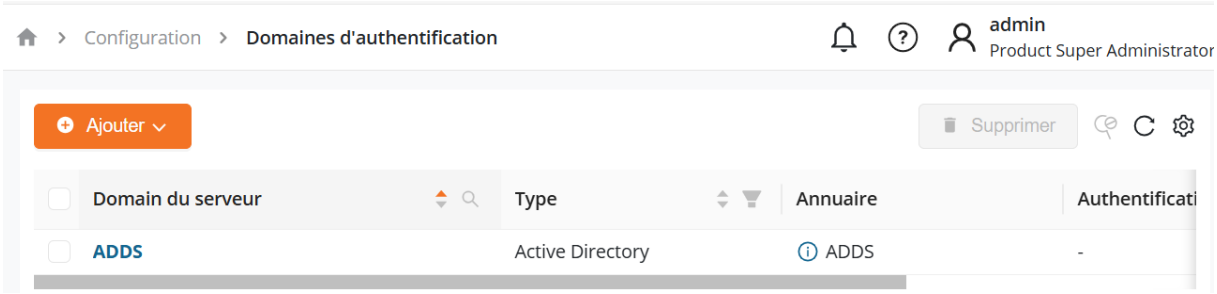


NB : ADDS, non du serveur

gerald.local = c'est le nom de mon contrôleur de domaine Active directory

- la suite

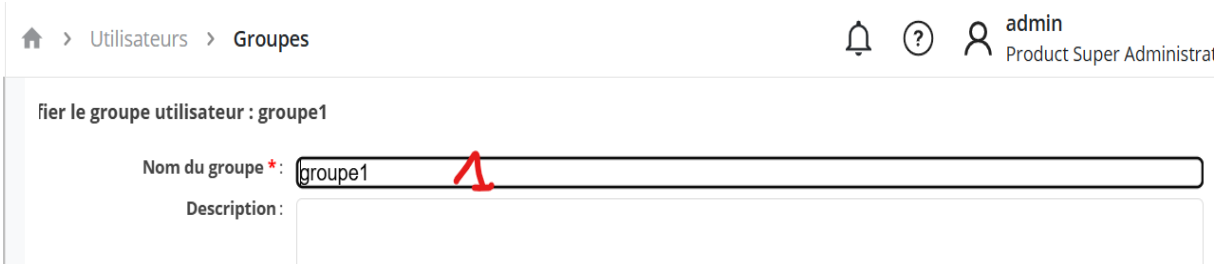
- Voilà comment cela se présente



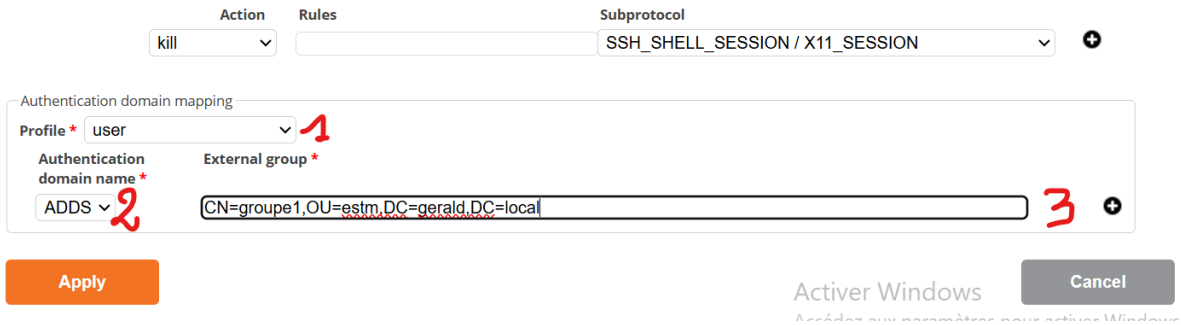
====== Une fois que nous avons crée une authentification externe et avons défini un domaine à cette authentification externe alors nous devons maintenant lui crée les users qui viendront s'authentifie dans ce domaine d'authent. Et ses user sont ceux qui sont dans active directoty que je dois pouvoir les remontés dans bastion. Et dans notre cas c'est les users (alice et bob) se trouant dans le groupe1 que je dois remonté dans bastion

- Allons dans groupe **Utilisateurs** puis **Groupes** cliqué sur **Ajouter un groupe**

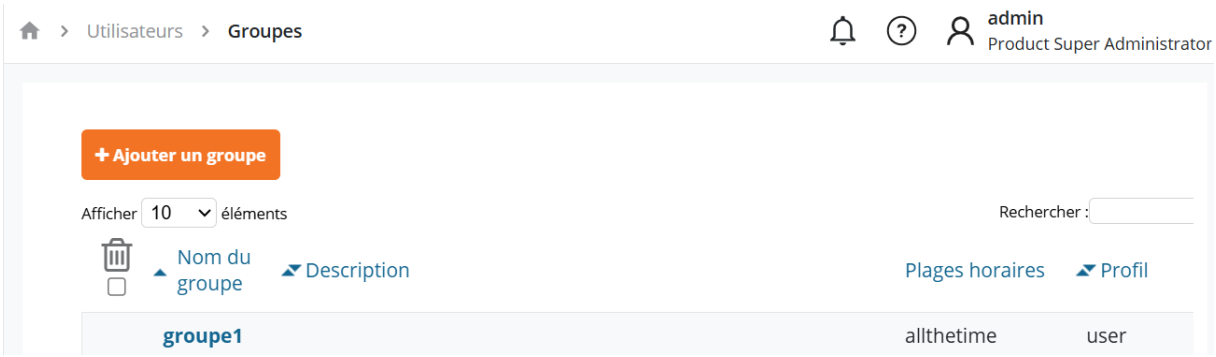
Puis rentré ses informations



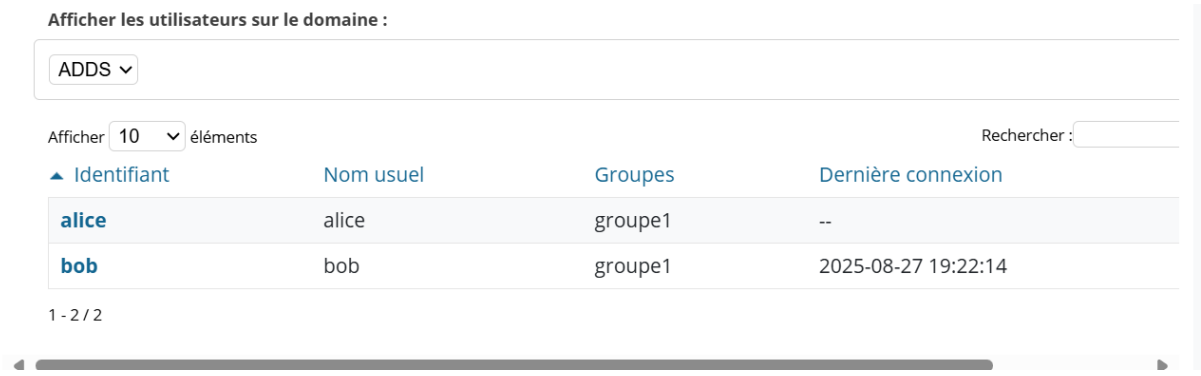
- En suite en bas de la même page choisir le profil **user** , mettez le distinguesheName du groupe 1 que vous irez prendre dans wind serveur puis appliqué



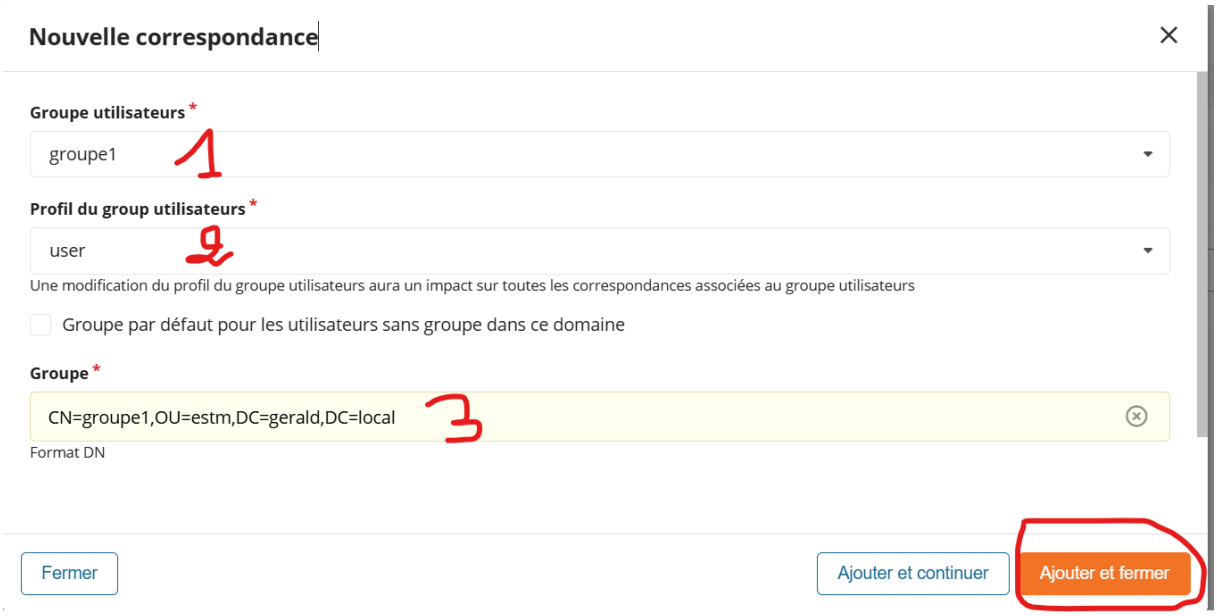
- Voici cela



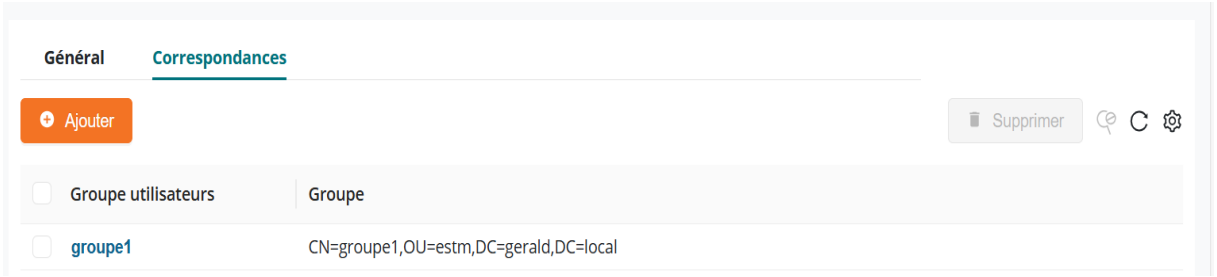
- Et dans **Utilisateurs** puis **Comptes** basculé de local à ADDS(le nom de votre machine wind serveur alors vous verrez automatique les users qui sont dans le groupe 1 (alice et bob) apparaitront



Dans le cas ou cela ne passe pas alors verifier des configurations au niveau de : **Configuration**, puis dans **Domaines D'authentification** allez dans la partie **correspondances** puis cliqué sur **Ajouter**

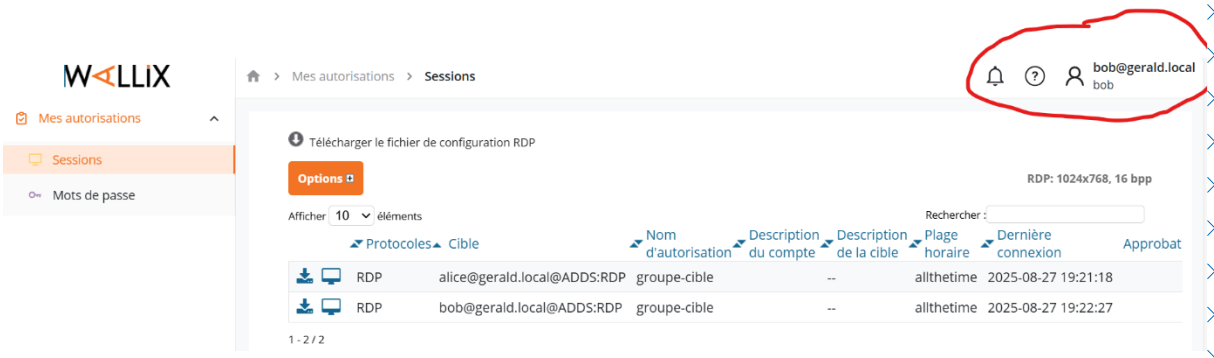


- Et on aura ceci puis allez voir si vos users (bob et alice) sont remontés



- Là je peux me connecté avec l'un des user soit bob ou alice pour voir si réellement wallix permet à ses user qui lui ont été remonté de se connecter

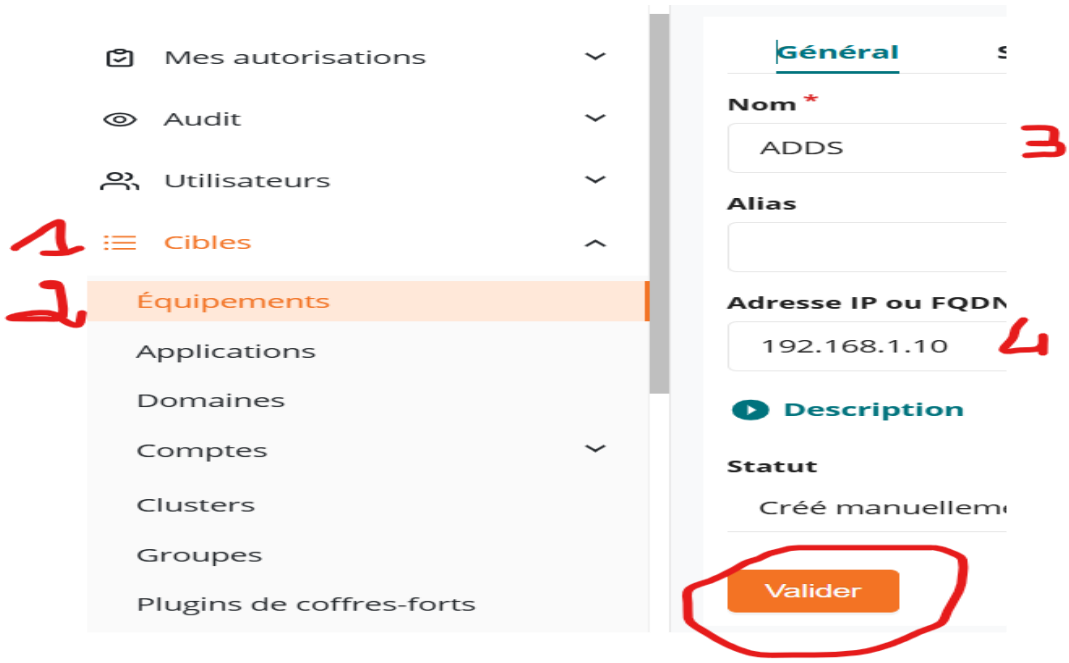
- Et bam on voit bien que le user bob c'est connecté au domaine gerald.local de mon contrôleur de domaine



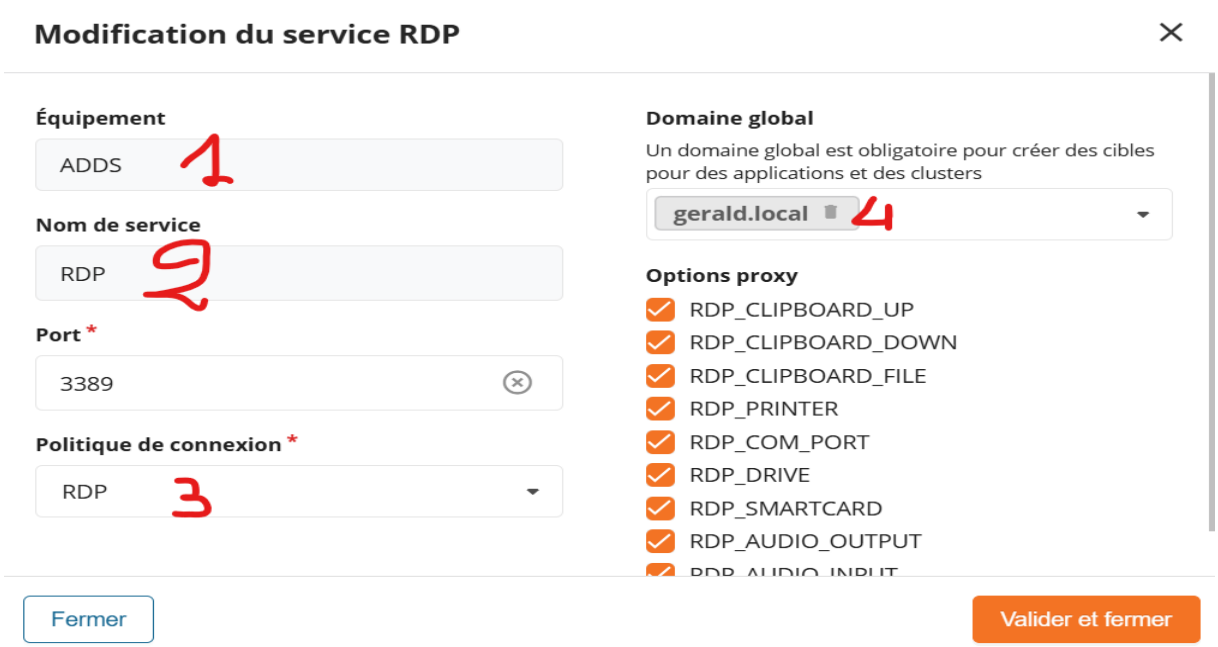
======== Ici les étapes que nous allons faire pour atteindre nos objectifs sont les suivantes :

- **Étapes 1 : Ajouter les cibles**
    - IP de la cible
    - Définir le service (RDP, SSH, VNC, RAWTCP, TELNET, RLOGIN)
- **Étapes 2 : Ajouter les targets accounts**
    - Login et mot de passe du compte cible
    - Choisir entre compte local ou global
- **Étapes 3 : Définir qui a le droit à quoi et comment**
- **Étapes 4 : Créer un groupe utilisateur**
- **Étapes 5 : Créer un groupe de cible**

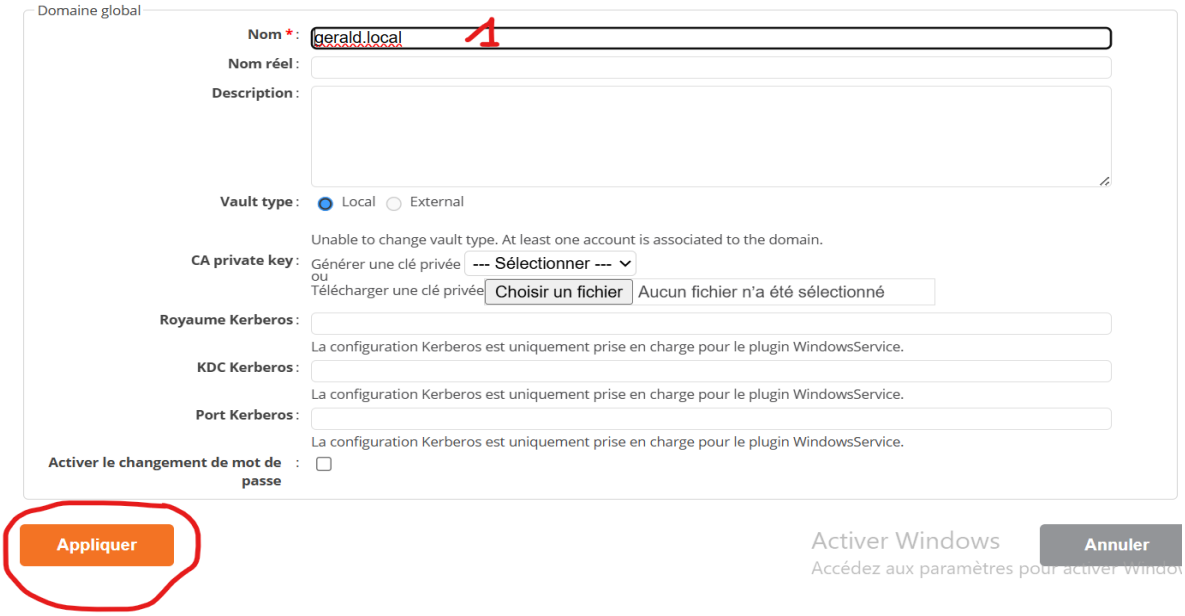
- Dans **Cibles** puis **Equipement** puis **Ajouter** et dans la partie **générale faite** rentrer ses infos



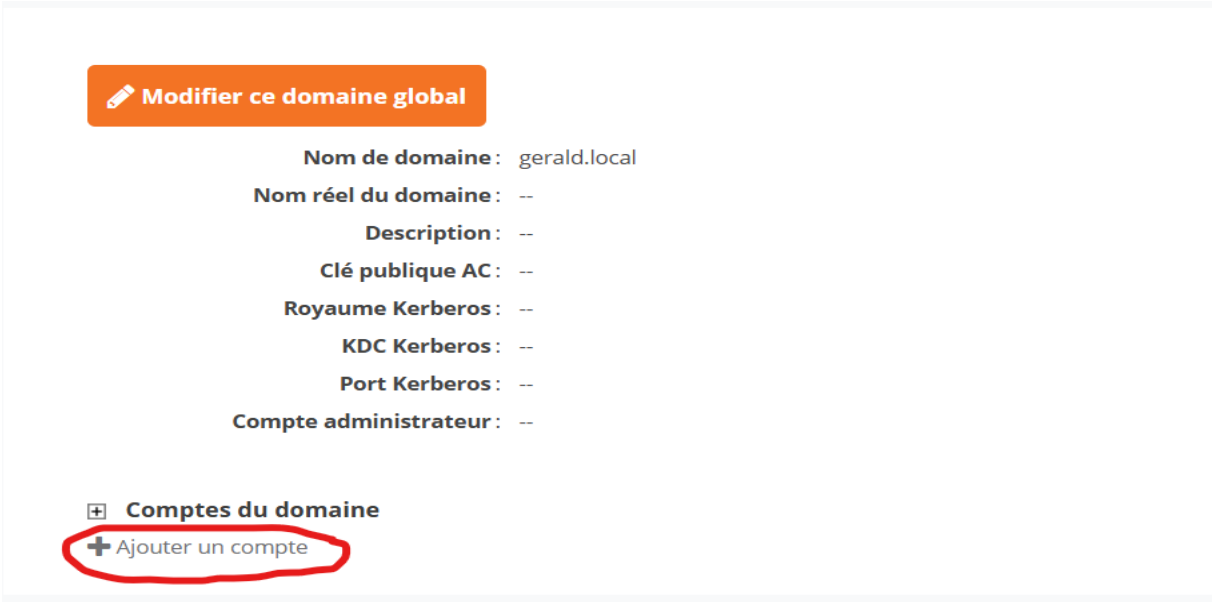
- Sur la même page dans la partie **services,** cliqué sur **Ajouter** pour choisir le protocole RDP ensuite remplir d'autre information



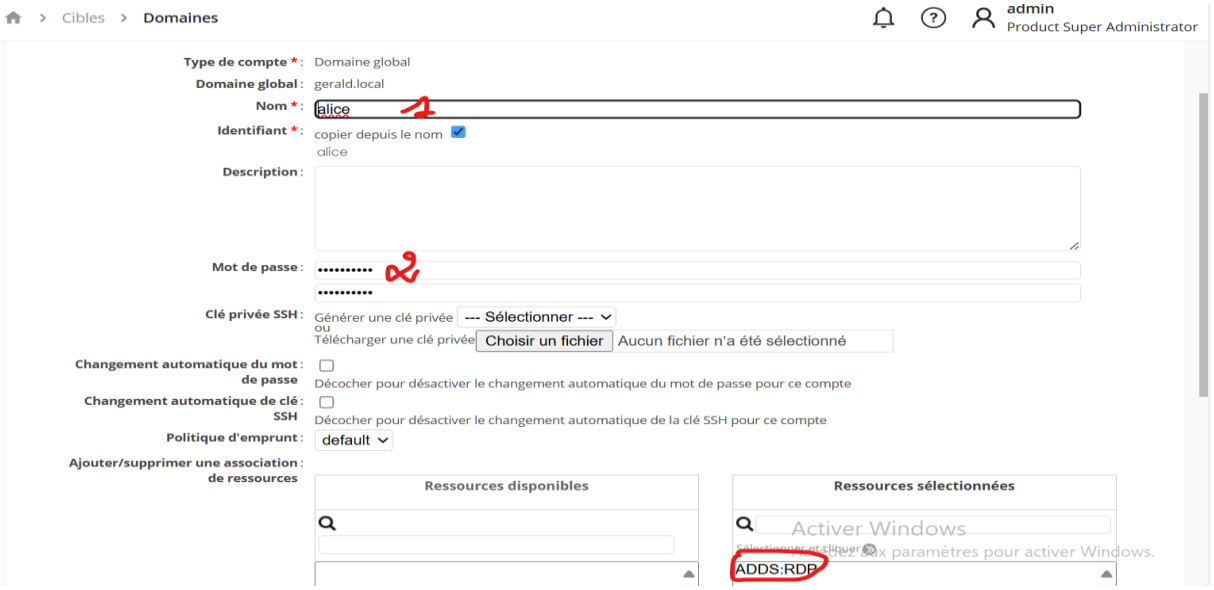
- Dans le même alignement dans la partie **Comptes locaux** on peut ajouter des comptes globaux ou une autre approche est d'allé dans l'onglet cible puis **comptes** puis **comptes globaux** . Mais bien avant cela créons tout d'abord le domaine
    - Dans mon cas je l'avais déjà créé voici comment procédé, allez dans **cibles** puis **domaines (**c'est le contrôleur de mon domaine wind serveur**),** cliqué sur **Ajouter un domaine global**



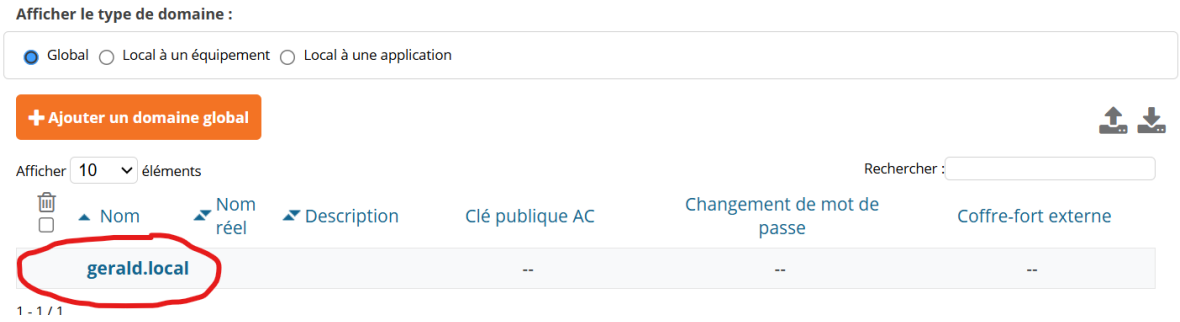
- Et juste après en bas cliqué sur **Ajouter un compte**



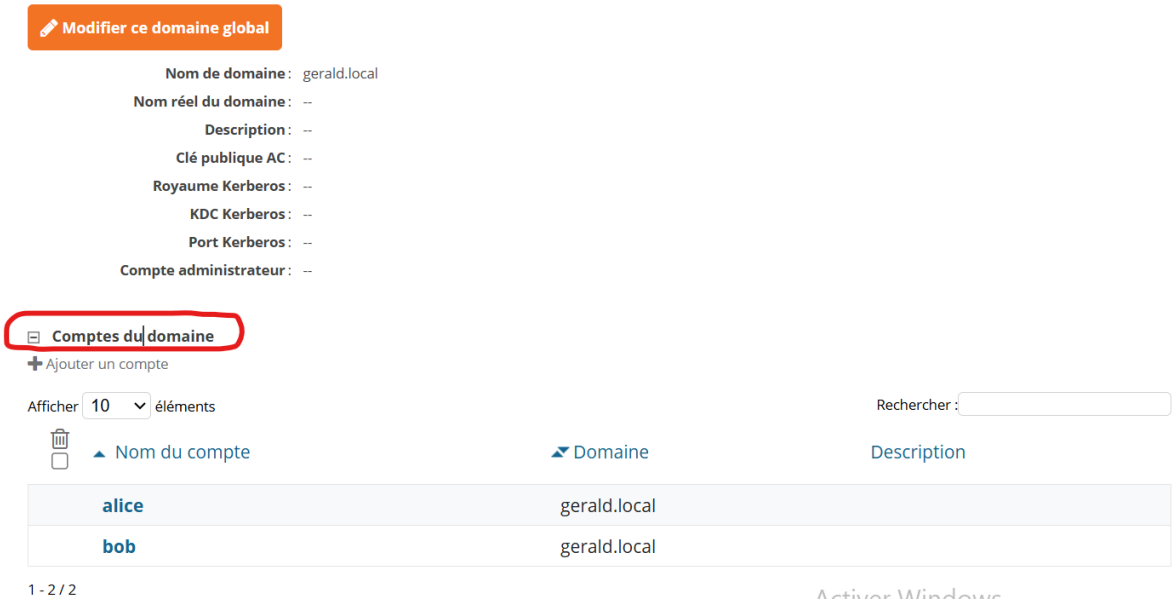
- Puis ajouter **alice** et appliqué à la suite faite la même chose pour **bob**



- À la fin nous aurons ceci



- Et si vous cliqué sur **gerald.com** cela vous conduira à cette capture et vous pouvez aussi cliquer sur Comptes du domaine et vous verrez vos deux users

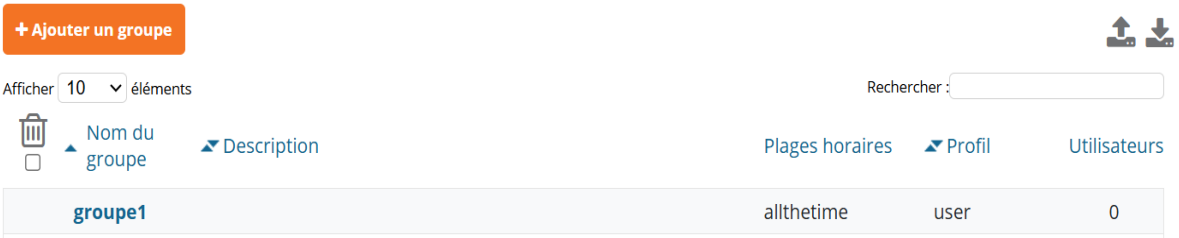


- Retournons maintenant sur nos comptes globaux pour associé nos équipements et services RDP aux deux comptes. Et suivant le même alignement mettez aussi le mot de passe de chaque user et répété le processus pour alice et bob

NB : partout nous devons avoir les mêmes mots de passe pour ses users externes (bob et alice)

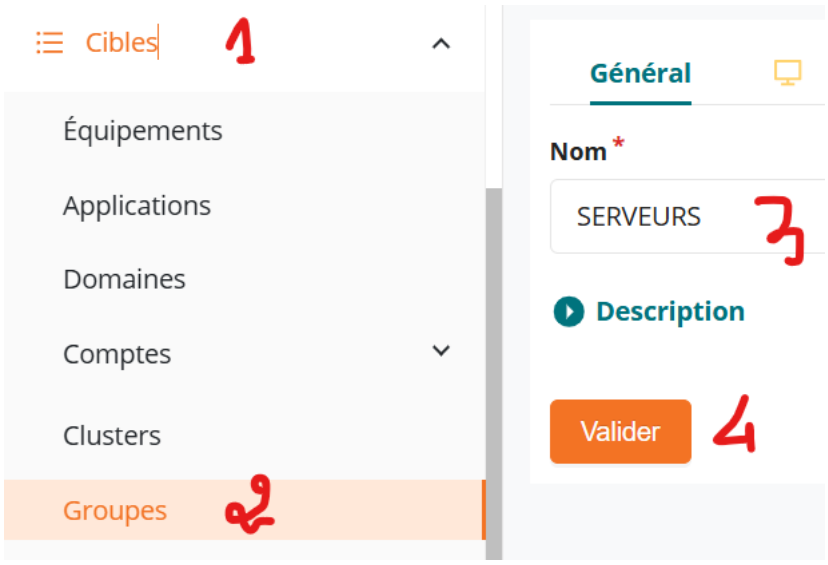
- Créons un utilisateur de groupre dans **Utilisateurs** puis dans **Groupes**

Dans notre cas nous l'avons déjà fait et on l'avait attaché aux distinguishedName du groupe1 de Wind serveur. Vous pouvez revoir tout haut et voir comment nous avons crée cela pour ensuite le crée si c'est pas encore fait



- Dans **Cibles** puis **Groupes** puis **Ajouter**

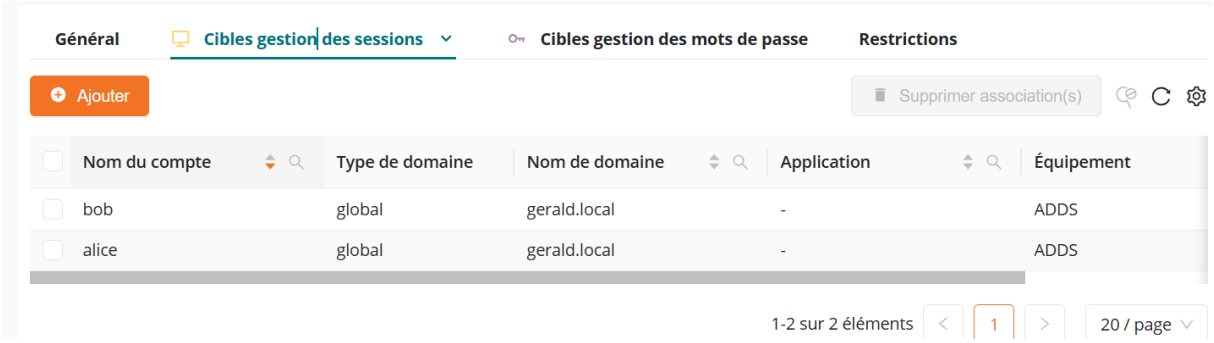
Dans la partie Général mettez le nom : SERVEURS (vous pouvez mettre ce que vs voullez) puis validez et la la partie cibles gestion des sessions déroulé et choisissez **compte** puis **Ajouter**



- Sur la même page dans la partie **Cibles de gestion de sessions déroulé** puis cliqué sur **Compte** après sur **Ajouter**

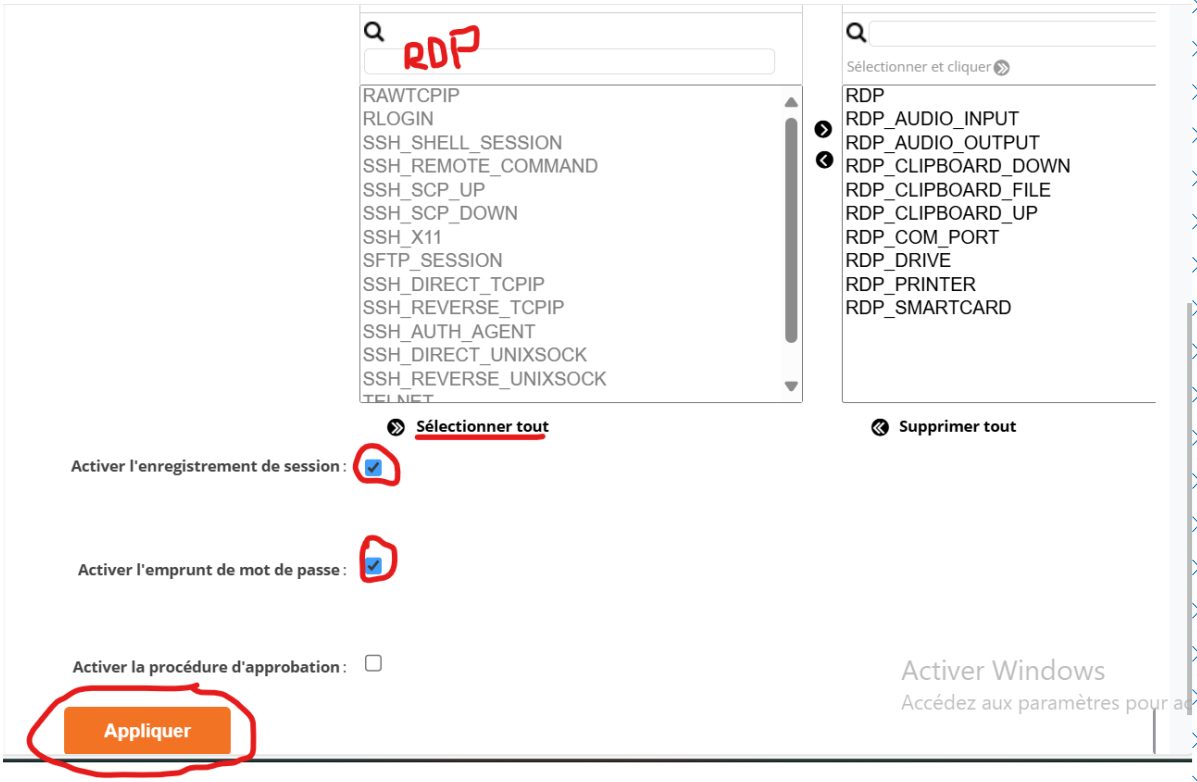
- Ensuite en bas nous aurons ceci puis **ajouter et fermer**

- Le resultat final donne ça



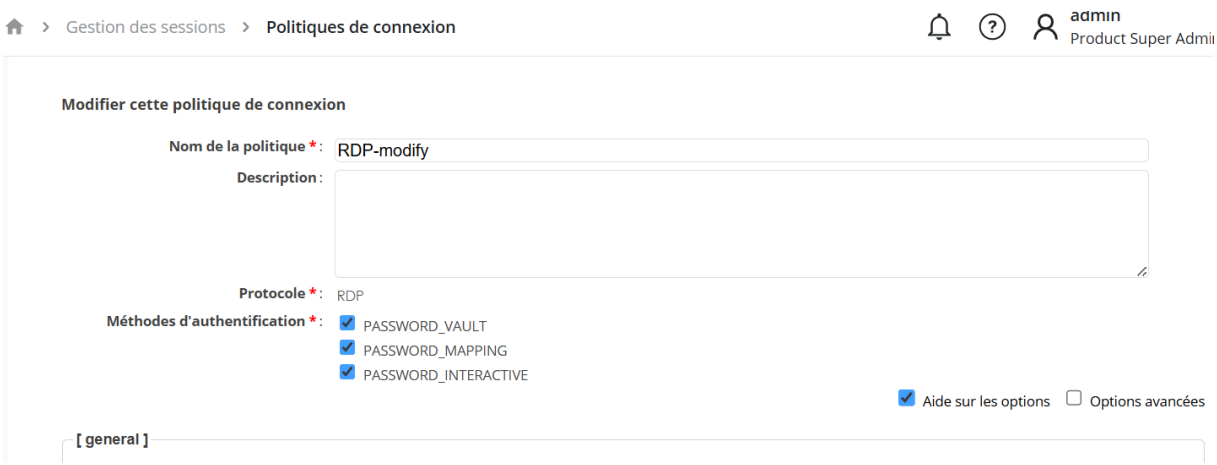
- Donnons les autorisations au groupe 1

===== sur la même page mettez à la barre de recherche RDP puis appuyer sur sélectionner tout vs aurez ce qui est dans la capture

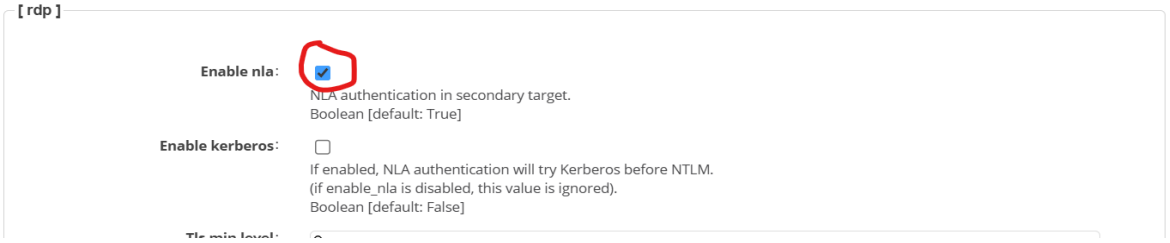


- Comme en à pas mis en place le kerberos pour pour la gestion des accès alors nous devons allez activer le NLA NTLM fallback qui nous permettra de se connecté en utilisant le NTLM donc au niveau de Gestion des sessions puis Politique de connexion et là vous verrez beaucoup de politique déjà établit alors pour aller vite dupliquée la politique RDP

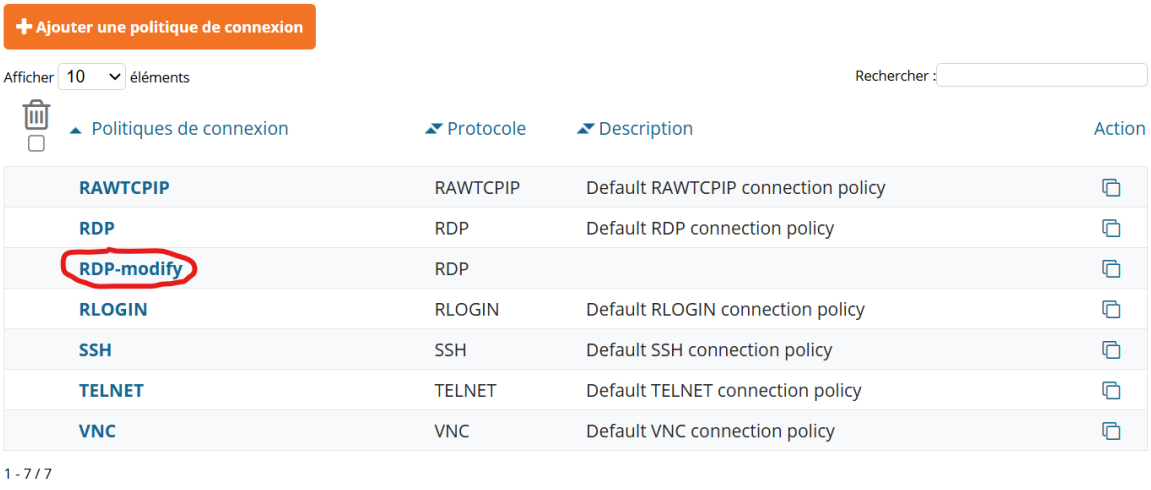
- une fois dupliqué alors cela vous conduira à une cette page puis rentré le nom et coché le



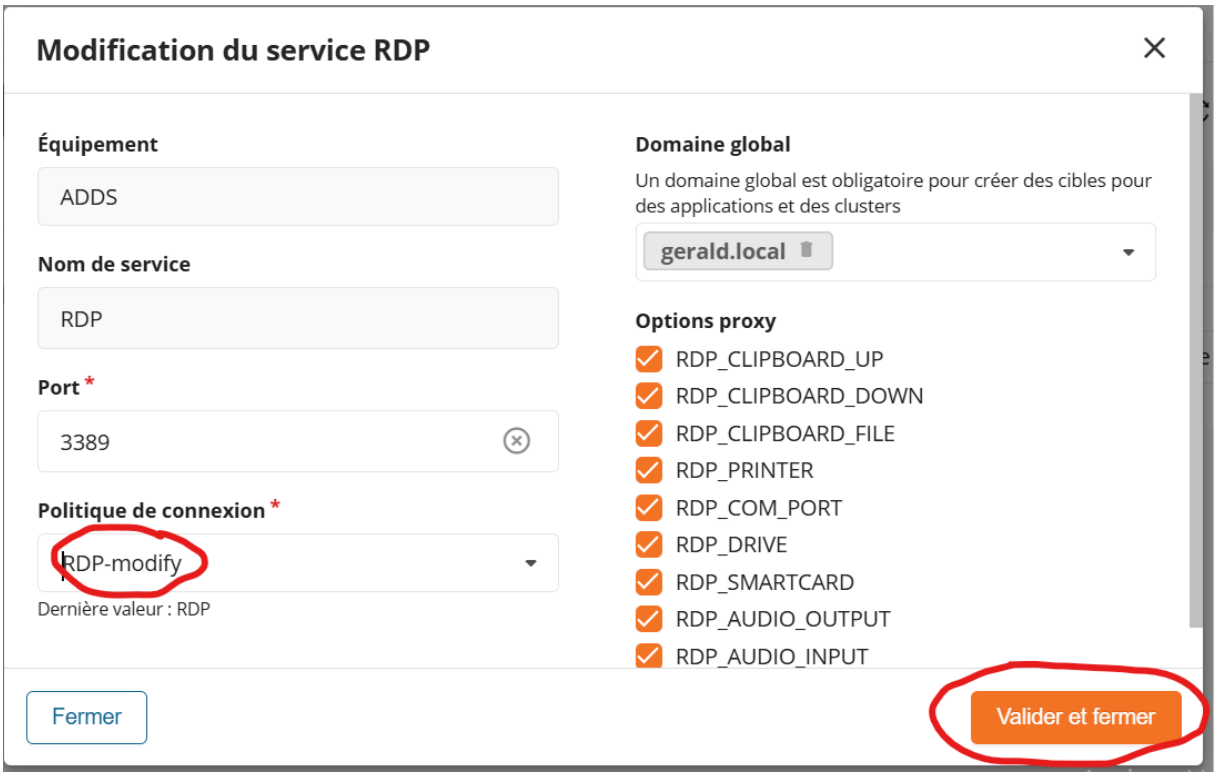
- Puis en bas de la page coché et appliqué



- Voila comment la nouvelle politique se présentera

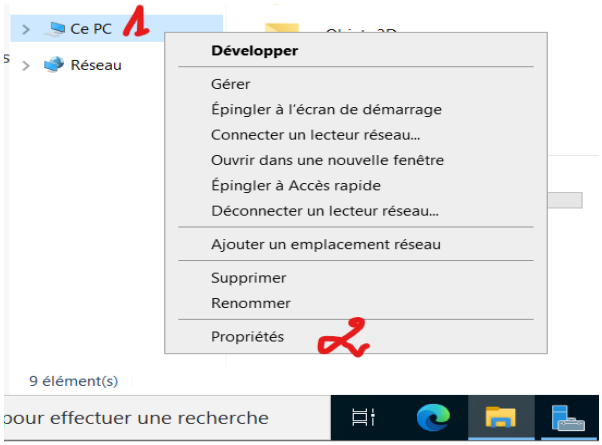


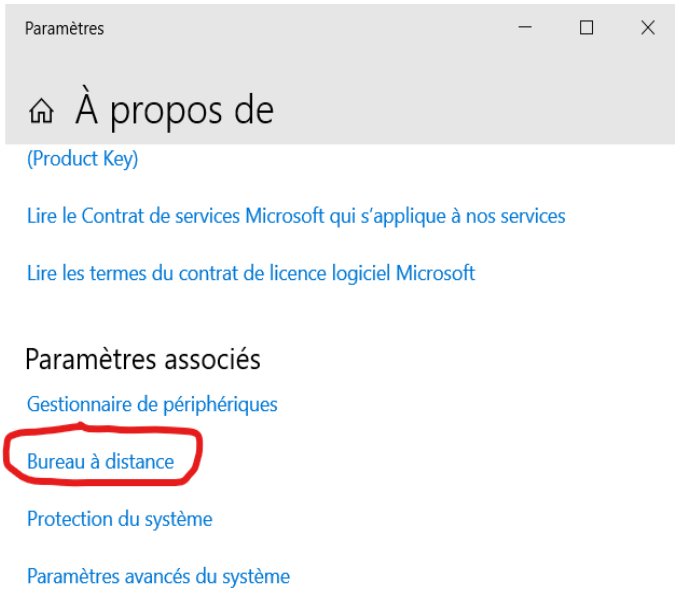
- Il faut maintenant associer ette politique à l'équipement pour cela aller dans **cibles** puis **Equipement** puis **services** cliqué sur RDP puis choisir **RDP-modify** et valider

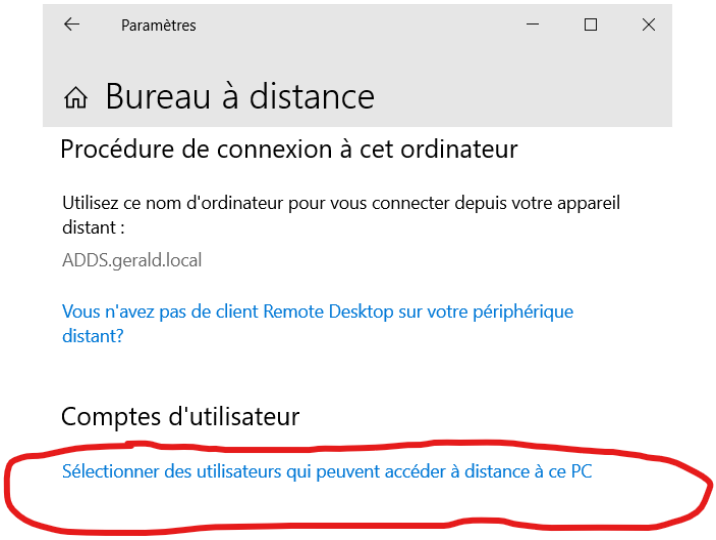


====== Testant pour voir si nos user externes remontés dans wallix se connecte à distante sur wind server et que dans Wallix on peut tracer les connexions et voir qui s'est connecté et à quelle heure

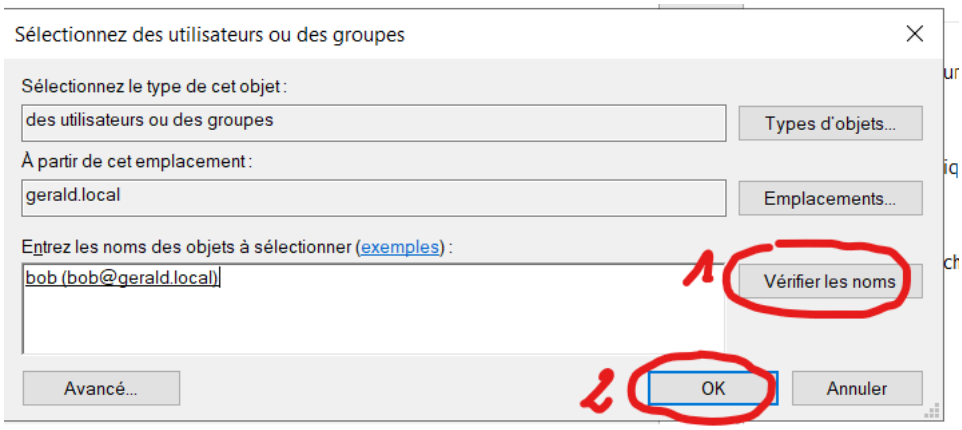
- Pour ce faire sur une autre machine tapons à la barre de recherche **Bureau à distance** mais bien avant nous devons configurer le bureau à distance dans notre Windows serveur



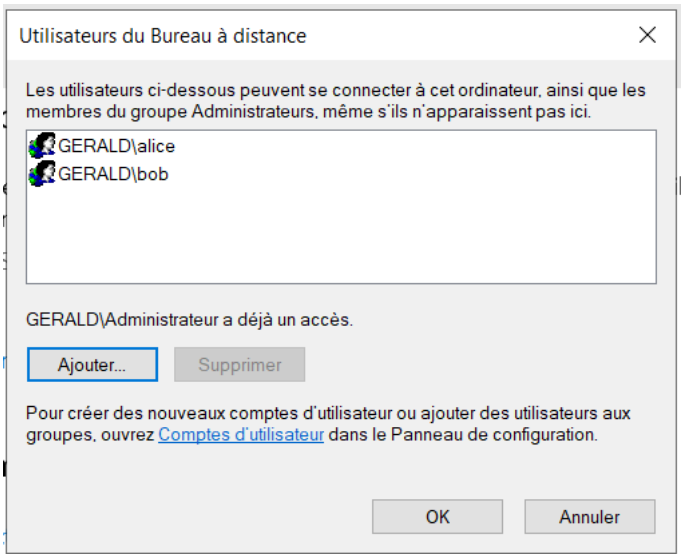




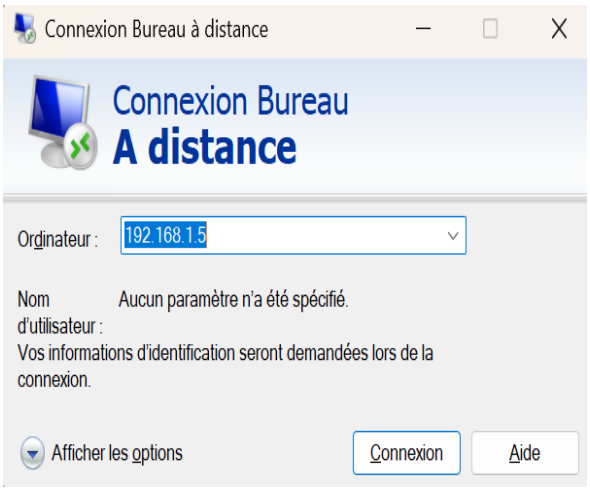
Et ensuite cliqué sur **Ajouté** puis mettez les users bob et alice puis veifier si bel et bien ils sont là et automatiquement le système va ajouter le contrôleur associée

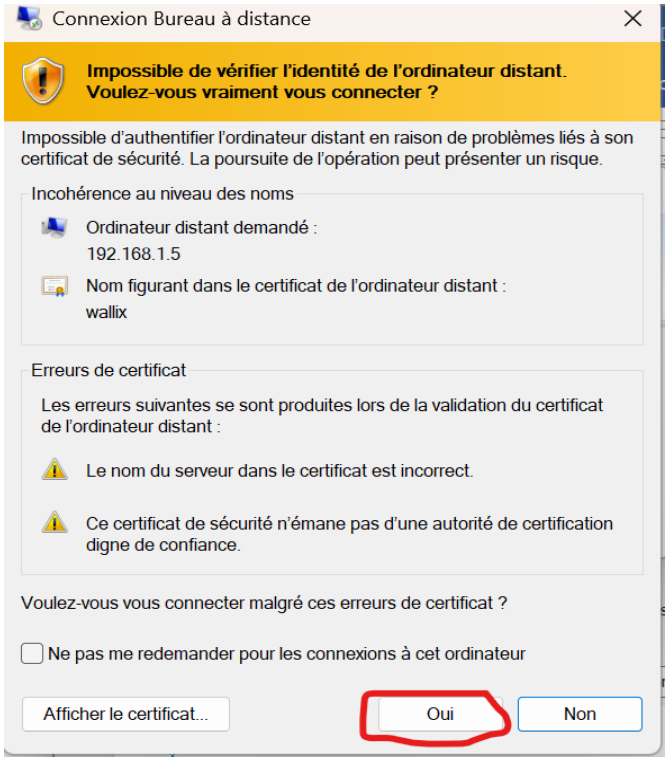


- Enfin nous aurons ceci

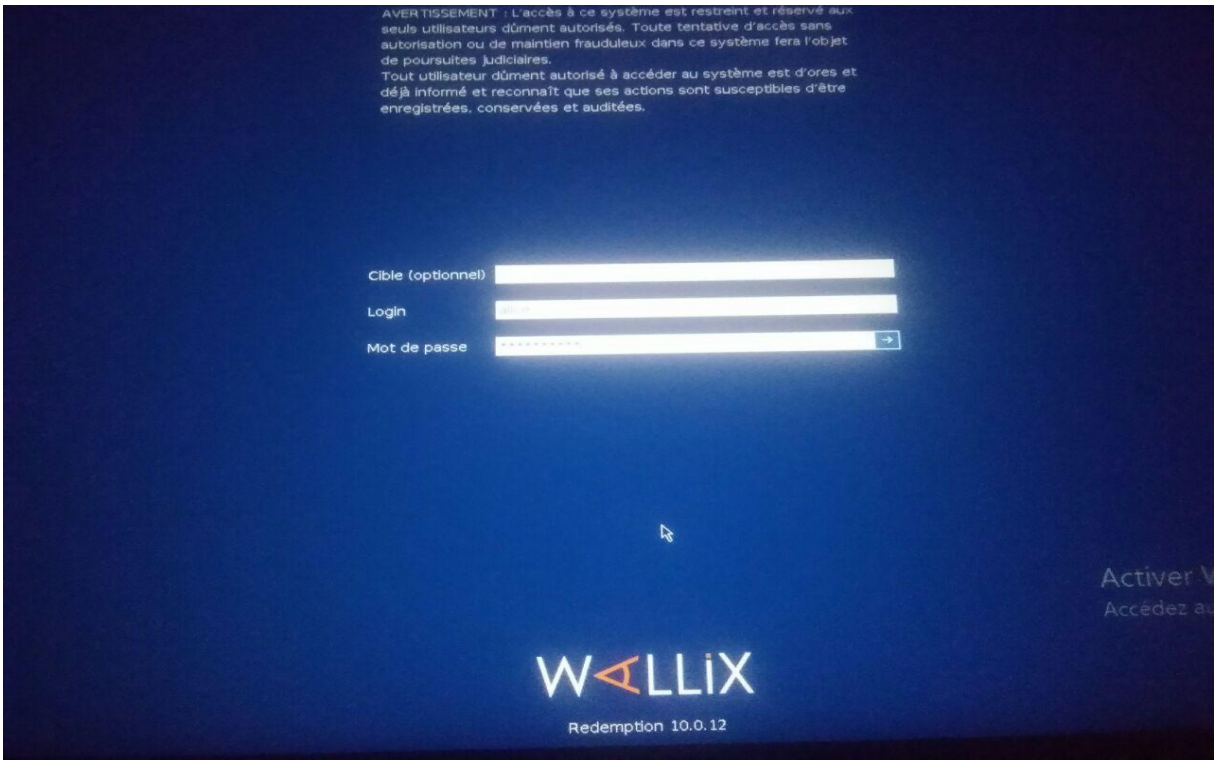


======== Alors sur la machine physique lançons le bureau à distance et mettons l'adresse de wallix qui est 192.168.1.5

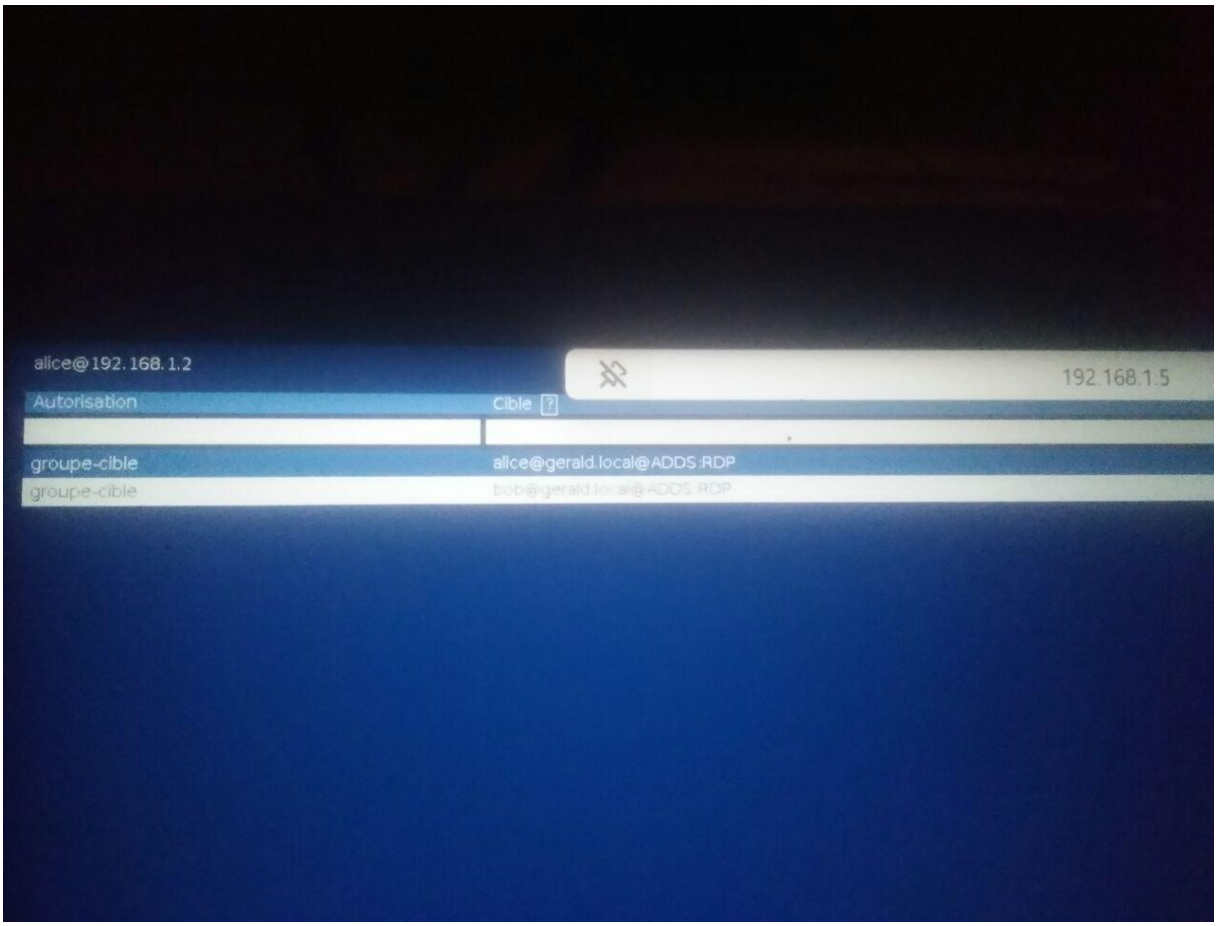




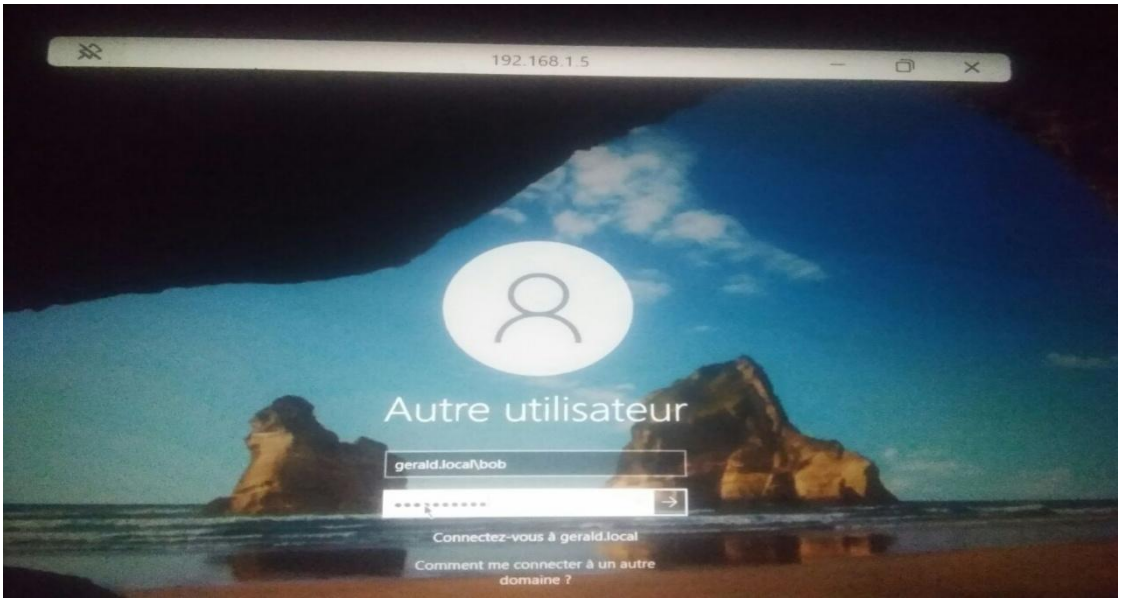
- On sera conduit à rentrer les identifiants, mettons celle de alice ou bob



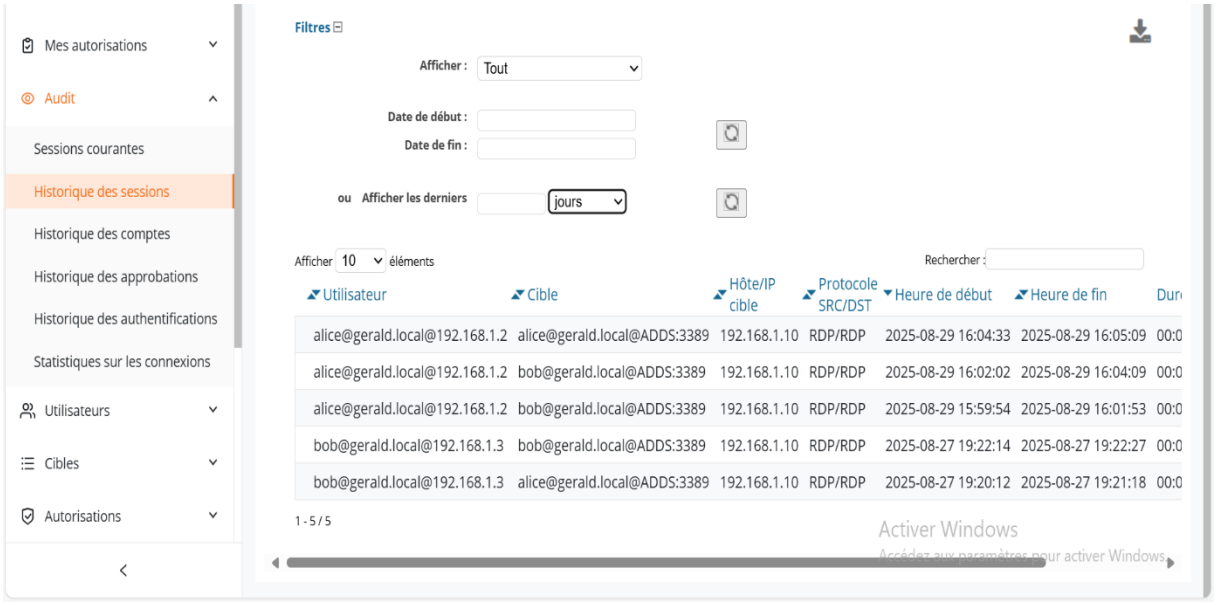
- une fois connecté nous serons sur le sélecteur et on peut choir alice ou bob



- Et après avoir cliqué sur bob ou alice nous serions conduit à l'interface de windows serveur mais comme dans nos config on avait pas donné bob et alice le droit d'utiliser telle fonctionnalité mais seulement de se connecté alors nous niveau de l'interface de wind serveur nous aurons l'échec mais neamoins cela n'empêchera pas le système établit de pouvoir enregistré toutes ses opérations de connexion dans wallix pour la traçabilité



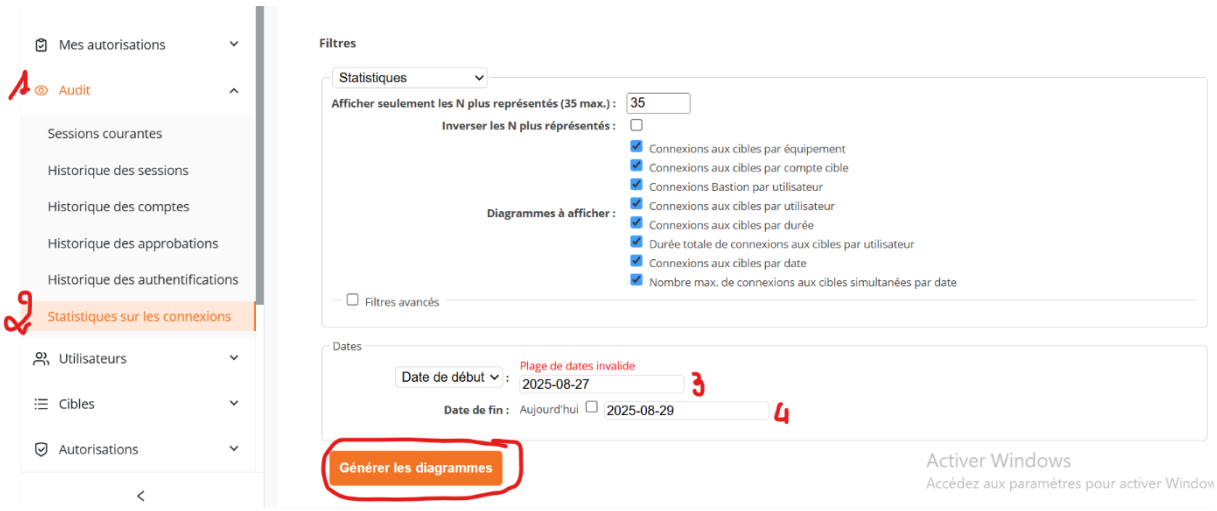
- Et dans wallix on observe bel et bien que toutes ses connexion sont enregistrées



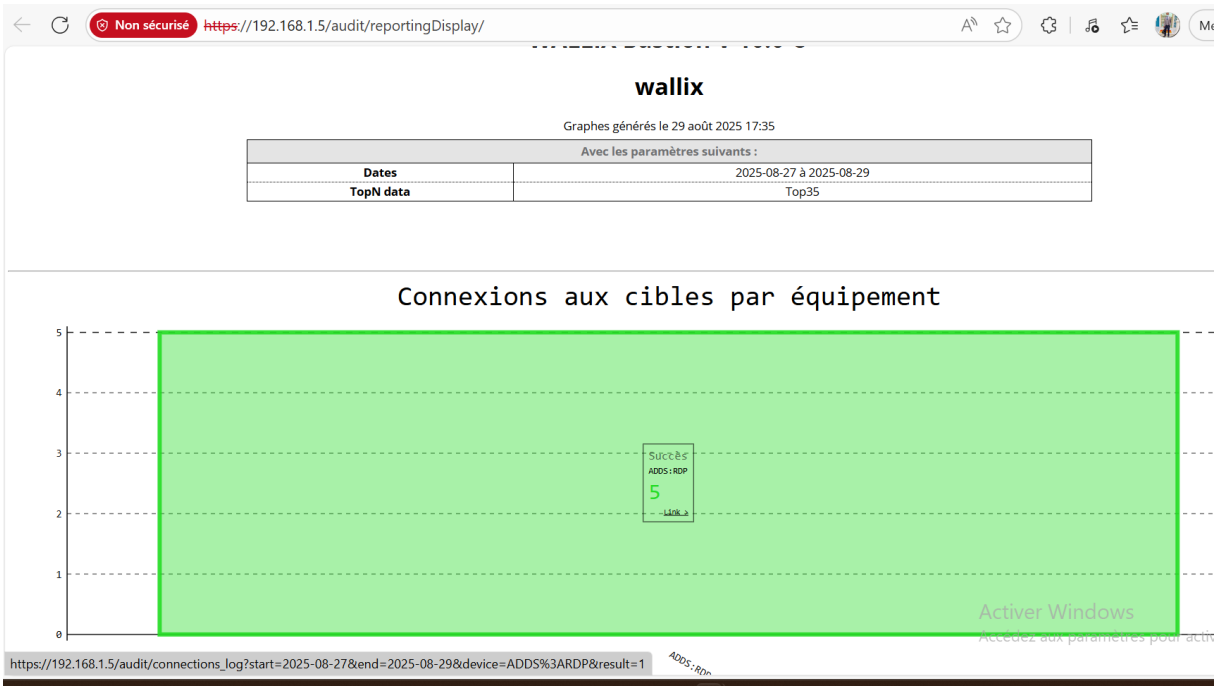
NB : on voit bien qu'il ya une traçabilité de :

1- Qui s'est connecter : Alice et bob à des intervalles différents
2- La machine qu'ils sont utilisé (dans mon cas machine physique)
3- La machine cible (window serveur)
4- Heure de debut de leurs connexion et heure de fin

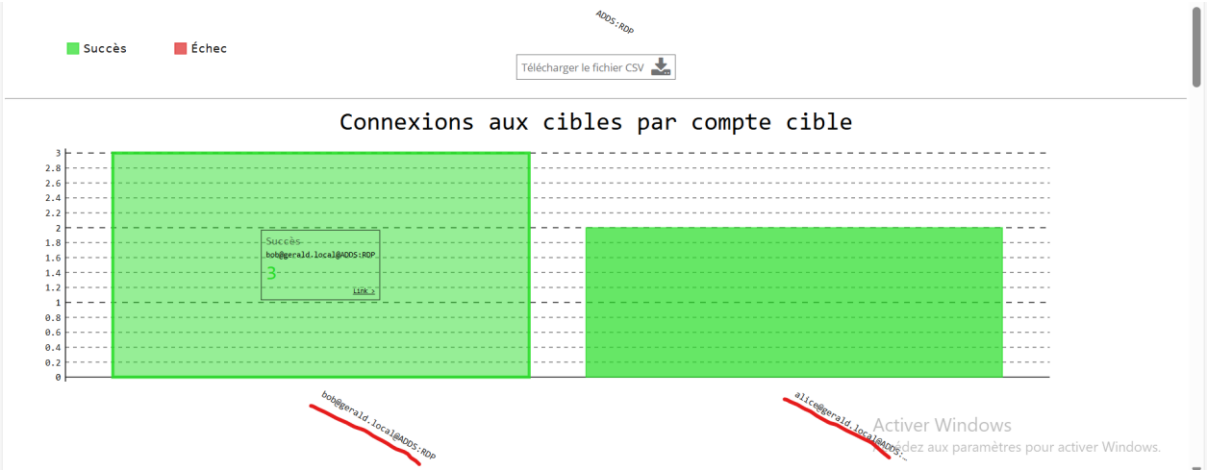
- On peux voir les statistiques de connexion



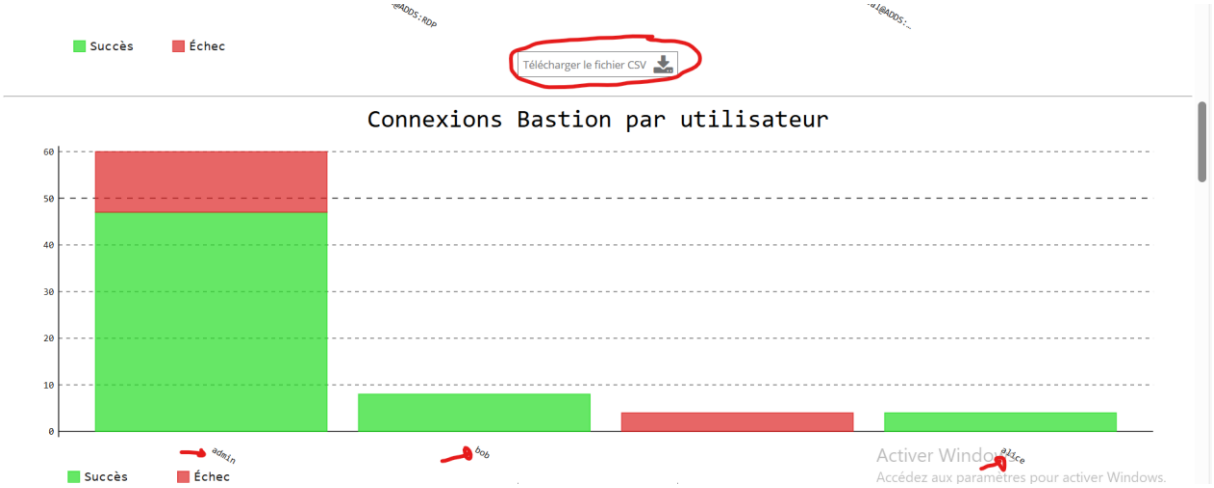
- Et nous aurons



- la suite

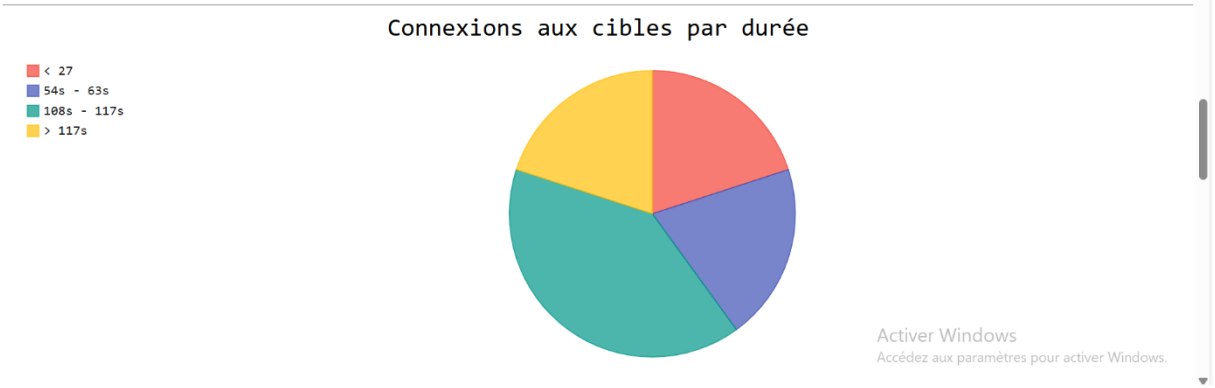


- Pour chaque catégorie de connexion nous avons les courbes qui vont avec

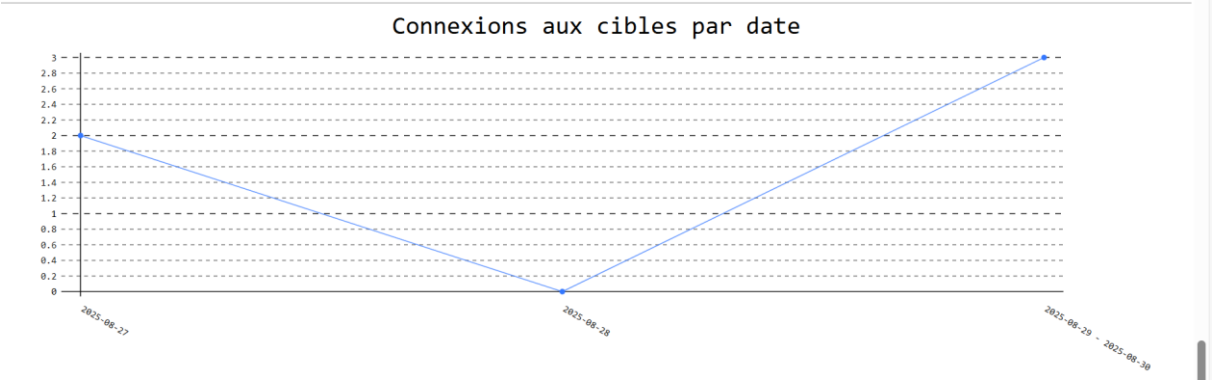


NB : On peu toujours télécharger ses statistique pour chaque analyse

- Pour la durée



- Pour les dates



Conclusion

La mise en œuvre du bastion WALLIX au sein de l'environnement virtualisé représente une avancée significative dans la sécurisation des accès privilégiés. Ce projet a permis de passer de la théorie à la pratique en démontrant concrètement comment centraliser et contrôler les accès aux systèmes critiques.

Les différentes étapes réalisées de l'import de l'appliance virtuelle à la configuration réseau, en passant par la création des utilisateurs, des groupes, des ressources cibles et surtout la définition fine des autorisations — ont permis d'ériger un point de passage obligatoire et sécurisé pour toutes les connexions administratives. La fonction d'**audit et d'enregistrement des sessions**, testée avec succès, constitue le cœur de la valeur ajoutée de la solution : elle

offre une traçabilité complète des actions réalisées sur les infrastructures, transformant ainsi la sécurité from a reactive to a proactive posture.

Ce travail jette les bases solaces d'une politique de moindre privilège et fournit les preuves d'activité nécessaires pour répondre aux exigences des audits de conformité réglementaire.

Perspectives

Ce projet ouvre la voie à plusieurs axes d'amélioration et d'approfondissement pour renforcer encore la posture de sécurité :