

RÉPUBLIQUE DU SÉNÉGAL



UN PEUPLE, UN BUT, UNE FOI

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DIRECTION DE L'ENSEIGNEMENT SUPÉRIEUR



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 ?

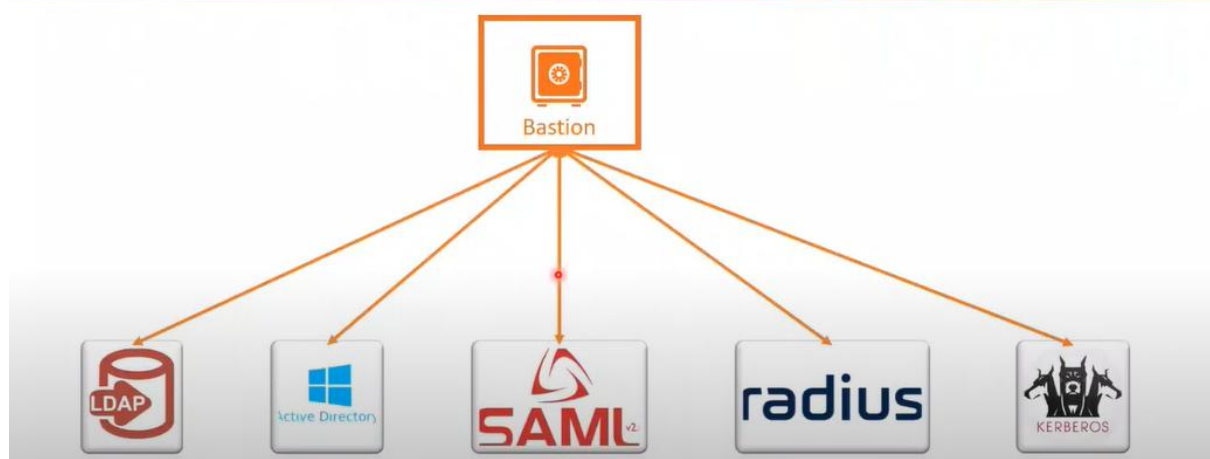
Dans le jargon de la cybersécurité, un bastion fait référence à un panneau d'administration de sécurité informatique. Celui-ci a pour but de fournir un point d'accès unique aux ressources informatiques les plus sensibles d'une société (données, CRM, logiciels SAAS, etc.). Pour protéger le patrimoine 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. »

====Étape 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

WALLIX

Configuration

Encryption

Configuration > Encryption

admin
Product Super Administrator

The definition of a passphrase involves a more complex access to Bastion and raises the protection of your data as no malicious users who do not know the passphrase can access your product. Moreover, at each system reboot, connections using Bastion proxies will not be usable as long as the passphrase is not entered by an administrator in the Web administration interface.

After the encryption initialization phase, we highly recommend you to back up Bastion at least once to keep a copy of the encryption key in a safe place.
If you do not perform this action and the passphrase is lost, you will no longer be able to access your data on remote storage.

Initialization
Please enter a passphrase to protect your system.
(You will be prompted to enter this passphrase to unlock your system after each reboot)

Passphrase *

Passphrase confirmation *

OR

No, I do not want a passphrase protection

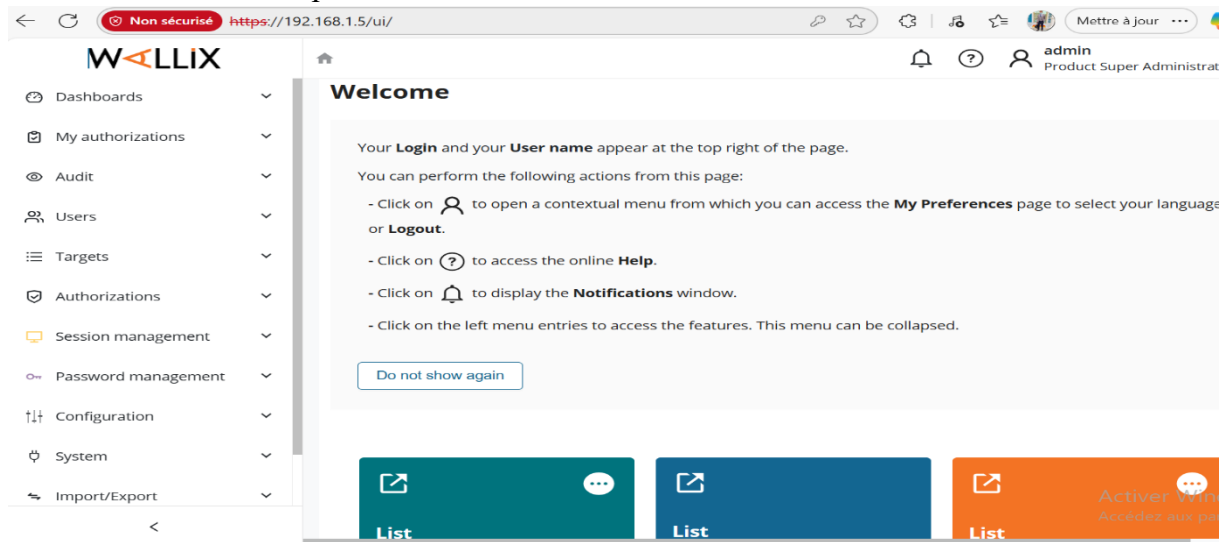
Bastion
Version 10.0.1

Activer Windc
Accédez aux paran

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.

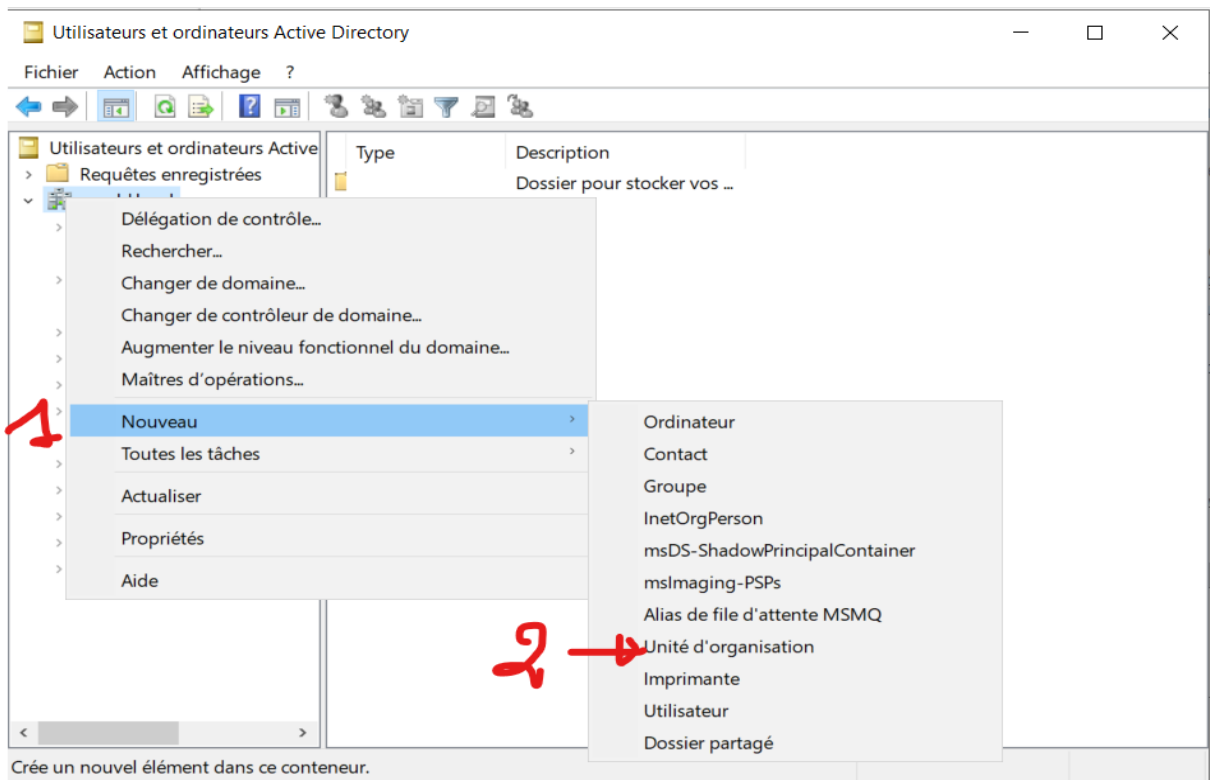
- Nous nous sommes connectés avec l'utilisateur admin que nous avons changé le mot de passe à la 1^{ère} connexion



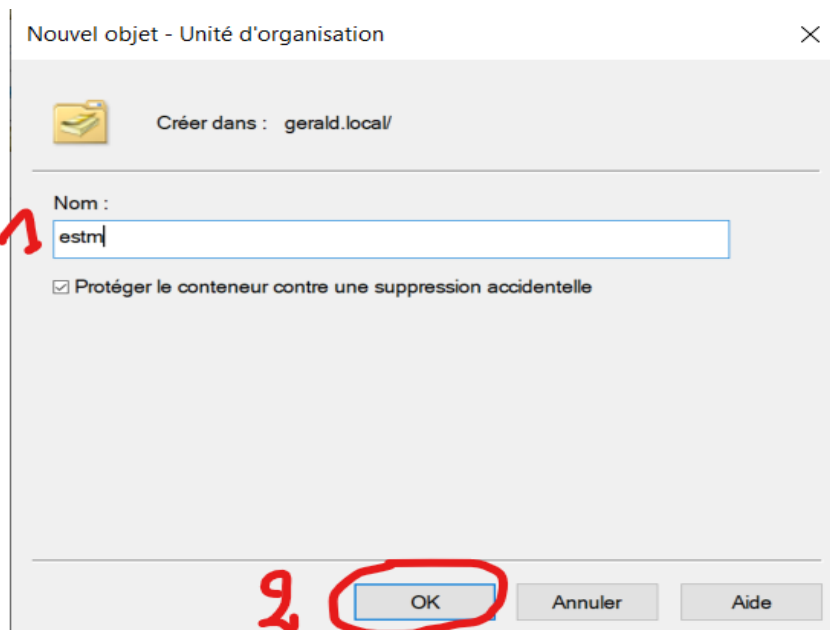
Rappel : dans les config de wallix nous avons eu à fixer l'adresse manuellement à 192.168.1.5 et la machine windows serveur est à 192.168.1.10 donc les deux machines sont dans le même réseau.

- Travail à faire sur votre windows serveur déjà opérationnel je suppose
 - 1- Après la création de votre contrôleur de domaine dans mon cas : gerald.local
 - 2- Créer une unité d'organisation dans mon cas : estm
 - 3- Créer un groupe dans cette unité d'organisation nommé dans mon cas : groupe1
 - 4- Puis à l'intérieur du groupe1 créer deux users : alice et bob puis un autre user à l'extérieur nommé : toto
 - 5-

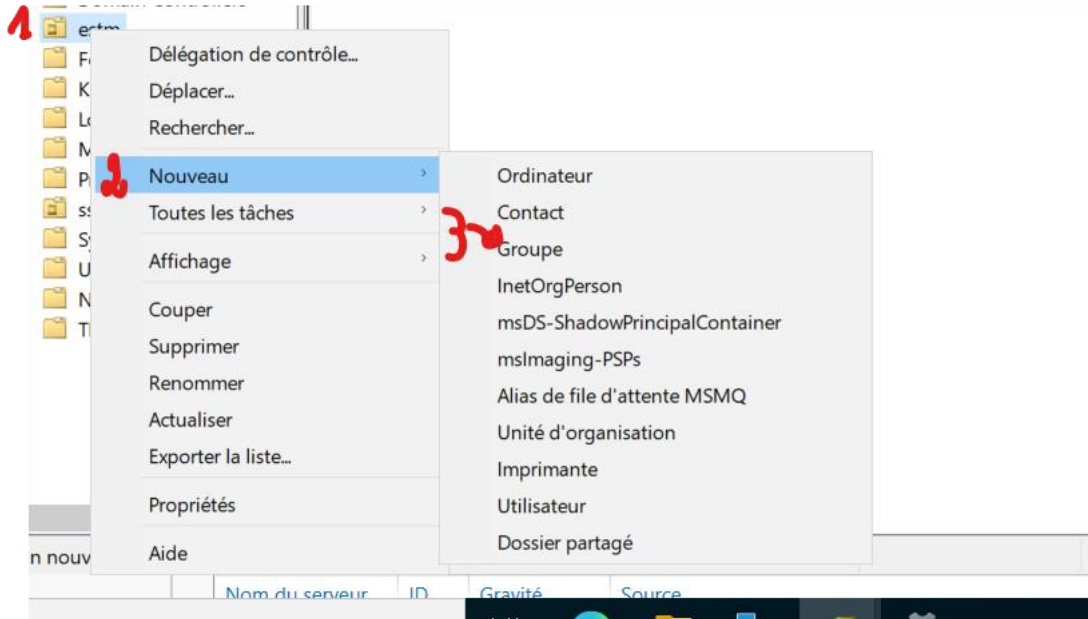
- clique droit sur le domaine **gerald.local** puis suivre la numerotation



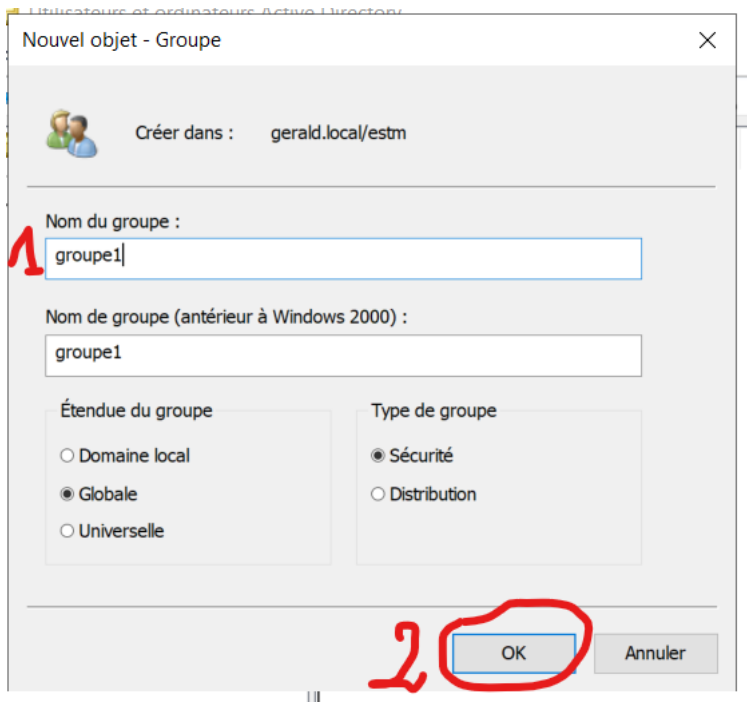
- Voici le nom de l'unité d'organisation



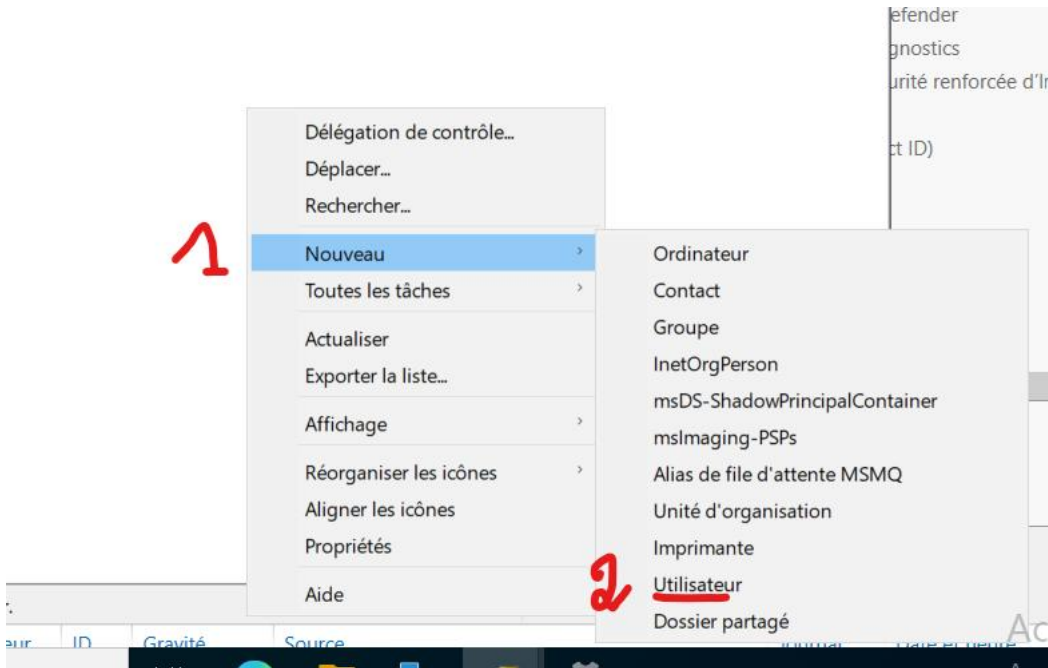
- Création du groupe dans cette u.o



- Nommé ce groupe : groupe1



- Création des utilisateurs



- User bob

A screenshot of the 'Nouvel objet - Utilisateur' (New Object - User) dialog box. The 'Créer dans' (Create in) field is set to 'gerald.local/estm'. The 'Prénom' (First name) field is filled with 'bob' and marked with a red arrow labeled '1'. The 'Nom' (Last name) field is empty. The 'Nom complet' (Full name) field is filled with 'bob'. The 'Nom d'ouverture de session de l'utilisateur' (User logon name) field is filled with 'bob' and marked with a red arrow labeled '2'. The domain dropdown is set to '@gerald.local'. Below, the 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' (User logon name (pre-Windows 2000)) fields are filled with 'GERALD\' and 'bob'. At the bottom, the 'Suivant >' (Next) button is circled in red.

- Son mot de passe

Nouvel objet - Utilisateur

Créer dans : gerald.local/estm

Mot de passe :

Confirmer le mot de passe :

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

< Précédent Suivant > Annuler

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

- Puis ajouter les user alice et bob dans le groupe1

Propriétés de : groupe1

Général Membres Membre de Géré par Objet Sécurité Éditeur d'attributs

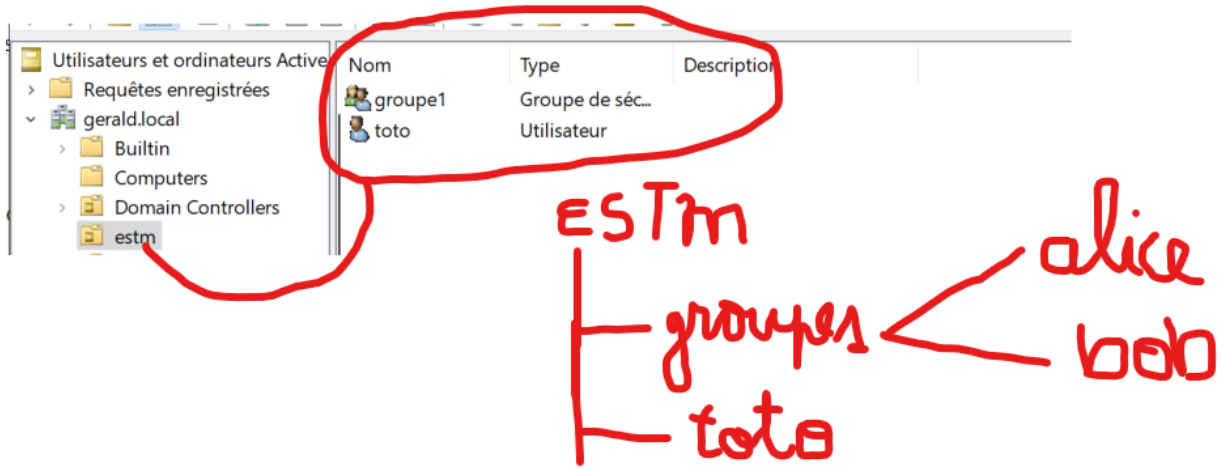
Membres :

Nom	Dossier Services de domaine Active Directory
alice	gerald.local
bob	gerald.local

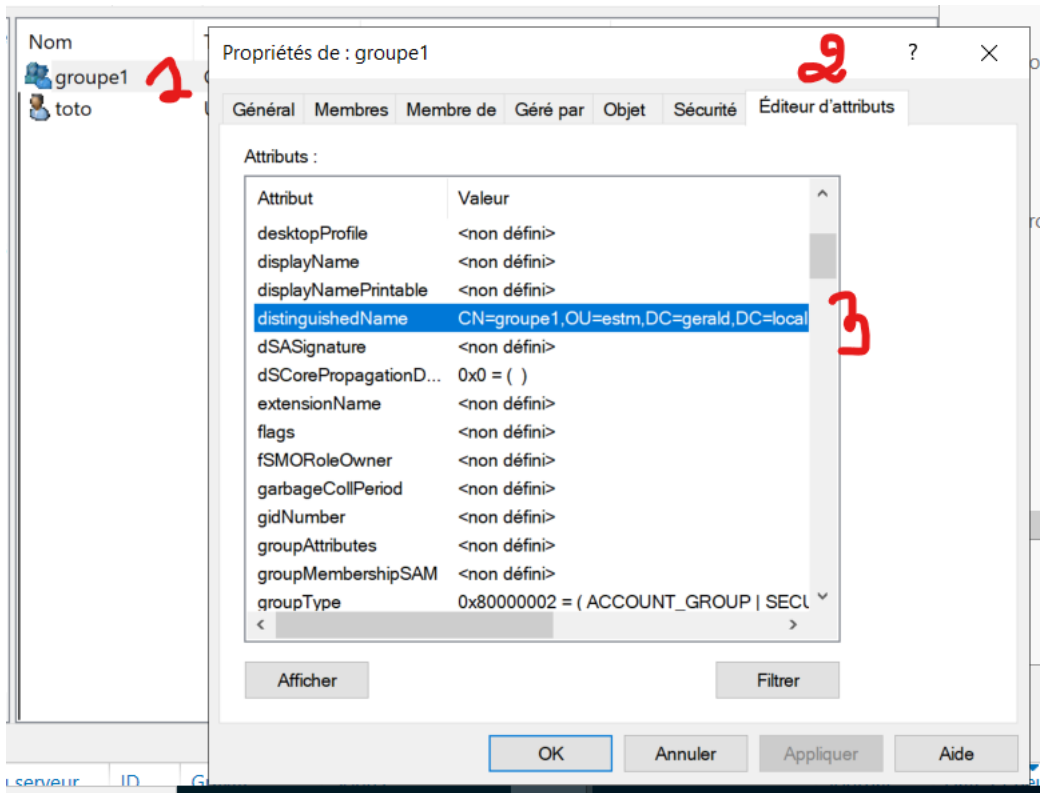
Ajouter... Supprimer

OK Annuler Appliquer Aide

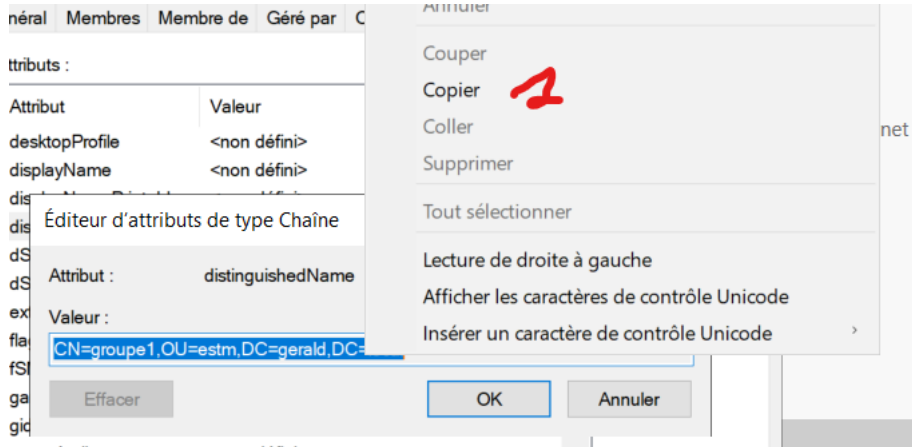
- Voici comment cela va se presenter



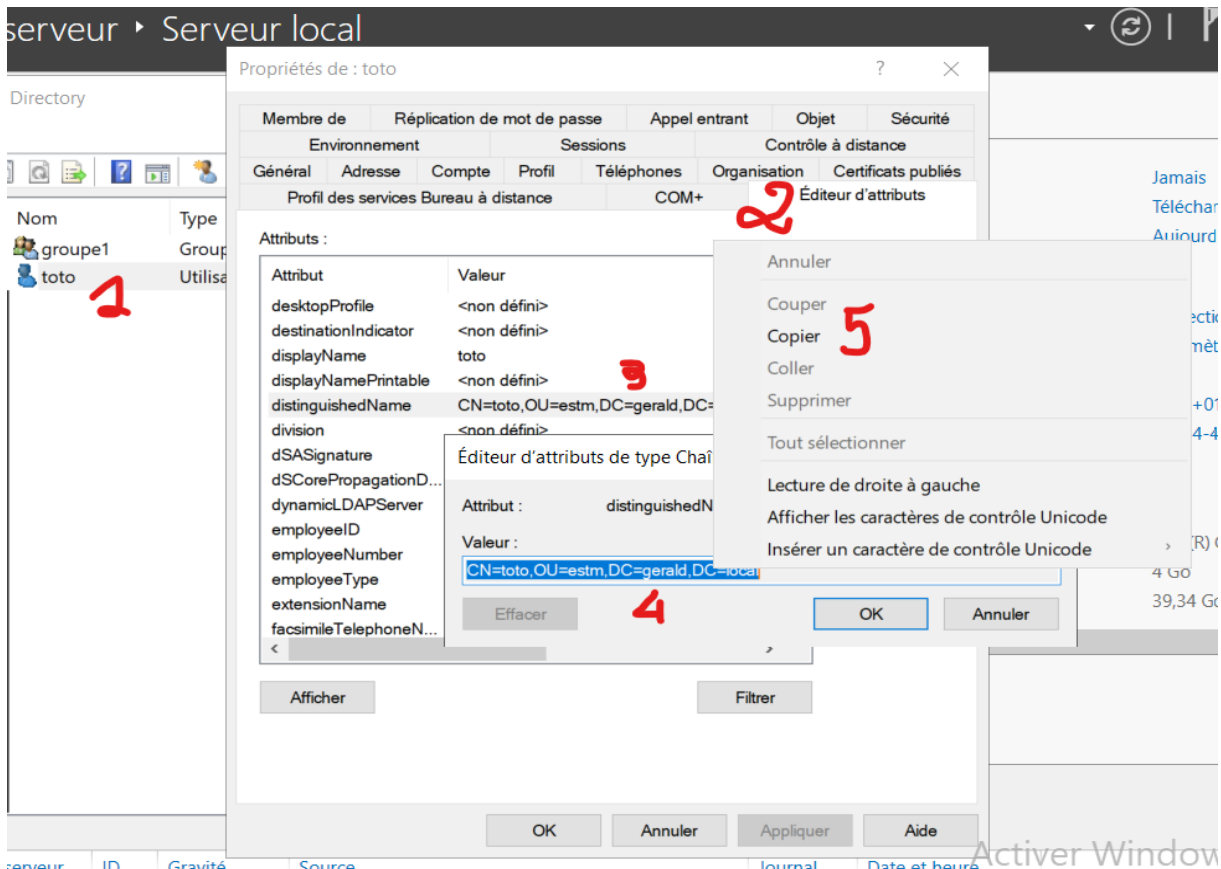
- Nous allons également se service du distinguishedName des utilisateurs toto et du groupe1 dans wallix voila comment copier cela



- Puis cliqué 2 fois sur ça et enfin copier, vous les utiliserez dans wallix donc nécessité vous oblige de connaître 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 renseignements n'oubliez pas de tester l'authentification

- et enfin

User attributes

Base DN (dc=...)*
 DC=gerald,DC=local

Login attribute*
 sAMAccountName

User name attribute*
 sAMAccountName

Apply

Activer Windows
 Accédez aux paramètres pour activer Windows.

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

Tableau de bord		Pour ADDS	
Tableau de bord	Seurver local	Nom de l'ordinateur	ADDS
Tous les serveurs	AD DS	Domaine	gerald.local
DHCP	DNS	Pare-feu Microsoft Defender	Public : Actif
Services de fichiers et d...		Gestion à distance	Activé
		Bureau à distance	Activé
		Association de cartes réseau	Désactivé
		Ethernet0	192.168.1.10, Compatible IPv6
			Dernières mise: Windows Upda
			Dernière recher
			Antivirus Micro
			Commentaires
			Configuration c
			Fuseau horaire
			ID de produit (l

- voici ce que ça donne

Nom	Type	Serveur	Port
ADDS	Active Directory	192.168.1.10	389

- 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

LDAP/AD attribute to retrieve the SSN public key and allow user authentication via an SSN key
Suggested value for AD server: "altSecurityIdentities"

Default email domain *

gerald.local

E.g.: example.com

Language attribute

preferredLanguage

Default language *

French



- 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 distingueshName du groupe 1 que vous irez prendre dans wind serveur puis appliqué

Action: kill | Rules: | Subprotocol: SSH_SHELL_SESSION / X11_SESSION

Authentication domain mapping

Profile * user ¹

Authentication domain name * ADDS ² | External group * CN=groupe1,OU=estm,DC=gerald,DC=local ³

Apply | Activer Windows | Cancel

- Voici cela

Utilisateurs > Groupes

+ Ajouter un groupe

Afficher 10 éléments

Nom du groupe	Description	Plages horaires	Profil
groupe1		allthetime	user

- 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

Afficher les utilisateurs sur le domaine :

ADDS

Afficher 10 éléments

Identifiant	Nom usuel	Groupes	Dernière connexion
alice	alice	groupe1	--
bob	bob	groupe1	2025-08-27 19:22:14

1 - 2 / 2

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**

Nouvelle correspondance ✕

Groupe utilisateurs *
groupe1 **1**

Profil du group utilisateurs *
user **2**

Une modification du profil du groupe utilisateurs aura un impact sur toutes les correspondances associées au groupe utilisateurs

Groupe par défaut pour les utilisateurs sans groupe dans ce domaine

Groupe *
CN=groupe1,OU=estm,DC=gerald,DC=local **3**

Format DN

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

Général **Correspondances**

<input type="checkbox"/> Groupe utilisateurs	Groupe
<input type="checkbox"/> groupe1	CN=groupe1,OU=estm,DC=gerald,DC=local

- 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



Connexion

bob

.....| 

CONNEXION

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

The screenshot shows the WALLIX web interface. On the left is a sidebar with 'Mes autorisations', 'Sessions', and 'Mots de passe'. The main area is titled 'Mes autorisations > Sessions'. At the top right, a user profile for 'bob@gerald.local' is shown, circled in red. Below this, there's a section for 'Télécharger le fichier de configuration RDP' with an 'Options' button. A table lists sessions with columns for 'Protocoles', 'Cible', 'Nom d'autorisation', 'Description du compte', 'Description de la cible', 'Plage horaire', 'Dernière connexion', and 'Approbato'. Two sessions are listed, both for RDP and 'alice@gerald.local@ADDS:RDP' and 'bob@gerald.local@ADDS:RDP' respectively, both with 'groupe-cible' as the target and 'allthetime' as the time range. The last connection for bob was on 2025-08-27 at 19:22:27.

Protocoles	Cible	Nom d'autorisation	Description du compte	Description de la cible	Plage horaire	Dernière connexion	Approbato
RDP	alice@gerald.local@ADDS:RDP	groupe-cible	--	--	allthetime	2025-08-27 19:21:18	
RDP	bob@gerald.local@ADDS:RDP	groupe-cible	--	--	allthetime	2025-08-27 19:22:27	

===== 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**

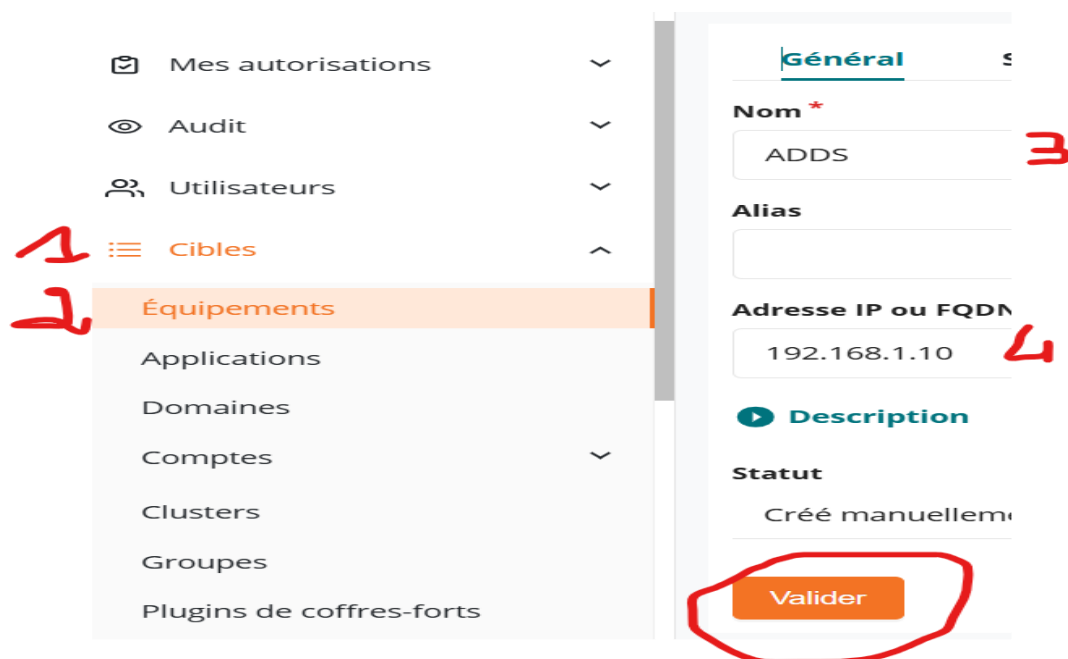
- Login et mot de passe du compte cible
- Choisir entre compte local ou global

- **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 **Équipement** 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

Modification du service RDP



Équipement

ADDS **1**

Nom de service

RDP **2**

Port *

3389

Politique de connexion *

RDP **3**

Domaine global

Un domaine global est obligatoire pour créer des cibles pour des applications et des clusters

gerald.local **4**

Options proxy

- RDP_CLIPBOARD_UP
- RDP_CLIPBOARD_DOWN
- RDP_CLIPBOARD_FILE
- RDP_PRINTER
- RDP_COM_PORT
- RDP_DRIVE
- RDP_SMARTCARD
- RDP_AUDIO_OUTPUT
- RDP_AUDIO_INPUT

Fermer

Valider et fermer

- 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**

Domaine global

Nom *: gerald.local **1**

Nom réel:

Description:

Vault type: Local External

Unable to change vault type. At least one account is associated to the domain.

CA private key: Générer une clé privée --- Sélectionner ---
ou
Télécharger une clé privée Choisir un fichier Aucun fichier n'a été sélectionné

Royaume Kerberos:

KDC Kerberos:

Port Kerberos:

La configuration Kerberos est uniquement prise en charge pour le plugin WindowsService.

Activer le changement de mot de passe:

Appliquer

Activer Windows

Annuler

Accédez aux paramètres pour activer windows

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

Modifier ce domaine global

Nom de domaine : gerald.local
Nom réel du domaine : --
Description : --
Clé publique AC : --
Royaume Kerberos : --
KDC Kerberos : --
Port Kerberos : --
Compte administrateur : --

Comptes du domaine
+ Ajouter un compte

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

Cibles > Domaines

admin Product Super Administrator



Type de compte *: Domaine global
Domaine global : gerald.local
Nom *: **alice** 1
Identifiant *: copier depuis le nom
alice
Description :
Mot de passe : 2
Clé privée SSH : Générer une clé privée --- Sélectionner ---
ou Télécharger une clé privée Choisir un fichier Aucun fichier n'a été sélectionné
Changement automatique du mot de passe :
Décocher pour désactiver le changement automatique du mot de passe pour ce compte
Changement automatique de clé SSH :
Décocher pour désactiver le changement automatique de la clé SSH pour ce compte
Politique d'emprunt : default
Ajouter/supprimer une association de ressources

Ressources disponibles	Ressources sélectionnées
	Activier Windows Ajouter des paramètres pour activer Windows. ADD5:RDP



- À la fin nous aurons ceci

Afficher le type de domaine :

Global Local à un équipement Local à une application

[+ Ajouter un domaine global](#)  

Afficher 10 éléments Rechercher :

 Nom	 Nom réel	Description	Clé publique AC	Changement de mot de passe	Coffre-fort externe
gerald.local	--	--	--	--	--

1 - 1 / 1

- 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


[Modifier ce domaine global](#)

Nom de domaine: gerald.local
Nom réel du domaine: --
Description: --
Clé publique AC: --
Royaume Kerberos: --
KDC Kerberos: --
Port Kerberos: --
Compte administrateur: --

Comptes du domaine

[+ Ajouter un compte](#)

Afficher 10 éléments Rechercher :

 Nom du compte	Domaine	Description
alice	gerald.local	
bob	gerald.local	

1 - 2 / 2

Activer Windows

- 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

🏠 > Cibles > Comptes > Comptes globaux > alice > Général

🔔 ?

Général **Mot de passe** **Clé privée SSH** Références

Domaine global

Nom du compte *

Identifiant du compte *

Association de ressources
 ⚠ Cette association s'applique uniquement aux équipements associés à des services RDP. Une association de ressources est obligatoire pour créer des cibles pour des applications et des clusters

Équipement : **Service RDP**
 :

Politique d'emprunt *

Changement automatique du mot de passe
 Décocher cette option pour désactiver le changement automatique du mot de passe pour ce compte

Changement automatique de la clé SSH
 Décocher cette option pour désactiver le changement automatique de la clé SSH pour ce compte

Validité du certificat
 sem j h min
 s
 La validité du certificat n'est pas nécessaire

Activer Windows

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

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

Dans notre cas nous l'avons déjà fait et on l'avait attaché aux distinguishedName du groupe 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

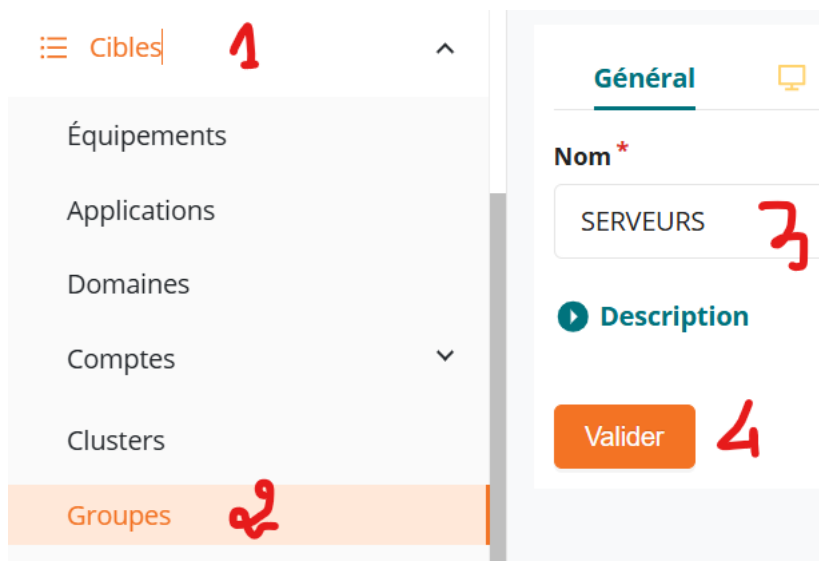
+ Ajouter un groupe

Afficher 10 éléments Rechercher :

Nom du groupe	Description	Plages horaires	Profil	Utilisateurs
groupe1		allthetime	user	0

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

Dans la partie Général mettez le nom : SERVEURS (vous pouvez mettre ce que vs voulez) 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**

Ajouter des comptes cibles pour la gestion des sessions

Groupe

SERVEURS 1

Depuis *

Un équipement et des comptes globaux 2

Équipement *

ADDS 3

Service *

RDP 4

Comptes globaux *

Sélectionner au moins un élément disponible

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

Comptes globaux*
Sélectionner au moins un élément disponible

Nom du compte	Nom de domaine	Déjà dans le groupe
alice	gerald.local	✓
bob	gerald.local	✓

1-2 sur 2 éléments < 1 > 20 / page

Fermer Ajouter et continuer **Ajouter et fermer**

- Le resultat final donne ça

Général **Cibles gestion des sessions** Cibles gestion des mots de passe Restrictions

+ Ajouter Supprimer association(s)

Nom du compte	Type de domaine	Nom de domaine	Application	Équipement
bob	global	gerald.local	-	ADDS
alice	global	gerald.local	-	ADDS

1-2 sur 2 éléments < 1 > 20 / page

- Donnons les autorisations au groupe 1

Autorisations 1

Gestion des autorisations 2

Mes approbations en cours
Mon historique d'approbations

Gestion des sessions
Gestion des mots de passe
Configuration
Système
Import/Export

Bastion
Version 10.0.1

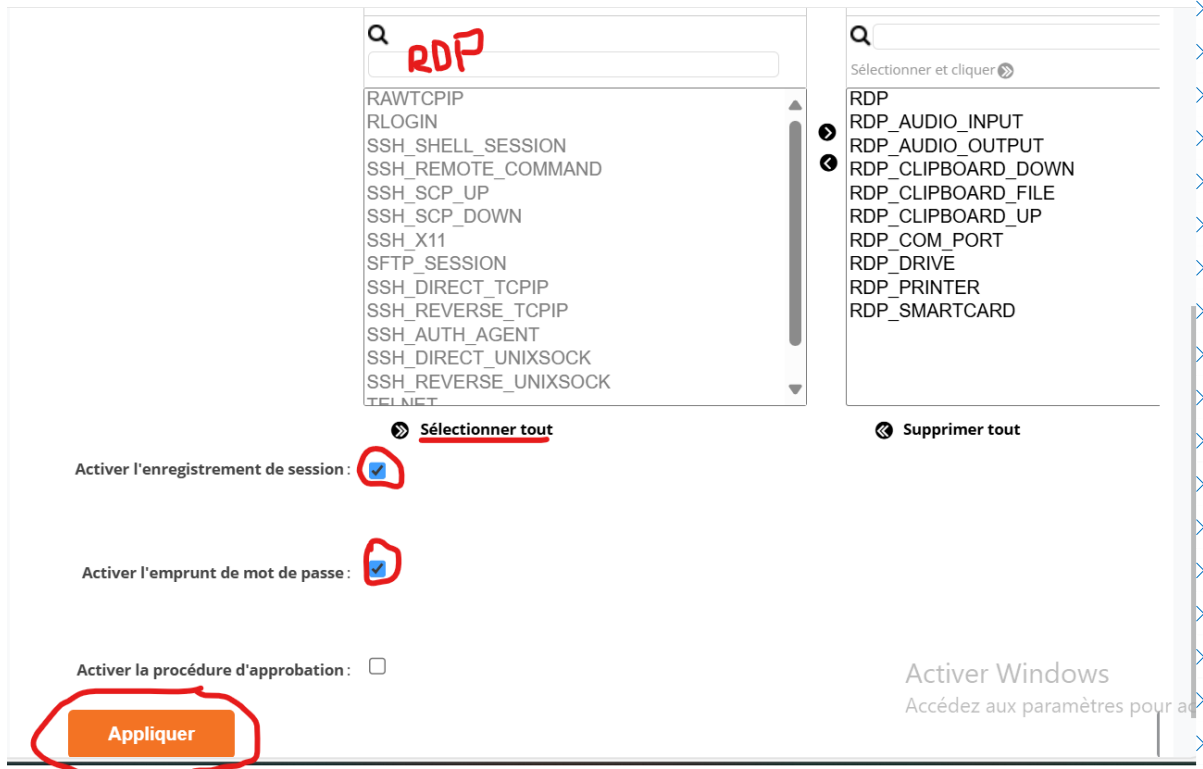
Modifier cette autorisation

Groupe utilisateurs*: groupe1
Groupes de cibles*: SERVEURS
Nom*: groupe-cible 3
Description:
Cibles critiques:

Activer les sessions:
Protocoles/sous-protocoles*:

Protocoles/sous-protocoles disponibles	Protocoles/sous-protocoles séle
RAWTCPIP RLOGIN SSH_SHELL_SESSION SSH_REMOTE_COMMAND SSH_SCP_UP SSH_SCP_DOWN SSH_X11 SFTP_SESSION	RDP RDP_AUDIO_INPUT RDP_AUDIO_OUTPUT RDP_CLIPBOARD_DOWN RDP_CLIPBOARD_FILE RDP_CLIPBOARD_UP RDP_COM_PORT RDP_DRIVE

===== 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 aller 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

[Gestion des sessions](#) > [Politiques de connexion](#)

 admin
Product Super Admini

Modifier cette politique de connexion

Nom de la politique *:

Description:

Protocole *: RDP

Méthodes d'authentification *: PASSWORD_VAULT
 PASSWORD_MAPPING
 PASSWORD_INTERACTIVE

Aide sur les options Options avancées

[general]

- Puis en bas de la page coché et appliqué

[rdp]

Enable nla:
NLA authentication in secondary target.
Boolean [default: True]

Enable kerberos:
If enabled, NLA authentication will try Kerberos before NTLM.
(if enable_nla is disabled, this value is ignored).
Boolean [default: False]

Time min level:

- Voilà comment la nouvelle politique se présentera

[+ Ajouter une politique de connexion](#)

Afficher éléments Rechercher:

	▲ Politiques de connexion	▲ Protocole	▲ Description	Action
	RAWTCPIP	RAWTCPIP	Default RAWTCPIP connection policy	
	RDP	RDP	Default RDP connection policy	
	RDP-modify	RDP		
	RLOGIN	RLOGIN	Default RLOGIN connection policy	
	SSH	SSH	Default SSH connection policy	
	TELNET	TELNET	Default TELNET connection policy	
	VNC	VNC	Default VNC connection policy	

1 - 7/7

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

Modification du service RDP ✕

Équipement

Nom de service

Port *

Politique de connexion *

Dernière valeur : RDP

Domaine global

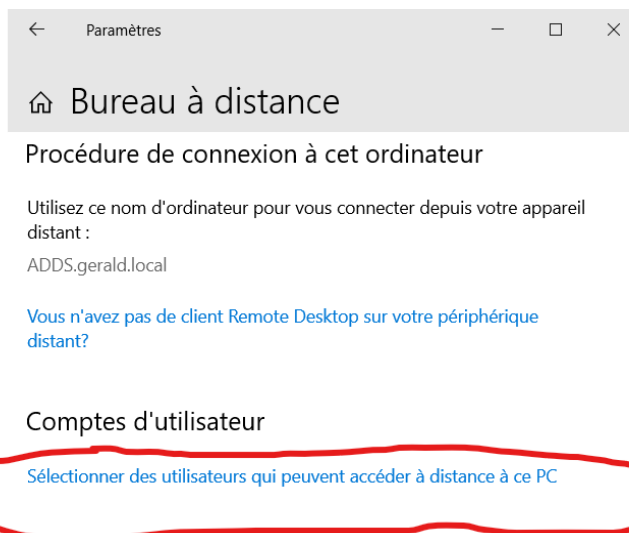
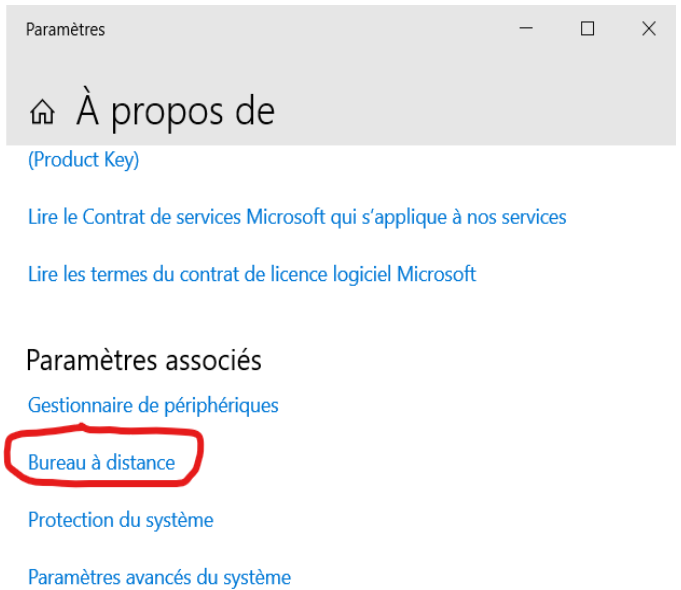
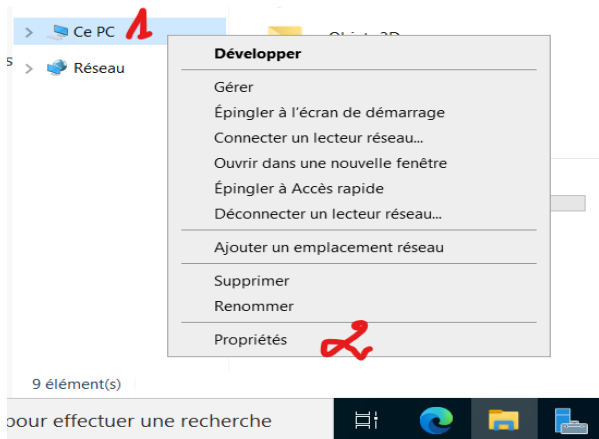
Un domaine global est obligatoire pour créer des cibles pour des applications et des clusters

Options proxy

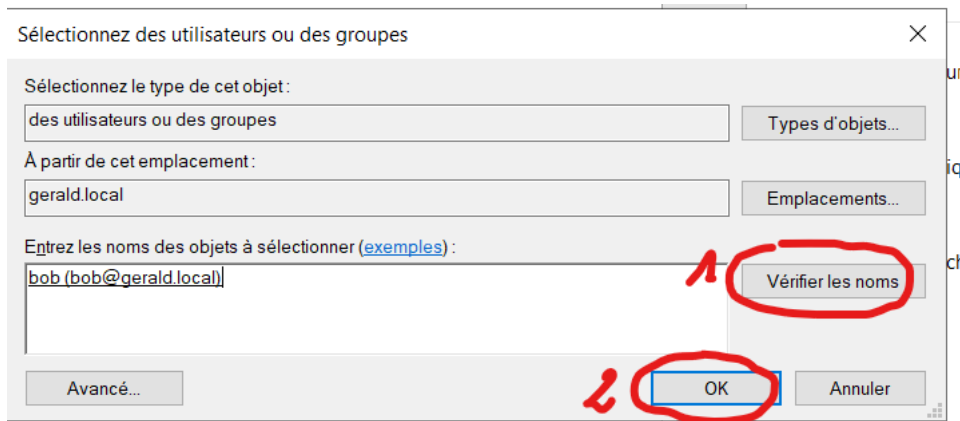
- RDP_CLIPBOARD_UP
- RDP_CLIPBOARD_DOWN
- RDP_CLIPBOARD_FILE
- RDP_PRINTER
- RDP_COM_PORT
- RDP_DRIVE
- RDP_SMARTCARD
- RDP_AUDIO_OUTPUT
- RDP_AUDIO_INPUT

===== 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

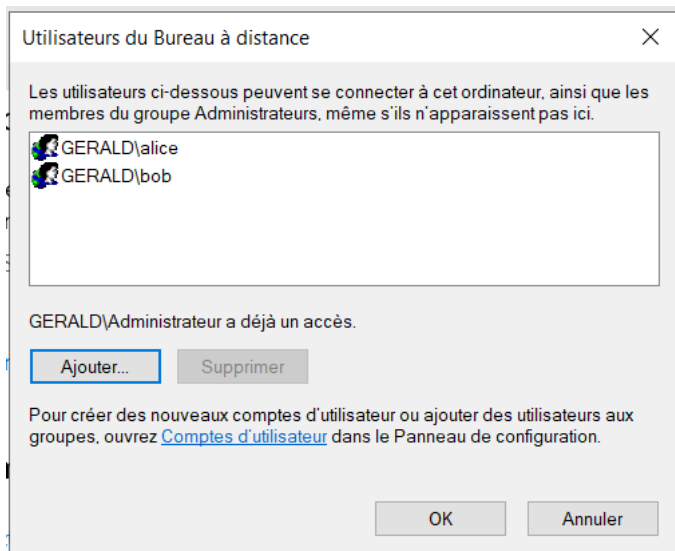
- Pour ce faire sur une autre machine tapons à la barre de recherche **Bureau à distance** mais bien avant nous devons configurer le bureau à distance dans notre Windows serveur



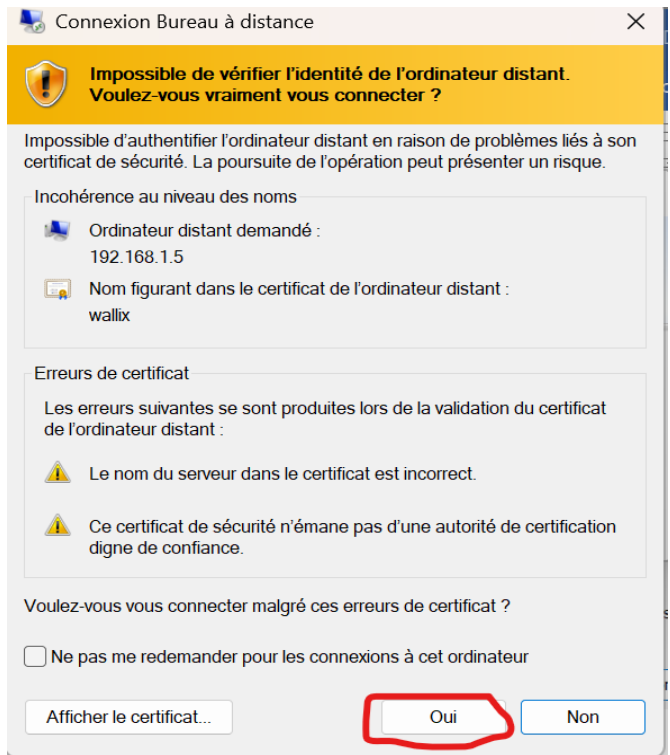
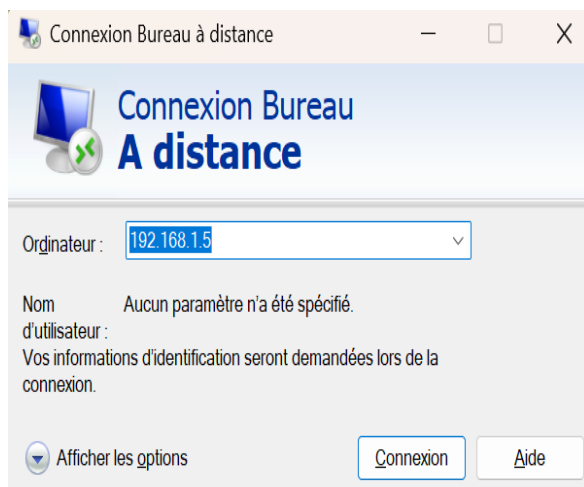
Et ensuite cliqué sur **Ajouté** puis mettez les users bob et alice puis veifier si bel et bien ils sont là et automatiquement le système va ajouter le contrôleur associée



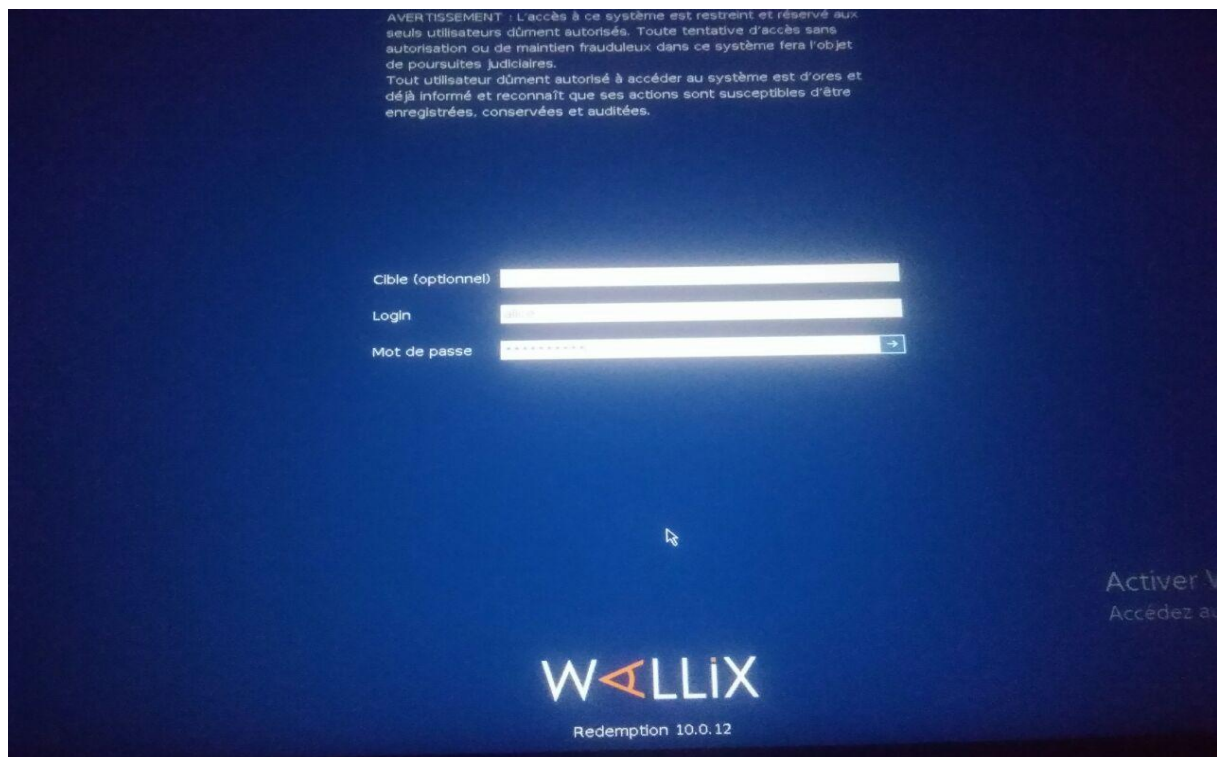
- Enfin nous aurons ceci



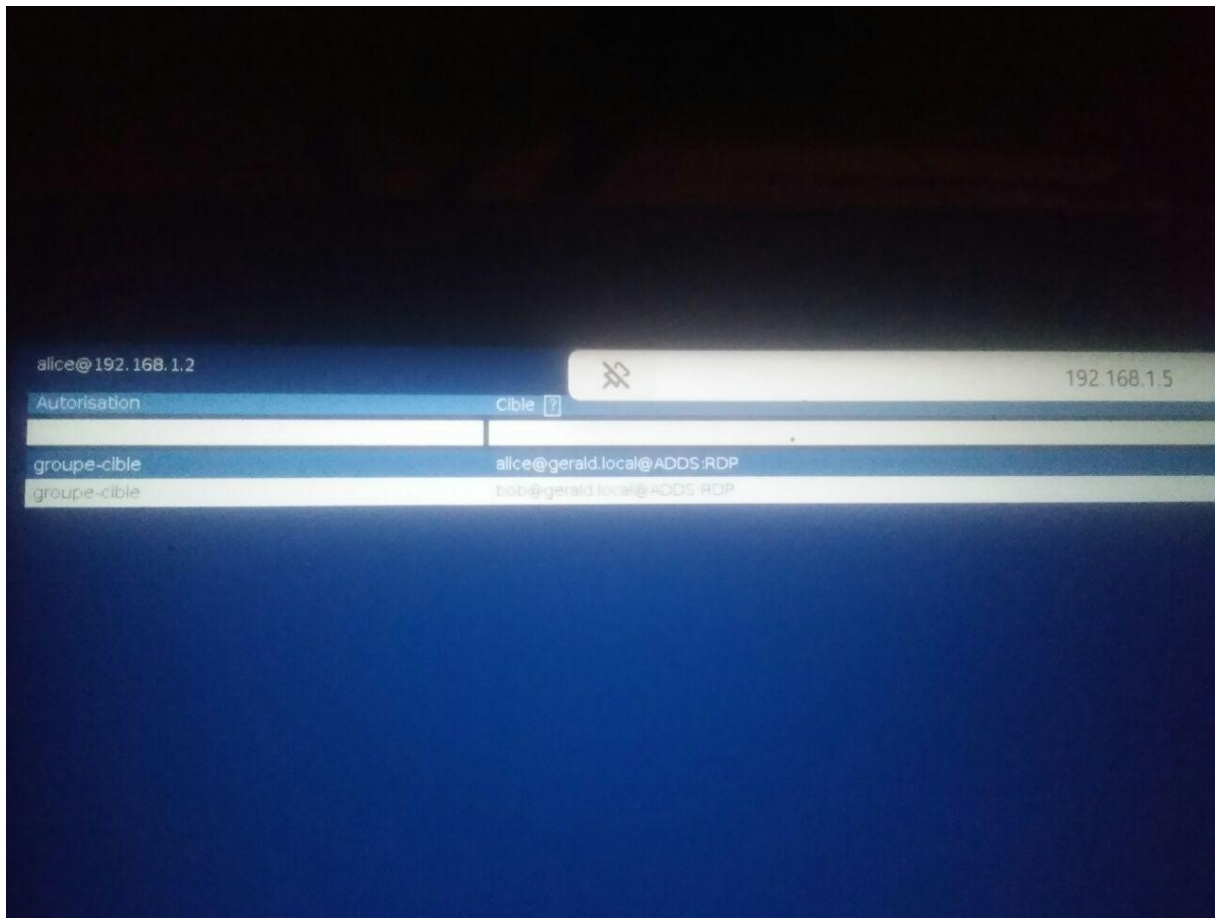
===== Alors sur la machine physique lançons le bureau à distance et mettons l'adresse de wallix qui est 192.168.1.5



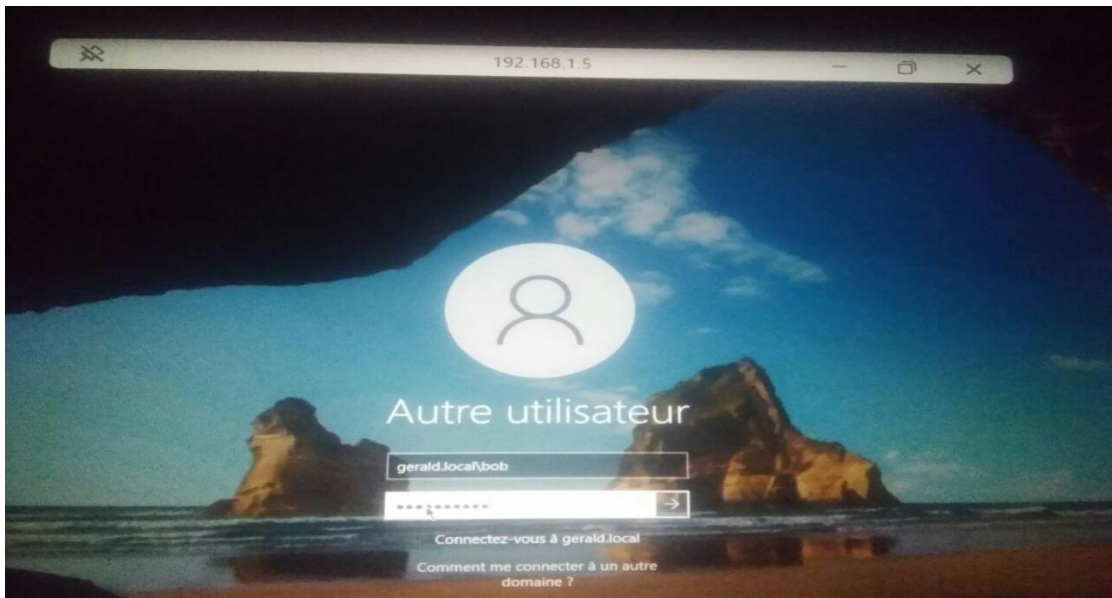
- On sera conduit à rentrer les identifiants, mettons celle de alice ou bob



- une fois connecté nous serons sur le sélecteur et on peut choisir 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 neanmoins 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

Utilisateur	Cible	Hôte/IP cible	Protocole SRC/DST	Heure de début	Heure de fin	Dur
alice@gerald.local@192.168.1.2	alice@gerald.local@ADDS:3389	192.168.1.10	RDP/RDP	2025-08-29 16:04:33	2025-08-29 16:05:09	00:0
alice@gerald.local@192.168.1.2	bob@gerald.local@ADDS:3389	192.168.1.10	RDP/RDP	2025-08-29 16:02:02	2025-08-29 16:04:09	00:0
alice@gerald.local@192.168.1.2	bob@gerald.local@ADDS:3389	192.168.1.10	RDP/RDP	2025-08-29 15:59:54	2025-08-29 16:01:53	00:0
bob@gerald.local@192.168.1.3	bob@gerald.local@ADDS:3389	192.168.1.10	RDP/RDP	2025-08-27 19:22:14	2025-08-27 19:22:27	00:0
bob@gerald.local@192.168.1.3	alice@gerald.local@ADDS:3389	192.168.1.10	RDP/RDP	2025-08-27 19:20:12	2025-08-27 19:21:18	00:0

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

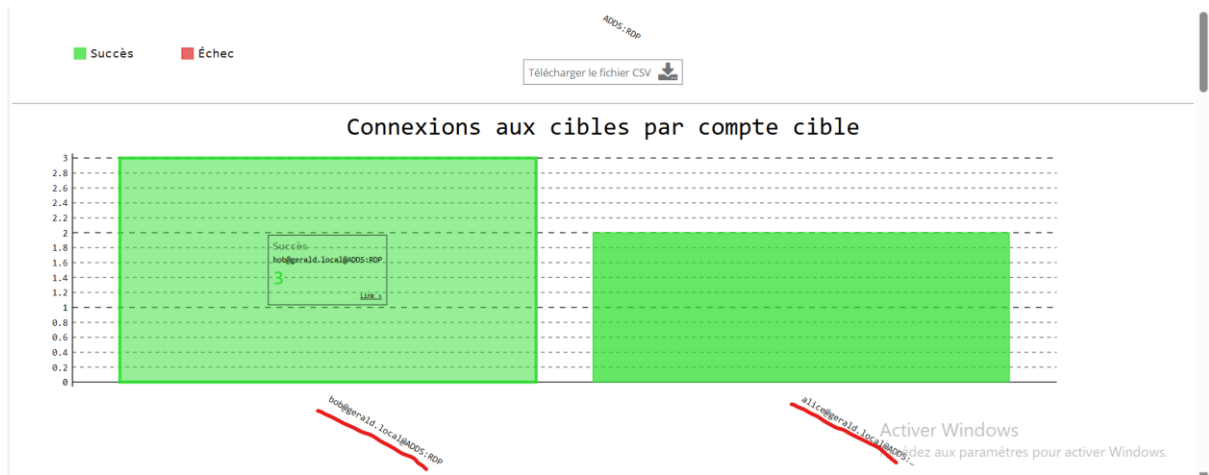
- 1- Qui s'est connecter : Alice et bob à des intervalles différents
- 2- La machine qu'ils sont utilisé (dans mon cas machine physique)
- 3- La machine cible (window serveur)
- 4- Heure de debut de leurs connexion et heure de fin

- On peut voir les statistiques de connexion

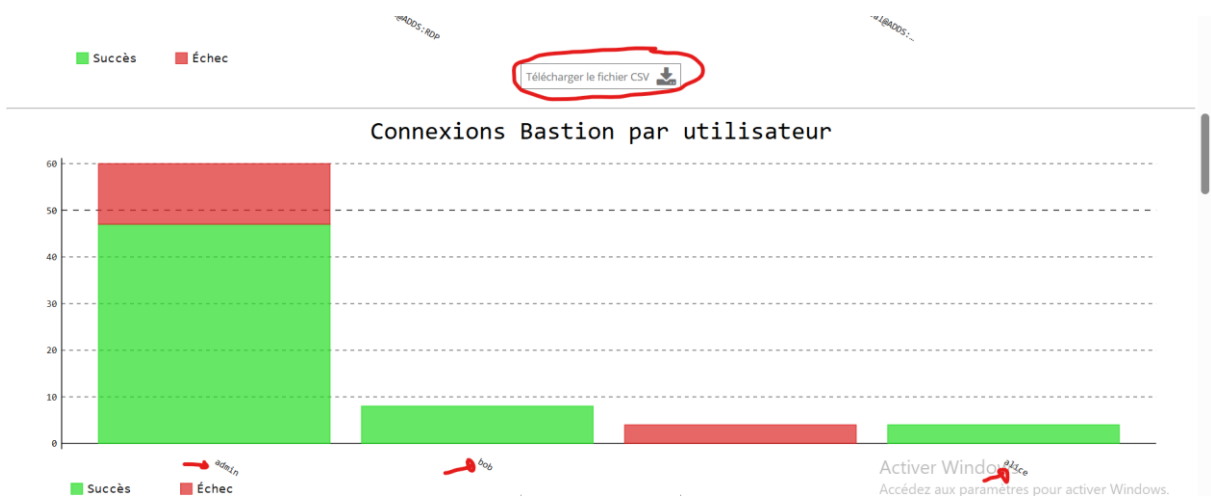
- Et nous aurons

Avec les paramètres suivants :	
Dates	2025-08-27 à 2025-08-29
TopN data	Top35

- la suite

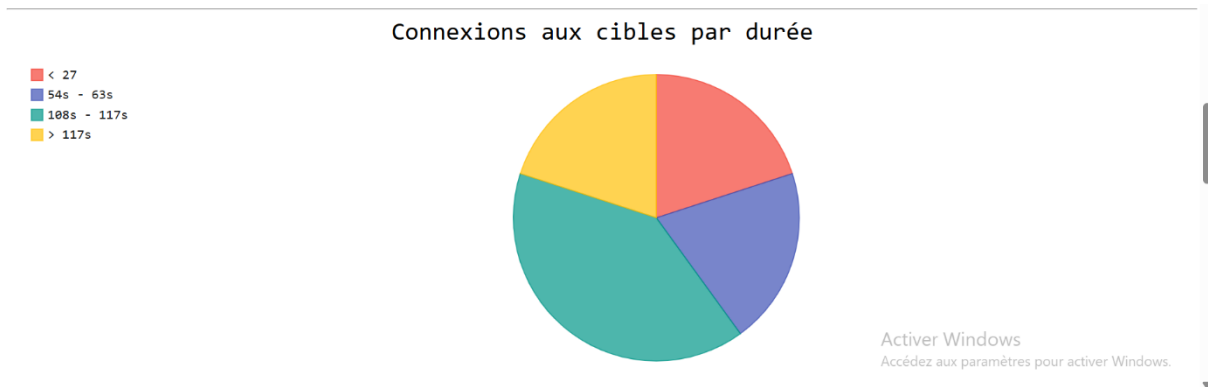


- Pour chaque catégorie de connexion nous avons les courbes qui vont avec

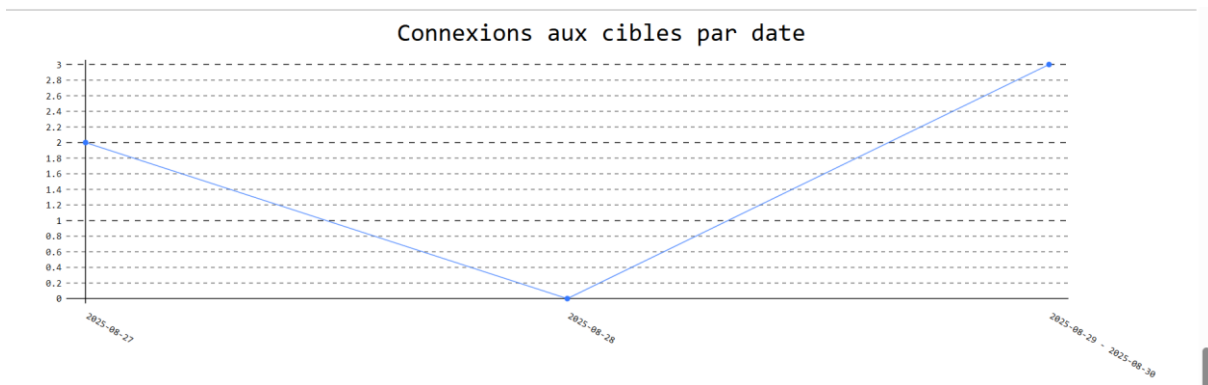


NB : On peut toujours télécharger ses statistiques pour chaque analyse

- 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 :