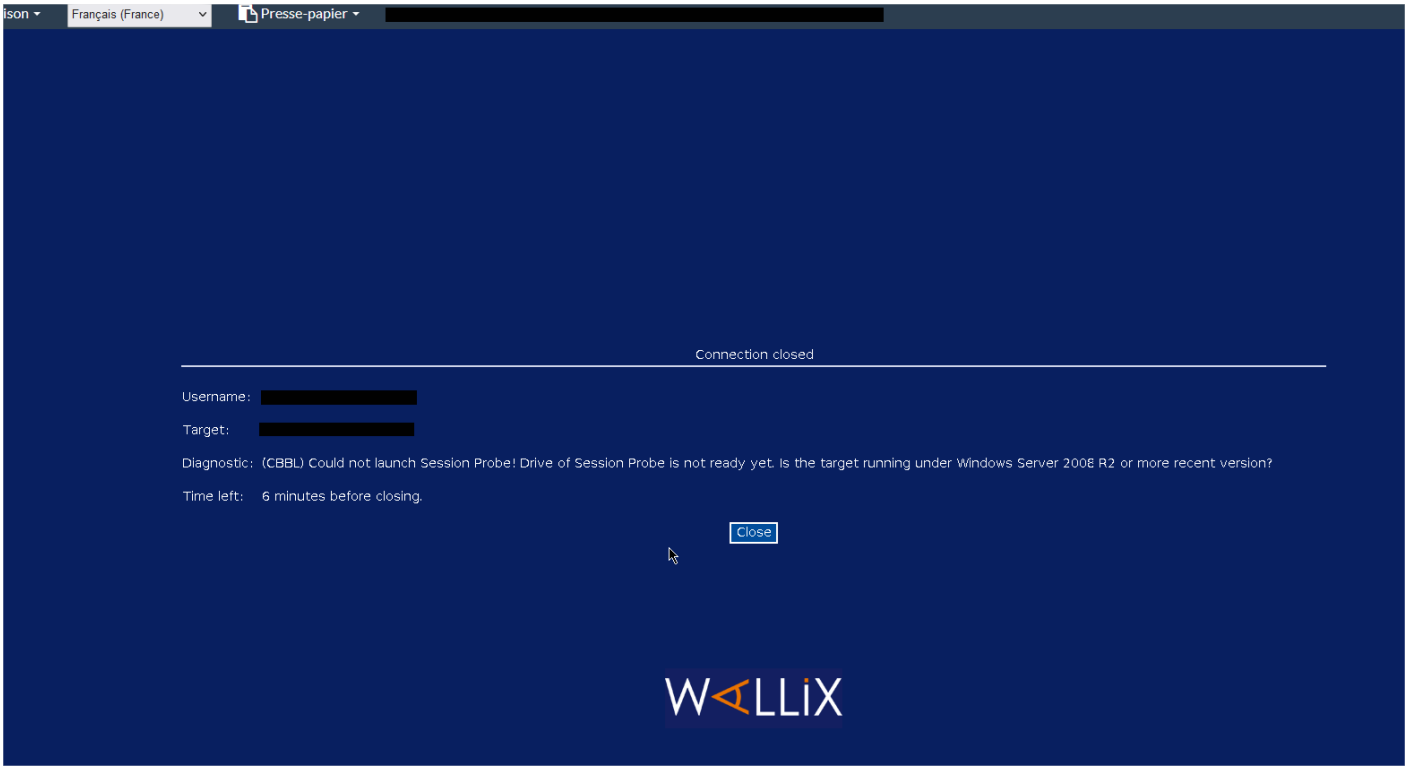
BASTION

- Incident - Session Probe Drive of Session Probe is not ready yet
- Bastion TMA
- Incident - TLS CERTIFICATE CHANGED

Incident - Session Probe Drive of Session Probe is not ready yet



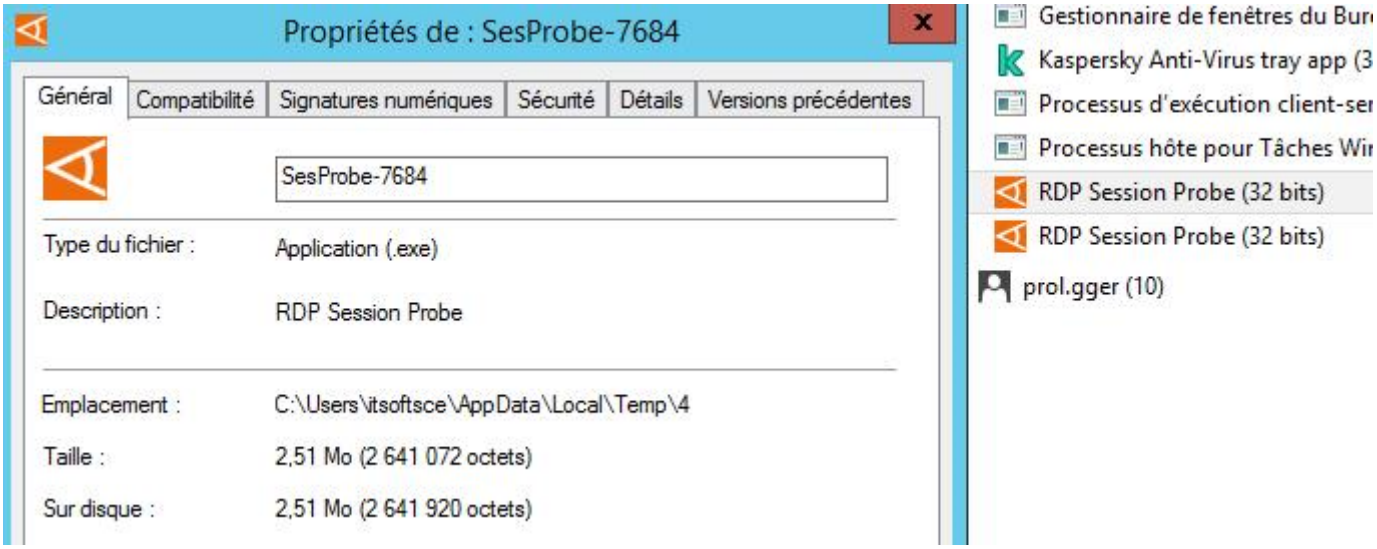
Erreur dans les logs :

> Aug 25 13:27:37 bastion1 rdpproxy[24076]: ERR (24076/24076) -- SessionProbeClipboardBasedLauncher :=> Drive of Session Probe is not ready yet. Is the target running under Windows Server 2008 R2 or more recent version?

> Aug 25 13:27:37 bastion1 rdpproxy[24076]: ERR (24076/24076) -- SessionProbeVirtualChannel::process_event_launch: Session Probe is not ready yet!

Pour l'erreur lié à la Session Probe, il y'avait une session "fantôme" itsoftsce en doublon avec peu 5 processus ouverts.
J'ai juste déconnecter l'utilisateur puis je me suis reconnecté depuis l'accès manager sans problème.

Quand, la session est ouverte depuis l'accès manager, cela ouvre deux processus SesProbe pour la session en cours comme sur la capture d'écran :



Note depuis le guide d'administration :

The session probe is loaded by a batch script. Without WALLIX Bastion, this script will cause the display of a non-user friendly black console window in the RDP session.
Moreover, the user may interact with it and disrupt the loading process.

Enabling the launch mask can block the display as well as mouse and keyboard inputs during the loading of the session probe loading phase. As a consequence, the console window becomes invisible.

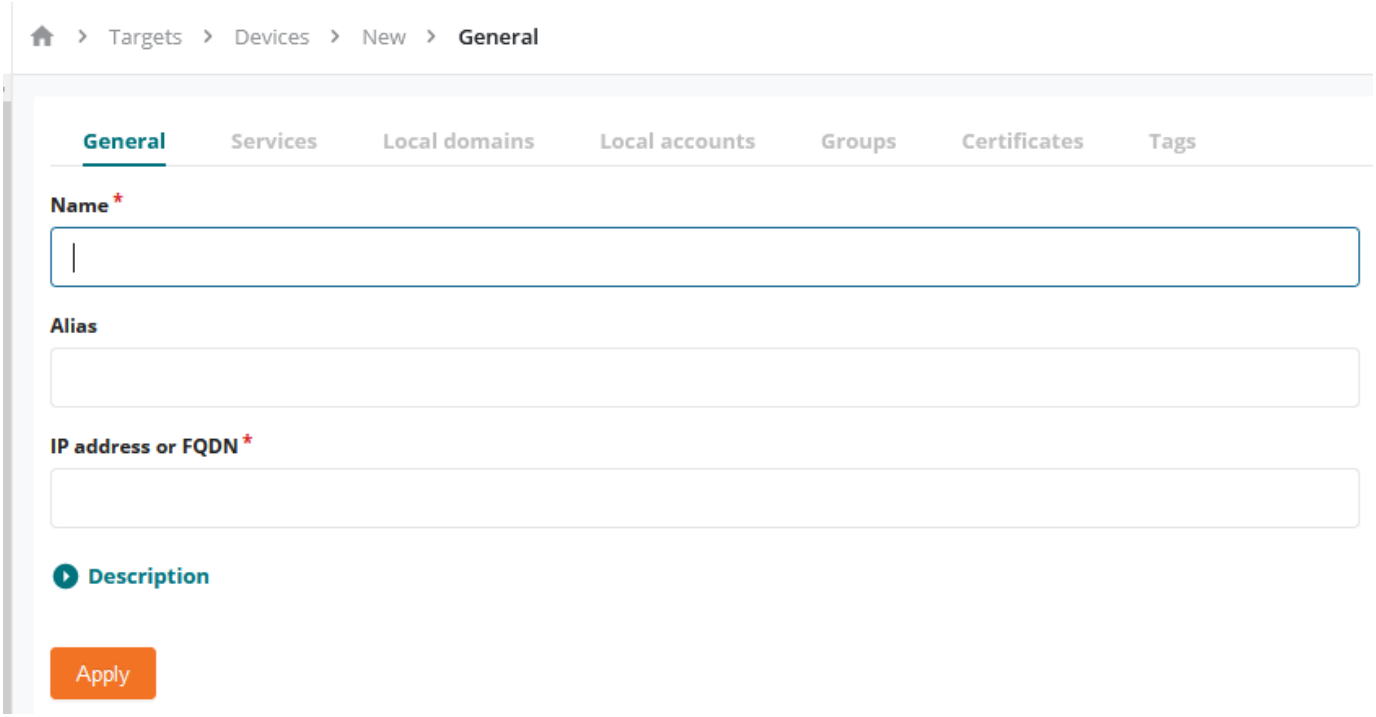
redirection of clipboard must be enabled by Terminal Services to be able to use the smart launcher (this is enabled by default).

Bastion TMA

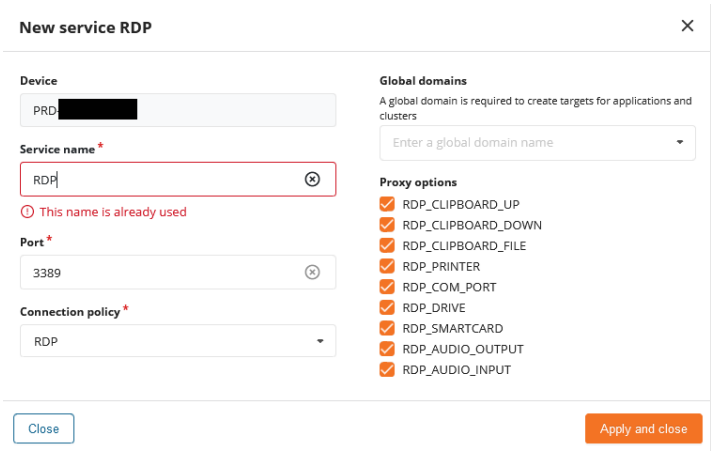
Interface d'admin :

Ajout des accès à des users à des serveurs non existants dans le bastion.

Ajout des serveurs:
Targets --> Devices --> Add



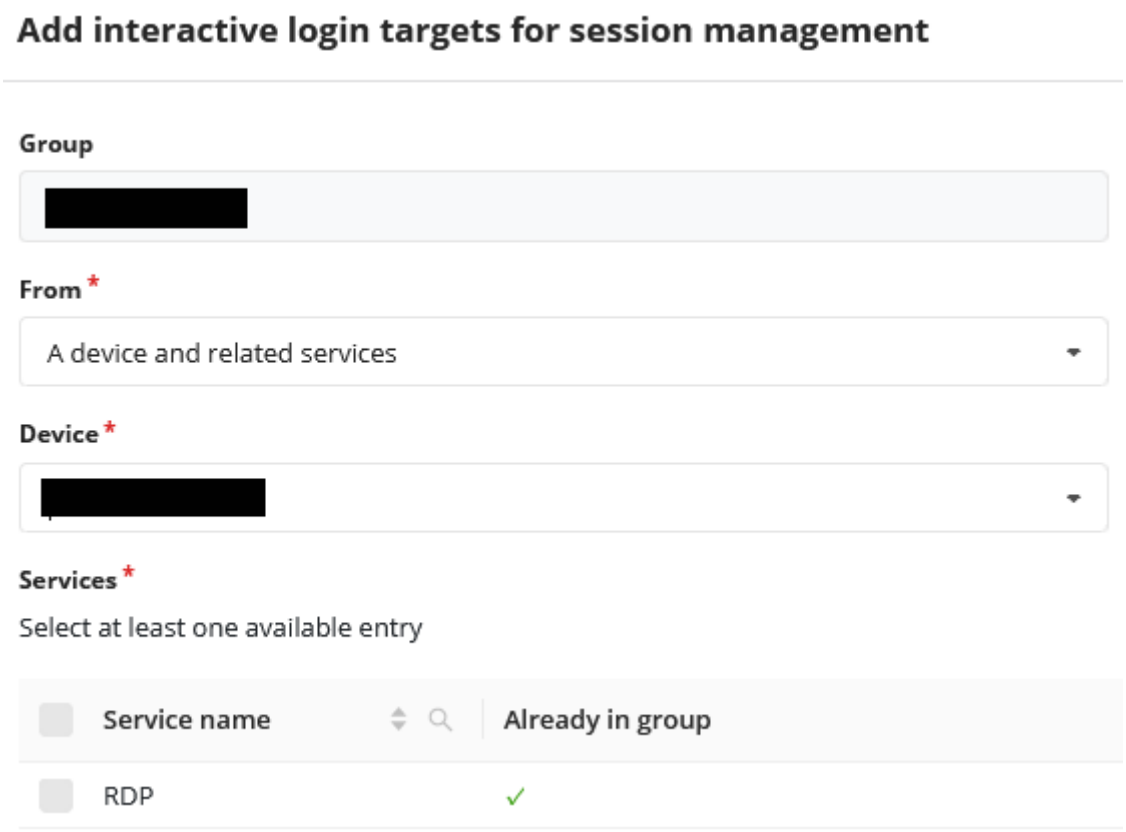
Mettre le nom du serveur et son IP puis cliquer sur apply.
Ensuite aller sur l'onglet services et cliquer sur ADD puis RDP pour serveurs Windows (SSH pour serveurs Linux)



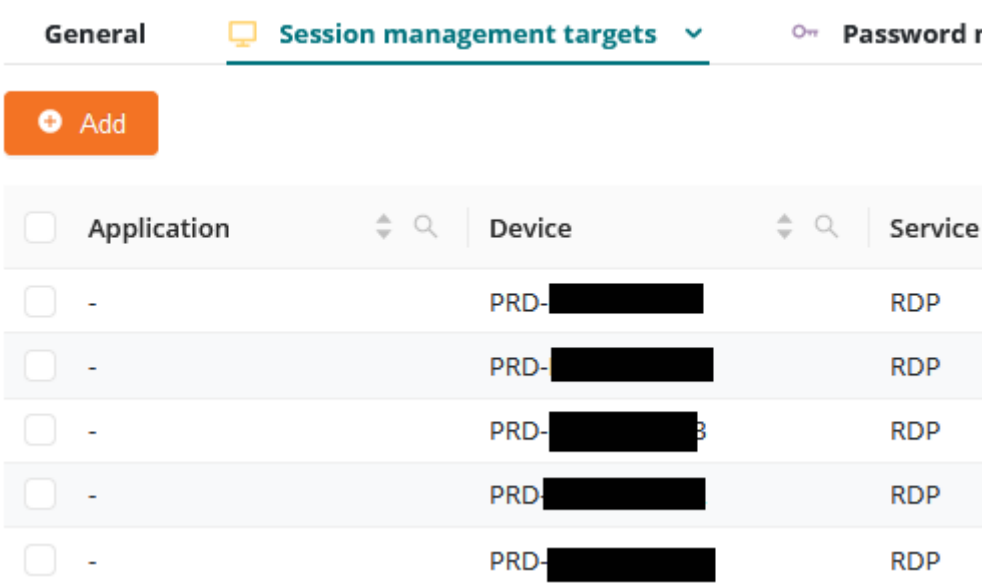
Faire apply and close. Ne pas prendre en compte l'erreur dans la PJ. La conf est déjà en place pour le serveur.

Création groupe de device :
Se rendre dans Targets --> Groups --> Add
Lui donner un nom puis apply

Aller sur l'onglet Session Management Targets puis interactive login:

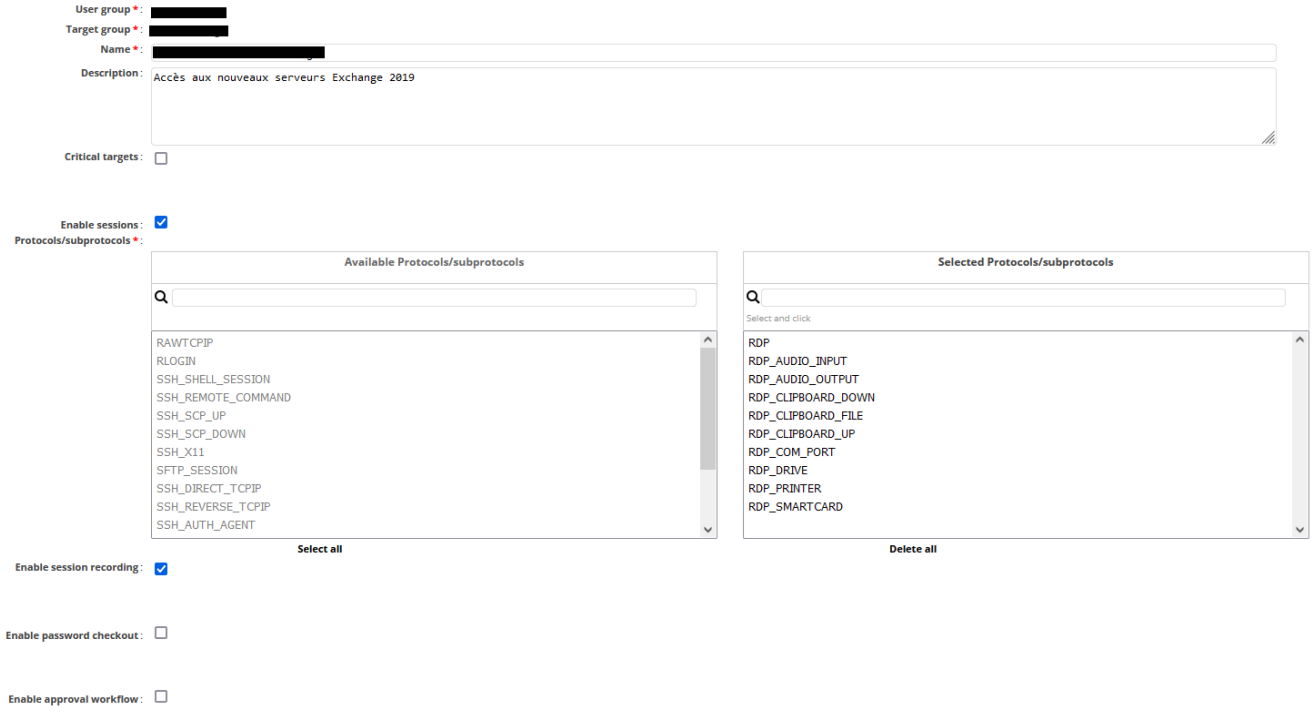


Penser à cocher RDP à chaque fois pour tous les serveurs.
Résultat final:



Attribution des accès aux users:

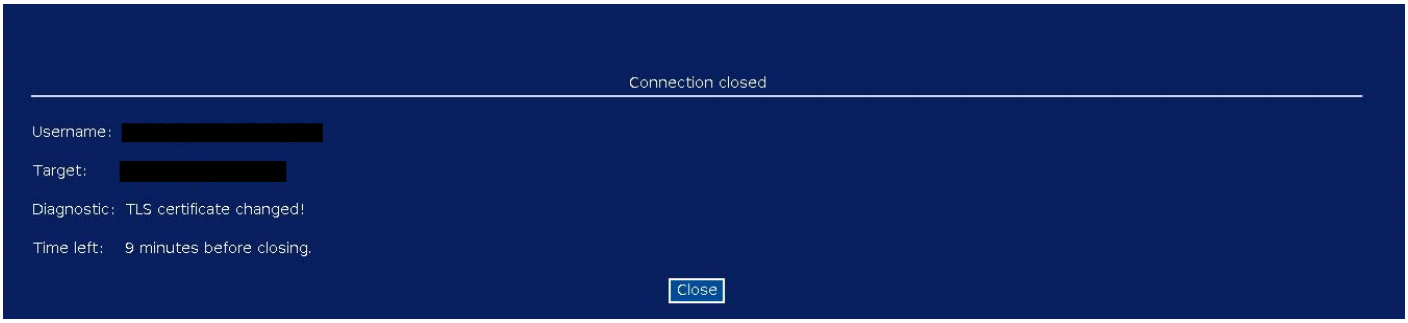
Aller dans Authorizations --> Manage authorizations --> + Add an autorisation



Demander de tester les accès.
Attention il faut que le port RDP 3389 soit ouvert entre les serveurs et le bastion TMA.

Incident - TLS CERTIFICATE CHANGED

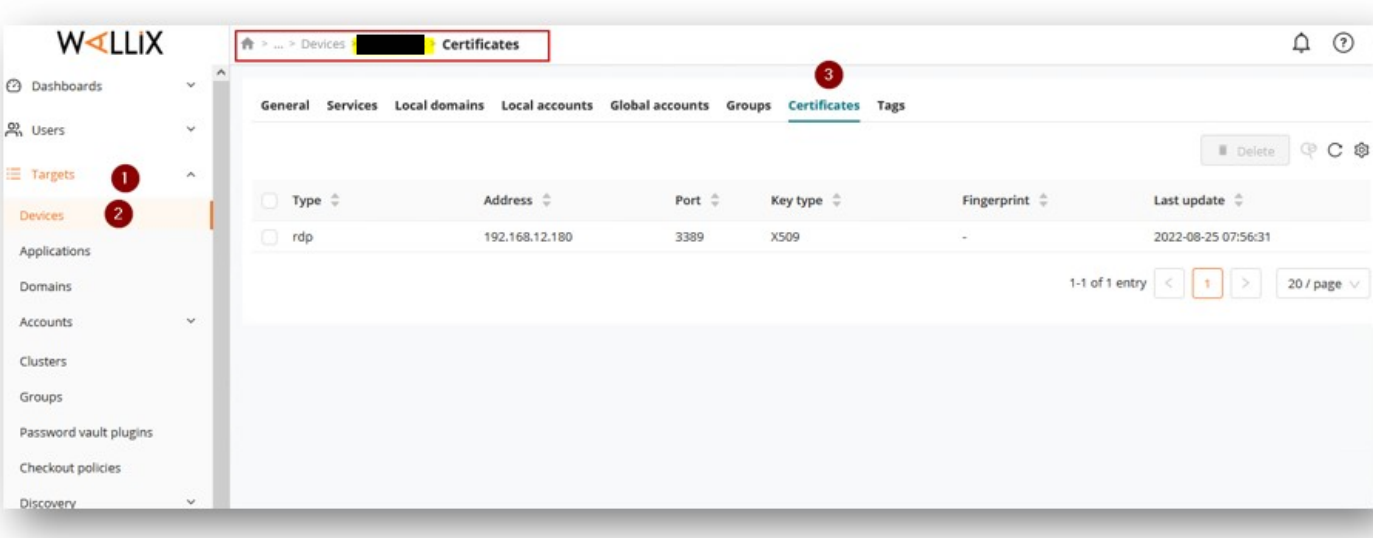
Type d'erreur :



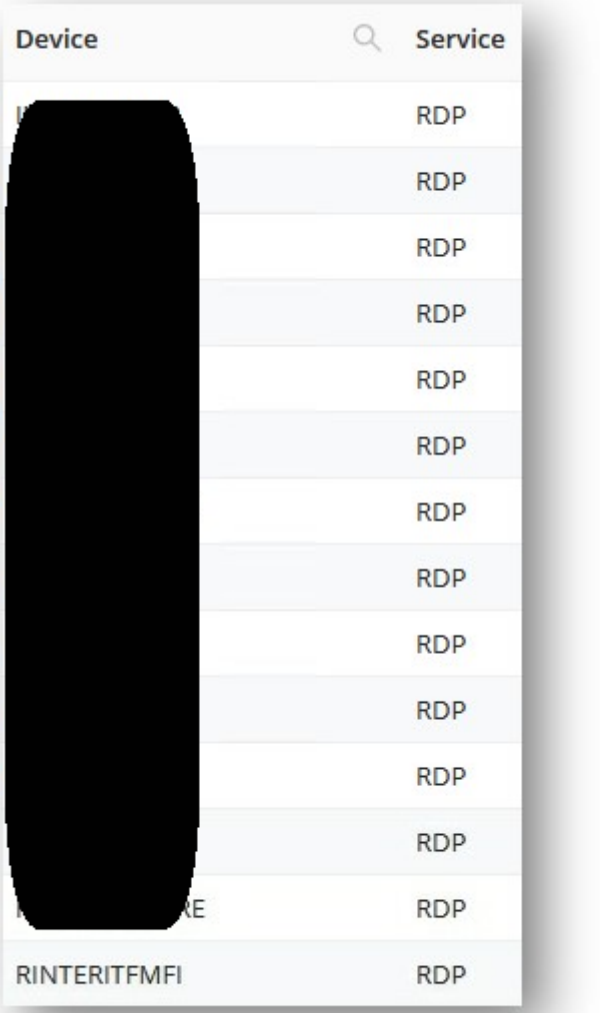
Suite à nos investigations et à l’appel auprès du support Wallix, les erreurs TLS_CERTIFICATE_CHANGED surviennent lorsque le serveur cible renouvelle son certificat de bureau à distance (RDP).
Le bastion ne remplace pas le certificat obsolète existant par le nouveau de la machine cible.

Le renouvellement est possible en supprimant en premier lieu le certificat dans le bastion et se reconnecter au serveur cible depuis l’accès utilisateur pour que le bastion récupère le nouveau certificat.
Il n’y a pas de réplication pour cette partie du certificat RDP pour la machine cible donc l’action de renouvellement du certificat RDP doit être effectuée sur les deux bastions.

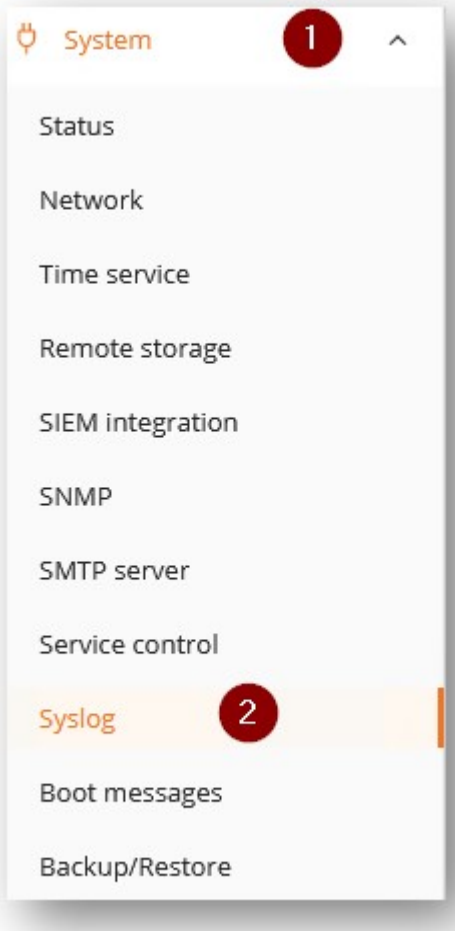
Note : Les certificats sont stockés localement sur les bastions à l’emplacement : /var/wab/cert/



J’ai vérifié et renouvelé sur les deux bastions lorsque cela a été nécessaire pour toutes les machines cibles du groupe AUTORISATION :



La connexion devrait être possible désormais pour les utilisateurs et le message TLS_CERTIFICATE_CHANGED ne devrait plus apparaître.
En complément, les détails de l’erreur apparaissent dans les logs du bastion dans System\Syslog.



Exemple de l’erreur :

Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- SSL_get_peer_certificate()
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate directory is: '/var/wab/cert/18074c309afb7897005056a2a787'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- certificate file is: '/var/wab/cert/18074c309afb7897005056a2a787/rdp,192.168.12.100,3389,X509.pem'
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- nb1=1107 nb2=1107
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509 existing::issuer=CN = INTER
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509 existing::subject=CN = INTER
Aug 24 12:57:43 bastion1 rdpproxy[12837]: INFO (12837/12837) -- TLS::X509