



Les BONNES PRATIQUES de sécurité avec votre serveur bureau distant TS2log

Les dégâts et préjudices financiers des cybers attaques sont malheureusement un constat récurrent et cet état de fait nous amène à vous communiquer les bonnes pratiques à mettre en place dans votre environnement informatique Terminal Serveur TS2log.

En effet, outre les solutions antivirus ou encore TS2log Security qui renforcent votre arsenal sécuritaire au niveau des serveurs, il s'avère indispensable de mettre en œuvre une politique de sécurité globale efficace.

Dans un souci de conseil auprès de nos clients, veuillez trouver ci-dessous nos recommandations pour la sécurisation de votre serveur Bureau à Distance ou applicatif.

Ces conseils s'adressent aux utilisateurs de notre solution d'accès à distance TS2log, mais également aux autres solutions d'accès à distance Multi-sessions et multi-utilisateurs comme par exemple TSE et Citrix.

LES UTILISATEURS :

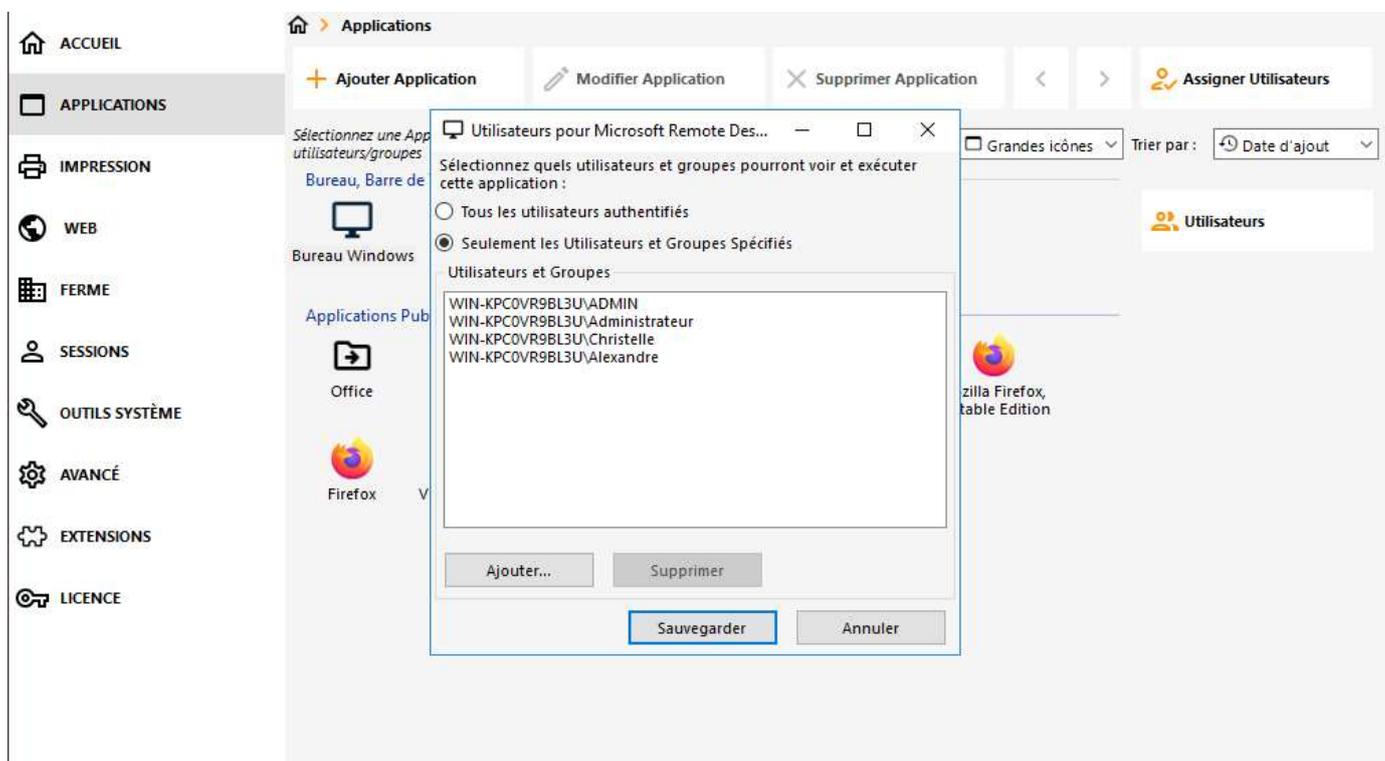
Assigner uniquement les utilisateurs qui doivent avoir un accès au serveur. Par défaut, tous les utilisateurs peuvent ouvrir une session à distance et accéder au Bureau de leur session Windows.

Dans AdminTool > Applications : double-cliquer sur une application publiée puis sélectionner les utilisateurs ou les groupes d'utilisateurs via le bouton 'Ajouter'.

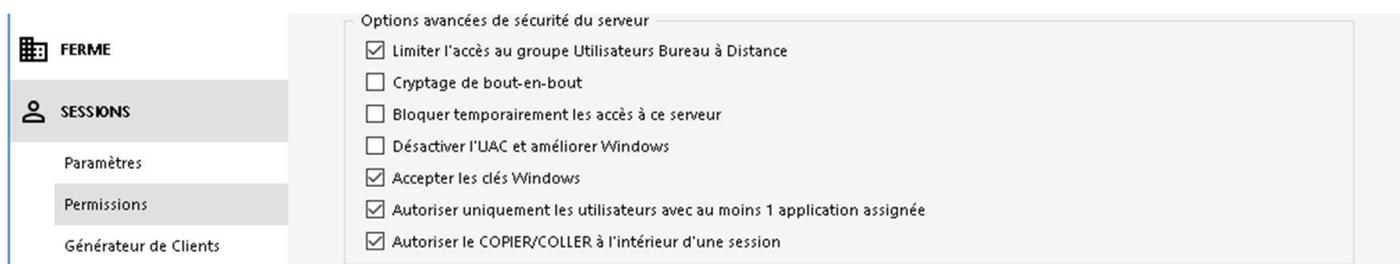
Pour donner accès à la session Windows complète, donc au Bureau, il faudra sélectionner l'application 'Microsoft Remote Desktop'.

Vérifier que le compte Administrateur dispose bien de l'application 'Microsoft Remote Desktop'.

Pour valider, cliquer sur le bouton 'sauvegarder' dans la fenêtre d'assignation.



Dans AdminTool > Sessions > Permissions : cocher la case 'Autoriser uniquement les utilisateurs avec au moins 1 application assignée'.



Désactiver le compte 'invité' ou changer son mot de passe.

Par défaut, le compte invité de Windows est activé. Ce compte ne dispose pas de mot de passe. Si le serveur est accessible depuis l'extérieur, il sera donc très facile d'ouvrir une session, d'accéder aux ressources ou d'exécuter des applications.

Par exemple il sera aisé d'exécuter un fichier Excel dont la macro supprimera ou cryptera des données sur le serveur.

Utiliser une stratégie de mot de passe forte.

Le mécanisme de sécurité Windows ne bloquera pas les tentatives de connexion avec un mot de passe erroné.

Les robots pourront donc effectuer autant de tentatives qu'ils le désirent, jusqu'à ce qu'ils trouvent le mot de passe et accèdent au serveur.

- Un mot de passe faible comme 'Jacques' ou 'AZEQSDWXC' sera 'cassé' dans la minute.
- Un mot de passe comme 'Nicole1225' prendrait plusieurs heures, si une partie du mot de passe n'est pas contenue dans le nom du profil Windows.
- Un mot de passe fort, par exemple '#45HoustonQHI75' ou 'Je mange des Chips à 11H !' ne sera pas 'cassé' avant plusieurs mois.

Les applications de gestion de mot de passe sont un bon moyen de renforcer la sécurité, car on n'a pas à se souvenir de chaque mot de passe. Cette stratégie devrait être appliquée aux mots de passe de messagerie, aux comptes marchands sur Internet, ...

LES ACCÈS :

Sécuriser les accès Web avec le certificat SSL.

TS2log Édition Mobile est livrée avec un module permettant de générer et d'utiliser une connexion cryptée et sécurisée entre le navigateur de l'utilisateur et le serveur.

Son déploiement est très simple, il suffit de disposer d'un nom de domaine et de rediriger ce dernier vers l'adresse ip publique du serveur (voir onglet 'Accueil', 'IP Publique').

Pour déployer le certificat SSL gratuit, ouvrir AdminTool > Web > HTTPS > Générer un certificat HTTPS gratuit.

Sécuriser les accès RDP en n'exposant pas le port par défaut.

Sur tous les systèmes d'exploitation, le port Connexion Bureau à Distance par défaut est le port TCP 3389.

Il est donc recommandé de modifier la règle de redirection du routeur / Box ADSL et configurer un port d'écoute RDP différent. Pour les connexions locales, au sein d'un réseau d'entreprise, ce port peut être utilisé.

Pour les connexions distantes, à l'extérieur du réseau, il faudra privilégier l'utilisation d'un port d'écoute public différent. En effet, le port public 3389 sera le premier port testé par les robots à la recherche d'une faille de sécurité.

Vérifier les ressources locales partagées.

Plus de 80% des attaques proviennent de l'intérieur d'un réseau (dépôt de fichiers malveillants, pièces-jointes de mails non vérifiées, base antivirus obsolète). Nous préconisons de vérifier régulièrement l'état de l'antivirus sur le serveur, de vérifier les droits d'accès aux ressources partagées ainsi que la sauvegarde.

Sur l'ordinateur utilisateur, il faudra vérifier régulièrement l'état de l'antivirus, surtout si l'utilisateur partage ses ressources locales avec le serveur distant, comme la remontée des disques locaux ou des supports amovibles comme une clé USB.

Sur les ordinateurs clients, il est fortement conseillé de disposer d'une solution antivirus disposant d'un module anti-ransomware, comme MalwareBytes Premium, Bitdefender, TotalAV ou encore ESET.

En cas de doute sur la sécurisation de vos serveurs, ou si vous avez une question d'ordre technique, n'hésitez pas à solliciter notre support technique :

<https://ts2log.com/demande-de-support/>

Nous vous invitons également à consulter la page dédiée à notre solution de sécurisation des serveurs Bureaux Distants TS2log Security : <https://ts2log.com/ts2log-security/>

LES MISES À JOUR

Mises à jour antivirales :

Il est extrêmement important de disposer d'une solution antivirus / anti-ransomware sur un serveur accessible depuis l'extérieur.

Cette solution de sécurité devra être à jour et active.

Certaines solutions antivirales désactivent le pare-feu Windows et peuvent potentiellement nuire à la sécurité si un ou plusieurs de leurs composants sont désactivés ou obsolètes.

Mises à jour Windows :

Les mises à jour Windows ne devraient pas être appliquées de manière automatique, mais planifiées. Par exemple deux fois par mois.

Certaines mises à jour appliquées de manières automatiques vont désactiver des services avant leur application.

Si le serveur n'est pas redémarré de manière automatique, ou parce que ce dernier est exploité par les utilisateurs, des failles de sécurité peuvent se produire jusqu'au prochain redémarrage.

Le serveur peut également avoir un comportement différent de son état normal.

Il sera également important d'appliquer uniquement les mises à jour importantes ou critiques préconisées par Windows Update. L'application des mises à jour 'Preview' n'est pas recommandée sur les serveurs en production.

Après l'application des mises à jour Windows, il est fortement recommandé de redémarrer le serveur et de vérifier que l'accès à distance fonctionne correctement.

Mises à jour TS2log :

Nous vous invitons à vérifier régulièrement la disponibilité des mises à jour de TS2log. Nous préconisons une vérification au moins une fois par trimestre, afin de disposer d'un produit toujours à jour, sécurisé et disposant des dernières fonctionnalités et correctifs. Pour vérifier la mise à jour, ouvrir AdminTool > ACCUEIL > la version actuelle et la version disponible pour la mise à jour sont affichées. Une croix rouge indique qu'une nouvelle version est disponible, une coche verte que vous utilisez la dernière version. L'historique des mises à jour TS2log sont disponibles depuis la page <https://ts2log.com/changelog-ts2log-remote-access/>