Bonnes pratiques 2

Au fil de l’évolution des différentes versions de Windows 10, je m’aperçois qu’il est nécessaire d’adapter la façon de configurer les autorisations sur le (registre) ainsi que sur le (services composants) afin de limiter les erreurs et les avertissements du journal Windows et à terme de limiter les disfonctionnements.

Il est certain que nous avons tous une façon propre pour l’installation d’un PC et que ces anomalies n’ont généralement pas d’impacts sur le bon fonctionnement des machines.

Personnellement et après l’installation de Windows je fais en sorte qu’un seul compte soit correct et seulement après j’ajoute les autre comptes ainsi que toutes autres connexion avec d’autres PC.

Je prends comme objectif à partir d’une installation basique et d’un seul compte local, arriver à n’obtenir aucune erreur et un minimum d’avertissement.

Donc je démarre ce sujet afin de confronter nos différents points de vue.

Partons d’une installation propre, avec les différents logiciels utilisés couramment comme, Antivirus (pour Windows 10 **Windows defender** suffit largement pour une utilisation courante) messageries, traitement de texte, logiciel photo, jeux, AcrobatReader, VLC, imprimante / scanner…, ainsi que la totalité des raccourcis d’applications installés et vérifiés.

 MAJ complètes, DISM ET scannow, clean ainsi que ZHPCleaner.

Le but étant, après avoir utilisé la totalité des fonctions durant environ 3 ou 4 jours, et arriver à ça :



Au temp dire que pour arriver à ce résultat, j’ai galéré un certain temps.

La version que j’utilise étant : Windows 10 Famille, 21H1.

Version système d’exploitation : 19043.962

Avant de rentrer dans le vif du sujet

Il est nécessaire de commencer par les attributions des autorisations.

Tout d’abord on se rend sur le disque C :

Clic droit sur C: (en admin)/propriétés/onglet Sécurité. Dans le panneau qui s’ouvre (Noms de groupes ou d’utilisateurs)

Utilisateurs authentifiés, Système, et Administrateurs (DESTOP-NVLU2xx) en contrôle total.

Pour Utilisateurs (DESKTOP-NVLU2xx\Utilisateurs) je sélectionne la ligne, clic sur Avancé puis accès effectif et sélectionner un Utilisateur, Dans les paramètres de sécurité avancés qui vient de s’ouvrir, clic sur Avancé, Rechercher et double-clic sur le nom du compte suivi de l’adresse si l’installation a été créé à partir d’un compte Microsoft. Puis OK

On peut vérifier en cliquant sur Afficher l’accès effectif que tout est vert.

Par contre en revenant aux propriétés de disque C : on voit que l’utilisateur (DESKTOP-NVLU2xxx) n’a pas le contrôle total.

Ceci afin d’obtenir une certaine forme de garde-fou. Je ne nomme pas l’administrateur, car le degré de sécurité en pâtirait.

Ensuite obtenir le contrôle total de Windows PowerShell Pour l’utilisateur.

Redémarrage du système, repérer l’heure du redémarrage, utilisé les différents programmes et vérifier sur le journal les événements qui se sont produit (penser également à relancer les MAJ)

Sur le journal on trouve généralement un certain nombre d’erreurs,

Je prends un exemple courant :

Les paramètres d’autorisation propres à l’application n’accordent pas l’autorisation Local Activation pour l’application serveur COM avec le CLSID

{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}

 et l’APPID

{15C20B67-12E7-4BB6-92BB-7AFF07997402}

 au SID DESKTOP-NVLU2Q7\jipid de l’utilisateur (S-1-5-21-4165693624-2675432978-306845691-1001) depuis l’adresse LocalHost (avec LRPC) s’exécutant dans le SID Non disponible du conteneur d’applications (Non disponible). Cette autorisation de sécurité peut être modifiée à l’aide de l’outil d’administration Services de composants.

En premier lieux faut s’octroyer les autorisations CLSID et APPID au niveau du registre.

Après, Sur la partie droite du Registre on peut trouver le nom de l’application qui pose problème.

Ici : PerAppRuntimeBroker

Ainsi que la clé APPID : 15C20B67-12E7-4BB6-92BB-7AFF07997402

On note le nom (PerAppRutimeBroker) pour la rechercher dans le service composant.

Dans services composant développer ordinateur, poste de travail, configuration DCOM

Clic sur détail, on trouve dans la liste PerAppRutimeBroker, dans les détails on doit retrouver le N° d’e la clé.

Clic droit sur la clé, et sécurité.

Et c’est à partir de là que les difficultés commencent :

Bien sur le but étant de s’approprier les autorisations, mes pas que !

Il faut vérifier les onglets : Général, emplacement, point de terminaisons, identité.

Faut également vérifier Autorisations d’exécution, Autorisations d’accès, Autorisation de config. Dans l’onglet Sécurité.

S’assurer que l’exécution processeur na rien bloqué.

Je le répète, ceci n’est qu’un exemple qui à partir de là mérite pas mal de recherches.

Si vous avez des idées, elles seront les bienvenues.