|  |  |
| --- | --- |
| formation-informatique-grenoble-cabare  http://[WWW.CABARE.NET](http://WWW.CABARE.NET) **©** | **Système Windows 10 Pro – sys XX – Sécurisation -** |
| **Installation Administration Windows**  **Michel Cabaré – Ver 1.0 – mai 2018-** |
|  |  |

**Systèmes Windows**

**Sécurisation**

**Michel Cabaré – Ver 1.0 – Mai 2018**

[www.cabare.net](http://www.cabare.net) ©

**table des matiÈres**

1-CNIL guide pour employeurs et salaries (2010) 4

Mail définition perso - pro 4

Fichier – Dossier définition perso - pro 4

Accès Par l'administrateur à un fichier Dossier perso 4

Connaître le mot de passe d'un Utilisateur 4

2-CNIL Sécurité des données personelles (2018) 5

Préconisations "à faire ": 5

Préconisations "à ne pas faire ": 5

Préconisations GPRD: 6

Mot de Passe Administrateur 7

Compte Administrateur 7

Fichiers stockés 7

Poste de travail à jour – y compris les applications : 7

Cartographie Réseau – accès internet: 8

Gestion des comptes Utilisateur: 8

Gestion des Ports USB : 8

Infection Virus: 8

Prise en main à distance: 8

Accès Réseau - WIFI: 9

Accès Site Web : 9

Transfert de données vers l'exterieur : 9

2-ANSSI Charte d'utilisaton (06-2017) 10

Charte d'utilisation des moyens informatiques et des outils numériques 10

Opposabilité 10

3- ANSSI Guide des bonnes pratiques (01-2017) 11

Guide des bonnes pratiques de l'informatique : 11

4- ANSSI Guide d'hygiène informatique (01-2017) 12

Renforcer la sécurité de son système d'information : 12

Connaitre le système d'information 12

Sensibiliser les utilisateurs aux bonnes pratiques 12

Si infogérence exterieure 12

Organiser la connexion au réseau aux équipements maitrisés 12

Authentifier et Controller les accès 12

Identifier chaque administrateur 12

Authentifier et Contrôler les accès 14

Sécuriser les postes 14

Sécuriser le réseau 15

Sécuriser l'administration 15

5-ANSSI Recommandations mot de passe (06-2012) 16

8 règles pour gérer les mots de passe 16

Bon mot de passe 16

Gestion Windows 17

Windows Kerberos / NTLMv2 18

6-ANSSI Recommandations relative à l'administration (04-2018) 20

Administration Sécurisée des systèmes d'information 20

Le poste administrateur 20

7-ANSSI préocupations relatives au respect vie privéee avec Widows 10 (07-2017) 22

Respect de la vie privée et confidentialité des données avec Windows 10 22

Télémétrie (p 5) 22

Cortana (p 8) 22

Experience Utilisateur – Desktop Search (p 8) 23

Applications universelles - Tuiles (p11) 23

Compte Microsoft - 23

Drive - 23

Microsoft - Gérer les connexions du système (01-2018) 24

Connexions aux services microsoft 24

SCT Security Compliance Toolkit et LGPO 24

# 1-CNIL guide pour employeurs et salaries (2010)

## Mail définition perso - pro

Sauf mention explicite "personnel" dans l'objet du message, les mails sont professionnels

Cela peut aussi être le mot "personnel" dans l nom du dossier dans lequel le mail est stocké.

Et les administrateurs ont un droit d'accès

## Fichier – Dossier définition perso - pro

Sauf mention explicite, les fichiers dossiers sont pro

Il faut clairement se mettre d'accord sur ce qui différencie un fichier perso d'un pro. Par exemple les initiales ou un dossier nominatif ne suffisent pas à définir l'aspect personnel de la ressource

* Il faut l'inscrire dans la charte d'utilisation des moyens informatiques

## Accès Par l'administrateur à un fichier Dossier perso

Un administrateur ne peut accéder à un fichier perso :

* qu'en présence du salarié,
* ou après notification-contact téléphonique préalable.

Le salarié ne peut s'y opposer ensuite !

* ou en cas d'évènement particulier !!!! cela sera au juge a apprécier

## Connaître le mot de passe d'un Utilisateur

Les identifiants et les mots de passe sont personnels, et non connus de l'employeur

Mais si il faut accéder au poste d'un absent, pour avoir des informations indispensables a la poursuite du fonctionnement de l'activité alors l'employeur peut exiger les codes, ou l'administrateur peut les changer.

# 2-CNIL Sécurité des données personelles (2018)

## Préconisations "à faire ":

Veille écran automatique + mot de passe en sortie

* GPO possible

Nécessité de rétablir une machine en l'état ?

* Image Système Windows + WinRE

Nécessité de sécuriser l'accès physique à une machine ?

Nécessité de sécuriser le vol d'une machine ?

* Conséquences d'un vol de machine ?

## Préconisations "à ne pas faire ":

Pas de données locales

* GPO redirection Bureau ou Mes documents
* Si obligé Sauvegarde intégrée fichiers Windows 10

Pas de Données non cryptées sur port USB / chiffrement des lecteurs amovibles

* Montage Volume **AxCrypt** ou cryptage de fichier **VeraCrypt**

Jamais déplacer un ordi lors d'une réaffectation, mais le désinstaller- réinstaller

* Outils de formatage / effacement données (même si reinstallation)
* Formatage de bas niveau ?

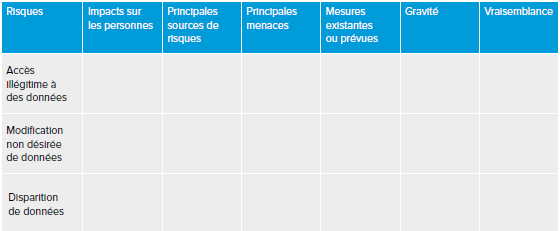
Jamais sortir un ordi, un disque dur pour "don", mais le désinstaller- réinstaller

Jamais laisser les sauvegardes en lignes " accessibles via le reseau", - au mins un jeu est stocké "hors ligne"

* Toujours une procédure de récupération "manuelle" / Exceptionnelle avec une authentification particulière
* Vérifier durée longévité des sauvegardes (CD 5 ans)

## Préconisations GPRD:

Pour evaluer la problematique, un tableau du genre



1-ANSSI les Fondamentaux

## Mot de Passe Administrateur

Sur cette question, plusieurs remarques

* Combien de personnes possèdent un tel mot de passe
  + Liste de toutes les personnes
* Partage de compte entre personnes ?
  + Le partage de compte est au minimum à quantifier, mais mieux à proscrire
* Partage de mot de passe ?
  + Le partage de mot de passe est à proscrire

## Compte Administrateur

Inventorier la liste des comptes administrateurs

Lorsqu'un administrateur travaille à autre chose qu'à des taches d'administration, quel type de compte utilise t il ?

* UAC User Accès Control
  + +RunAs + Clic Droit/Executer en tant que

## Fichiers stockés

Qui fait quoi avec ces fichiers ?

* Audit - Observateur d'évènement
* FSRM -
  + traque modification type de fichier
  + interdit le stockage de certains fichiers
  + empêche l'exécution de certains fichiers
  + journal des derniers accès

**https://docs.microsoft.com/fr-fr/windows-server/storage/fsrm/schedule-set-of-reports**

## Poste de travail à jour – y compris les applications :

Problématique des MAJ

* WSUS avec le protocole TLS/SSL sur le réseau, afin de ne pas pouvoir éditer les binaires via une attaque de l’homme-du-milieu. Avoir un serveur WSUS pour chaque niveau de l’architecture niveau de sécurité à atteindre
  + Machines hors branches
  + Machines Hors OS
  + Isolation / surveillance accrue
* Applications ?

## Cartographie Réseau – accès internet:

Vrai cartographie du Réseau +

* Ou sont les accès Internet ?
* Protection de chaque Accès

## Gestion des comptes Utilisateur:

Vie du compte d'un utilisateur

* Fiche – procédure destruction de compte
* Fiche procédure Désactivation de compte
  + PAM Priviledge Access management (2016)

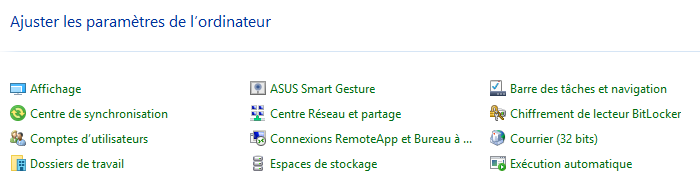
## Gestion des Ports USB :

Désactivation autorun sur Périph"rique USB

* Gpo Autorun et GPO Autoplay

http://www.thewindowsclub.com/enable-disable-autoplay-windows

Panneau de configuration / Execution automatique



## Infection Virus:

Après un virus détecté sur une machine

* Scan des autres postes

## Prise en main à distance:

Un utilisateur doit toujours valider la prise en main sur son poste ( même par un simple OK)

Un utilisateur doit savoir quand la prise en main sur sa machine est en cours sur sa machine

Un utilisateur doit savoir quand la prise en main sur sa machine se termine (même par un simple message)

## Accès Réseau - WIFI:

Séparer le réseau WIFI des invités du reseau interne

Chiffrement WIFI WPA2 ou WPA2-PSK avec mot de passe complexe (Proscrire WPA)

Accès Réseau via Internet par TLS/SSL, ou VPN (proscrire telnet,

## Accès Site Web :

Utliser TLS/SSL

Limiter les ports de communication que 443, bloquer tous les autres

Ne pas passer dans une URL des identifiants

Ne pas utiliser des serveurs comme site de travail (surtout pour messagerie ou accès web)

## Transfert de données vers l'exterieur :

Chiffrer les données avant stockage sur CD – DVD

Envois de la clé par une autre canal

Utiliser HTPS et SFTP uniquement

# 2-ANSSI Charte d'utilisaton (06-2017)

## Charte d'utilisation des moyens informatiques et des outils numériques

Permet de définir 4 axes:

* Usages permis
  + Peut on utiliser internet à titre privé
* Règles de Sécurité
  + Peut on transférer des fichiers x clé USB
  + Peut on transférer des fichiers par pièce jointe d'Email
* Mesures de contrôle
* Sanctions possibles
  + Echelle de sanctions

Et les droits el les devoirs des Utilisateurs

Les administrateurs peuvent être traités à part, avec une charte spécifique pour eux

Pas BYOD

## Opposabilité

A faire signer par les Utilisateurs

A incorporer dans les contrats des sous traitants ou des entreprises

Si non signée – non opposable !

# 3- ANSSI Guide des bonnes pratiques (01-2017)

## Guide des bonnes pratiques de l'informatique :

En plus de ce que l'on a pu dire jusqu'à présent

Attention aux accès smartphone professionnels

Attentions aux accès des applications installés dessus

Désactivation bluetooth

Ne jamais utiliser une Clé USB à l'exterieur, puis à l'intérieur de l'entreprise

Ne jamais utiliser une Clé USb "offerte"

Avant de partir, modifier le mot de passe administrateur local, , le remodifier en rentrant

Ne télécharger que des soft depuis le site editeur, jamais depuis des sites tiers

# 4- ANSSI Guide d'hygiène informatique (01-2017)

## Renforcer la sécurité de son système d'information :

En plus de ce que l'on a pu dire jusqu'à présent

## Connaitre le système d'information

Former ou faire des fiches sur les mesures mises en œuvre

Surtout pour les externes

### Sensibiliser les utilisateurs aux bonnes pratiques

* Connexion possible d'équipement personnels au réseau d'entreprise ?
* Signature de la charte pour opposabilité

### Si infogérence exterieure

* Conformité des pratiques de sécurité apportée par la structure ?
* Hébergement cloud à proscrire

### Organiser la connexion au réseau aux équipements maitrisés

Ne jamais faire utiliser de BYOD

Ni de Cloud

## Authentifier et Controller les accès

En plus de ce que l'on a pu dire jusqu'à présent

### Identifier chaque administrateur

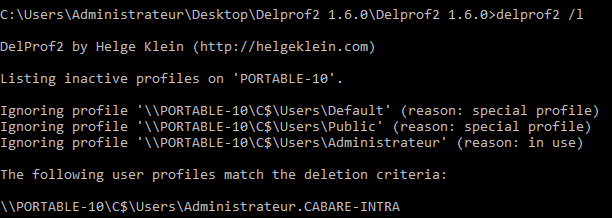
Ne jamais se loguer en tant qu'administrateur sur un poste autre que un poste securisé (bureau fermable et accès protégé) sinon effacer le profil !

Base de registre

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList

Nouvel utilitaire

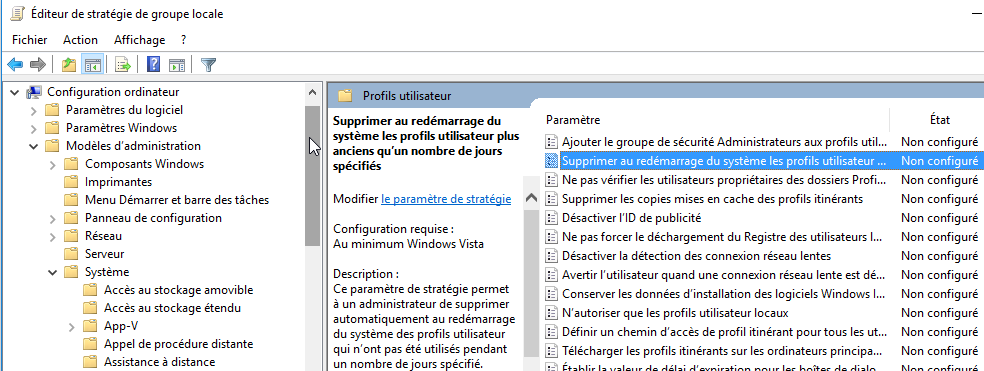




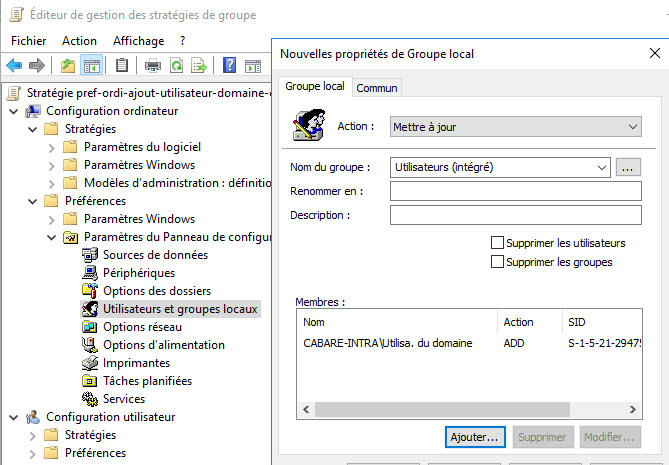
Suivit de



Nouvlle fonctionnalité de la GPO



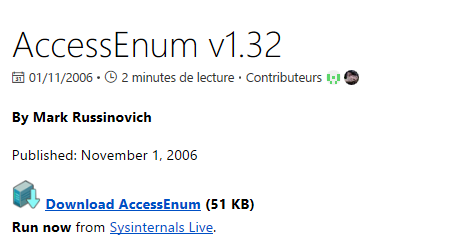
Mais il faut absolument ajouter les comptes utilisateur du domaine dans le groupe local des utilisateurs (voire invité)

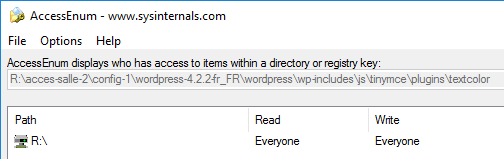


### Authentifier et Contrôler les accès

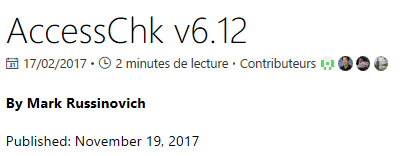
Lister les accès sur les dossiers ou fichiers

AccessEnum en interface graphique





Accesschk en invite de commande



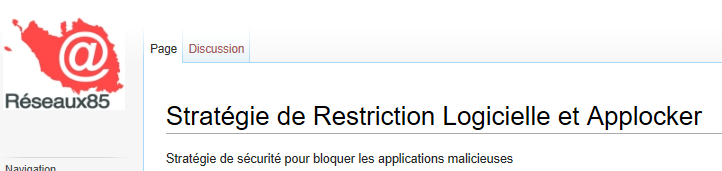
## Sécuriser les postes

Le niveau minimal serait un ensemble de 4 éléments

* Limitation appli + modules optionnels des navigateurs
* Pare-feu + antivirus sur tous les postes
* Chiffrage partitions de données
* Désactivation autorun

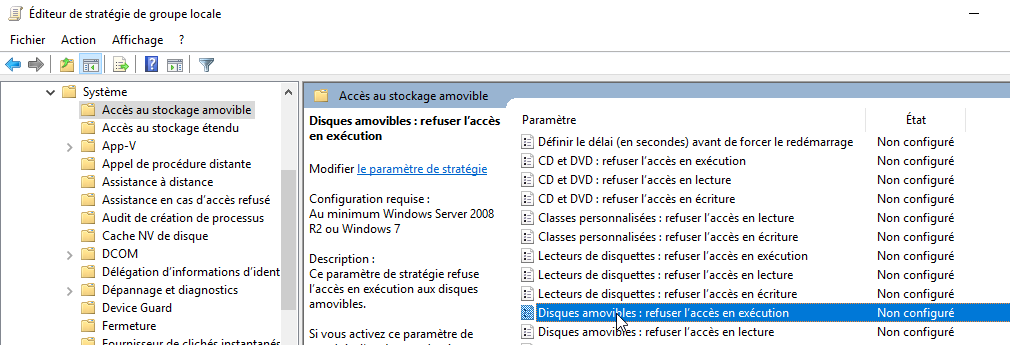
N'autoriser que les appllications voulues APPLOCKER

<http://reseaux85.fr/index.php?title=Strat%C3%A9gie_de_Restriction_Logicielle_et_Applocker>



<https://michaelfirsov.wordpress.com/applocker-in-windows-10-enterprise/>

GPO desactivation execution depuis un stockage amovible



## Sécuriser le réseau

Sécurisation des "accès physiques" /accès prises connectées sur le réseau

## Sécuriser l'administration

* Jamais d'administration despuis un poste ayant accès au web !

# 5-ANSSI Recommandations mot de passe (06-2012)

## 8 règles pour gérer les mots de passe

* Systèmes différents, mot de passe différents
  + Exemple mot de passe différent pour messagerie Pro-Perso
* Mot de passe nom lié à l'identité
  + Nom d'entreprise, date de naissance (GPO)
  + Ne Jamais faire créer son mot de passe par 1 tiers / le changer
* Ne jamais garder un mot de passe par défaut (donné à initialisation – livraison système)
* Renouveler les mots de passes régulièrement
  + 90 jours en moyenne (GPO)
* Ne jamais stocker les mots de passe dans 1 fichier sur le poste exposé (avec un accès web par exemple), encore moins sur un papier…
* Ne pas s'envoyer les mots de passe via sas messagerie perso
* Ne jamais mémoriser les mots de passe dans les logiciels, navigateurs…
  + Ou les effacer en fin de session

## Bon mot de passe

Mot de passe uniquement:

* Longueur mini 12 (si plus de 15 stockage sh LM désactivé)
  + 3 a 4 groupes de caractères avec Min-Maj-Car spécial-Chiffre

Mot de passe + tempo si 2-3 infructueux + blocage si 5-10 accès infructueux:

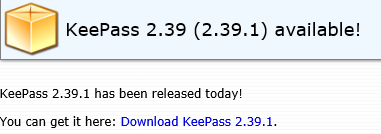
* Longueur mini 8 (si plus de 15 stockage sh LM désactivé)

Mot de passe associé à un materiel (double facteur):

* Longueur mini 4 (si plus de 15 stockage sh LM désactivé)

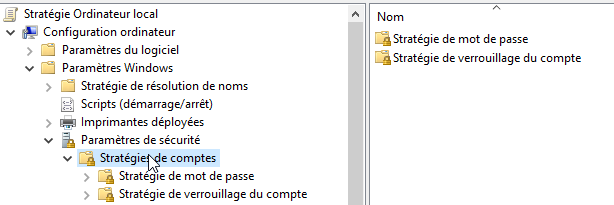
Se créer un mot de passe fort mais facile à retenir, sinon il sera noté

* Méthode phonétique
  + Ght8CD%euro7am J'ai acheté 8 CD pour 100 euro cet après midi
* Méthode des premières lettres
  + 1Tvmq2Tl'a 1 Tiens vaut mieux que 2 Tu l'auras
* Gestionnaire de mot de passe

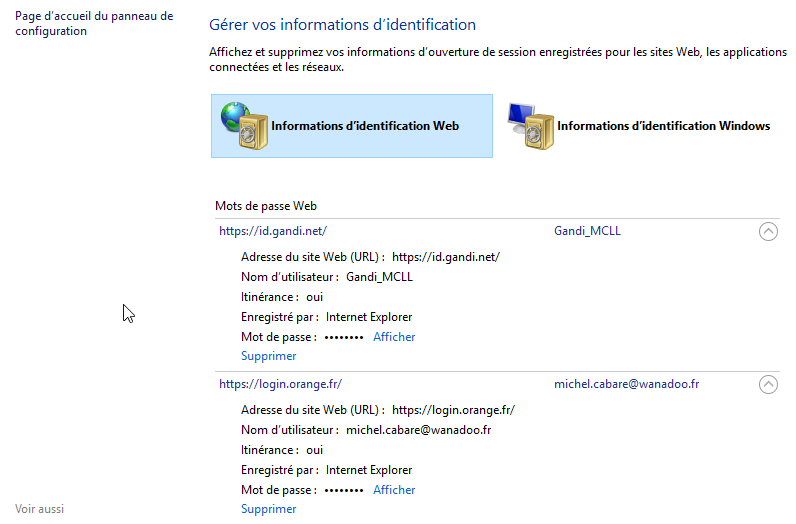


## Gestion Windows

**GPO Configuration Ordinateur**



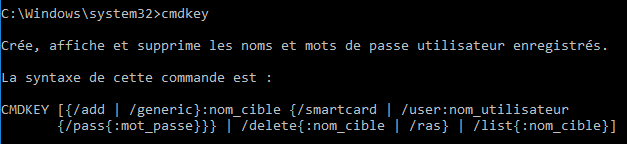
**Panneau de configuration/ Comptes Utilisateurs/ Gérer vos informations d'identification**



<https://docs.microsoft.com/fr-fr/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication>

<https://searchenterprisedesktop.techtarget.com/tip/Clear-cached-credentials-with-the-cmdkey-and-PowerShell>

La partie information d'identification windows peut se gérer par la commande en ligne **cmdkey**



## Windows Kerberos / NTLMv2

Tous les systèmes Windows, Win2K et produits ultérieurs utilisent Kerberos pour l’authentification de domaines par défaut. De tels systèmes doivent aussi utiliser au moins un protocole d’authentification non Kerberos (comme LM, NTLM ou NTLMv2) pour des logins non-domaine et autres tâches. Après un test approfondi pour vérifier que les applications et systèmes hérités (et même certaines applications plus récentes) n’en souffriront pas, désactivez l’utilisation des protocoles LM et NTLM. Si les mots de passe sont suffisamment complexes, aucun programme de percement ne peut franchir l’authentification NTLMv2

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852207(v=ws.11)>

#### GPO stockage Hash LM

Les serveurs Windows 2000 et Windows Server 2003 peuvent authentifier les utilisateurs qui se connectent sur des ordinateurs qui exécutent toute version antérieure de Windows. Toutefois, les versions de Windows antérieures à Windows 2000 n'utilisent pas Kerberos pour l'authentification. À des fins de compatibilité descendante, Windows 2000 et Windows Server 2003 prennent en charge l'authentification LAN Manager (LM), l'authentification Windows NT (NTLM) et l'authentification NTLM version 2 (NTLMv2). Les authentifications NTLM, NTLMv2 et Kerberos utilisent le hachage NT, également connu sous le nom de hachage Unicode. Le protocole d'authentification LM utilise le hachage LM.

<https://support.microsoft.com/fr-fr/help/299656/how-to-prevent-windows-from-storing-a-lan-manager-hash-of-your-passwor>

a court terme, mot de passe de plus de 15 caractères.

<https://blogs.technet.microsoft.com/miriamxyra/2017/11/07/stop-using-lan-manager-and-ntlmv1/>

Note pour le bureaux à distance Microsoft

*Protection des informations d’identification à distance Windows Defender*

*WindowsDefenderCredentialGuard à distance sur Windows Server2016 et mise à jour anniversaire Windows10vous permet également de protéger les informations d’identification pour les utilisateurs avec les connexions Bureau à distance. Auparavant, tout le monde à l’aide des Services Bureau à distance devrait se connecter à leur ordinateur local et ensuite être requis pour se connecter à nouveau lorsqu’ils effectuée une connexion à distance à leur ordinateur cible. Cette deuxième connexion serait transmettre des informations d’identification à l’ordinateur cible, les exposer à des Pass-the-Hash ou les attaques Pass-the-Ticket.*

*Avec WindowsDefenderCredentialGuard à distance, Windows Server2016 implémente de l’authentification unique pour les sessions Bureau à distance, en éliminant la nécessité d’entrer de nouveau votre nom d’utilisateur et un mot de passe. Au lieu de cela, elle s’appuie sur les informations d’identification que vous avez déjà utilisé pour ouvrir une session sur votre ordinateur local. Pour utiliser WindowsDefenderCredentialGuard à distance, le client Bureau à distance et le serveur doivent répondre aux exigences suivantes:*

* *Doit être joint à un domaine ActiveDirectory et se trouver dans le même domaine ou d’un domaine avec une relation d’approbation.*
* *Doit utiliser l’authentification Kerberos.*
* *Doit être en cours d’exécution au moins Windows10 version1607 ou Windows Server2016.*

*L’application Windows classique de bureau à distance est requise. L’application à distance Bureau plateforme Windows universelle ne prennent pas en charge WindowsDefenderCredentialGuard à distance.*

*Vous pouvez activer WindowsDefenderCredentialGuard à distance à l’aide d’un paramètre de Registre sur le serveur des services Bureau à distance et d’une stratégie de groupe ou d’un paramètre de connexion Bureau à distance sur le client Bureau à distance. Pour plus d’informations sur l’activation de WindowsDefenderCredentialGuard à distance, voir informations d’identification de protéger les services Bureau à distance avec WindowsDefenderCredentialGuard à distance. Avec WindowsDefenderCredentialGuard, vous pouvez utiliser WindowsDefenderCredentialGuard à distance pour aider à protéger les identités privilégiées sur Windows Server2016.*

# 6-ANSSI Recommandations relative à l'administration (04-2018)

## Administration Sécurisée des systèmes d'information

En plus de ce que l'on a pu dire jusqu'à présent

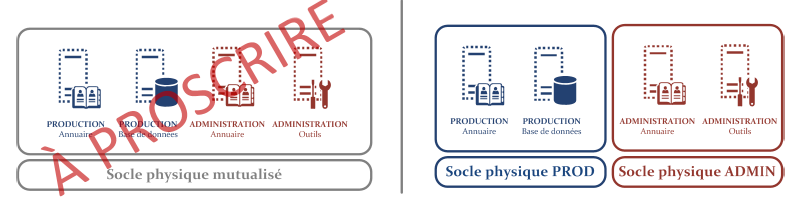
Le rôle d'administrateur est assujetti à :

* Loyauté (respect des règles d'éthique)
* Transparence (respect des règles informatiques – charte)
* Confidentialité (secret professionnel)

Il faut découper le système d'information en zones de confiance pour lesquelles les niveaux de sécurité sont identiques.

Cette découpe en zone peut se faire sur des critères de "risque", de "fonctionnalité" ou de zone "géographique."

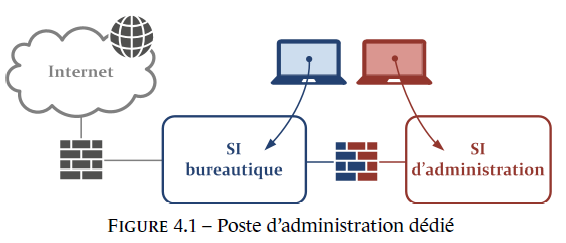
* Le cloisonnement doit être étanche ! (principe du moindre privilège)
* En cas de virtualisation, On ne peut stocker sur le même host physique 2 environnements correspondant / appartenant à 2 zones différentes



## Le poste administrateur

BYOD à proscrire absolument pour tout poste / outils d'administration

De plus dans l'idéal il faudrait 2 postes d'administration

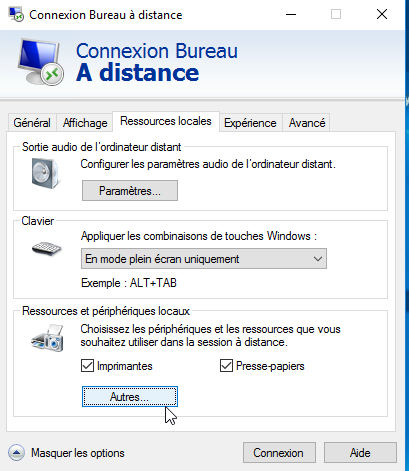


Si on utilise une connexion e type bureau à distance, il faudrait



Mais pas



Et encore à condition de déconnecter systématiquement :

Fonction copier / coller

Périphériques USB

Partages Réseaux

* Il ne doit **avoir aucun accès à Internet** (Sinon, cf p47 échanges en dehors du SI d'administration
* Les **administrateurs SI ne devraient pas être administrateurs du poste depuis lequel ils administrent** !!! (Prévention erreur humaine et limite conséquence d'une attaque virale)

# 7-ANSSI préocupations relatives au respect vie privéee avec Widows 10 (07-2017)

## Respect de la vie privée et confidentialité des données avec Windows 10

En plus de ce que l'on a pu dire jusqu'à présent

Les services inter-agissant et collecteur de données par Windows 10 sont :

* le **service de télémétrie** (connu sous les nom de Diagnostic Tracking Service ou de Universal Telemetry Client). Ce service Windows est utilisé pour identifier des problèmes de sécurité et de fiabilité. Ce service est également présent sur les versions antérieures de Windows.
* L’assistant personnel **Cortana** et le composant **Windows Desktop Search** ;
* les paramètres de personnalisation de l’expérience utilisateur (rapports d’erreur Windows, apprentissage de la saisie clavier, programme d’amélioration de l’expérience utilisateur, etc.) ;
* les applications universelles appelées Windows Apps, Packaged Apps (applications empaquetées), Metro style apps ou bien encore Modern Apps) ;
* l’utilisation de comptes Microsoft d’ouverture de session ;
* le service de stockage dans le nuage OneDrive (c’est-à-dire le Cloud, terme souvent utilisé par anglicisme).

## Télémétrie (p 5)

le **service de télémétrie** (connu sous les nom de Diagnostic Tracking Service ou de Universal Telemetry Client). A été revu à la baisse depuis windows 1703 dans son niveau de base. (Ne collecte plus adresse IP nombre de connexions réseaux, caractéristiques des réseaux)

GPO télémétrie niveau "Base" – (ou Sécurité pour educaton – et entreprise)

Préférence Panneau de configuration service Diaktrack arrêt remontée d'erreurs

## Cortana (p 8)

Il faut désactiver Cortana

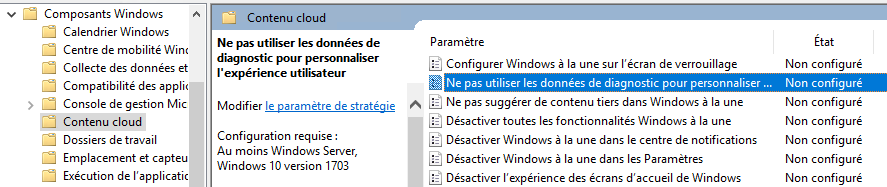
GPO ordinateur Composants Windows Rechercher

## Experience Utilisateur – Desktop Search (p 8)

Il faut limiter les inter-actions et durcir un peu le poste

Cf support windows 10 Experience Utilisateur

**GPO Utilisateur / modèles d'administration / Composants Windows /Contenu Cloud**



## Applications universelles - Tuiles (p11)

Il faut limiter les inter-actions et durcir un peu le poste

Cf gestion des tuiles Windows 10

## Compte Microsoft -

GPO gestion Compte utilisateur

Cf Windows 10

## Drive -

GPO gestion Drive

Cf Windows 10

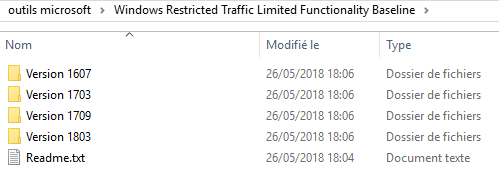
# Microsoft - Gérer les connexions du système (01-2018)

## Connexions aux services microsoft



https://docs.microsoft.com/fr-fr/windows/configuration/manage-connections-from-windows-operating-system-components-to-microsoft-services

## SCT Security Compliance Toolkit et LGPO



Voir

Microsoft a publié pour Windows 10 un **Security Compliance Toolkit** (**SCT**) remplaçant le **Security Compliance Manager** (**SCM**) de windows 7.

L’outil en ligne de commande appelé **LGPO** vient donc remplacer le script **LocalGPO.swf** fourni auparavant pour **Seven** dans **Security Compliance Manager** (**SCM**).