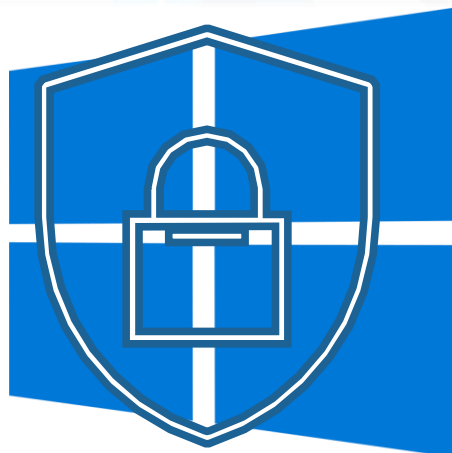


Guide hardening Windows

En date du 24 mars 2021





Rédaction

Date	Prénom Nom	Fonction	Action	Statut
	Jérémie RODRIGUEZ	Etudiant Ynov	Rédaction	OK
	Thibaut SANJUAN	Etudiant Ynov	Rédaction	OK

Suivi de version

Version	Auteur	Dates	Commentaires
1.0	Jérémie RODRIGUEZ Thibaut SANJUAN	18/03/2021	
1.1	Jérémie RODRIGUEZ Thibaut SANJUAN	25/03/2021	



TABLE DES MATIERES

TABLE DES MATIERES 2

1. INFORMATIONS 3

- A. DEFINITION DU GUIDE 3
- B. CIBLE 3

2. PRECONISATIONS D'USAGE – BONNES PRATIQUES 4

- A. PLUSIEURS COMPTES : PRIVILEGES RESTREINTS – PRIVILEGE ELEVES 4
- B. CHANGEMENT DES MOTS DE PASSE PAR DEFAUT : 4
- C. MOT DE PASSE ROBUSTE : 4
- D. POLITIQUE DE CHANGEMENT DE MOT DE PASSE : 4
- E. GESTIONNAIRE DE MOT DE PASSE : 4
- F. ENCADRER SA NAVIGATION SUR INTERNET : 5
- G. LIMITER L'EXPOSITION D'INFORMATIONS SUR LES RESEAUX SOCIAUX : 5
- H. ENCADRER SES ECHANGES PAR EMAILS : 5
- I. VERIFIER REGULIEREMENT LES ADRESSES MAILS ET MOTS DE PASSE UTILISES 5
- J. NE PAS ECRIRE SES MOT DE PASSES DE FAÇON VISIBLE PHYSIQUEMENT ET NUMERIQUEMENT 6
- K. DISPOSER D'UN ANTI-VIRUS A JOUR AVEC PAREFEU ACTIF ET SOLUTIONS ENDPOINT AVANCEES 6
- L. NE PAS EXPOSER DE SERVICE SUR INTERNET SANS SECURITE 6
- M. OUTILS ET LOGICIELS PRECONISES POUR REDUIRE L'EXPOSITION A LA FUITE D'INFORMATIONS 7

3. GUIDE DE HARDENING ET MODE OPERATOIRE 7

- A. APPLICATION DES MISES A JOUR : SERVEUR - DESKTOP 7
- B. MISE A NIVEAU D'OS ET DE VERSION APPLICATIVE EN FIN DE VIE 8
- C. STRATEGIE DE SECURITE LOCALE : STRATEGIE DE MOT DE PASSE ET VERROUILLAGE DU COMPTE 9
- D. DESACTIVER LES COMPTES LOCAL PAR DEFAUT ADMINISTRATEUR ET LE COMPTE INVITE 10
- E. SECURISER DROITS UTILISATEURS - SERVEUR - DESKTOP 11
- N. F. OPTIONS DE SECURITE SERVEUR - DESKTOP 13
- O. G. PROTOCOLE SMB V1 SERVEUR - DESKTOP 15
- P. H. ACCES BUREAU DISTANT – PROTOCOLE RDP SERVEUR - DESKTOP 17
- Q. I. ACTIVE DIRECTORY ET RESEAU SERVEUR - DESKTOP 20
- R. J. STRATEGIE D'AUDIT JOURNAUX (LOGs) SERVEUR - DESKTOP 22
- S. K. CONFIGURATION SERVEUR - DESKTOP 24
- T. L. SECURITE PHYSIQUE SERVEUR - DESKTOP 26
- U. M. INTERNET EXPLORER SERVEUR - DESKTOP 27
- V. SECURITE ENDPOINT SOPHOS INTERCEPT X ET MALWAREBYTES SERVEUR - DESKTOP 28
- W. DESACTIVER IPV6 SERVEUR - DESKTOP 28
- X. SAUVEGARDES VEEAM SERVEUR - DESKTOP 29
- Y. AUDIT AUTOMATISEE DES VULNERABILITES SERVEUR - DESKTOP 29
- Z. ENUMERATION GLOBALE VIA UTILITAIRES OU SCRIPTS SERVEUR - DESKTOP 29
- AA. R. REFERENCES 30



1. INFORMATIONS

A. DEFINITION DU GUIDE

Ce guide a pour but de sensibiliser aux bonnes pratiques liées à l'utilisation du système d'exploitation Microsoft Windows ainsi que de durcir la configuration des machines afin d'accroître leur sécurité et leur résilience face aux menaces potentielles dans un système d'information.

Ce guide s'axe sur les quatre grands principes généraux de sécurité et de durcissement.

Principe de la minimisation (réduction de la surface d'attaque)

Principe du moindre privilège (contrôle des droits sur le système et le domaine)

La défense en profondeur (Plusieurs couches de sécurité)


Veille et maintenance (Journalisation et mise à jour /mise à niveau)

B. CIBLE

Windows dans ses versions bureaux (windows 7-10)

Windows serveurs (2008, 2012, 2016, 2019,..)

Les versions précédentes de Windows sont jugées comme obsolètes.

 Dans le cas de l'existence d'un OS antérieur, la machine sera placée dans une DMZ (zone démilitarisée, isolée dans le réseau) et c'est cette zone qui sera sécurisée à défaut de pouvoir sécuriser ou durcir le système d'exploitation.



2. PRECONISATIONS D'USAGE – BONNES PRATIQUES

A. *PLUSIEURS COMPTES : PRIVILEGES RESTREINTS – PRIVILEGE ELEVES*

L'utilisation d'un compte à privilège élevé doit être utilisée uniquement pour les actions d'administration.

L'utilisation courante de la machine doit être faite avec un compte à privilèges restreints. Notamment la navigation sur internet.

Les mots de passe de ces deux comptes doivent impérativement être différents.

B. *CHANGEMENT DES MOTS DE PASSE PAR DEFAUT :*

Les mots de passe par défaut doivent systématiquement être changés au plus tôt.

C. *MOT DE PASSE ROBUSTE :*

Un mot de passe robuste est préconisé pour les comptes.

Il est recommandé d'utiliser au moins 12 caractères alphanumériques avec majuscules et minuscules ainsi qu'au moins un caractère spécial en excluant des mots du dictionnaire ou des éléments liés à notre environnement (nom d'entreprise, prénom) ou de contexte (années, mois en cours...)

L'ANSSI propose un guide à ce sujet.

<https://www.ssi.gouv.fr/guide/mot-de-passe/>

Ainsi qu'un outil pour calculer la force des mots de passe

<https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/>

D. *POLITIQUE DE CHANGEMENT DE MOT DE PASSE :*

Il est important de changer ses mots de passe, tous les 2 mois par exemple.

Cette politique est d'autant plus importante pour les comptes à privilèges élevés de type administrateur par exemple.

E. *GESTIONNAIRE DE MOT DE PASSE :*



L'utilisation d'un coffre-fort pour gérer ses mots de passe est préconisée, cela permet d'utiliser des mots de passe robustes et éviter de stocker ses mots de passe sur la machine en clair par exemple dans le navigateur.

L'ANSSI recommande KEEPASS mais d'autres alternatives existent comme Bitwarden.

F. ENCADRER SA NAVIGATION SUR INTERNET :

La navigation sur internet doit être encadrée et maîtrisée. La navigation sur des sites douteux doit être proscrite et aucune information ne doit être échangée sur un site n'étant pas sécurisé. (adresse en http et non https)

Un lien sécurisé est matérialisé par un petit cadenas dans la barre de navigation au début de l'URL.

Aucun logiciel ou autre exécutable ne doit être téléchargé et exécuté s'il provient d'une source douteuse.

Utiliser un navigateur plus sécurisé comme Brave ou installer des extensions pour limiter les interactions du navigateur peut être une option. Extensions comme AD Block, Ghostery ect...

G. LIMITER L'EXPOSITION D'INFORMATIONS SUR LES RESEAUX SOCIAUX :

L'exposition d'informations sur les réseaux sociaux dans le cadre personnel ou professionnel est à encadrer et à contrôler.

Toute information divulguer peut permettre à une personne mal intentionnée de profiter de celle-ci pour une action malveillante.

H. ENCADRER SES ECHANGES PAR EMAILS :

Il est important de faire preuve de vigilance en manipulant ses courriers électroniques, surtout quand ils comportent des liens ou des pièces-jointes.

Il faut s'assurer de bien vérifier l'expéditeur réel du message et en cas de doute, n'effectuer aucune action.

Toute notion d'urgence dans un mail qui incite à action impliquant de cliquer sur un lien, de télécharger une pièce jointe ou d'appeler un numéro de téléphone pointe souvent un mail frauduleux.

I. VERIFIER REGULIEREMENT LES ADRESSES MAILS ET MOTS DE PASSE UTILISES



Des fuites de données ont lieu régulièrement suite à des compromissions de système d'information ou des erreurs de configurations de tiers détenteurs de données.

Les liens suivants permettent de vérifier si nos données ont été dérobées et s'il est nécessaire de changer ses mots de passe.

Adresse email :

<https://cybernews.com/personal-data-leak-check/>

<https://haveibeenpwned.com/>

Mot de passe :

<https://haveibeenpwned.com/Passwords>

J. NE PAS ECRIRE SES MOT DE PASSES DE FAÇON VISIBLE PHYSIQUEMENT ET NUMERIQUEMENT

Il est à proscrire d'écrire ses mots de passe sur papier ou post-it, ou encore sur des fichiers en clair sur son ordinateur comme un fichier texte.

L'utilisation d'un gestionnaire de mot de passe à la place est préconisée.

K. DISPOSER D'UN ANTI-VIRUS A JOUR AVEC PAREFEU ACTIF ET SOLUTIONS ENDPOINT AVANCEES

Il est important de disposer d'un antivirus actif et à jour sur sa machine Windows.

Les antivirus modernes peuvent intégrer des fonctions avancées comme la protection contre els ransomware, des HIDS (host IDS) ou EDR ainsi qu'un pare-feu et des filtrages WEB ou encore filtrages d'utilisation matériel tel que les périphériques USB.

Il faut aussi compléter sa protection avec un anti spyware/adware afin de supprimer les mouchards ou les logiciels non désirés (adware – spyware – PUA)

Le guide aborde la solution préconisée dans le point « O ».

L. NE PAS EXPOSER DE SERVICE SUR INTERNET SANS SECURITE

Aucun service ne doit être exposé sur internet s'il ne dispose pas d'une sécurité adéquate et testée.

Certains services comme le protocole de bureau distant de Windows (RDP) ne doivent en aucun cas être exposés sur internet.



M. OUTILS ET LOGICIELS PRECONISES POUR REDUIRE L'EXPOSITION A LA FUITE D'INFORMATIONS

Le site [privacytools](https://www.privacytools.io/) propose différents logiciels et outils adaptés aux préconisations et aux bonnes pratiques mentionnées ci-dessus permettant de réduire son exposition et de se prémunir de certaines menaces.

<https://www.privacytools.io/>

3. GUIDE DE HARDENING ET MODE OPERATOIRE

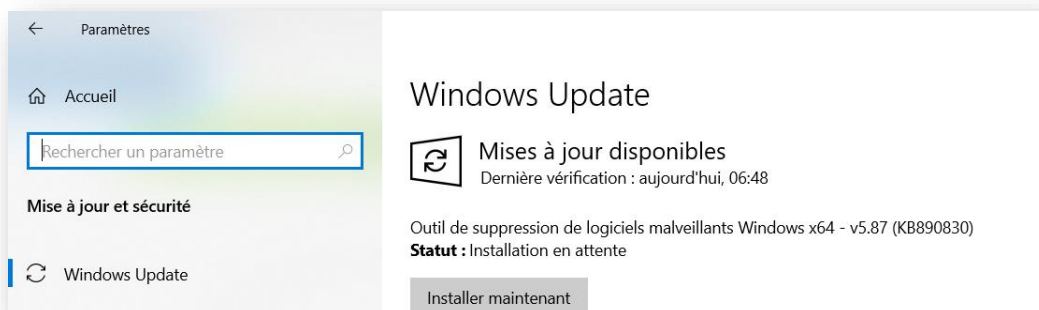
A. APPLICATION DES MISES A JOUR : **SERVEUR** - **DESKTOP**

Il est important de garder un environnement en condition de sécurité avec les mises à jour. Une grande partie des correctifs de sécurité de vulnérabilités découvertes sont corrigés par ce biais.

Desktop : Pour une machine type Desktop (Windows 10) les mises à jour peuvent être appliquées automatiquement.

Sur Windows 10 et Windows serveur :

Paramètres – Mise à jour et sécurité :



Serveur : Pour les serveurs, il est possible d'activer les notifications de mises à jour et dans un environnement professionnel qui ne permet pas d'appliquer automatiquement celles-ci.

On utilise le WSUS : Windows Server Update Services afin de contrôler les mises à jour à appliquer.

Lien microsoft Wsus :




<https://docs.microsoft.com/fr-fr/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>

B. MISE A NIVEAU D'OS ET DE VERSION APPLICATIVE EN FIN DE VIE

La fin de vie des systèmes d'exploitation et des versions applicatives doit être encadrée. La fin de vie signifie l'arrêt du support et par extension l'arrêt des correctifs de sécurité, la machine est donc vouée à être vulnérable aux nouvelles vulnérabilités ou vulnérabilités déjà existantes et possiblement exploités par des individus ou des logiciels malveillants.

On constate souvent la présence de machines avec des OS en fin de vie dans les systèmes d'information.

Fin de vie OS Windows Client

Version	Extended Support End
Windows XP SP3	4/8/2014
Windows Vista SP2	4/11/2017
Windows 7 SP1	1/14/2020
Windows 8.1	1/10/2023
Windows 10 (si mis à jour)	10/13/2026
 Windows 10 non mis à jour De 1507 à 1709	End of life

Fin de vie OS Windows serveur

Version	Extended Support End
Windows 2003 SP2	7/14/2015
Windows 2008 SP2	1/14/2020
Windows 2008 R2 SP1	1/14/2020
Windows 2012	1/10/2023
Windows 2012 R2	1/10/2023
Windows 2016	1/12/2027
Windows 2019	1/9/2029

Dates des supports pour Office :

Office 2007 (01/2007) : 10/10/2017 (support étendu).

Office 2010 (07/2010) : 13/10/2020 (support étendu).

Quelques versions à prendre en compte :

- Serveurs WEB IIS



- Sharepoint
- Serveur Exchange
- Microsoft SQL server

Les liens suivants fournissent la liste des fins de vie des produits microsoft ces dernières années :

<https://docs.microsoft.com/fr-FR/lifecycle/overview/product-end-of-support-overview>

<https://docs.microsoft.com/fr-fr/lifecycle/end-of-support/end-of-support-2021>

<https://docs.microsoft.com/fr-fr/lifecycle/end-of-spport/end-of-support-2020>

<https://docs.microsoft.com/fr-fr/lifecycle/end-of-support/end-of-support-2019>

<https://docs.microsoft.com/fr-fr/lifecycle/end-of-support/end-of-support-2018>

C. STRATEGIE DE SECURITE LOCALE : STRATEGIE DE MOT DE PASSE ET VERROUILLAGE DU COMPTE

Serveur – Desktop

La stratégie de sécurité locale permet de contrôler plusieurs paramètres notamment celle du verrouillage des comptes et les paramètres liés à un mot de passe.

Le verrouillage de compte permet de lutter contre les tentatives de découverte d'un mot de passe type bruteforce.

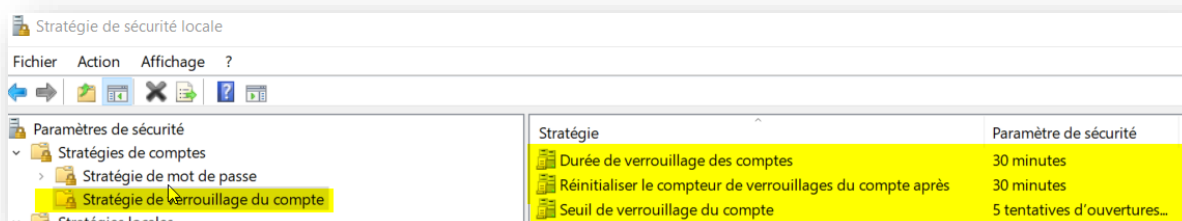
La stratégie de mot de passe permet de paramétrer, la durée de vie, l'historique des mots de passe conservés et la complexité de ceux-ci.

1. Pour ouvrir la Stratégie de sécurité locale, dans l'écran de **Démarrage**, tapez **secpol.msc**, puis appuyez sur ENTRÉE.
2. Sous les **Paramètres de sécurité** de l'arborescence de la console :
Cliquez sur les **Stratégies de compte** pour modifier la **Stratégie de mot de passe** et la **Stratégie de verrouillage de compte**.

Exemple de configuration du verrouillage

Au bout de 5 échecs d'authentification sur une période de 30 minutes le compte sera bloqué 30 minutes.

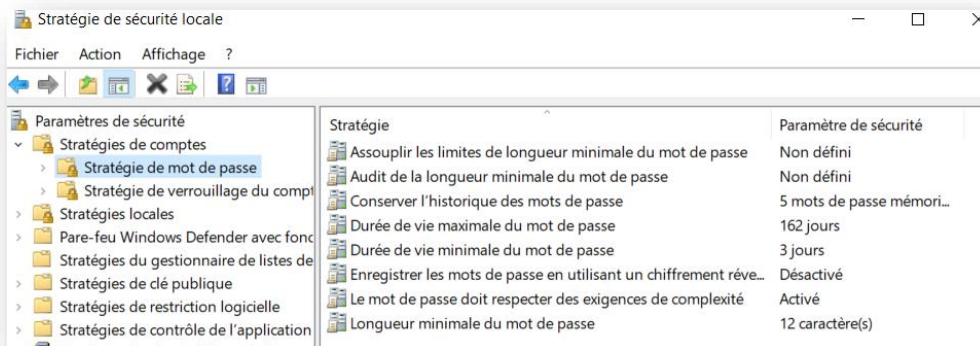
Le compteur d'échecs d'authentification ne se remettra à 0 qu'au bout de 30 minutes.



Exemple de stratégie :



Le mot de passe doit être modifié tous les 162 jours. Il doit être différent des 5 derniers mots de passe utilisés. Il doit être de 12 caractères minimum et comporte au moins une majuscule, un chiffre et un caractère spécial et surtout de ne pas enregistrer le mot de passe dans un chiffrement réversible.



Il est à noter que ces paramètres peuvent être gérés par GPO dans un domaine Active Directory, ils sont ainsi imposés aux utilisateurs du domaine, ce sont les préconisations élémentaires en entreprise.

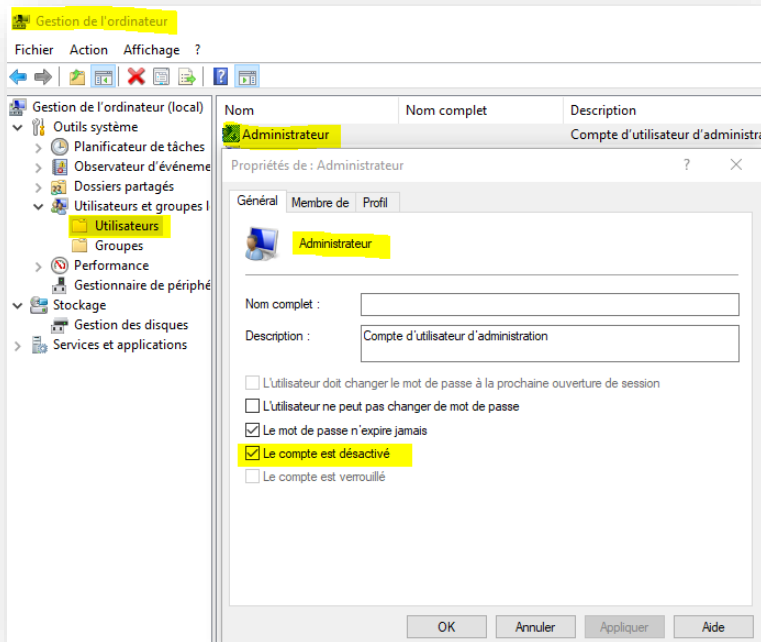
⚠ Pour visualiser les mots de passe et sessions stockés localement, faites `cmdkey /list` dans une invite de commande CMD.

D. DESACTIVER LES COMPTES LOCAL PAR DEFAUT ADMINISTRATEUR ET LE COMPTE INVITE

Serveur – Desktop

Le compte local administrateur ainsi que le compte invité doivent être désactivés

Dans la gestion de l'ordinateur, sélectionner le compte Administrateur et cocher « le compte est désactivé » puis valider avec OK.

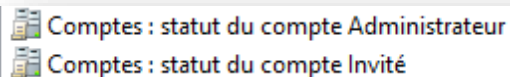


Si celui-ci ne peut pas être désactivé, son accès peut être encadré et renforcé:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-h--securing-local-administrator-accounts-and-groups>

Procéder de la même façon pour le compte invité

Il est aussi possible d'accéder à ces désactivations dans les options de sécurité de la stratégie locale de sécurité :



E. SECURISER DROITS UTILISATEURS - SERVEUR - DESKTOP

Les paramètres suivants abordent les droits utilisateurs avec les accès et les actions potentiellement exécutables.

Ils sont paramétrables via GPO ou dans la stratégie de sécurité locale comme vu précédemment. Ces options pourraient permettre l'utilisation frauduleuse d'une machine.

➤ Accès aux machines :

Dans un environnement Active Directory , il est recommandé de contrôler les accès aux machines via les droits des utilisateurs.



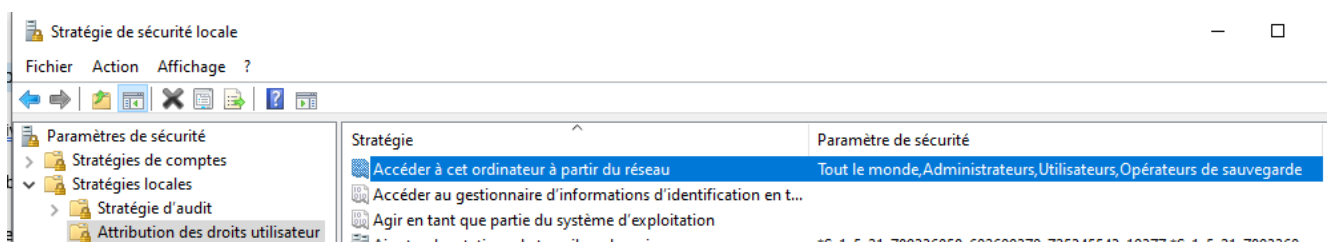
Serveur :

Sur les serveurs, il est recommandé de n'autoriser l'accès aux groupes de sécurité concernés ou aux administrateurs le cas échéant.

A défaut le minimum sera « utilisateur authentifié » afin de pas autoriser d'accès non authentifié.

Il faut respecter les bonnes pratiques en matière de groupe de sécurité notamment avec des comptes utilisateurs dans des groupes de sécurité et des droits attribués aux groupes de sécurités.

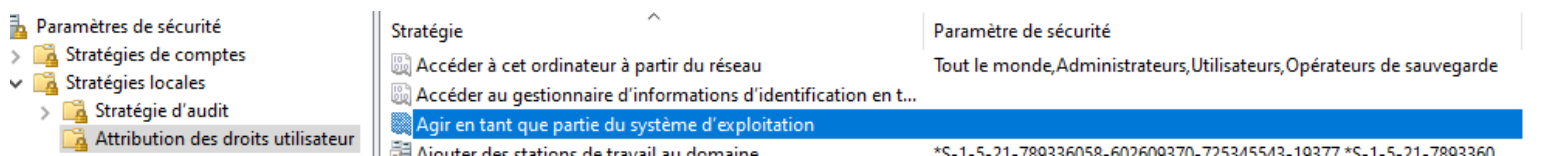
Exemple de configuration trop permissive :



➤ Agir en tant que partie du système d'exploitation :

Ne pas attribuer le droit « Agir en tant que partie du système d'exploitation » aux utilisateurs standards

Exemple d'une configuration n'autorisant pas cette fonction :



➤ Ouvrir une session en tant que Service

Refuser le droit « Ouvrir une session en tant que Service » aux utilisateurs invités, et ce localement ou à distance via Connexion Bureau à distance.

Exemple : Aucun utilisateur invités n'est mentionné dans cette option.



➤ Pas de droits sur les services, les processus et la base de registre (et autorun) pour l'utilisateur courant

Le compte utilisateur courant , utilisé au quotidien ne doit pas avoir de droits de modification des services, processus, ou la base de registre.



Cela empêchera l'escalade de privilèges par ce biais.

Il est possible de vérifier les services qui démarrent automatiquement via la commande :
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

L'utilisateur courant ne doit pas avoir de droits de modifications de ces services.

➤ Chemin d'exécutable avec des espaces sans guillemets haut ou quote

Il est risqué d'utiliser un chemin d'exécutable avec espace sans guillemets hauts (quotes) car cela peut mener à une escalade de privilèges.

Il est possible de taper la commande **wmic service get name,pathname** dans une invite de commande CMD pour contrôler les chemins d'accès :

A éviter :

```
C:\Program Files (x86)\Privacyware\Privatefirewall 7.0\pfsvc.exe
```

Correct :

```
"C:\Program Files (x86)\BraveSoftware\Update\BraveUpdate.exe" /svc
```

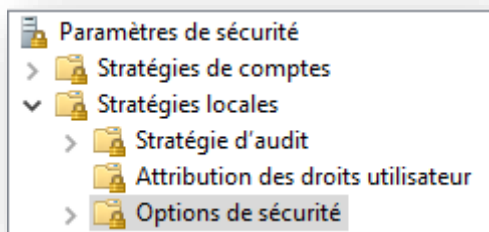
➤ Tâches planifiées et tâches exécutées au démarrage.

Les tâches planifiées et exécutées au démarrage doivent être encadrées et inaccessibles à l'utilisateur courant.

Si la tâche planifiée pointe un fichier (exécutable, batch, powershell..), il ne doit pas être modifiable par un utilisateur courant.

N. F. OPTIONS DE SECURITE SERVEUR - DESKTOP

Dans la stratégie locale, plusieurs options de sécurité peuvent être configurées, il est possible de le faire localement ou par GPO.



➤ SAM : Coffre-fort de mot de passe Windows



L'accès au SAM qui est en quelque sorte l'endroit où sont stockés les empreintes des mots de passe en local doit être restreint avec les deux options ci-dessous de l'image ci-dessous :

Stratégies du gestionnaire de listes de	Accès réseau : modèle de partage et de sécurité pour les comptes locaux	Classique - les utilisat
Stratégies de clé publique	Accès réseau : ne pas autoriser l'énumération anonyme des comptes et partages SAM	Activé
Stratégies de restriction logicielle	Accès réseau : ne pas autoriser l'énumération anonyme des comptes SAM	Activé

Requérir la combinaison de touches Ctrl+Alt+Suppr pour les ouvertures de session interactives

Il est envisageable de forcer la combinaison des touches ctrl+ alt +suppr pour l'ouverture des sessions afin de limiter les risques liés aux automatisations de logiciels malveillants ou d'exploits diverses.

Ouverture de session interactive : ne pas afficher le nom du dernier utilisateur connecté	Désactivé
Ouverture de session interactive : ne pas demander la combinaison de touches Ctrl+Alt+Suppr.	Non défini
Ouverture de session interactive : nécessite l'authentification par le contrôleur de domaine pour le déverrouillage d...	Désactivé

Configurer la limite d'inactivité du serveur pour protéger les sessions interactives

Limiter la durée des sessions permet de limiter l'exploitation d'une session potentiellement compromise et de potentiellement couper un accès qui ne pourra être retrouvé à l'issue ou de limiter la possibilité d'exploiter une session ouverte et inactive.

Dans tous les cas il s'agit d'une bonne pratique de fonctionnement. Une multitude de sessions inactives sur un serveur ou poste client n'est pas forcément recommandé.

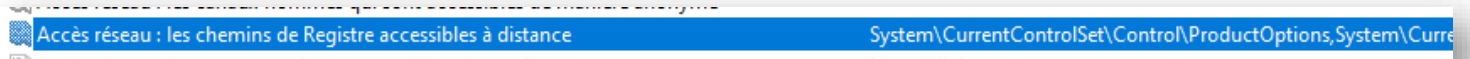
Ouverture de session interactive : Windows Hello Entreprise ou carte à puce nécessaire	Désactivé
Ouverture de session interactive : limite d'inactivité de l'ordinateur	Non défini
Ouverture de session interactive : seuil de verrouillage du compte d'ordinateur	Non défini

Ne pas autoriser d'accès aux partages réseau de manière anonyme

Accès réseau : les partages qui sont accessibles de manière anonyme	Non défini
Accès réseau : modèle de partage et de sécurité pour les comptes locaux	Classique - les utilisat



Désactiver l'accès distant au registre quand c'est possible :



O. G. PROTOCOLE SMB V1 **SERVEUR** - **DESKTOP**

Le protocole SMB en version 1 n'est plus considéré comme sécurisé et présente de nombreuses vulnérabilités. Plusieurs logiciels malveillants utilisent ce protocole dont plusieurs rançongiciels dans le cadre de leur propagation ou de l'infection initiale.

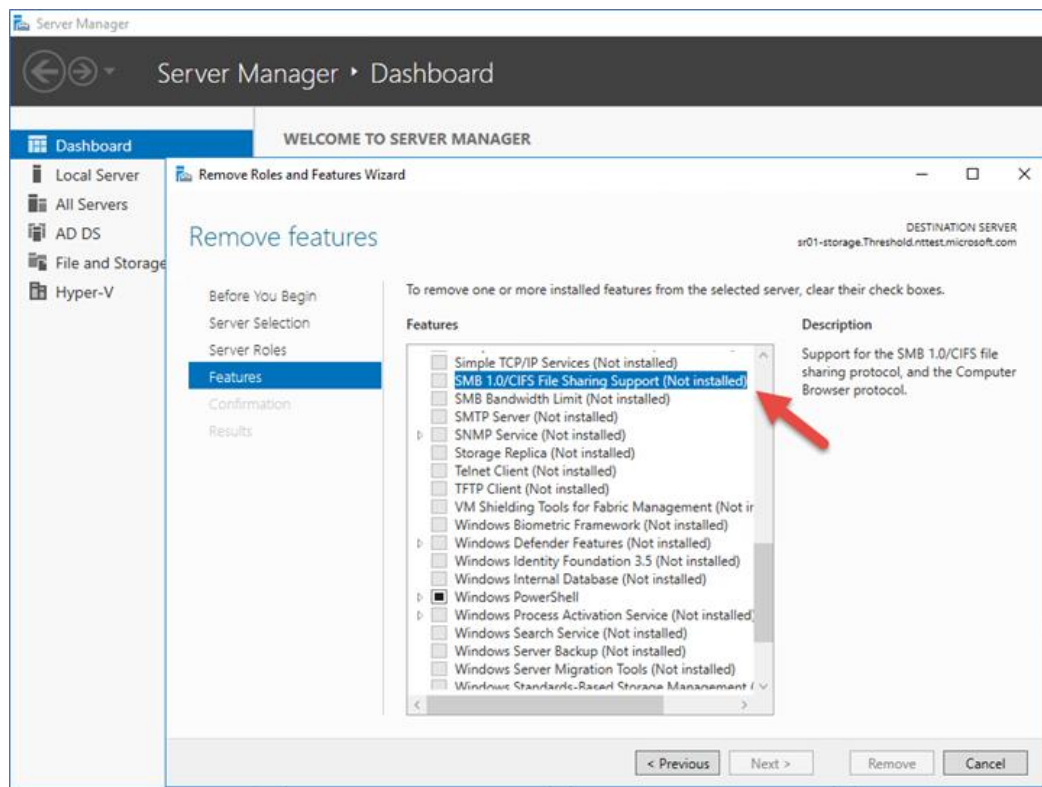
Plusieurs méthodes peuvent être utilisées :

Détecter et désactiver avec Powershell : **Serveur** - **Desktop**

Ce guide explique comment détecter et désactiver un protocole SMB avec Powershell :

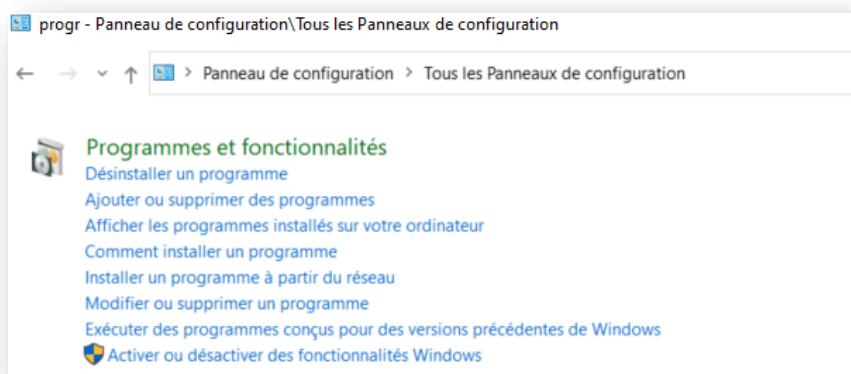
<https://docs.microsoft.com/fr-fr/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>

Avec le gestionnaire de serveur : **Serveur**



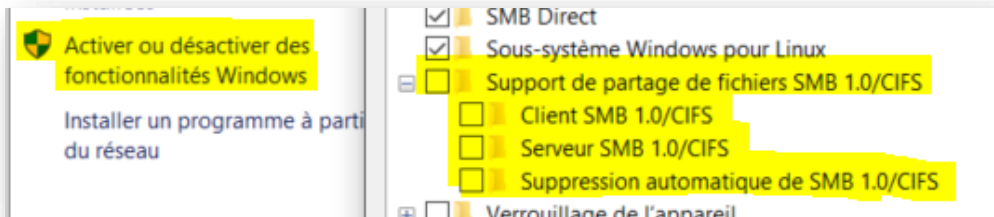
Depuis le panneau de configuration :

Menu « Programmes et fonctionnalités »

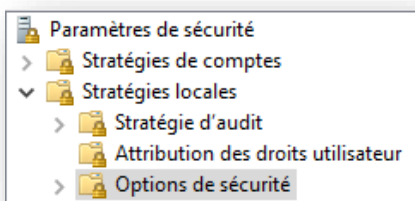


Sous partie « Activer ou Désactiver des fonctionnalités Windows »

Et « Support de partage de fichiers SMB 1.0/CIFS »

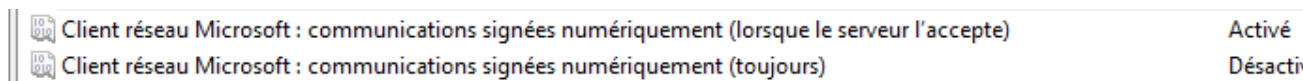


Plusieurs options de sécurité liées dans la stratégie de sécurité locale peuvent être modifiées :



Desktop Sur client :

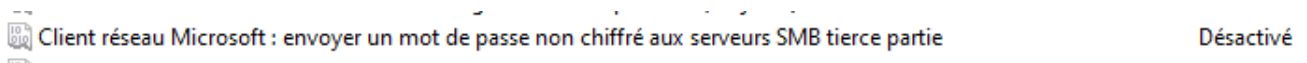
- Configurer le Client réseau Microsoft pour signer les communications numériquement (toujours)
- Configurer le Client réseau Microsoft pour signer les communications numériquement (lorsque le serveur l'accepte)



Serveur Sur serveur :

- Configurer le Serveur réseau Microsoft pour signer les communications numériquement (toujours)
- Configurer le Serveur réseau Microsoft pour signer les communications numériquement (lorsque les clients l'acceptent)

Serveur – Desktop Désactiver l'envoi de mots de passe non chiffrés à des serveurs SMB tiers :





Le protocole de bureau distant permet une prise en main à distance en ouvrant une session sur une machine depuis une autre machine. Ce protocole est souvent utilisé pour les compromissions.

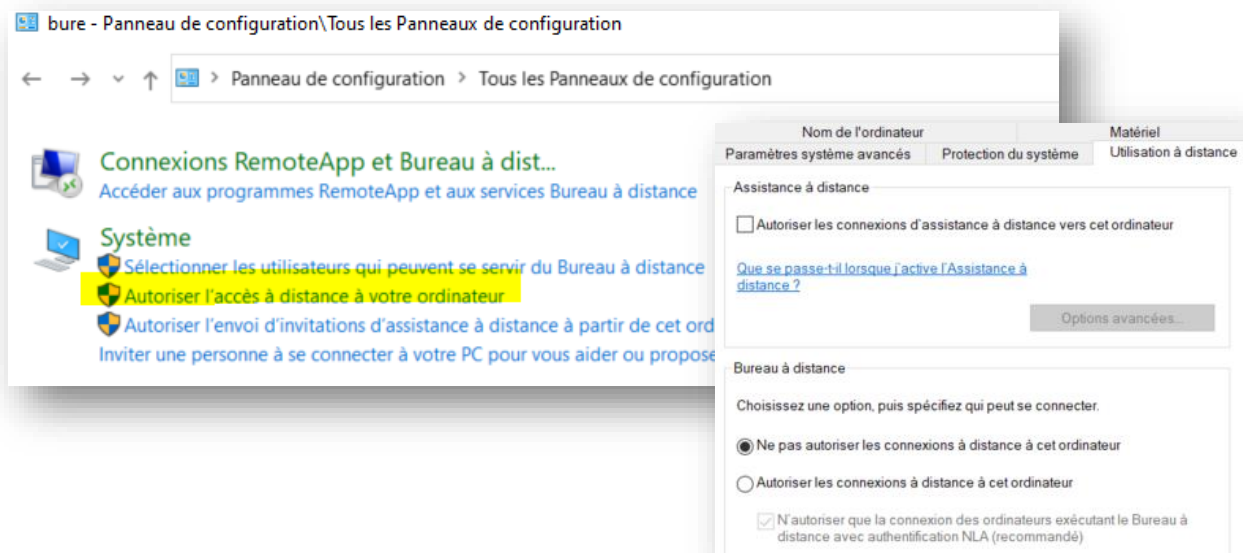
Les options peuvent être configurées localement ou pas GPO.

Desktop Sur client : Le désactiver par défaut quand ce n'est pas nécessaire.

Pour vérifier le statut et le désactiver le cas échéant :

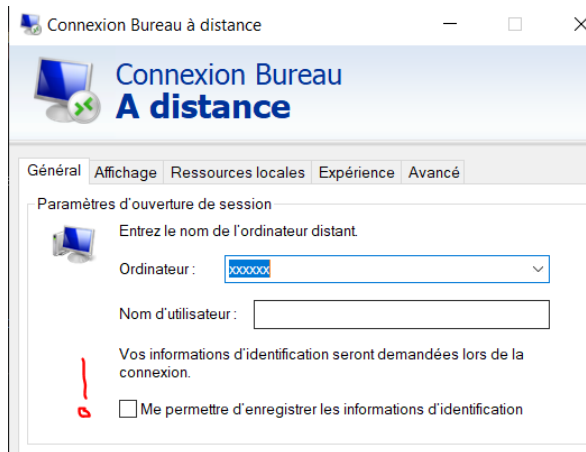
Rendez-vous dans panneau de configuration :

Système – Autoriser l'accès à distance à votre ordinateur et vérifiez que le service soit désactivé.



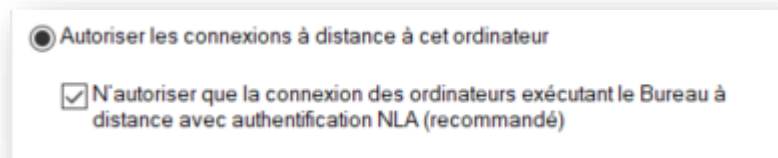
Obligation de fournir un mot de passe à la connexion et ne pas sauvegarder de mot passe:

Il est possible d'enregistrer son mot de passe lors d'une connexion RPD client, c'est à proscrire.



Serveur Sur serveur, ce protocole est souvent nécessaire à l'administration, il faut donc durcir l'utilisation du protocole pour le sécuriser au maximum.

Activation du NLA : (Network Level Authentication)



Utilisation du chiffrement SSL avec un certificat :

Dans le cas de l'utilisation du SSL on notera l'utilisation du protocole TLS 1.1 minimum voire TLS 1.2.

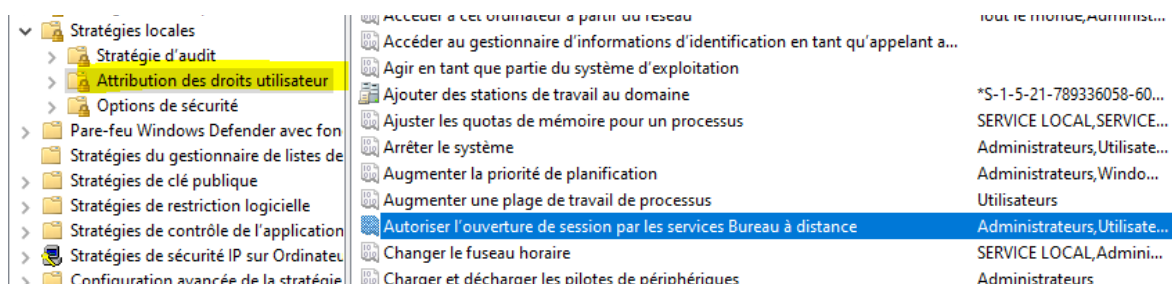
Les protocoles SSL 2, SSL3 et TLS 1.0 étant dépréciés.

Ce guide explique l'activation de ces 2 fonctionnalités. Ne pas prendre en compte la mention du TLS 1.0

<https://www.informatiweb-pro.net/admin-systeme/win-server/ws-2012-2012-r2-rds-activer-le-nla-et-utiliser-le-ssl-tls-1-0.html>

Choisir qui peut ouvrir une session distante :

Dans la stratégie de sécurité locale, on peut déterminer les groupes d'utilisateurs qui peuvent ouvrir une session distante.



Activer le Remote Credential Guard

Il est possible d'activer une fonctionnalité de durcissement du protocole RDP à partir des versions Windows serveur 2016 et Windows 10.

Un guide technique est disponible sur le site de Microsoft

<https://docs.microsoft.com/fr-fr/windows/security/identity-protection/remote-credential-guard>

Important

- ⚠ **Le protocole RDP sur le port 3389 ne doit jamais être ouvert directement sur internet. Directement sur un serveur ou via redirection du parefeu.**

On utilisera d'abord un VPN pour se connecter à un SI puis le protocole RDP ensuite.

- ⚠ **Plusieurs alternatives existent comme VNC ou d'autres logiciels type AnyDesk. Elles sont à proscrire car trop peu sécurisées. Si ces logiciels sont détectés, elles doivent être désinstallés**

Q. I. ACTIVE DIRECTORY ET RESEAU SERVEUR - DESKTOP

Plusieurs éléments peuvent être pris en compte dans un environnement active directory

Le chiffrement SSL pour les serveurs : Desktop

Les protocoles de chiffrement SSL2.0 , SSL3.0, TLS 1.0 et TLS 1.1 portent un nombre important de vulnérabilités et doivent être désactivés si possible au profit de TLS 1.2 et TLS 1.3.

La désactiver des protocoles doit être testé pour contrôler les effets de bord.

Dans l'idéal il faut :

Activer TLS 1.2, désactiver SSL.2.0, SSL3.0 TLS 1.0 et TLS 1.1

Si cela pose problème : Garder le TLS 1.1 actif



En cas de soucis il est possible de revenir en arrière :

```
Remove-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0' -Recurse  
Remove-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0' -Recurse  
Remove-Item 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1' -Recurse
```

Le guide suivant explique la procédure pour désactiver les protocoles SSL 2.0, 3.0 et TLS 1.0 , 1.1 puis activer TLS 1.2

<https://www.petenetlive.com/KB/Article/0001675>

Désactiver le NTLM v1

Le protocole NTLM version 1 sert à authentifier un compte dans un environnement Active Directory. Aujourd'hui déprécié, il est sujet à de nombreuses vulnérabilités, notamment celle de stocker le mot de passe dans le mémoire du service LSA.

Une GPO doit être mise en place pour désactiver le protocole.

<https://bobcares.com/blog/disable-ntlm-authentication-in-windows-domain/>

Désactiver RC4

RC4 (River Cipher 4) est un algorithme de chiffrement déprécié depuis 2016 car vulnérable.

Toujours présent sur d'anciens systèmes, il est recommandé de le désactiver.

Une mise à jour de sécurité est disponible sur le site de Microsoft selon la version de Windows concernée.

<https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-for-disabling-rc4-479fd6f0-c7b5-0671-975b-c45c3f2c0540>

Bonnes pratiques Active Directory

Un environnement Active Directory nécessite l'application de bonnes pratiques notamment en matière de sécurité.

L'ANSSI (Agence Nationale de la sécurité des systèmes d'information) propose un guide des points de contrôles pour Active Directory ainsi qu'un guide des recommandations de sécurité

Guide des points de contrôles Active Directory de l'ANSSI

<https://www.cert.ssi.gouv.fr/uploads/guide-ad.html>

Recommandations de sécurité Active Directory de l'ANSSI

<https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/>



Une stratégie d'audit sous Windows permet de conserver les événements se produisant sur une machine sous forme de journaux.

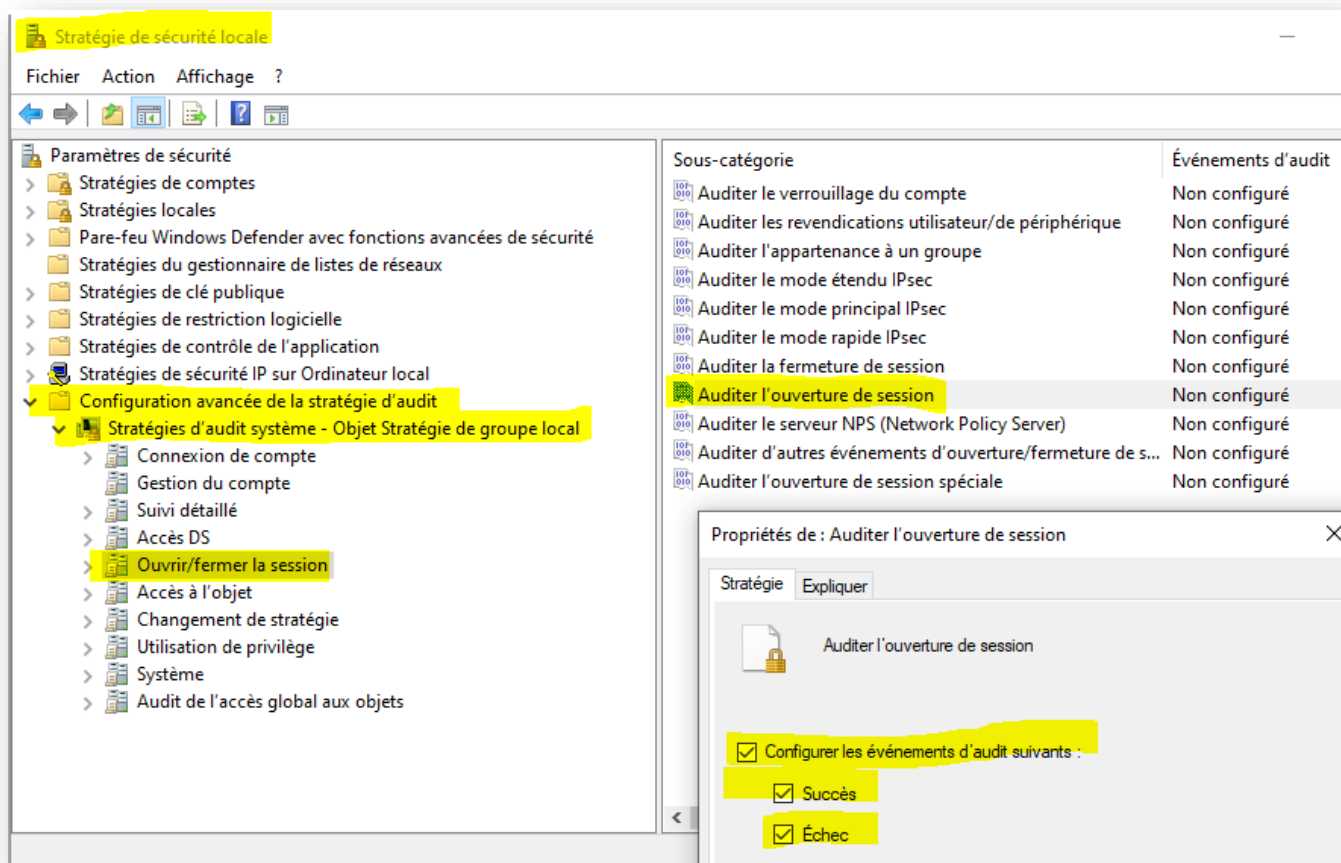
Les principaux éléments à auditer sont :

- Les ouvertures de session sur un compte
- La gestion des comptes utilisateurs
- Les ouvertures et fermetures de sessions
- Les changements de stratégie
- L'utilisation des privilèges

Il est à noter que sur un serveur, la stratégie d'audit devra être plus ciblée et adaptée aux services portés par la machine.

En local, la configuration se fait dans la Stratégie de sécurité locale

Exemple pour les ouvertures de session



Microsoft recommande une stratégie d'audit pouvant être implémentée localement ou pas GPO.



<https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

Et une stratégie dédiée à la surveillance des intrusions

<https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

Il est possible d'enrichir les journaux de sécurité avec SYSMON dans le cadre de la sécurité

- ⚠ **Les journaux pouvant être supprimés, il est conseillé d'externaliser les logs en les envoyant vers un serveur dédié, voire un SIEM pour superviser la sécurité. Ces opérations peuvent être effectuées avec les fonctions de Windows Event Forwarding ou un agent Syslog à installer sur la machine tel que NXLOG.**

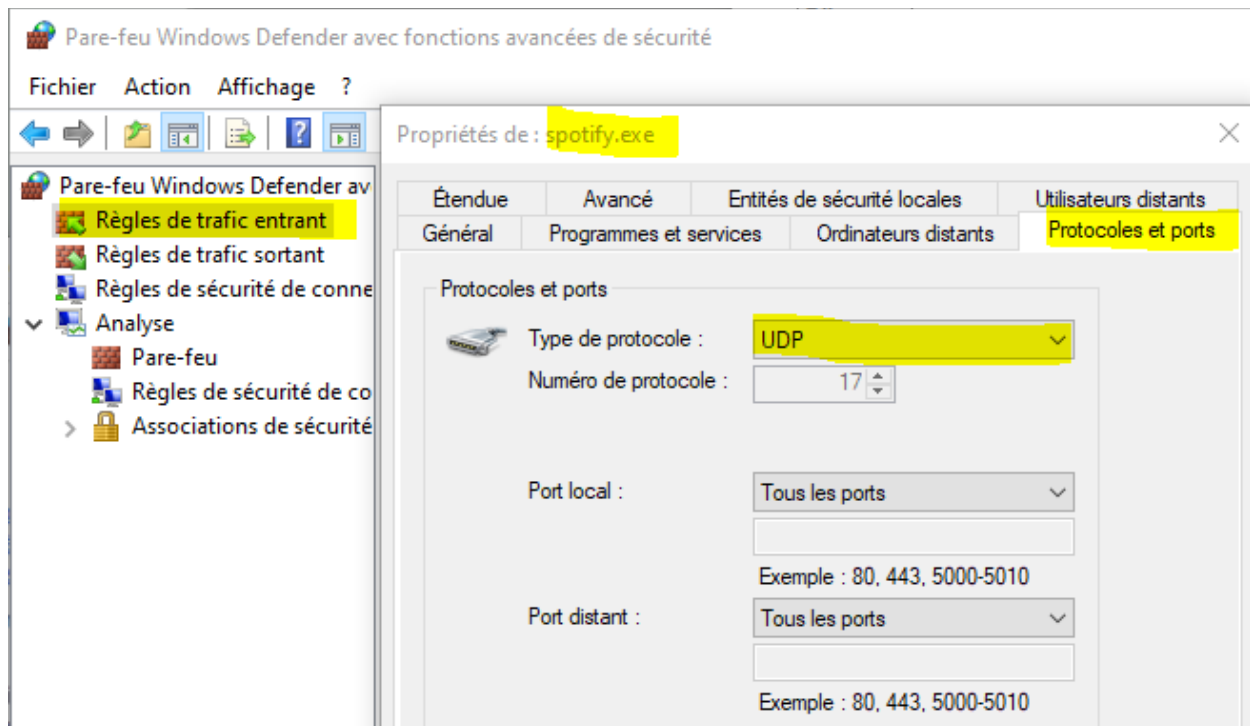
S. K. CONFIGURATION SERVEUR - DESKTOP

Fermer port et/ou trafic non nécessaire

A l'aide du pare-feu Windows ou d'un pare-feu tiers on peut contrôler les flux entrants et sortants de la machine :

Dans le panneau de configuration cliquez sur Pare-feu Windows Defender. Vous pouvez alors visualiser le trafic entrant et sortant.

Dans cet exemple : une règle autorise le trafic entrant pour Spotify.exe sur tous les ports UDP.



NTP : Network time protocol Serveur - Desktop

Le Network time protocole est un protocole important permettant de garantir que toutes les machines d'un système d'information soient synchronisées sur une heure identique. Ce protocole est important sur le plan de l'administration mais aussi de la sécurité, notamment pour les journaux d'évènements et les tâches planifiées.

Une machine intégrée dans un domaine Active Directory sera automatiquement configurée mais si la machine n'est pas intégrée au domaine il faut configurer le NTP avec un serveur de temps faisant autorité.

<https://docs.microsoft.com/fr-fr/windows-server/networking/windows-time-service/how-the-windows-time-service-works>

BITLOCKER Serveur - Desktop

Bitlocker permet le chiffrement des données stockées sur un ordinateur. Il va réduire la vulnérabilité à un accès non autorisé sur une machine perdu ou volée par exemple.

Le guide suivant permet d'activer BITLOCKER.

<https://uit.stanford.edu/service/encryption/wholedisk/bitlocker#:~:text=Click%20Start%20%2C%20click%20Control%20Panel,it%20meets%20the%20system%20requirements.>

Services non utilisés Serveur - Desktop



Par défaut de multiples services opèrent sous Windows. Dans le cadre d'une compromission, les services et processus de Windows sont souvent utilisés pour masquer des processus malveillants.

Il est recommandé de contrôler les services qui s'exécutent sur une machine et le cas échéant d'en limiter l'exécution au strict nécessaire.

UAC Desktop

Le contrôle de compte utilisateur permet de réduire l'impact d'un malware sur une machine. Désactivé par défaut sur les serveurs, il est activé sur les machines de type Desktop.

Cette fonctionnalité peut parfois paraître contraignante mais peut s'avérer utile en cas de compromission. Il est recommandé de garder cette fonctionnalité.

<https://securityboulevard.com/2019/04/you-better-think-twice-before-you-disable-uac-windows-10/>

T. L. SECURITE PHYSIQUE SERVEUR - DESKTOP

Un accès physique à une machine Windows permet dans la majorité des cas une compromission de celle-ci. Afin de réduire les risques inhérents à un tel accès, plusieurs éléments sont à prendre en compte :

Locaux sécurisés

Les machines doivent être conservés dans des locaux sécurisés, fermés et si possible avec contrôle d'accès pour prévenir d'un accès physique.

Accès au BIOS/UEFI limité

Lors du démarrage, le BIOS/UEFI doivent être protégé par mot de passe.

Pour accéder au BIOS/UEFI :

<https://lecrabeinfo.net/acceder-utilitaire-de-configuration-bios-uefi-pc.html>

Contrôler l'ordre des périphériques de démarrage :

L'ordre du BOOT doit être configuré de façon à ne pas autoriser le redémarrage sur un média externe type clé USB par exemple.

Ecran de verrouillage de session

Un écran de verrouillage automatique doit être configuré après un temps d'inactivité.



A configurer en local ou pas GPO.

Restreindre l'utilisation de périphérique de stockage externe

Bien que très contraignant, il est possible de contrôler l'utilisation des périphériques de stockage externe via le verrouillage des ports USB.

Cela peut être utile pour les serveurs comme pour les machines de type desktop.

U. M. INTERNET EXPLORER SERVEUR - DESKTOP

Présent par défaut sur la majorité des machines Windows, le navigateur Internet Explorer présente de nombreuses vulnérabilités par sa simple présence sur une machine.

Son utilisation est à proscrire.

Dans le cas où il n'est pas possible de se passer de son utilisation, celle-ci doit être encadrée et il doit être utilisé uniquement pour joindre l'application qui nécessite son utilisation dans un réseau interne.

Pour supprimer Internet explorer :

*Ouvrez le **Panneau de configuration** puis choisir **Programmes et fonctionnalités** ou appuyez simultanément sur les touches Windows+R puis tapez **appwiz.cpl** et validez en appuyant sur OK.*

Dans Programmes et fonctionnalités, sélectionnez l'item nommé Activer ou désactiver des fonctionnalités Windows.

Dans la fenêtre Composants de Windows, défilez jusqu'à la ligne Internet Explorer XX (généralement Internet Explorer 11).

Cliquez sur "Désinstaller" (ou décochez la case le cas échéant) puis validez.

Redémarrez Windows pour que les modifications soient effectives.

Un guide accessible est disponible ici :

<https://fr.wikihow.com/compl%C3%A8tement-d%C3%A9installer-Internet-Explorer>



V. SECURITE ENDPOINT SOPHOS INTERCEPT X ET MALWAREBYTES **SERVEUR - DESKTOP**

Endpoint type **Desktop**:

Sophos Intercept X

La solution choisie de sécurité Endpoint Sophos Intercept X Advanced doit être installée sur toutes les machines de type Desktop.

Elle permet de couvrir une grande partie des menaces type malwares, ransomware, exploit

La configuration de la console centrale Sophos sera appliquée après installation de la solution.

<https://www.avanet.com/en/kb/install-sophos-central-intercept-x-windows/>

Malwarebytes :

Malwarebytes viendra en complément sur les postes type Desktop de Sophos pour nettoyer les menaces de types Adware/Spywares

Pour l'installer :

<https://support.malwarebytes.com/hc/en-us/articles/360038479134-Download-and-install-Malwarebytes-for-Windows>

Malwarebytes antirootkit :

⚠ En cas de hardening tardif ou de période de vulnérabilité constatée, il est préconisé d'utiliser en plus, Malwarebytes anti rootkit pour analyser les couches basses qui pourraient abriter un malware dissimulé

<https://fr.malwarebytes.com/antirootkit/>

Endpoint type **Serveur**:

La solution intercept X Advanced pour serveur est adapté aux endpoint de ce type.

Un guide d'installation est disponible ici :

<https://phoenixnap.com/kb/sophos-intercept-x-advanced-for-server-installation-guide>

Les serveurs critiques bénéficieront de la solution intercept X Advanced avec EDR

<https://www.sophos.com/fr-fr/products/endpoint-antivirus/edr.aspx>

W. DESACTIVER IPV6 **SERVEUR - DESKTOP**



IPV6 est souvent à l'origine de faille de sécurité dû au faible encadrement de ce protocole par rapport à l'IPV4 or il est parfois activé.

S'il n'est pas utilisé et encadré, IPV6 doit être désactivé.

Voici deux guides pour désactiver IPV6 :

<https://www.malekal.com/desactiver-ipv6-windows/>

<https://www.tutos.eu/6450>

X. SAUVEGARDES VEEAM **SERVEUR** - **DESKTOP**

Il est important d'appliquer à la machine la politique de sauvegarde dédiée.

VEEAM

L'agent VEEAM sera nécessaire.

Un guide explique le déploiement de l'agent sur Windows


<https://helpcenter.veeam.com/docs/agentforwindows/userguide/quickstart.html?ver=50>

Outil Windows

Il est aussi possible d'utiliser l'utilitaire de sauvegarde et de restauration si VEEAM n'est pas accessible.

Voici un guide.

<https://support.microsoft.com/fr-fr/windows/sauvegarde-et-restauration-dans-windows-10-352091d2-bb9d-3ea3-ed18-52ef2b88cbef>

 Cette méthode ne protégera pas en cas de chiffrement par rançongiciel (Ransomware)

Y. AUDIT AUTOMATISEE DES VULNERABILITES **SERVEUR** - **DESKTOP**

La gestion des vulnérabilités est effectuée via la solution Qualys.

Il convient donc d'installer l'agent Qualys via le guide ci-dessous :

<https://www.qualys.com/docs/qualys-cloud-agent-windows-install-guide.pdf>

Le fichier pour installer l'agent correspondant à l'OS choisi vous sera fourni.

Un rapport des vulnérabilités sera disponible à l'issue des premiers scans

Z. ENUMERATION GLOBALE VIA UTILITAIRES OU SCRIPTS **SERVEUR** - **DESKTOP**



Il est possible d'énumérer différents points de contrôle à l'aide d'utilitaires ou de scripts pour contrôler que la machine ne présente pas de vulnérabilités :

Il convient d'étudier les points mis en avant lors de l'exécution de ces scripts.

Winpeas :

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS/winPEASexe/binaries>

Seatbelt

<https://github.com/GhostPack/Seatbelt>

SharpUp

<https://github.com/GhostPack/SharpUp>

PowerUp.ps1

<https://github.com/PowerShellEmpire/PowerTools/blob/master/PowerUp/PowerUp.ps1>

⚠ Il est impératif de supprimer les scripts et utilitaires de la machine une fois utilisé.

AA. REFERENCES

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>

<https://hichamkadiri.wordpress.com/2017/12/22/os-hardening-checklist-que-vous-devez-connaître-pour-mieux-sécuriser-votre-infrastructure-windows-server-2016/>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>

<https://activedirectorypro.com/active-directory-security-best-practices/>

https://www.netwrix.fr/windows_server_hardening_checklist.html

<https://docs.microsoft.com/fr-fr/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always>

<https://www.securiteinfo.com/conseils/securite-physique-et-logique-du-materiel-informatique.shtml#:~:text=Si%20quelqu'un%20r%C3%A9ussit%20%C3%A0,aux%20ordinateurs%20et%20aux%20%C3%A9quipements.>

<https://tryhackme.com/room/windows10privesc>