Formation Windows 10/11 Pro Ent LTSC - Sr 10-11 – Système Cours

Michel Cabaré / www.cabare.net / michel@cabare.net

Windows 10-11 Système Pro Entreprise Education LTSC - 21H2 - Sr 10-11 - Cours Système V3.0 - Décembre 2021



https://WWW.CABARE.NET©



Microsoft Partner Ce Support a pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion du système Windows 10 -11 mis à jour. Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

En effet, et c'est là **sa vocation première**, ce document doit "servir de support à la prise de notes en formation, et sera donc avantageusement complété par vos soins". Son but est de permettre une présentation de vos notes plus structurée et donc plus facilement utilisable ensuite.

Bon Travail

Michel Cabaré

Table des Matières

ASSISTANT CREATION DE PROFIL	7
Nouveau profil « manuel »: Profil sur Windows 10 pro - 21H2: Profil sur Windows 11 pro- 21H2:	7 7 9
LES PROCESSUS SOUS WINDOWS	12
SEQUENCE POST : POWER ON SELF TEST	12 12 13 14 15 16 18 20 22 23 23 24
LISTER LES SERVICES - POWERSHELL	24
OUTH & CESTION DE DISOUE	24
Deep a gment ation of $\nu D \in \mathcal{P}$.	<u>20</u> 26
NETTOYAGE DE DISQUE:	26
INTEGRITE WINDOWS 10	
LES DLL (DYNAMIC LINK LIBRARIES) : WRP PROTECTION DES DLL : sfc - system file checker	28 28 29
UAC- USER ACCOUNT CONTROL	30
OBJECTIF VISE : IL – INTEGRITY LEVEL : GESTION DE L'UAC (PANNEAU DE CONFIGURATION): GESTION DE L'UAC (STRATEGIES LOCALES): Désactivation de l'UAC ; Désactivation de l'UAC pour les Administrateur : Désactivation l'UAC pour les Utilisateurs : Activation l'UAC aussi pour le compte Administrateur Root : EXECUTER EN MODE ADMINISTRATEUR: Depuis un raccourci. Depuis l'invite executer. Depuis un executable Runas changement de login (pas de gestion de l'UAC)	30 32 33 33 33 33 34 35 35 35 36 36
INSTALLATIONS ET VIRTUALISATION	
PRECONISATION MICROSOFT : VIRTUALISATION DES PROCESSUS : COMPATIBILITE AVANT WINDOWS 10	38 38
EXECUTER EN MODE COMPATIBILITE:	40 41



PROTECTION DEP	
PRINCIPE DEP DATA EXECUTION PREVENTION:	42
DESACTIVATION COMPLETE DE DEP :	42
DESACTIVATION POUR UNE APPLICATION DE DEP :	42
TEST MEMOIRE	
Depuis Windows 10	43
AUTHENTIFICATION WINDOWS 10	44
Plusieurs Mode possibles UAF - U2F:	44
PAR CODE PIN :	44
PAR TRACE SUR UNE IMAGE :	
LOGIN SUR SAM OU AD :	
COMPTE MICROSOFT (COUPLE A UN COMPTE LOCAL) :	47
Désactivation compte Microsoft (login sur la machine)	
Désactivation compte Microsoft (via le Web) - msapolicy.admx	
ECRAN DE VERROUILLAGE – ECRAN D'ACCUEIL :	52
BUREAU - ECRAN D'ACCUEIL:	54
LE BUREAU	56
ECRAN ACCUEIL PAR DEFAUT	
MENU DEMARRER WINDOWS	
CORTANA & WINDOWS SEARCH	
Ι 'Αςρεςτ δε Codtana	58
L'ASPECT DE CORTANA Refuser Cortana à l'installation	
Cortana Gpo - désactiver – search.admx	
*	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	59
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	59 61
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	59 61
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	59 61 61
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	59 61 61 62
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX AVATAR DU LOGIN MODIFICATION DE L'AVATAR LES TUILES TUILES PAR DEFAUT APPLICATIONS APPS : UWP - APPLICATIONS SYSTEME - APPLICATIONS GESTION DES APPX INSTALLEES ET OU APPROVISIONNNEES EN POWERSHELL SUPPRESSION DES PACKAGES UTILISATEUR EN COURS (INSTALLEES) SUPPRESSION DES PACKAGES PROVISIONNES <i>Supprimer tous les packages</i> GESTION WINDOWS STORE CANEVAS – ECRAN D'ACCUEIL CANEVAS ECRAN D'ACCUEIL - EXPORT-STARTLAYOUT COMPTES UTILISATEURS COMPTE D'UTILISATEURS – SESSION: CONNEXION MULTIPLES UTILISATEUR DESACTIVER LA BASCULE RAPIDE UTILISATEUR DESACTIVER LA BASCULE RAPIDE UTILISATEUR	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX AVATAR DU LOGIN MODIFICATION DE L'AVATAR LES TUILES TUILES PAR DEFAUT APPLICATIONS APPS : UWP - APPLICATIONS SYSTEME - APPLICATIONS GESTION DES APPX INSTALLEES ET OU APPROVISIONNNEES EN POWERSHELL SUPPRESSION DES PACKAGES UTILISATEUR EN COURS (INSTALLEES) SUPPRESSION DES PACKAGES PROVISIONNES. Supprimer tous les packages GESTION WINDOWS STORE CANEVAS – ECRAN D'ACCUEIL CANEVAS – ECRAN D'ACCUEIL - EXPORT-STARTLAYOUT. COMPTES UTILISATEURS COMPTE D'UTILISATEURS CONPES UTILISATEURS SUPPRESSION MULTIPLES UTILISATEUR. DESACTIVER LA BASCULE RAPIDE UTILISATEUR Regedt32.exe SID SECURITY IDENTIFIER : WHOAMI : COMPTES VISIBLES PRE-DEFINIS :	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX. AVATAR DU LOGIN	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX. AVATAR DU LOGIN MODIFICATION DE L'AVATAR LES TUILES TUILES PAR DEFAUT APPLICATIONS APPS : UWP - APPLICATIONS SYSTEME - APPLICATIONS GESTION DES APPX INSTALLEES ET OU APPROVISIONNEES EN POWERSHELL SUPPRESSION DES PACKAGES UTILISATEUR EN COURS (INSTALLEES) SUPPRESSION DES PACKAGES PROVISIONNES. Supprimer tous les packages. GESTION WINDOWS STORE CANEVAS – ECRAN D'ACCUEIL CANEVAS ECRAN D'ACCUEIL - EXPORT-STARTLAYOUT. COMPTES UTILISATEURS COMPTE D'UTILISATEURS – SESSION: CONNEXION MULTIPLES UTILISATEUR. DESACTIVER LA BASCULE RAPIDE UTILISATEUR Regedi32.exe SID SECURITY IDENTIFIER : WHOAMI : COMPTES VISIBLES PRE-DEFINIS : COMPTES INVISIBLES PRE-DEFINIS : COMPTES INVISIBLES SYSTEME : UTILISATEURS LOCAUX: GESTION DES COMPTES:	
RECHERCHE SEARCH WINDOWS (ET CORTANA) - SEARCH.ADMX	



GROUPES LOCAUX	76
NOTIONS DE GROUPES :	76
GROUPES LOCAUX PREDEFINIS :	76
PROFILS UTILISATEURS	77
LIENS SYMBOLIQUES – RACCOURCIS – JONCTIONS :	77
Objectif :	77
PROFIL LOCAL:	
EMPLACEMENT PROFILS LOCAUX SEVEN:	
STRUCTURE DES PROFILS WINDOWS 10 :	
STRUCTURE D'UN PROFIL UTILISATEUR	80
PROFIL PAR DEFAULT	
PROFIL PUBLIC (FX-ALL USERS)	
SUPPRIMER TOUS LES PROFILS LOCALIX WINDOWS 10.	83
Par GPO	
Par base de registre	
Par utilitaire delprof2	
INTERFACE WINDOWS 10	
	05
ACCES PARAMETRES WINDOWS 10:	83
Reseau et internet Mise à Jour et Sécurité	
PANNEAU DE CONFIGURATION STYLE 7:	
L'EXPLORATEUR WINDOWS:	
INTERFACE AERO:	
MENU CONTEXTUEL / ACCUEIL WIN+X	90
COMPROMIS PERFORMANCES – ARRET SERVICES:	91
BUREAUX VIRTUELS:	
HISTORIQUE DES ACTIVITES – TIMELINE - OSPOLICY.ADMX	
MENU WIN-X	95
GESTION ACCES RAPIDE:	95
STRUCTURE MENU WINDOWS-X	96
TEST MODIFICATION MENU WIN-X WINDOWS 10 (1709 – 1803)	97
UTILITAIRE WIN-X EDITOR 3.0	
Ajouter un groupe	
Ajouter un executable	
Ajouer un element au panneau de configuration ou outit à daministration Restaurer le menu initial	
ACCES RAPIDE EXPLORATEUR	
GESTION ACCES RAPIDE:	
OUVERTURE EXPLORATEUR SUR C: + PAS D'ACCES RAPIDE AUTOMATIQUE	
DESINSTALLER L'ACCES RAPIDE:	103
DESINSTALLER ONEDRIVE	
ICONES POINTS DE LANCEMENT ONEDRIVE:	105
DESACTIVATION DE ONEDRIVE:	
INCLASSABLES WINDOWS 10	
Menu etendus MAJ + clic droit:	
OUTILS DXDIAG:	
OUTILS SHUTDOWN:	
WHOAMI / RUNAS:	
HISTORIQUE DE FIABILITE – PERFMON /REL :	109
ENREGISTREUR D'ACTION - PSR.EXE:	



CONSOLE MMC	
MICROSOFT MANAGEMENT CONSOLE:	
CREER UNE CONSOLE PERSONNALISEE:	
LIMITER LES FONCTIONS D'UN COMPOSANT LOGICIEL :	114
ENREGISTRER LA CONSOLE UTILISATEUR :	115
GPEDIT.MSC	116
SECPOL.MSC - RAPPEL STRATEGIES LOCALES ET GPO DE DOMAINE	116
GPEDIT.MSC - EDITEUR DE STRATEGIE DE DOMAINE "LOCALE" !:	116
LISTE DE TOUTES LES STRATEGIES – POLICYSETTINGS—1809.XLS :	117
Policysettings – 10-21H2.xls :	118
POLICYSETTINGS – 11-21H2.XLS :	
VOIRE LES NOUVEAUTES PAR BRANCHE :	119
TELECHARGER (INSTALLER) DES ADMX MODELE DE GPO 10-1809 (SUR UN SERVEUR)	
TELECHARGER (INSTALLER) DES ADMX MODELE DE GPO 10-21H2 (SUR UN SERVEUR)	
TELECHARGER (INSTALLER) DES ADMX MODELE DE GPO 11-21H2 (SUR UN SERVEUR)	
GPO WINDOWS 10 QUI DISPARAISSENT (SOUS WINDOWS 11):	
SERVICES- NOMS LONG - COURTS	
SERVICES PAR NOMS COURTS	
SERVICES PAR NOMS LONGS - FR	



ASSISTANT CREATION DE PROFIL

Nouveau profil « manuel »:

Lorsque l'on crée un nouvel utilisateur, sur un poste Windows, un nouveau profil sera créé pour son environnement lors de sa première ouverture de session.

Il récupèrera des éléments éventuellement posés dans le profil par défaut mais déroulera aussi une 1° séquence découlant des obligations RGPD et des obligations de confidentialités.

Cette séquence varie assez selon les branches. Elle peut être bien sur paramétrée par des GPO ou des réglages sur le poste, mais le déroulement « natif » permet d'avoir une idée des réglages minimum que l'on peut avoir envie de gérer

Après une 1° authentification réussie, il y a donc création du profil utilisateur

Nous préparons votre système

Profil sur Windows 10 pro - 21H2:

Les questions « profil » utilisateurs posées sont les suivantes :













Profil sur Windows 11 pro- 21H2:

Les questions « profil » utilisateurs posées sont les suivantes :





Améliorer l'écriture manuscrite et la saisie

Choisissez vos paramètres, puis sélectionnez **Accepter** pour les enregistrer. Consultez le lien **En savoir plus** pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.







Autoriser les applications à utiliser l'identifiant de publicité

Choisissez vos paramètres, puis sélectionnez **Accepter** pour les enregistrer. Consultez le lien **En savoir plus** pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.



Les applications peuvent utiliser l'identifiant de publicité pour proposer des publicités plus personnalisées conformément à la politique de confidentialité du fournisseur d'applications.



Vous verrez toujours autant d'annonces, mais il se peut qu'elles soient moins pertinentes pour vous.

En savoir plus

Accepter



LES PROCESSUS SOUS WINDOWS

Séquence POST : Power On Self Test

C'est la séquence que tout PC déroule, indépendamment du système. Le **BIOS** ou le **EFI** du PC vérifient la présence de certains matériels, (mémoire, disque, périphériques). Après cette séquence l'ordinateur doit trouver le gestionnaire de démarrage nommé **Bootmgr**.



Msconfig permet de dire ce que l'on veut ou non Désactivable avec **SHIFT** au moment de l'ouverture de session



Vocabulaire système sous Windows 10 :

Schématiquement on peut distinguer :



- LA HAL Oou couche d'abstraction matérielle : fournie des fonctions pour contrôler le bus système, canaux DMA, déclenchement des interruptions, horloge système... toutes ces fonctions sont utilisées dans les autres parties du noyau
- Le Kernel (micro kernel) : c'est le noyau toujours en mémoire, traite les interruptions, permet au CPU d'allouer du temps aux différents processus, appelé aussi threads.
- L'exécutif

 (serveur noyaux) : c'est l'ensemble des services système de gestion mémoire – périphériques –fichiers – appellé donc threads système. Chaque service système progresse à son propre rythme
- les services noyaux sous systèmes environnement

 : il s'agit de supporter différentes interfaces...: win32 posix Os2... par exemple l'executif de windows défini un ensemble de fonction nommée API (Access Programming Interface).
 Un programme utilisateur fait appel à des API système pour dialoguer avec l'OS.
- les services noyaux systèmes

 nécessaires comme le spool
 d'impression, task manager ... et les services de sécurité associés
- Certaines applications peuvent utiliser directement des **DLL Dynamic Link** Library... qui elles feront appel si nécessaire aux API système

Les appels entres ces de programmes sont nommés LPC Local Procedure Call s'ils se font sur une machine, ou RPC Remote Procedure Call à distance.



Lister les Processus - les Services :

Appelable via CTRL+ALT+SUPPR ou via les propriétés de la barre des tâches, le Gestionnaire des tâches donne une vision plus complète de la chose !

Plusieurs onglets sont disponibles, l'onglet Processus regroupe

Des Application :

Gestionnaire des tâches

Programme lancé par l'utilisateur, ΟU lancé automatiquement au démarrage de Windows. Tourne dans une interface fenêtre, normalement sans incidence sur le fonctionnement de <u>Windows</u>

1.0							
Fichier O	ptions Affich	age					
Processus	Performance	Historique des ap	pplications	Démarrag	je Utilisateu	rs Détails	Services
	^				3%	25%	5 1'
Nom			Statut		Processeur	Mémoir	e Disqu
Applicat	ions (6)						
> 清 Exp	olorateur Windo	ows			0%	34,3 M	0 Mo
> 🙀 Ge	stionnaire des t	âches			0,4%	29,9 M	0 Mo
> 🧧 Mi	crosoft Edge (1	0)			2,3%	766,9 M	0 Mo
> 👿 Mi	crosoft Word (2	!)			0%	98,1 M	0 Mo
> 🗯 Sna	aglt - La captur	e d'écran sous			0%	3,1 M	0 Mo
> 💆 Uti	litaire de config	juration sys			0%	2,3 M	0 Mo
Process	us en arrière	e-plan (57)					
> 🔳 Ad	aptateur invers	e de performa			0%	1,6 M	0 Mo
> 🗖 Ad	obe Acrobat Up	odate Service (0%	0,7 M	0 Mo

Des Processus :

Correspond à des programmes vus par le système d'exploitation. Un processus est caractérisé par le fait

qu'il a une indentification (PID) au niveau du système, des dépendances et une priorité d'exécution. Il peut contenir plusieurs services.

Depuis υn processus on peut demander vie le menu contextuel Accéder aux Détails pour voir si un executable précis correspond, avec son PID

Applications (3)	App	lications	(3)
------------------	-----	-----------	-----

Bloc-notes

📄 Explorateur Windows

Isitionnaire des tâches							
	Développer						
Processus en arrière-p	Fin de tâche						
Application sous-syst	Valeurs de ressources						
👂 🔒 Indexeur Microsoft W	Créer un fichier de vidage						
KMS Connection Bro	Accéder aux détails						
Processus hôte pour	Ouvrir l'emplacement du fichier						

Processus Performance Historique des applications Démarrage Utilisateurs Détails Services

Nom	PID	Statut	Nom d'utilisateur	Pro	Mémoire (Description
💷 wlms.exe	1312	En cours d'exé	Système	00	276 Ko	Service de contrôle des licence
💷 winlogon.exe	532	En cours d'exé	Système	00	496 Ko	Application d'ouverture de ses
wininit.exe	468	En cours d'exé	Système	00	372 Ko	Application de démarrage de V
🙀 Taskmgr.exe	2344	En cours d'exé	Administrateur	00	9 768 Ko	Gestionnaire des tâches

l'onglet **Services :** regroupe les programmes géré par le système d'exploitation comme "partie intégrante du système". Un service est caractérisé par le fait qu'il peut se gérer via le gestionnaire de service Windows, et est lancé dans un processus, (souvent associé avec d'autres services).

👰 Gestion	Ş Gestionnaire des tâches − □ ×								
Fichier O	Fichier Options Affichage								
Processus	Processus Performance Historique des applications Démarrage Utilisateurs Détails Services								
Nom	~	PID	Description			Statut		Groupe	^
🔍 AdobeA	RMservice	3560	Adobe Acro	bat Update Se	ervice	En cou	ırs d'exé		
AJRoute	r		Service de re	outeur AllJoyr	ו 	Arrêté		LocalSe	rviceN



Système Windows Pro/Edu/Ent/LTSC https://www.cabare.net Page 14/139 - Michel Cabaré -

Arrêter Démarrer une Application, un Processus, un Service :

Dans le gestionnaire de tâches, on distingue Les **applications**, dont l'arrêt ne compromet pas le système, elles sont lancées en général par l'utilisateur

👰 Gestionnaire des tâches								
Fichier Options Affichage								
Processus	Performance	Utilisateurs D	étails Services					
	^			4%	92%			
Nom			Statut	Processeur	Mémoire			
Applicat	tions (17)	à distance		0%	217.6 Mo			
> 🙀 Ge	stionnaire des t	âches		0,5%	27,6 Mo			
> <i> [</i> Int	ernet Explorer (6	5)		0,1%	79,1 Mo			
> 💽 Int	erpréteur de co	mmandes Wi		0%	7,9 Mo			
> 💽 Mi	crosoft Edge (12	2)		0%	372,7 Mo			
> 📕 Mi	crosoft Manage	ment Console		1,0%	25,4 Mo			
> 👿 Mi	crosoft Word			0%	73,0 Mo			

On peut demander fin de tâche directement depuis l'onglet Processus...

>	> \overline Microsoft Management Console				28,2 Mo
>	W Microsoft Word			0%	78,7 Mo
>	Server Mana	Développer		0%	80.2 Mo
	Server manag	Fin de tậche		0.0	00,21110
>	🗰 Snaglt - La ci	Valeurs de ressources	>	0%	3,5 Mo

Si on demande d'afficher les détails via Accéder aux détails

>	Interpréteur de com		0%	7,9 Mo	
>	💽 Microsoft Edge (2)		0%	105,7 Mo	
>	> 👼 Microsoft Management Console				28,1 Mo
>	W Microsoft Word			0%	74,9 Mo
>	ᡖ Server Manager	Développer		0%	83,0 Mo
>	🗰 Snaglt - La capi	Valeurs de ressources	>	0%	3,6 Mo
>	🖳 Virtual Machine	Créer un fichier de vidage		0%	175,2 Mo
>	🖳 Virtual Machine	Accéder aux détails 📡		0%	169,6 Mo
>	🖳 Virtual Machine	Ouvrir l'emplacement du fichier		0%	176,3 Mo

Alors depuis cetonglet Détails... c'est parfois plus efficace, on pourra demander Fin de Tâche / Terminer l'arborescence du processus

Processus Performance	e Utilisate	urs Détails Services		
Nom	PID	Statut	Nom d'utilisateur	^
	528	En cours d'exécution	Administrateur	
vmconnect.exe	9732	En cours d'exécution	Administrateur	
WINWORD.EXE	9864	En cours d'exécution	Administrateur	
vmwp.exe	Fin c	3B-AE94FC		
dwm.exe	Term	niner l'arborescence du proc	esaus	D-ACC10E

Depuis l'onglet **Détails**... on peut repérer un **PID**, il pourra être utilisé en ligne de commande (cf **taskkill** par exemple) pour forcer l'arrêt d'une application « recalcitrante »



Arrêter Démarrer un Processus, un Service :

Dans le gestionnaire de tâches, on distingue Les processus, dont l'arrêt peut compromettre le système, elles sont lancées en général par le système lui-même ou les applications

Exemple, le processus Application sous-système spouleur

n Gestionnaire des tâches						
Fichier Options Affichage						
Processus	Performance	Utilisateurs	Détails	Services		
	^				4%	92%
Nom				Statut	Processeur	Mémoire
Process	us en arrière					
> 🗖 Ad	obe Acrobat Up	date Service	(32 b		0%	0,9 Mo
🕜 Aic	? Aide et support Microsoft				0%	3,2 Mo
 > 🖶 Ap	plication sous-	système spou	leur		0%	10,1 Mo
📝 Ch	argeur CTF		63		0%	3,8 Mo

On peut demander également d'afficher les détails via Accéder aux détails et on voit que cela corresponds donc à l'executable **Spoolsv.exe**

Processus	Performance	Utilisate	eurs Détails	Services		
Nom		PID	Statut		Nom d'utilisateur	
smss.ex	e	432	En cours d'	exécution	Système	
🖶 spoolsv	.exe	1006	En cours d'	evécution	Suctàme	
svchost	.exe	Fin de	tâche			
svchost	.exe	Termi	ner l'arboreso	ence du p	rocessus	
📧 svchost	.exe	Défini	e la priorité		、 、	
📧 svchost.exe						
svchost	.exe	Définir l'affinité				
svchost	.exe	Analy	ser la chaîne	d'attente		
svchost	.exe	Virtua	lisation du co	ontrôle de	compte d'utilisateur	
svchost	.exe	Créer	un fichier de	vidage		
svchost	.exe	Creer	un nenier de	viuage		
svchost	.exe	Ouvri	r l'emplacem	ent du fich	nier	
svchost	.exe	Reche	erche en ligne	2		
📧 svchost	.exe	Propri	iétés			
📧 svchost	.exe	Accéd	las aux sanvisi	<u>_</u>		
sychost	exe	Acced	ier aux servic	~3		

Si on veut accéder aux services (puisque c'est un service) alors une fois dans la console gestion des services (ouvris les services, par exemple)

Processus Performance U	Utilisateurs	Détails	Services			
Nom	PID	Desc	ription		Statut	Groupe
SDTC 😳	1076	Coo	rdinateur de transactions	distrib	En cours d'exé	
🔍 Spooler	1096	Spou	uleur d'impression		En cours d'exé	
🔍 igfxCUIService2.0.0.0	1104	3	Démarrer	S	En cours d'exé	
🔍 nsi	1216		Arrêter	u	En cours d'exé	LocalService
🔍 W32Time	1224		Redémarrer		En cours d'exé	LocalService
🎑 Imhosts	1232				En cours d'exé	LocalServiceN
🔍 UsoSvc	1268		Ouvrir les services		En cours d'exé	netsvcs



Système Windows Pro/Edu/Ent/LTSC https://www.cabare.net Page 16/139 - Michel Cabaré -

Il va falloir comment il se nomme ! Ici Spooler d'impression

Services (local)	Nom	Descript	tion		État	Type de démarrage
	Service SSTP (Secure Socket	Prend er	n charge la connexi	on par le protocole S	En cours d'exécu	Manuel
	🥋 Services Bureau à distance	Autorise	e les utilisateurs à se	connecter de mani		Manuel
	🤹 Services de chiffrement	Fournit	trois services de ge	tion : le service de b	En cours d'exécu	Automatique
	Shared PC Account Manager	Manage	s profiles and acco	unts on a SharedPC		Désactivé
	🖏 SMP de l'Espace de stockag	Service I	hôte du fournisseur	de gestion de l'Espa		Manuel
	Spouleur d'impression	Ce servi	ce met en spoule le	s travaux d'impressi	En cours d'exécu	Automatique
	🖏 Station de travail 😽	Crée et i	maintient des conn	exions de réseau clie	En cours d'exécu	Automatique
	🖏 Stockage des données utilis	Gère le s	stockage des donné	es utilisateur structu		Manuel
Et effective	ement, lorsque l'	on	Propriétés de Spo	uleur d'impression ((Ordinateur local)	×
demande le	es propriétés de	се	riophetes de ope	arear a impression (oramatear localy	
service, Wind	lows nous indique b	ien	Général Connex	on Récupération D	épendances	
aue c'est le	fichier spoolsv.exe	aui				
en est à l'oric	nine	90.	Nom du service	Spooler		•
		×	Nom complet :	Spouleur d'impressi	ion	•
		-				
Nomdusoni			Description :	Ce service met en : et gère l'interaction	spoule les travaux d'in avec l'imprimante. Si	npression A
Nom au servi	Ce -			arrâtaz ce service	voue ne nourrez nlue	imprimer ni
Spoole	er		Chemin d'accès	des fichiers exécutable	s:	•
•			C:\Windows\Sy	tem32\spoolsv.exe		
Nom comple	et i		▼ _			
Snoule	our d'impression		Type de demarra	ge: Automa	tique	~
opould						
Nom Executo	able					
Speele						
Spools	SV.EXE		État du service :	En cours d'exécutior	1 I	· · · · ·
			Démarrer	Arrêter	Suspendre	Reprendre
			Vous pouvez spo service.	ècifier les paramètres qu	ui s'appliquent au dén	narrage du

En résumé donc on a pas moins de 4 appellations différentes selon le niveau ou l'on se place dans le **gestionnaire de tâche**, ou le **gestionnaire de services** (si le **processus** correspond à un **service**):

Dans le	e Gestionnaire o	des tâches	Dans le Gestionna	aires des services
Onglet Processus (nom)	Onglet Détail (nom + Pid)	Onglet Services (nom service + Pid + Description)	Si Français (nom complet / nom long + Description)	Si US (nom complet / nom long + Description)
Application sous- système spouleur	Spoolsv + PID	Spooler + PID + Spouleur d'impression	Spouleur d'impression + « descriptif »	Print Spooler + « description »



Fichier Options Affichage							
Processus	Performance	Historique des applications		Démarrage	Utilisate	eurs Détails	Services
Nom	*	PID	Statut	Nom d'util	Pro	Mémoire (Description
👰 Taskmgi	r.exe	2124	En cours d'exé	Administr	02	7 880 Ko	Gestionnaire des tâc
💷 taskhost	ex.exe	1976	En cours d'exé	Administr	00	1 000 Ko	Processus hôte pour
System		4	En cours d'exé	Système	02	72 Ko	NT Kernel & System
svchost.	exe	652	En cours d'exé	Système	00	1 360 Ko	Processus hôte pour

Ainsi souvent un processus générique **svchost** intègre comme son nom le laisse supposer plusieurs services – traçables avec le PID (dans l'example 652)

Fichier Options Affichage							
Processus Performance Historique des applications Démarrage Utilisateurs Détails Services							
Nom	PID	Description	Statut	Groupe			
🔍 Power	652	Alimentation	En cours d'exé	DcomLaunch			
🔍 PlugPlay	652	Plug-and-Play	En cours d'exé	DcomLaunch			
Sa LSM	652	Gestionnaire de session locale	En cours d'exé	DcomLaunch			
CeviceInstall		Service d'installation de périphér	Arrêté	DcomLaunch			
🔍 DcomLaunch	652	Lanceur de processus serveur DC	En cours d'exé	DcomLaunch			
BrokerInfrastructure	652	Service d'infrastructure des tâch	En cours d'exé	DcomLaunch			
🔍 defragsvc		Optimiser les lecteurs	Arrêté	defragsvc			

Processus Performance Historique des applications Démarrage Utilisateurs Détails Services

Dans l'onglet **Services** on peut

Arrêter/Démarrer/redémarrer un service: selon son état, Et accéder à la gestion des services via Ouvrir les services...

Nom	PID	Description	Statut	Gr	
🔍 Power	652	Alimentation	En cours d'exé	De	
🔍 PlugPlay	652	Plug-and-Play	En cours d'exé	Do	
🔍 LSM	652	Gestionnaire de session lo	En cours d'exé	Do	
🔍 DeviceInstall		Service d'installation	4	A	-20
🔍 DcomLaunch	652	Lanceur de processu	r	De	
🔍 BrokerInfrastructure	652	Service d'infrastructu	Arrêter		De
🔍 defragsvc		Optimiser les lecteur	Redéma	rrer	le
🧠 vmicrdv		Service de virtualisati	0		c
🧠 vmicheartbeat	1712	Service Pulsation Mic	Ouvrir le	s services	c
1 etieve		Acquisition d'image	Recherc	he en ligne	

Gestionnaire de Services

Accessible via le gestionnaire des tâches, en bas on trouve Ouvrir les services

Fichier O	ptions Affich	age							
Processus	Performance	Historique o	les applications	Démarrage	Utilisateu	rs Détails	Service	25	
Nom		PID	Description			Statut		Groupe	1
WSearch WMPNe	ı tworkSvc	1036	Windows Se Service Part	earch age réseau du	Lecteu	En cours d Arrêté	ľexé		

mais aussi via Clic droit - Ce PC / Gérer / Services





OU Panneau de configuration / Outils d'administration /

.	Services	de	com	posants
		_		

Services

📷 Sources de données ODBC (32 bits)

Ou en invite de commande services.msc

On obtient						
🎑 Services					>	×
Fichier Action Af	fichage ?					
	à 📑 🛛 📷 🕨 🔳 II 🕩					
🔍 Services (local)	Services (local)					
	Explorateur d'ordinateurs	Nom	Description	État	Type de démarrage	^
	<u>Arrêter</u> le service <u>Redémarrer</u> le service	 dmwappushsvc Données de contacts_332d6 Dossiers de travail 	Service de r Indexe les d Ce service s	En co	Manuel (Déclencher Manuel Manuel	
	Description : Tient à jour une liste des ordinateurs présents sur le réseau et fournit cette liste aux ordinateurs désignés comme navigateurs. Si ce service est arrêté, la liste ne sera pas mise ou tenue à jour. Si ce service est désactivé, les services qui en décandent pas pourent pas	 Elan Service Événements d'acquisition d Expérience audio-vidéo hau Expériences des utilisateurs Explorateur d'ordinateurs Extensions et notifications d Fichiers hors connexion 	Lance les ap qWave (Qu Le service d' Tient à jour Ce service o Le service Fi	En co En co En co	Automatique Manuel Manuel Automatique Manuel (Déclencher Manuel Manuel (Déclencher	

Pour un service ou une application particulière, on peut avoir son PID

/				
G Browser	5172	Explorateur d'ordinateurs	En cours d'exé	netsvcs

On à le nom de l'executable, le nom du service en francais, et en anglais...

on peut demander



et on peut avoir une idée des dépendances...



Propriétés de Explorateur d'ordinateurs (Ordinateur local)

Général Connexion Récupération Dépendances Certains services dépendent d'autres services, pilotes système ou groupes d'ordre de chargement. Si un composant système est arrêté ou ne fonctionne pas correctement, les services dépendants peuvent être affectés. Explorateur d'ordinateurs Ce service dépend des composants système suivants : 🖃 🥘 Serveur 🗄 🤷 Gestionnaire de comptes de sécurité Pilote de serveur SMB 2.xxx 🖃 🥘 Station de travail De qui ce service Mini-redirecteur SMB 2.0 dépend... 🖳 Pilote de prise en charge du navigateur v 💿. Service Interface du magasin réseau Les composants système suivants dépendent de ce service Qui dépends de ---- ce service... Que faire en cas de plantage Propriétés de Explorateur d'ordinateurs (Ordinateur local) \times Général Connexion Récupération Dépendances Sélectionnez la réponse de l'ordina Services de défaillance de ce service. Dbtenir de l'aide pour configurer les actions de récupération. Première défaillance : ~ Redémarrer le service Deuxième défaillance : Redémarrer le service Défaillances suivantes : ~ Ne rien faire

0

2

jours

Parcourir...

minutes

 \times

Msconfig.exe - gérer le lancement des services (temporairement):

Réinitialiser le compteur de défaillances après :

☐ Activer les actions en cas d'arrêt avec erreur. ◄ Options de redémarrage de l'ordinateur...

Redémarrer le service après :

Exécuter un programme Programme :

Lançable en fenêtre d'execution par **msconfig**

N.B: Les onglets 1-2-4 ne sont plus valables sous Windows10, on n'utilise **msconfig** maintenant uniquement avec l'onglet 3 pour choisir les **services à lancer au démarrage** :



On vient utiliser le 3°onglet Services :



P	Configuration du système				×
	Général Démarrer Services Démarra	age Outils			
	Service	Fabricant	Statut	Date désactivée	-
	 Expérience d'application Service de la passerelle de la co Gestion d'applications 	Microsoft Corporation Microsoft Corporation Microsoft Corporation	En cour Arrêté Arrêté		

On peut demander de Masquer services Microsoft, et lorsque l'on décoche un service, marque pour info la date de désactivation... qui restera ainsi jusquà ce que l'on revienne annuler le changement.

néral Démarrer Services Démar	rage Outils			
Service	Fabricant	Statut	Date de désa	cti ^
Adobe Acrobat Update Service	Adobe Systems Incorporated	En cour	21/05/2018 0	9:
Intel(R) Content Protection H	Intel Corporation	Arrêté		
Elan Service	ELAN Microelectronics Corp.	En cour		
✓ Intel(R) HD Graphics Control P	Intel Corporation	En cour		
McAfee Agent Common Services	McAfee LLC.	En cour		
McAfee Agent Service	McAfee LLC.	En cour		
McAfee Agent Backwards Com	McAfee LLC.	En cour		
McAfee Firewall Core Service	McAfee, LLC	Arrêté		
McAfee Service Controller	McAfee, LLC	En cour		
McAfee Validation Trust Prote	McAfee, LLC	En cour		
NVIDIA Display Container LS	NVIDIA Corporation	En cour	21/05/2018 0	9:
OpenSSH Authentication Agent	Inconnu	Arrêté	21/05/2018 0	9: 🗡
lotez que certains services Microsoft : ésactivés. <u>∂ M</u> asquer tous les services Microsof	sécurisés peuvent ne pas être t	Acti <u>v</u> er	tout <u>D</u> és	activer tout

Par exemple le 1° onglet Général est remplacé par :

MAJ + Redémarrage Options avancées »sDiagnostic = Mode sans Echec (ex F8)

Général	Démarrer Services Démarrage Outils	
Sélec D (tion du mode de démarrage émarrage normal Charger tous les pilotes de périphérique et tous les services	
	émarrage en mode diagnostic Jharger seulement les pilotes de périphérique et les services de t	base
0	émarrage sélectif	
	/ Charger les services système	

Le 4°onglet Démarrage de msconfig est remplacé par le Gestionnaire de tâche, dans lequel on a un onglet Démarrage:

Conf	iguration d	u système	•			×	
Général	Démarrer	Services	Démarrage	Outils			
	Pour gérer les éléments de démarrage, utilisez la section Démarrage du Gestionnaire des tâches.						
				Ouvrir l	e Gestionnaire des tâches		

Démarrage







Gérer les programmes au Démarrage:

Appelable via **CTRL+ALT+SUPPR** ou via les propriétés de la barre des tâches, le **Gestionnaire des tâches** permet cela avec l'onglet **Démarrage**:

😰 Gestionnaire des tâches — 🗆										×
Fich	nier O	ptions Affichage								
Pro	cessus	Performance Historique	des applications	Démarrag	e Utilisateurs	Détail	s Services			
						Dernië	re heure du	u BIOS	: 10.5 se	econdes
No	m	^	Éditeur		Statut	Ir	npact du d	é		
	🗋 bg	info-cabare.bat			Activé	N	lon mesuré			
	S co	leaner	Piriform Ltd		Désactivé	А	ucun			
>	Co	mmon User Interface	McAfee LLC.		Activé	H	aut			
	K ET	D Control Center	ELAN Microele	ctronics	Activé	В	as			
	📑 Hk	cmd			Activé	Ν	lon mesuré			
	🔳 Igf	xpers			Activé	Ν	lon mesuré			
	🧾 igf	xTray.exe			Activé	В	as			
	i Mi	crosoft OneDrive	Microsoft Corp	oration	Activé	N	loyen			
	≪ N\	/IDIA Update Backend	NVIDIA Corpor	ation	Désactiver	-				
	🛟 Wi	ndows Defender notificati ndowsUpdateNotifier	Microsoft Corp Christoph Pan <u>c</u>	orati gerl	Ouvrir l'emplac Recherche en li Propriétés	ement gne	du fichier			

Rappel des emplacements utilisés

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce X:\ProgramData\Microsoft\Windows\Start Menu\Programmes\Démarrage X:\User\%username%\AppData\RoamingMenu\Microsoft\Windows\ Start Menu \ Programmes\Démarrage





Tasklist (SEVEN - XP):

Cette commande porte pas mal de zone d'ombre...

Tasklist

```
C:\Documents and Settings\Administrateur>tasklist /?
TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]]
[/M [module] ¦ /SUC ¦ /U] [/FI filtre] [/F0 format] [/NH]
```

Si ces options fonctionnent, les autres options ont l'air plus délicates à utiliser...

Tasklist /SVC Tasklist /M

Taskkill (depuis SEVEN - XP):

Cette commande aussi porte pas mal de zone d'ombre...

Taskkill

C:\Documents and Settings\Administrateur>taskkill /? TASKKILL [/S système] [/U utilisateur [/P mot_de_passe]]] { [/FI filtre] [/PID ID_processus ¦ /IM image] } [/F] [/T]

Si ces options fonctionnent, les autres options ont l'air plus délicates à utiliser...

Taskkill /PID x

avec

Taskkill /PID x /F

Et

Taskkill /PID x /F /T

```
C:\>taskkill /pid 940
Opération réussie : un signal de fin a été envoyé au processus de PID 940.
C:\>taskkill /pid 940 /f
Opération réussie : le processus avec PID 940 a été terminé.
```



Quelques Processus de base

Processus	Type Arrêt	Commentaires
Smss.exe	Vital pour l'OS	Gestionnaire de session, lancé par le système et appelant a son tour Crss.exe et Winlogon
Csrss.exe -	Vital pour l'OS	Portion de sous système
Winlogon	Vital pour l'OS	Demande d'identification
Lsass.exe	Arrêt par PID unique	Serveur authentification local, génère pour winlogon a l'aide de msgina.dll un jeton
Svchost.exe	Arrêt par PID unique	Processus générique servant d'hôte pour d'autres processus On peut fouiller avec tasklist
Services	Arrêt par PID unique	Gestionnaire de contrôle des services
Spoolsv.exe	Arrêt par PID unique	Gestion des tâches d'impression

Depuis les premiers processus vitaux lancé par le système... on peut retrouver

Listes les services - powershell

Quelques services avec leur nom français, anglais, et les noms des processus associés, en français. Pour un service particulier

Lister - Arreter les Processus (services, applications):

😰 Gestionnaire des tâches								
Fichier O	ptions Afficha	age						
Processus	Performance	Utilisateurs	Détails	Services				
	^					16%	92%	
Nom			Stat	Statut		Processeur	Mémoire	
Applications (17)								
> 🎭 Connexion Bureau à distance						0,7%	217,6 Mo	
> 🐂 Explorateur Windows					0%	46,0 Mo		
> 🙀 Ge	stionnaire des t	âches				1,2%	22,3 Mo	

Correspond à

🔳 dwm.exe	1136	En cours d'exécution	DWM-1	00	57 016 Ko	Non autorisé
📊 explorer.exe	9,40	En cours d'exécution	Administr	01	47 360 Ko	Non autorisé
fontdrvhost.exe	વેલ્ટે	En cours d'exécution	UMFD-0	00	1 432 Ko	Non autorisé

III advantation							
傑勒	Explorateur d'ordinateur	Tient à jour un	ne liste des ordinate	urs présents sur v	otre réseau	Démarré	Automatiqu
11 OM	Server a contract of the server of the serve						



On à le nom de l'executable, le nom du service en francais, et en anglais...

	1	
Nom	Service	Description
Smss.exe	Vital pour l'OS	Gestionnaire de session, lancé par le système et appelant a son tour Crss.exe et Winlogon
Csrss.exe -	Vital pour l'OS	Portion de sous système
Winlogon	Vital pour l'OS	Demande d'identification
Lsass.exe	Arrêt par PID unique	Serveur authentification local, génère pour winlogon a l'aide de msgina.dll un jeton
Svchost.exe	Arrêt par PID unique	Processus générique servant d'hôte pour d'autres processus On peut fouiller avec tasklist
Services	Arrêt par PID unique	Gestionnaire de contrôle des services
Spoolsv.exe	Arrêt par PID unique	Gestion des tâches d'impression



OUTILS GESTION DE DISQUE

Defragmentation chkdsk /F /R:

Disponible dans les **outils** d'administration en interface graphique, Défragmenter et optimiser les lecteurs

Il est plus puissant et complet en invite de commande

👞 Administrateur : Invite de commandes - chkdsk	
Microsoft Windows [version 10.0.17763.1] (c) 2018 Microsoft Corporation. Tous droits réservés.	
C:\WINDOWS\system32>chkdsk Le type du système de fichiers est NTFS.	
Le nom de volume est vm-os-systeme.	

Les étapes peuvent prendre énormément de temps

Windows a a Aucune autr	analysé le système de fichiers sans trouver de problème. re action n'est requise.
75951311	Ko d'espace disque au total.
36424080	Ko dans 159433 fichiers.
133060	Ko dans 54843 index.
0	Ko dans des secteurs défectueux.
355947	Ko utilisés par le système.
65536	Ko occupés par le fichier journal.
39038224	Ko disponibles sur le disque.
4096	octets dans chaque unité d'allocation.
18987827	unités d'allocation au total sur le disque.
9759556	unités d'allocation disponibles sur le disque.

Les option **/F** et **/R** peuvent nécessiter un redémarrage de l'OS, (pour éviter un accès préemptif sur le lecteur) et nécessiter selon la taille du disque <u>plusieurs</u> <u>heures</u>

Nettoyage de disque:

Disponible dans les outils d'administration en interface graphique,



15/09/2018 09:29

Dans une machine on peut souvent trouver des dossiers ou des fichiers et des partitions « bizarres »

Windows.old	07/10/2018 19:59	Dossier de fichiers
\$WINRE_BACKUP_PARTITION.MARKER	07/10/2018 19:11	Fichier MARKER

Sans besoin de faire le détail,





on peut demander sur une machine stable de faire le ménage total !

Antivirus Windows Defender	2,73 Mo
🗹 📫 Fichiers journaux de la mise à niveau de Wind	187 Mo
🗹 📙 Fichiers programmes téléchargés	0 octet(s)
🗹 🔒 Fichiers Internet temporaires	873 Ko
🗹 📄 Le système a créé des fichiers de rapport d'err	486 Ko
🗹 📄 Cache de nuanceur DirectX	0 octet(s)
Fichiers d'optimisation de livraison	15,9 Mo
🗹 📱 Packages de pilotes de périphériques	164 Ko
🗹 🕂 Téléchargements	1,06 Mo
Fichiers de ressource linguistique	0 octet(s)
🗹 輶 Précédente(s) installation(s) de Windows	20,5 Go
🗹 🚺 Corbeille	751 Ko
Fichiers temporaires	0 octet(s)
Miniatures	4,00 Mo



les DLL (Dynamic Link Libraries):

les **DLL** sont des bibliothèques de routines chargées en mémoire au moment de leur appel (contrairement à un programme EXE qui se charge entièrement avant même de s'exécuter). Plusieurs avantages sont présents :

- En cas de modification de la bibliothèque de routines, il n'est donc pas nécessaire de recompiler tout le programme, le remplacement du fichier DLL est suffisant. Le programme utilise automatiquement les fonctions modifiées au prochain lancement.
- Les fonctions issues de la DLL ne sont alors plus chargées plusieurs fois, car plusieurs programmes peuvent se référer simultanément à une instance de la DLL présente en mémoire

Des inconvénients existent :

- La gestion des versions de DLL est complexe...
- Il faut éviter la mise à jours sauvage, et la gestion des packages pour garantir une stabilité du système

Il est toujours difficile de connaître la liste des DLL nécessaires (ou plus nécessaires au bon fonctionnement d'un programme). On peut utiliser des utilitaires mais la tâche reste complexe. A cet effet, un gestionnaire d'installation, à partir de win98, travaille normalement à partir des fichiers **.msi** pour maintenir cette liste à jour. Mais les applications ne prévoient pas forcement une procédure correcte....

WRP Protection des DLL :

Il existe un mécanisme intégré à windows permettant de vérifier les versions protégés de certains fichiers (.sys .dll .exe .ttf .fon .ocx) et de remplacer a la volée par leur version d'origine pour assurer l'intégrité du système. Ce mécanisme nommé **WRP** (windows Ressource protection) qui remplace la version 2000-XP de **WFP** (windows File protection) évite l'écrasement de fichier sensibles par des applications peut scrupuleuses...

A cet effet un cache contenant une "copie" d'origine des fichiers existe en

%systemroot%Winsxs

En cas d'écrasement d'un fichier, WFP puisera de l'aide dans :

- 1. le dossier Winsxs,
- 2. le Média d'origine,
- 3. le point d'installation réseau...

Le remplacement/mise à jour des fichiers système protégés est pris en charge uniquement dans les cas suivants :

- 1. installation de Service Pack ou de correctifs à l'aide d'Update.exe ;
- 2. mises à niveau du système d'exploitation à l'aide de Winnt32.exe ;
- 3. Windows Update.
- 4. A travers une API spéciale



sfc - system file checker

il existe une invite en ligne de commande **Sfc** permettant de forcer la vérification de l'intégrité du système Windows (sans attendre la vérification en tache de fond)

C:\Users\Adminis	strateur>sfc /help
Vérificateur de Copyright (c) M:	ressources Microsoft(R) Windows(R) version 6.0 icrosoft Corporation. Tous droits réservés.
Analyse l'intégn les versions inc	rité de tous les fichiers système protégés et remplace correctes par les versions Microsoft appropriées.
SFC [/SCANNOW] [/VERIFYFIL] [/OFFWINDIR /OFFBOOTDI]	[/UERIFYONLY] [/SCANFILE= <fichier>] E=<fichier>] =<répertoire connexion="" hors="" windows=""> R=<répertoire connexion="" hors="" windows="">]</répertoire></répertoire></fichier></fichier>
∕SCANNOW	Analyse l'intégrité de tous les fichiers système protégés et répare les fichiers endommagés dès que possible
∕VERI FYONLY	Analyse l'intégrité de tous les fichiers système protégés, Augune réparation p'est effectuée.
∕SCANFILE	Analyse l'intégrité du fichier référencé et le répare si des problèmes ont été identifiés. Spécifiez le chemin d'accès complet dans (fichien)
∕VERIFYFILE	Vérifie l'intégrité du fichier ayant comme chemin commlet (fichier) Augune rénamation p'est effectuée
∕OFFBOOTDIR	l'emplacement du répertoire de démarrage hors
∕OFFWINDIR	connexion. Pour les réparations hors connexion, spécifier l'emplacement du répertoire Windows hors connexion.

N.B: Cette commande peut provoquer l'accès au Media de Windows



Objectif Visé :

Ce n'est pas un moyen de se protéger contre les virus infaillible, mais plutôt une manière d'éduquer les utilisateurs et développeurs d'applications.

Sur Vista le compte par défaut fait partie du groupe des Administrateurs mais à des droits d'accès restreints au système.

Le principe est de lancer toutes les tâches en tant qu'utilisateur standard, que vous soyez administrateur ou non !

- ✓ Lorsqu'une opération requière des droits élevés, une boite de dialogue demande l'élévation des droits pour ce processus. (une simple confirmation)
- ✓ SI l'utilisateur ne fait pas partie du groupe des administrateurs, la boite de dialogue lui demande alors un compte et un mot de passe ayant des droits d'administration...

N.B : en réglage standard, seul le compte administrateur d'origine, (désactivé par défaut lors de l'installation) ne subit pas l'UAC !

IL – Integrity Level :

Lorsque vous ouvrez une session de manière générale avec Windows, le service de sécurité **LSASS** va créer un jeton qui contiendra le **SID** de l'utilisateur. C'est ce jeton qui sera utilisé pour lancer des applications.

Avec Windows 8, lorsque vous ouvrez une session, **LSASS** va créer deux jetons. Un qui va contenir toutes les informations comme dans Windows XP et un autre jeton "restreint" qui ne contiendra que les privilèges d'un utilisateur standard.

Chacun de ces jetons possède le même **SID** utilisateur plus, un SID de type **S-1-5-40-xXx** où xXx représente le niveau d'intégrité afin de les isoler.

C'est donc grâce à ces niveaux d'intégrité obligatoire et inchangeable durant leur durée de vie que va se baser toute la partie contrôle d'intégrité

C'est donc ce deuxième jeton qui sera utilisé pour lancer les différentes applications. Pour utiliser le premier jeton, celui avec tous les privilèges, vous devrez passer par une élévation de privilège

N.B : pour lancer ses applications en utilisant tout le temps le jeton avec tous les privilèges. Il suffit de cocher une case dans les propriétés de l'exécutable



Propriétés de snagit32.exe	×
Général Compatibilité Sécurité Détails Versions précédentes	
Si vous rencontrez des problèmes avec ce programme alors qu'il fonctionnait correctement sur une version antérieure de Windows, sélectionnez le mode de compatibilité adapté à cette version antérieure.	
Mode de compatibilité	
Exécuter ce programme en mode de compatibilité pour :	
Windows XP (Service Pack 2)	
Paramètres	51
Exécuter en 256 couleurs	
Exécuter avec une résolution d'écran de 640 x 480	
Désactiver les thèmes visuels	
Désactiver la composition du Bureau	
Désactiver la mise à l'échelle de l'affichage pour les résolutions élevées	
Niveau de privilège	
Exécuter ce programme en tant qu'administrateur	

L'UAC repose aussi sur un nouvel attribut dont sont dotés les processus, les fichiers les clés du registre : le niveau d'intégrité. Dit **IL** pour **Integrity Level**.

Les principaux niveaux IL : Limité – Utilisateur - Administrateur – System

- Il faut savoir que les processus Utilisateur / LUA ne peuvent pas modifier les processus s'exécutant dans un niveau d'intégrité supérieur. (mais ils peuvent les lire pour obtenir des infos...)
- Le groupe des administrateurs à un IL élevé
- Pour un utilisateur, les processus qu'il lance et ses fichiers ont un **IL** niveau moyen



Dans cette optique pax exemple, lorsque

l'on lance IE (par exemple) on lance en fait 2 processus, avec des niveaux IL différents...

lexplorer : avec un II d'utilisateur (pour stocker ses favoris...)

lexplorer : avec un II bas pour executer les activex et autres...

1 2	Gestionnaire des tâches						×	
Fichier Op	otions Afficha	age						
Processus	Performance	Historic	ue des applications	Démarrage Utilisat	eurs Dét	ails Services		
Nom	A	PID	Statut	Nom d'utilisateur	Pro	Mémoire (Description	^
🔲 dwm.exe	•	740	En cours d'exé	DWM-1	00	18 480 Ko	Gestionnaire de fenêtres du Bureau	
🥃 explorer.	exe	1928	En cours d'exé	Administrateur	00	22 988 Ko	Explorateur Windows	
🥘 iexplore.e	exe	2936	En cours d'exé	Administrateur	00	4 460 Ko	Internet Explorer	
🥘 iexplore.@	exe	3024	En cours d'exé	Administrateur	00	5 824 Ko	Internet Explorer	

Autre exemple: lorsque l'on récupère une pièce jointe, et que on la stocke, si c'est un exécutable, sont application a un IL de bas niveau, dont ne peut interférer avec les processus système ayant un IL élevé...



Gestion de l'UAC (panneau de configuration):

Le seul compte par défaut exempt de l'**UAC** étant le compte Administrateur (crée lors de l'installation) il faut essayer de gérer les effets de l'UAC

Il est recommandé de ne pas désactiver les invites du contrôle de compte d'utilisateur dans les paramètres de stratégie de groupe ou en agissant sur le curseur.

Bien que l'invite d'élévation soit la partie la plus visible du contrôle de compte d'utilisateur, celui-ci fournit également les composants sous-jacents comme :

- Mode protégé d'Internet Explorer
- Virtualisation de fichiers système et du Registre

Si on veut paramétrer cette gestion (...) via l'interface graphique il faut demander dans



la commande Modifier les paramètres de contrôle de compte d'utilisateur



la prise en compte de cette commande peut demander un redémarrage.



Gestion de l'UAC (stratégies locales):

Dans les stratégies locales de sécurité, se retrouvent les réglages de l'UAC

Dans le Panneau de Configuration / Outils d'administration /

😨 Outils d'administration

Puis Stratégies de sécurité locales 🗟 Stratégie de sécurité locale

Puis dans les **Stratégies locales / Options de sécurité** les stratégies repérées par la mention : Contrôle de compte d'utilisateur

🚡 Paramètres de sécurité	Stratégie
D Stratégies de comptes	Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Adminis
a 📴 Stratégies locales	Contrôle de compte d'utilisateur : mode Approbation duministrateur pour le compte Administrateur :
Stratégie d'audit	Controle de compte d'utilisateur : passer au bureau securise fois d'une demande d'elevation
Attribution des droits utilisateur	Controle de compte d'utilisateur : autoriser les applications UIAccess à demander l'elevation s
Options de sécurité	Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrate
Pare-feu Windows avec fonctions av	📓 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs st
Stratégies du gestionnaire de listes d	E Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévat
Stratégies de clé publique	📓 Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des
Stratégies de restriction logicielle	🐻 Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés
Stratégies de contrôle de l'application	B Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approba
Stratégies de sécurité IP sur Ordinate	Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre da
Configuration avancée de la stratégi	Contrôleur de domaine : conditions requises pour la signature de serveur l DAP
Configuration avancee de la strategi	we controled de domaine : conditions requises pour la signature de serveur LDAP

Désactivation de l'UAC :

Sans doute le plus ... radical

🖾 Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur





N.B : re-démarrage du PC obligatoire

Désactivation de l'UAC pour les Administrateur :

Il existe un moyen de préserver L'UAC et d'enlever cette boite de dialogue lors d'une demande d'approbation administrateur

📓 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Ad..

Propriétés de : Contrôle de compte d'utilisateur : c 📍 🌉
Paramètre de sécurité locale Expliquer
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur
Demande de consentement pour les binaires non Windows
Élever les privilèges sans invite utilisateur
Demande d'informations d'identification sur le bureau sécurisé Demande de consentement sur le bureau sécurisé Demande d'informations d'identification Demande de consentement Demande de consentement pour les binaires non Windows

Si la valeur par défaut est "Demande de consentement".

la valeur Elever les privilèges sans invite utilisateur est très pratique pour les administrateur!





Système Windows Pro/Edu/Ent/LTSChttps://www.cabare.netPage 33/139Sr10-11 – Système Cours - Ver 3.0- Michel Cabaré -

Désactivation l'UAC pour les Utilisateurs :

Lorsque les logiciels anciens deviennent incompatibles

📖 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard

Activation I'UAC aussi pour le compte Administrateur Root :

Cela permet de généraliser l'UAC au compte Administrateur d'origine (!!!).

🖾 Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

Paramètre de curseur	Paramètres de stratégie de groupe équivalents
Toujours m'avertir	 Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Demande de consentement sur le bureau sécurisé. Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est activé.
M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur (valeur par défaut)	 Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Demande de consentement pour les binaires non Windows. Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est activé.
M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur (avec bureau sécurisé)	 Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Demande de consentement pour les binaires non Windows. Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est désactivé.
Ne jamais m'avertir ØRemarque	 Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Élever les privilèges sans invite utilisateur.
Ce paramètre requiert un redémarrage pour entrer en vigueur.	 Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est désactivé.
	 Le paramètre de stratégie Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur est désactivé.
	 Le contrôle de compte d'utilisateur est désactivé.

DONC... il ne faut jamais utiliser en standard le compte Administrateur intégré pour travailler avec Windows 10, puisque un compte administrateur "autre" bénéficiera de l'effet protecteur de l'UAC sans occasionner de gêne (il suffit de demander une élévation de privilège silencieuse).

On peut demander une invite d'élévation automatique, mais on peut laisser l'UAC faire son travail...

N.B: une modification des réglages de l'UAC nécessite le plus souvent un redémarrage du poste, voir la réouverture de session, pour être sûr de la prise en compte des nouveaux paramètres. Surtout celle qui active / désactive l'UAC.



Executer en mode administrateur:

Pour lancer une application / fenêtre en mode administrateur, (ce qui suppose que l'UAC soit activé) il est possible

Depuis un raccourci

Si cela est possible demander clic/droit Exécuter en tant qu'administrateur



Si c'est possible on peut aussi paramétrer le raccourci pour qu'il mémorise le réglage de manière permanente.

Dans les Propriétés du raccourci, Avancé, on demande Executer en tant qu'administrateur

Propriété	s de : Invite o	le commandes			×		
Sécu	irité	Détails		Versions préc	édentes		
Général	Raccourci	Options	Police	Configuration	Couleurs		
0: \		Invite de comma	andes		Propriétés avanc	cées	
Type de cib	le :	Application		_	Choisiss	ez les propriétés avancées de ce raccourd	
Emplacement :		system32		Cette option permet d'exécuter ce raccourci en tant			
Cible :		%windir%\system32\cmd.exe					
					qu'administr	ateur, tout en protégeant votre ordinate	
Démarrer da	ins :	%HOMEDRIVE	%%HOMEPA	TH%	toute activi	té non autorisée.	
Touche de	Touche de raccourci : Aucun						
Exécuter :	Exécuter : Fenêtre normale				✓ Exécuter da	ans des zones mémoires différentes	
Commentair	e:	Effectuez des fo	onctions à bas	se de texte (ligne d			
Emplace	mont du fichio	Changer	d'icâne	August		ОК	

Depuis l'invite executer

Si cela est possible on valide par CTRL+MAJ+Entrée au lieu de ok

💷 Exéci	ıter	×
	Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.	
Ouvrir:	cmd	\sim
	OK Annuler Parcouri	r



Depuis un executable

Si on pointe l'executable, par exemple 1 Acrobat reader, il faut aller dans l'onglet **compatibilité**

🚺 Prop	riétés de : Adb	eRdr11004_fr_FR.exe				×		
Général	Compatibilité	Signatures numériques	Sécurité	Détails	Versions précédente	s		
Si ce pi de Win compat	Si ce programme ne fonctionne pas correctement sur cette version de Windows, essayez en lançant la résolution des problèmes de compatibilité.							
Comme	er la résolution d nt choisir manue de compatibilite	les problèmes de compati ellement les paramètres d é	e compatib	ilité ?				
Ы	écuter ce progr	amme en mode de comp	atibilité pou	r:				
Wind	dows 8		\sim					
Paran	nètres ode couleur réd eur 8 bits (256)	uit 🗸						
Exécuter avec une résolution d'écran de 640 x 480								
Désactiver les optimisations du mode plein écran								
Б	écuter ce progr	amme en tant qu'adminis	trateur					
Mod	lifier les paramèt	tres PPP élevés						

Runas changement de login (pas de gestion de l'UAC)

Si on pointe l'executable, par exemple cmd.exe

runas /user:util /savecred "c:\windows\system32\cmd.exe"



La première exécution donnera

invite de commande pour util
Tentative de lancement de c:\windows\write.exe en tant qu'utilisateur "POSTE-10-1803\util" ...
Entrez le mot de passe de util : _____

Mais ne redemanderas plus d'identification par la suite!




Les identifiants stockés via RUNAS /savecred peuvent être effacés via le panneau de configuration/ comptes utilisateurs / Gérer vos informations d'identification



Et on efface les informations d'identification Windows

Gestionnaire d'identification				—		×
← → × ↑ 🧧 « Tous les Panr	eaux de configuration > Gestionnaire d'identification	~ Ū	Rechercher			Q
Fichier Edition Affichage Outils						
Page d'accueil du panneau de configuration	Gérer vos informations d'identification	enregistrées pour les	sites Web les app	lication	<.	0
	connectées et les réseaux.	inegistices pour les	sites tree, ies opp		-	
	Informations d'identification Web	Informations d'id	lentification Win	dows		
	Sauvegarder les informations d'identification Restaurer les in	formations d'identifi	cation			
	Informations d'identification Windows Ajout	ter des informations	d'identification W	indows		
0	POSTE-10-1803\util (Ouverture de session interactive)	Mo	odifié : Aujourd'h	ui 📀		
	Informations d'identification à base de certificatAjouter des inf	formations d'identifi	cation à base de c	ertificat		
	Aucun certificat.					



INSTALLATIONS ET VIRTUALISATION

Préconisation microsoft :

Microsoft recommande que les programmes d'installation d'application globaux s'exécutent avec les droits administratifs et

- créent un répertoire sous le répertoire %ProgramFiles% (pour stocker les fichiers de l'application exécutables et les données auxiliaires)
- ✓ créent une clé sous HKEY_LOCAL_MACHINE\Software (pour leurs paramètres d'application.)

Lorsqu'une application s'exécute, elle peut le faire dans différents comptes utilisateur et devrait donc

- enregistrer les données spécifiques à l'utilisateur dans un répertoire %AppData% (propre à chaque utilisateur)
- ✓ enregistrer des paramètres propres à chaque utilisateur dans le profil d'annuaire de l'utilisateur sous HKEY_CURRENT_USER\ Software.

Les comptes utilisateur standard n'ont pas de droits d'écriture dans le répertoire %ProgramFiles% ou dans HKEY_LOCAL_MACHINE\Software, Mais puisque la plupart des systèmes de Windows sont à utilisateur unique et que la majorité des utilisateurs étaient administrateurs..., les applications qui enregistrent de façon inexacte des données utilisateur et des paramètres à ces emplacements fonctionnaient quand même.

Virtualisation des processus :

Si un programme d'installation se lance sans tous les droits administrateurs comme il va tenter d'écrire dans des dossiers systèmes ou protégés il court à l'échec. Pour prévoir ce type de problème, Microsoft a créé tout un système de virtualisation de dossier dans Windows 8.

- Sous Windows XP, dans un environnement limité, vous lanciez l'installation jusqu'au moment où un fichier a besoin d'être écrit dans un espace protégé Cette opération va faire "crasher" l'installation rendant le logiciel à moitié installé et donc inutilisable
- Windows 10 déroule toute l'installation pour savoir si il a besoin d'aller écrire dans les dossiers système ou des parties réservées du registre. Si c'est le cas, et que l'installateur n'a pas les autorisations suffisantes, alors un système de dossiers virtuels est mis en place.

En effet, au final toutes les applications peuvent écrire dans les dossiers systèmes et sécurisés de Windows. Seulement, parfois, ce ne sont pas les vrais dossiers systèmes de Windows. Ce sont en fait des dossiers virtualisés situés dans le profil de l'utilisateur. **... AppData\local\VirtualStore\...**

Ensuite une application, devant être exécutée avec les privilèges administrateur parce qu'elle va écrire dans **Program Files** ou dans la clef de registre **HKLM**, est exécutée avec un jeton "restreint", il n'y aura aucune erreur de la part du système.

Lors du lancement de l'application, celle-ci ira dans un premier temps regarder dans le dossier virtuel du profil, et si elle ne trouve rien, elle chargera les



paramètres dans le Program Files réel. Grâce à ce système, près de 90% des applications non réécrites pour Windows 10 allant écrire dans **Program Files** ou dans des dossiers systèmes fonctionnent. On parle de « **programmes hérités** »

Windows 10 traite un processus comme « virtualisable » si :

- il fait 32 bits (et non 64 bits),
- il ne s'exécute pas avec les droits administratifs,
- il n'a pas un fichier de signature spécifique pour Windows 10

Les emplacements de système de fichiers qui sont virtualisés pour les processus d'héritage sont

- %ProgramFiles%
- %ProgramData%
- %SystemRoot%

Cependant, tous les fichiers possédant une extension exécutable, y compris .exe, .bat, .scr, .vbs et autres, sont exclus par défaut de la virtualisation. (Cela signifie que les programmes qui se mettent à jour à partir d'un compte utilisateur standard échouent au lieu de créer des versions privées de leurs exécutables)

N.B : on peut vérifier si une application est virtualisable dans le gestionnaire de tâche, en ajoutant la colonne **Virtualisation**

Processus	Performance	Histo	rique des appli	cations	Démarrage	Utilisate	eurs Détails	Services	
Nom	^	PID	Statut		Nom d'utilisa	teur	Proc	Mémoire (Description
cmd.exe	1	1540	En cours d	′exé	Administrate	ur	00	384 Ko	Interpréteui
on conhost	.exe	1016	En cours d	'exé	Administrate	ır	00	916 Ko	Hôte de la f
CSrss.exe	•	368	En cours		Sélectio	onner d	les colonn	es 🛛 🗙	ocessus d
Csrss.exe	2	3016	En cours						ocessus d
dwm.ex	e	1416	En cours	Sélec	tionnez les colon	nes qui a	pparaîtront d	ans la table.	estionnair
🥃 explorer	.exe	1544	En cours						plorateur
Interrup	tions système	-	En cours		Octets de lecture	e d'E/S		^	pels de p
Isass.exe		540	En cours		Octets d'écriture	d'E/S			cal Secur
MsMpEr	ng.exe	1204	En cours		Octets d'autres (opération	s d'E/S		ntimalwar
Process	us inactif du	0	En cours		Nom du chemin d	racces de	l'image		urcentag
🙈 Searchir	dexer.exe	1596	En cours		Contexte du svs	iue tème d'ex	nloitation		dexeur M
services	exe	512	En cours		Plateforme	cenie diez	plottation		plication
smss.exe	2	280	En cours		Élevé				stionnair
🖶 spoolsv.	exe	736	En cours		Virtualisation du	contrôle d	de compte d'u	tilisateur 🖌	oplication
SppExtC	omObj.Exe	1984	En cours		rescription				AS Conne
sppsvc.e	exe	1468	En cours		Prévention de l'e	xécution	des données	×	rvice de l
nnant									
Processus	Performance H	istorique	e des application	s Dém	arrage Utilisate	urs Détai	ls Services		
Nom	P	ID :	Statut	Nom	d'utilisateur	Proc	Mémoire (Virtualisation	Description
cmd.exe	15	540	En cours d'exé	Admir	nistrateur	00	384 Ko	Non autorisé	Interpréteur de
conhost.	exe 10	016	En cours d'exé	Admir	nistrateur	00	916 Ko	Non autorisé	Hôte de la fenê
csrss.exe	30	58	En cours d'exé	Systèr	ne	00	832 Ko	Non autorisé	Processus d'exé
csrss.exe	30	016	En cours d'exé	Systèr	ne	00	908 Ko	Non autorisé	Processus d'exé

N.B : Comme les informations sont stockées dans le répertoire utilisateur, cela peut être gênant. Par exemple, pour une application qui stocke les meilleurs scores : l'utilisateur fera toujours le meilleur score !



COMPATIBILITE AVANT WINDOWS 10

Exécuter en mode compatibilité:

Si un programme fonctionnait correctement sur une version antérieure à Windows 10, et que vous ne disposez pas de la version spécifique, on peut tenter de demander de l'exécuter en mode compatibilité. Par exemple

ERDISK 23/03/2005 10:17 Application

On demande clic-droit sur l'exécutable, propriétés onglet Compatibilité

Propriétés de : Bginfo.exe
Général Compatibilité Signatures numériques Sécurité Détails
Si ce programme ne fonctionne pas correctement sur cette version de Windows, essayez en lançant la résolution des problèmes de compatibilité.
Lancer la résolution des problèmes de compatibilité
Comment choisir manuellement les paramètres de compatibilité ?
Mode de compatibilité
Exécuter ce programme en mode de compatibilité pour :
Windows XP (Service Pack 3) v
Paramètres
Mode couleur réduit
Couleur 8 bits (256) V
Exécuter avec une résolution d'écran de 640 x 480
Désactiver la mise à l'échelle de l'affichage pour les résolutions élevées
Niveau de privilège
Exécuter ce programme en tant qu'administrateur
Modifier les paramètres pour tous les utilisateurs
OK Annuler Appliquer

- si il y a besoin d'exécuter avec un privilège d'administrateur
- On peut choisir un mode de compatibilité

Mode de compatibilité Exécuter ce programme en mode de compatibilité pour : Windows 8 Windows 95 Windows 98 / Windows Me Windows XP (Service Pack 2) Windows Vista Windows Vista (Service Pack 1) Windows Vista (Service Pack 2) Windows Vista (Service Pack 2) Windows 7 Windows 8



Séquence possible:

Parfois il faut demander ce mode sur les fichiers setup d'installation, Puis sur l'exécutable installé...

Il se peut qu'il faille désactiver l'UAC

Il se peut qu'il faille installer un autre OS avec Hyper-V pour pouvoir installer l'application



Principe DEP Data Execution Prevention:

Il s'agit d'une technologie développée par AMD, connue sous l'appellation **NX** (No eXecute), liée aux adressages **PAE**. (Physical Address Extension)) censée empêcher le "dépassement de mémoire tampon" (*buffer overflow*. L'objectif est donc de marquer comme non exécutable des emplacements mémoire non occupés par une application, pour éviter que des vers s'auto-répliquent dans le système. Dans XP (Sp2 mini), la fonction qui implémente NX etait baptisée **DEP**, pour **Data Execution Prevention**

Désactivation Complète de DEP :

La fonctionnalité DEP, permettant de sécuriser Windows 10 contre les virus, peut être responsable de crashs intempestifs sur votre système

bcdedit.exe /set {current} nx AlwaysOff Puis re démarrage

La réactivation de la protection se fait par

bcdedit.exe /set {current} nx Option

(et re démarrage)

Désactivation pour une application de DEP :

Il est possible de désactiver cette protection pour une application précise.





ISC https://www.cabare.net Page 42/139 - Michel Cabaré -

TEST MEMOIRE

Depuis Windows 10

Via le menu panneau de Configuration / Outils d'administration

On demande Diagnostic de mémoire Windows

Analyseur de performances 🔂 Configuration du système desktop.ini



F1 permet d'executer des tests plus complets...

Correspondant à l'outil mdsched.exe





AUTHENTIFICATION WINDOWS 10

Plusieurs Mode possibles UAF - U2F:

Le choix peut se faire via Paramètres, Comptes et Options de Connexion

← Paramètres	– 🗆 X
🐯 COMPTES	Rechercher un paramètre ρ
Adresse de messagerie et comptes	Certains paramètres sont gérés par votre entreprise.
Options de connexion	Fuizer une companier
Accès professionnel	
Autres utilisateurs	absence ?
Synchroniser vos paramètres	Lorsque le PC sort du mode veille \vee

- Par code PIN (4 chiffre) .
- Par image (tracé sur une surface tactile) •
- Par Biométrie •
- Par double authentification .

Microsoft, faisant partie de l'alliance FIDO définissant 2 types d'authentification. On n'y est pas encore en standard, mais c'est possible

PASSWORDLESS EXPERIENCE (UAF standards)

SECOND FACTOR EXPERIENCE (U₂F standards)



Par Code PIN :

A n'utiliser que sur des tablettes et non sur des postes, mais pas systématiquement. Il est associé au périphérique sur lequel on se trouve ! (U2F)

Dans Paramètres, et Comptes on trouve Options de connexion on cherche Code PIN

C	Со
	Co

omptes Comptes, e-mail, synchronisation, travail, autres

Code PIN

Créez un code PIN à utiliser à la place des mots de passe. Il vous sera demandé lorsque vous vous connectez à Windows, aux applications et aux services.

Ajouter





Le code confidentiel (ex Code PIN windows) doit avoir 4 caractères minimum.

Sécurité V	Vindows		×
Config	gurer un code cor	nfidentiel	
Créez u passe. L procédu et à vos	n code confidentiel util a définition d'un code d ire de connexion à votr services.	isable à la place des mots de confidentiel simplifie la e appareil, à vos applications	
ij	Nouveau code confi Confirmer le code co	dentiel onfidentiel et des symboles	
	OK	Annuler	

Lorsque l'utilisateur va ouvrir une session, il verra des options de connexion disponibles

¢	test	la	Code 4 chif ogin	fre
	Options de connexion		Options de connexion	n

N.B : il est possible de désactiver cela dans pour les utilisateurs d'un domaine par une stratégie

C'est Activer la connexion par code confidentiel dans

Configuration Ordinateur\Modèles d'administration\ Système\Ouverture de session

<u>I</u>	Éditeur de stratégie de groupe locale	
Fichier Action Affichage ?		
Net Logon	 Paramètre	État
 Options d'arrêt Ouverture de session Panneau de configuration des perfc Profils utilisateur 	Activer la connexion par code confidentiel Désactiver la connexion par mot de passe image Affecter un domaine par défaut pour l'ouverture de session	Désactivé Non configuré Non configuré

Par Tracé sur une image :

On mémorise une action à effectuer sur une image !

C'est peu sécurisé, à n'utiliser que sur des tablettes (écran tactile) ! Valable pour un compte Microsoft / et ou un compte local. Comptes

Comptes, e-mail, synchronisation, travail, autres





Dans Paramètres, et Comptes on trouve Options de connexion on cherche Mot de passe Image

🖂 Mot de passe image

Pour de meilleurs résultats, configurez un mot de passe image sur l'écran que vous utilisez pour vous connecter à votre PC.

Ajouter

Il faut bien sûr choisir une image, puis effectuer les 3 gestes dessus...

Lorsque Test va ouvrir une session, il verra des options de connexion disponibles



N.B : il est possible de désactiver cela dans pour les utilisateurs d'un domaine par une stratégie

C'est Désactiver la connexion par mot de passe image dans

Configuration Ordinateur\Modèles d'administration\ Système\Composants Windows\

Ouverture de session

<u>I</u>	Éditeur de stratégie de groupe locale	
Fichier Action Affichage ◆ ◆ ☑ ○ ☑ ○ ☑		
Net Logon Options d'arrêt Ouverture de session Panneau de configuration des p Porfils utilisateur	Paramètre Activer la connexion par code confidentiel Désactiver la connexion par mot de passe image Affecter un domaine par défaut pour l'ouverture de session	État Non configuré Activé Non configuré

Login sur SAM ou AD :

Login Classique soit local (dans la Sam)

Il est mieux de passer par gestion des utilisateurs pour les comptes locaux





Créer un Compte Microsoft (couplé à un compte local) :

Grâce à son compte Microsoft, tel qu'un compte de messagerie Hotmail, l'utilisateur va ouvrir une session et retrouver ses propres paramètres et applications, ainsi que ses documents, depuis n'importe quel ordinateur pourvu de Windows 10. Ce service est basé sur le Cloud Computing ...

N.B : L'emplacement des données de l'utilisateur dans le nuage n'est pas connu de celui-ci.

L'authentification grâce à un compte Microsoft synchronise un certain nombre d'éléments suivants :

- Applications téléchargées depuis Windows Store.
- Favoris, thèmes, préférences linguistiques.

• Mise à jour de votre réseau social Facebook, Hotmail, Twitter... Photos et autres fichiers stockés sur des services tels que SkyDrive, Flickr...

Lorsque l'on crée un compte depuis l'interface graphique, il vaut toujours mieux créer un compte local, via la **gestion de l'ordinateur**...

Par exemple *michel*...

Estion de l'ordinateur (local)	Nom Nom complet	Description
 Vilion Système Planificateur de tâches Planificateur d'événeme Observateur d'événeme Obssiers partagés Mutilisateurs et groupes l 	E Administrat DefaultAcco Invité util util	Compte d'utilisateur d'administra Compte utilisateur géré par le syst Compte d'utilisateur invité
 Utilisateurs Groupes Performance Gestionnaire de périphé Stockage Gestion des disques Services et applications 	Nouvel utilisateur Nom d'utilisateur : Mom complet : Description : Mot de passe : Confirmer le mot de passe : L'utilisateur doit changer le mot de passe : L'utilisateur doit changer le mot de passe :	? ×

Puis se logguer avec ce compte *michel* ...

et lui associer un identifiant microsoft en demandant de **Se connecter plutôt avec un compte Microsoft**





Appropriez-le-vous !	
Votre compte Microsoft vous permet d'accéder à un large éventail d'avantages. En savoir plus.	
) 🛦 🕫 G 🖷 🕹 🦻 🛒	
michel@cabare.net	Login et MDP
<u>ه</u>	Du compte microsoft
l'ai oublié mon mot de passe	à associer
Vous n'avez pas de compte ? Créez-en un !	
Déclaration de confidentialité Microsoft	
Se connecter	

puis demande du mot de passe du compte windows local (pour confirmation), avant de lui substituer le mot de passe du login internet... c'est clair non ?

Х

À part passe confic	tir de maintenant, vous déverrouillerez ce périph de votre compte Microsoft ou de votre code cor juré un. De cette facon, vous pouvez obtenir de l	érique à l'aide du mot de nfidentiel si vous en avez l'aide de Cortana, vous
pouve auton	zz retrouver votre périphérique si vous le perdez natiquement synchronisés.	et vos paramètres seront
Pour i votre Winde	nous assurer qu'il s'agit bien de vous, nous auror mot de passe Microsoft actuel. Lors de votre pro ows, vous utiliserez le mot de passe de votre com	ns besoin une dernière fois de ichaine connexion à npte Microsoft.
Si vou Suivar	is n'avez pas de mot de passe Windows, laissez la nt.	a zone vide et sélectionnez
•		

Il est possible de définir un code PIN, mais on peut ignorer cette étape



			×			
	Configurer un code confidentiel	not de				
	passe, et nous espérons que cette méthode vous séduira. Comment un code confidentiel peut-il être plus sécurisé qu'un long mot de	e passe ?				
		3				
	Ignorer cette étape Définir	un PIN				
Et vo	ilà !					
÷	Paramètres				_	
~	COMPTE	Г	Pacharcharup	aramàtra	_	 -

LOS COMPTES	Rechercher un paramètre
Adresse de messagerie et comptes	michel@cabare.net
Options de connexion	
Accès professionnel	Informations de facturation, contrôle parental, abonnements, paramètres de sécurité, etc.
	Gérer mon compte Microsoft
Synchroniser vos paramètres	Vous devez confirmer votre identité sur ce PC.
———	Vérifier
	Se connecter plutôt avec un compte local

Comme l'appareil devient un élément d'authentification, il est nécessaire de confirmer son identité sur ce PC... par Vérifier

Aidez-nous à protéger vos informations	
Quand vous accédez à des informations confidentielles depuis votre compte ou votre appareil, ou si nous détectons une crivité suspecte sur votre compte, nou demandons un code de sécurité pour vérifier votre identité. (Si vous vous connectez fréquemment sur cet appareil, nous ne redemandons plus de code aj cela.)	ı ıs près
Comment souhaitez-vous recevoir le code ?	
Comment souhaitez-vous recevoir le code ? E-mail mi****@cabare.net	
Comment souhaitez-vous recevoir le code ? E-mail mi*****@cabare.net Pour vérifier qu'il s'agit bien de votre adresse de messagerie, entrez-la ci-dessous et cliquez sur « Suivant » pour recevoir votre code.	



Compte Microsoft / Compte local ou AD :

Sur les anciennes versions de Windows 10, on pouvait trouver cela sur **adresse de messagerie et comptes.** Et on demande **Se connecter plutôt avec un compte local**



Il faut abandonner les identifiants du compte internet pour en recréer un jeu pour le compte local...

Passer à un compte local
Vous pouvez utiliser un compte sur cet ordinateur uniquement, au lieu de vous connecter à l'aide de votre compte Microsoft. Enregistrez votre travail maintenant, car vous devez vous déconnecter pour effectuer cette opération.
Nous devons d'abord vérifier votre mot de passe actuel.
R michel@cabare.net michel@cabare.net
Mot de passe actuel

Bien sur à ne pas utiliser dans un domaine

Désactivation compte Microsoft (login sur la machine)

On peut en environnement professionnel interdire l'utilisation d'un compte Microsoft. Dans les stratégies de sécurité locales, dans les **stratégies locales**, / **Options de sécurité**

On <u>Active</u> le fait de **bloquer les comptes Microsoft**, (et de ne pas pouvoir se connecter avec un compte microsoft)



 Mean ordinateur Stratégies 	^	Stratégie	Paramètres de Non défini
 Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Scripts (démarrage/arrêt) Imprimantes déployées Paramètres de sécurité 		Propriétés de : Comptes : bloquer les comptes Microsoft Paramètre de stratégie de sécurité Expliquer Comptes : bloquer les comptes Microsoft	? ×
 > all Stratégies de comptes > all Stratégies locales > all Stratégie d'audit > all Attribution des droits utilisateur > all Options de sécurité > all Journal des événements 		 Définir ce paramètre de stratégie Les utilisateurs ne peuvent pas ajouter de comptes Microsof Cette stratégie est désactivée Les utilisateurs ne peuvent pas ajouter de comptes Microsof Les utilisateurs ne peuvent pas ajouter de comptes Microsof 	ft, nise ∨ ft. ft, nise con

On pourra le vérifier par exemple via les paramètres Windows, / Comptes / synchroniser vos paramètres



dans lesquels au niveau Synchronisation par exemple on affichera l'impossibilité de mettre en oeuvre la fonction

← Paramètres	- 0
வ் Accueil	Synchroniser vos paramètres
Rechercher un paramètre	*Certains paramètres sont masqués ou gérés par votre organisation.
Comptes	Certaines fonctionnalités Windows ne sont disponibles que si vous utilisez un compte Microsoft ou un compte professionnel.
RE Vos informations	
E-mail et comptes	Comment la synchronisation fonctionne-t-elle ?
🔍 Options de connexion	Paramètres de synchronisation Désactivé
🖻 Accès Professionnel ou Scolaire	
A, Autres utilisateurs	Paramètres de synchronisation individuels
${\mathcal C}$ Synchroniser vos paramètres	Activé

Désactivation compte Microsoft (via le Web) - msapolicy.admx

Depuis la version 1703 on a également la possibilité de demander dans

Configuration ordinateur / Modèles d'administration / Composants Windows /Compte Microsoft

De bloquer l'accès à un compte microsoft via le WEB







Ecran de Verrouillage – Ecran d'accueil :

L'écran de verrouillage (ou lockscreen en anglais) se présente dorénavant sous la forme d'une grande image sur laquelle il faut cliquer (ou qui nécessite l'appui sur une touche de clavier) en sortie de veille de l'ordinateur. Il apparait lorsqu'aucune session inter-active n'est ouverte.

N.B: ne faut pas confondre **l'écran de verrouillage** avec **l'écran d'accueil** qui s'affiche au démarrage du système d'exploitation, juste avant de saisir son identifiant et mot de passe. Des que l'on s'est loggué on tombe sur **le Bureau**

Il n'est pas pour l'instant possible de contourner l'écran d'accueil, mais on peut désactiver / paramétrer l'écran de verrouillage.



Via Paramètres / Personnalisation / Ecran de verrouillage

N.B : si la désactivation de l'écran de verrouillage est necessaire (car si on n'est pas sur une tablette, cela ne se justifie pas..) cela peut se gérer via les stratégies via **Gpedit.msc (**depuis **ver 1607** sur version **entreprise**, uniquement)

Configuration ordinateur / Modèles d'administration / Panneau de Configuration / Personnalisation





et on demande ne pas afficher l'écran de verrouillage...



N.B : le choix d'une image pourl'écran de verrouillage est possible, cela peut se gérer via les stratégies via Gpedit.msc (depuis ver 1803 sur version entreprise, uniquement)

Configuration ordinateur / Modèles d'administration / Panneau de Configuration /Forcer une image de l'écran de verrouillage et d'ouverture de session par défaut spécifique



et on indique un chemin de fichier.jgp

La case à cocher

Désactiver les faits fantaisistes....

empêche l'apparition de pub sur l'écran de verrouillage, et donc on peut estmier que pour ne pas avaoir de publicité, il faut avoir un version entreprise, et non pro!

il peut être necessaire de mettre à jour le modèle Admx controlpaneldisplay.admx

Chemin d'accès de l'image de l'écran de verrouillage :

\\nas\cabare-intra\fond-ecran-ctrl-alt-su

Exemple : avec un chemin local : C:\windows\web\screen\verrouillage.jpg

Exemple : avec un chemin UNC : \\Serveur\Partage\Corp.jpg

Désactiver les faits fantaisistes, conseils, astuces et plus encore sur l'écran de verrouillage







Bureau - Ecran d'accueil:

Lorsque l'on ouvre une session(après authentification) on tombe sur le bureau Qui est personnalisable « classiquement » en modifiant l'aspect du bureau.



L'interface «Tuile» à laquelle on accède en cliquant en bas à gauche sur l'icône Windows se nomme l'écran d'accueil...



Corb	eille								
COID									
\otimes	util		Coup d'oeil sur les	activités		Jouer et explorer			
Les pli	us utilisées Price en main		test	Compatible	e avec Gmail	D'autres façons de	6	1000	
s 🖀	Sway		Calendrier	Courrier		Jouer. Rejo	Groove Musia	Films et TV	
2	Cartes					XBOX LIVE			
	Calculatrice		e		0		ා ජ 🗐 🖁	1 🖭 🔹 6	
$\overline{\odot}$	Alarmes et horloge		Microsoft Edge	Photos	Cortana	Microsoft Solitaire Collection	En attente	En attente	
R	Outil Capture d'écran		<u></u>	_			_	_,	
Récerr	iment ajoutées		- - - -) 🕸 🕸 🕻		L	=1	
**	Contacts		Météo	Assistant Mob	En attente	Finance	Actualité		
			<u>e</u>				Ma	•	
) 🕸 😵 🕻	🕅 🛎 🌚 🖁	NE	IJ	
۵.	φlorateur de fichiers		Windows Store	Vidéo Skype	En attente	En attente	OneNote	Obtenir Office	
€ĝi Pa	aramètres								
() №	larche/Arrêt								
Ēτα	outes les applications								
	Je suis Cortana. Posez-	moi une	e question.	(D) 🤤				^ 🌄 🔩	17:08

Son aspect est personnalisable via le menu Windows/Démarrer





← Paramètres	– 🗆 X
C PERSONNALISATION	Rechercher un paramètre \wp
Arrière-plan	
Couleurs	Exemple de texte
Écran de verrouillage	
Thèmes	Aa
Accueil	
	Afficher plus de vignettes
	Désactivé



Ecran Accueil par défaut

On l'a vu, l'interface «Tuile» à laquelle on accède en cliquant en bas à gauche sur l'icône Windows se nomme **l'écran d'accueil**...





Menu Démarrer Windows

Il remplace le menu Démarrer des versions précedentes

On peut Choisir les dossiers qui doivent apparaître via Paramètres / Personnalisation / Accueil / Choisir les dossiers affichés dans l'écran d'accueil

← Paramètres	
CHOISIR LES DOSSIERS AFFICHÉS DANS L'ÉCRAN D'ACCUEIL	圆 Explorateur de fichiers
Explorateur de fichiers	l Paramètres
Activé	🖒 Marche/Arrêt
Paramètres	≣ Toutes les applications
Activé	🖷 O 🖽 🧲
Documents	
Désactivé	

On peut aussi stopper tous les ajouts automatiques au "fil du temps" via **Paramètres / Personnalisation / Accueil**

← Paramètres	- 0 X	
S PERSONNALISATION	Rechercher un paramètre	
Arrière-plan	Afficher plus de vignettes	^
Couleurs Écran de verrouillage	Désactivé Afficher occasionnellement les suggestions dans l'écran d'accueil Désactivé	
Accueil	Afficher les applications les plus utilisées Désactivé	
	Afficher les applications récemment ajoutées Désactivé Utiliser le menu Démarrer en plein écran Désactivé Afficher les éléments récemment ouverts dans les Listes de raccourcis de l'écran d'accueil ou la barre des tâches Désactivé Désactivé Choisir les dossiers affichés dans l'écran d'accueil	
		屓 Explorateur de fichiers
		??????????????????????????????????
		(¹) Marche/Arrêt
		≣ Toutes les applications



O []]

CORTANA & WINDOWS SEARCH

L'aspect de Cortana

Le principe de recherche via la **Charm Bar** de **Windows 8.1** est maintenu mais refondu dans la recherche nommée maintenant **Cortana.** Cette recherche est disponible dans la barre des tâches



Un clic droit dessus permet un menu contextuel dans lequel on peut modifier sons aspect, et notamment la réduire en icone



Lorsque l'on clique dessus, on effectue une recherche sur la machine, et sur le web en même temps... cette recherche « vaste » et ses autres fonctions multiples se paramètre via le menu **Paramètres**





Refuser Cortana à l'installation



Cortana Gpo - désactiver - search.admx

Pour limiter les remontées d'information, on doit désactiver CORTANA dans Modèle d'administration / Composants Windows / Rechercher on choisit

De Désactiver Autoriser Cortana

	📔 Plateforme de protection d 🔺	Paramètre			État	^
	🣔 Processus d'ajout de foncti	Autoricer Cortana			Non configuré	
	Programme d'amélioration				Non configure	
>	Rapport d'erreurs Windows	📗 👰 Autoriser Cortan	ia			
	📔 Rechercher					
	🦰 Saisie de texte	🛛 📅 Autoriser Cortan	a		Paramètre p	récéder
>	🦰 Sécurité Windows				. Sidificate p	
	Service d'installation Active		Commentaire :			
	🦰 Service Digital Locker					
>	Service Journal des événem	○ Activé				
>	🧮 Services Bureau à distance					
	Stratégies d'exécution auto	Desactive	Duin an alternation			
	Synchroniser vos paramètre		Pris en charge sur :	Au moins Windows	Server 2016, Windo	ws 10

Recherche Search Windows (et Cortana) - search.admx

Mais le mieux c'est de passer par GPO, via gpedit.msc



Dans Modèle d'administration / Composants Windows / Rechercher on choisit Ne pas effectuer des recherches sur le web ou afficher des résultats Web dans Search

^

Éditeur de stratégie de groupe locale		- 0	×
Fichier Action Affichage ?			
🗢 🔿 🙍 📊 🔒 🛛 🖬 🛛 🍸			
> 📔 Rapport d'erreurs Wine 🔺	Paramètre	État	^
Rechercher	📰 Ne pas autoriser la recherche Web	Non configuré	
Service d'Installation A	Ne pas effectuer des recherches sur le Web ou afficher des r	Activé	
	Ne pas effectuer des recherches sur le Web ou afficher des r	Non configuré	





Système Windows Pro/Edu/Ent/LTSChttps://www.cabare.netPage 59/139Sr10-11 – Système Cours - Ver 3.0- Michel Cabaré -

N.B: depuis la branche **1803** sur les versions **PRO** cette **GPO** ne fonctionne plus (il faut la version **entreprise** ou **EDU**). Une solution de contournement pourrait consister dans ces modifications / ajout dans le registre

Si on veut on peut faire une préférence utilisateur pour ces modifications

$\label{eq:heat} \texttt{HKEY}_\texttt{CURRENT}_\texttt{USER}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Microsoft}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Microsoft}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Microsoft}\end{tabular} \\ \texttt{Software}\end{tabular} \\ \texttt{Softwa$

On ajoute 3 clés, respectivement :

AllowSearchToUseLocation	dword	0
BingSearchEnabled	dword	0
CortanaConsent	dword	0

De manière optionnelle, on veut on peut aussi faire une **préférence ordinateur** pour ces modifications

On ajoute 2 clés, respectivement :

	AllowCortana	dword	0						
	ConnectedSearchUseWeb	dword	0						
	Meilleur résultat		Meilleur résultat						
ŵ	WordPad Application de bureau	ŵ	WordPad Application de bureau						
ŝ	Windows Store	\$							
	Word Mobile								
<u>.</u>	Word 8 - View & Edit your Documents Instantly!	Ě							
	Web								
	∽ wordreference								
	∽ wordpad								
	𝒫 word								
	,∽ wordle								
	𝒫 wordreference anglais-français								
	\mathcal{P} word online								
	∽ word 2007	0	Rechercher dans mes documents						
0	Mes documents $ ho$ Web	0	personnels						
	word		word						
	A 🗆 🤤 📑 🗐		クロ 🤁 🥫 🛱						

N.B: ce paramétrage affecte **CORTANA**, mais aussi l'outil **Search** de Windows (indépendamment de l'activation ou non de CORTANA **II semblerait bon de le paramétrer systématiquement** !



Modification de l'avatar

L'avatar associé par défaut à un compte peut être modifié par GPO via:

Configuration Ordinateur/ Modèle d'administration / Panneau de Configuration/ Compte d'utilisateurs / Appliquer l'avatar de compte par défaut à tous les utilisateurs



L'avatar de compte par défaut est enregistré dans le dossier %PROGRAMDATA%\Microsoft\User Account Pictures\user.jpg.

→ CePC → os-syst	eme (C:) > ProgramData > Microsoft >	User Account Picture	s								
steur	^		_	_		_	_				_
			\cap	\circ		\circ	\cap				0
nts			$ $ \rtimes $ $	\sim		$ $ \times $ $	$\left \right. \right. $	Q	8	8	\cap
	Administratour d	defaulturen0 dat	quert hmp	quest page	toto dat	userbmo		LIFER 22 000	urser 40 ppg	uses 48 ppg	urer-102 ppg
	Administrated.u	deraultusero.uat	guescomp	guescoping	toto.uat	useromp	user.prig	user-sziping	user-wo.prig	user-worping	user-raziping

Que l'on peut remplacer par



L'avatar d'invité par défaut se trouve dans le dossier %PROGRAMDATA%\Microsoft\User Account Pictures\guest.jpg.

N.B : Si on active le paramètre de stratégie les personnalisations ne sont pas autorisées. Si vous désactivez ce paramètre de stratégie, les utilisateurs peuvent personnaliser leur avatar de compte.



LES TUILES

Tuiles par défaut

l'écran d'accueil windows 10 demande une résolution mini de 1366 x 768 px



Les 2 types d'applications suivants s'exécutent sur Windows10, nommées respectivement **Windows Apps**, et les applications traditionnelles dites **Win32**:

- Applications dites "Apps": introduites à partir de Windows 8 et 10, elles sont principalement installées à partir du Windows Store (mais pas toutes)
- Applications dites «Win32»: applications Windows classiques.

Applications Apps : UWP - Applications système - Applications

Pour ces **Applications dites "Apps"**: introduites à partir de Windows 8, on peut les sub-diviser en 3 genres

- Applications de la plateforme Windows universelle (UWP): conçues pour fonctionner sur toutes les plateformes, peuvent être installées sur plusieurs plateformes, notamment le client Windows, Windows Phone et Xbox. Pn peut dire que toutes les applications UWP sont donc des applications Windows, (mais par contre toutes les applications Windows ne sont pas forcément des applications UWP)
- Applications systèmes: applications qui sont installées dans le répertoire C:\Windows. Ces applications font partie intégrante du système d'exploitation
- Applications: toutes les autres applications sont installées dans le répertoire C:\program Files\WindowsApps. Et on distinguera 2 classes d'applications : Approvisionnées – Installées
 - Applications Approvisionnées : elles seront installées la première fois qu'un utilisateur se connecte
 - Applications Installées elles sont installées en tant que partie du système d'exploitation



Gestion des Appx installées et ou Approvisionnnées en Powershell

On passe en powershell. Tache que l'on lance en mode administrateur

Windows PowerShell Application de bureau

Si besoin Set-ExecutionPolicy Unrestricted

La commande Get-Module -ListAvailable permet de recenser 2 modules importants pour la gestion des tuiles : Appx et Dism



Si besoin, on importe juste le module appx **Import-Module appx**

PS C:\Users\Administrateur> PS C:\Users\Administrateur> C:\Users\Administrateur> Import-Module appx

On peut vérifier les les commandes importées par un

(Get-Module appx).exportedcommands

PS C:\Users\Administrate	eur> (get-module appx).exportedcommands
Кеу	Value
Add-AppxPackage	Add-AppxPackage
Add-AppxVolume Dismount-AppxVolume	Add-AppxVolume Dismount-AppxVolume
Get-AppxDefaultVolume Get-AppxPackage	Get-AppxDefaultVolume Get-AppxPackage
Get-AppxPackageManifest	Get-AppxPackageManifest
Mount-AppxVolume	Mount-AppxVolume
Move-AppxPackage Remove-AppxPackage	Move-AppxPackage Remove-AppxPackage

Suppression des packages utilisateur en cours (installées)

Get-AppXPackage donne la liste de tous les des packages courant,

PS C:\Users\Admini	strateur> get-appxpackage
Name	: Microsoft.VCLibs.140.00
Publisher	: CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture	: X64
ResourceId	
Version	: 14.0.22929.0
PackageFullName	: Microsoft.VCLibs.140.00_14.0.22929.0_x648wekyb3d8bbwe
InstallLocation	: C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.22929.0_x648wekyb3d8bbwe
IsFramework	: True
PackageFamilyName	: Microsoft.VCLibs.140.00_8wekyb3d8bbwe
PublisherId	: 8wekyb3d8bbwe
IsResourcePackage	: False
IsBundle	: False
TsDevelonmentMode	: False

La liste des nom de packages complets pour l'utilisateur courant s'obtient alors avec

Get-Appspackage | select packagefullname

PS C:\Windows\system32> Get-AppxPackage select packagefullname
PackageFullName
Microsoft AND Rockerplugin 1000 1734 1 A neutral neutral_cwsnin2txyewy
Microsoft Windows ShallExperienceHost 10 0 17134 1 neutral neutral cw5n1h2txyewy
windows.immensivecontrolpanel 10.2.1000 neutral neutral cw5n1b2tyvevy
Microsoft.Windows.Cortana 1.10.7.17134 neutral neutral cw5n1h2txvewy
Microsoft.MicrosoftEdge 42.17134.1.0 neutral 8wekyb3d8bbwe
Microsoft.Windows.ContentDeliveryManager_10.0.17134.1_neutral_neutral_cw5n1h2txyewy
Microsoft.VCLibs.140.00_14.0.25426.0_x648wekyb3d8bbwe
Microsoft.VCLibs.140.00_14.0.25426.0_x868wekyb3d8bbwe
Microsoft.NET.Native.Framework.1.6_1.6.24903.0_x648wekyb3d8bbwe
Microsoft.NET.Native.Framework.1.6_1.6.24903.0_x868wekyb3d8bbwe



Si on veut supprimer un package courant, on le supprime d'abords pour l'utilisateur Administrateur Build-In courant, avec son fullname !

Remove-AppxPackage fullname



Suppression des packages provisionnés

Si on veut le supprimer définitivement de la machine (et donc pour pour les autres users (a venir...) il faut supprimer le **package provisionné**

Get-appxprovisionedPackage –online donnera la liste des packages installés sur le poste dans l'image(que l'on appelle packages provisionnés)



La liste des nom de packages provisionnés s'obtient alors avec

Get-AppXprovisionedpackage -online | select Displayname



La liste des nom complets de packages provisionnés s'obtient alors avec

Get-AppXprovisionedpackage –online | select packagename

PS C:\Windows\system32> Get-AppXprovisionedpackage -online select packagename
PackageName
Microsoft.BingWeather_4.24.11294.0_neutral_~_8wekyb3d8bbwe
Microsoft.DesktopAppInstaller_2018.402.2359.0_neutral_~_8wekyb3d8bbwe Microsoft.GetHelp 10.1706.10952.0 neutral ~ 8wekyb3d8bbwe
Microsoft.Getstarted_6.10.10872.0_neutral_~_8wekyb3d8bbwe
Microsoft.Messaging_2018.222.2231.0_neutral_~_8wekyb3080bwe Microsoft.Microsoft3DViewer_4.1804.19012.0_neutral_~_8wekyb3d8bbwe
Microsoft.MicrosoftOfficeHub_2017.1219.520.0_neutral_~_8wekyb3d8bbwe

Si on veut supprimer un package provisionné

Remove-AppxProvisionedPackage –PackageName:fullname –online







On peut utiliser cette commande pour s'affranchir du numero de version

Get-AppxPackage Microsoft.ZuneMusic Т Select-Object -Expand PackageFullName | Remove-AppxPackage

N.B : si on ne fait pas les deux, lors d'un eventuel sysprep il peut y avoir erreur

N.B: Windows 10 Enterprise LTSB (Long Term Servicing Branch) edition, n'a aucune application pré-packagée

Supprimer tous les packages

Les commandes ci-dessous sont un peu draconniennes... puisqu'elles permettent de supprimer tous les pakages existants sur le poste

Get-AppXPackage | Remove-AppxPackage

Get-AppXProvisionedPackage -online | Remove-AppxProvisionedPackage online

get-appxprovisionedpackage -online | remove-appxprovisionedpackage

N.B: même si on demande de supprimer toutes les applications, un certains nombre de fait ne sont pas désinstallables.

Gestion Windows Store

l'icone Windows Store ne peut être supprimée, mais elle peut être désactivée de manière a ce que les utilisateurs ne puissent ajouter n'importe qu'elle tuile sur leur poste.



on pourra par stratégie gpedit.msc

Configuration Utilisateur Modèles d'administration 1 **Composants Windows**



chercher l'entrée Windows Store





N.B : depuis **Windows 1607** la possibilité de désactiver complètement le Store est réservé aux version **education** et **entreprise**... (dans le doute on peut désactiver tous les réglages store que l'on trouvera dans la GPO...)

N.B: Si on décide de laisser **Windows Store** actif, alors il faut que l'**UAC** soit en place...y compris donc pour les comptes Administrateurs, donc dans les

stratégies de sécurité locale /



UAC actif, y compris pour les administrateur (et aussi l'admin intégré)

🕼 Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur

Activé

même si on peut demander une élévation automatique, donc

📓 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Admini... Élever les privilèges sans invite...

¥

donc

Paramètre de sécurité locale		Expliquer
	Contrôle de compte d'élévation pour les Administrateur	e d'utilisateur : comportement de l'invite s administrateurs en mode d'approbation

Élever les privilèges sans invite utilisateur

CANEVAS – ECRAN D'ACCUEIL

Canevas écran d'accueil - export-startlavout

Par défaut les tuiles présentes sur le menu démarrer sont peu utiles. Cette personnalisation peut se faire via la création d'un modèle (canevas) sur un poste "maître" qui sera ensuite déployé sur les postes de travail souhaité.

Ce canevas servira de trame a appliquer sur un profil par défaut, faire extremement attention à la Branche Version Windows 10 utilisée !!!!

Création du canevas

Une fois l'écran d'accueil personnalisé une capture du canevas est nécessaire.

La commande Powershell Export-StartLayout est utilisée

Windows PowerShell
Windows PowerShell Copyright (C) 2015 Microsoft Corporation. Tous droits réservés.
PS C:\Users\Administrateur> Export-StartLayout

Comme dans

PS C:\> Export-StartLayout -Path "C:\stock\startmenu.xml"

PS C:\Users\Administrateur> export-startlayout -path c:\stock\startmenu.xml |e

fichier XML généré contient l'ensemble des informations relatives à la position et à la taille des tuiles de l'écran d'accueil "type".

> C	e PC > Disque local (C:) > stock	
cal (C:) ^	Nom	
ft-tool	🔮 startmenu.xml	

ve\

N.B: depuis Windows 1809 la commande dot

être utilisées avec un paramètre supplémentaire UseDesktopApplicationID

Comme dans

PS C:\> Export-StartLayout -UseDesktopApplicationID -Path "C:\stock\startmenu.xml"

Déploiement du canevas

Par PowerShell La commande Powershell Import-StartLayout est utilisée

Windows PowerShell PS C:\Users\Administrateur> Import-StartLayout Comme dans

\$env:Sys	stemD	yout rive\	-LayoutPath		C:\stock\cai	nevas.x	mi -Mic	ountPath	
PS C:\Users	Adminis	strateur> in	port-startlayout	-layo	utpath c:\stock	\startmenu	.xml -mountpat	h \$env:systemd	°i
Dans	le	profil	Users	١	default	on	trouve	alors	
Appdata	\Local\	Microsof	t\Windows\Sh	nell					



.

- «	Ap	opData → Local → Microsoft → Wind	dows > Shell ↓	Ō	
	^	Nom	Modifié le		Ту
Files (DefaultLayouts.xml	30/10/2015 08:21		Do
mes		LayoutModification.xml	14/12/2015 15:49		Do

Par GPO Modèle d'administration / Menu Démarrer et barre des tâches / Disposition de l'écran de démarrage

N.B: Par GPO le déploiement d'un canevas rend les tuiles statiques, les utilisateurs ne pourront plus les modifier. On peut cependant avoir un canevas en partie fixe, et en partie modifiable, **Cf Tp** Tuiles et Startlayout.xml



COMPTES UTILISATEURS

Compte d'utilisateurs – session:

On parle de **compte utilisateur** lorsque l'on définit un individu nommément désigné, généralement par un nom d'utilisateur, et un mot de passe et des propriétés

C'est pourquoi toute session de travail sur un ordinateur débute par une boîte de dialogue (ou une image à cliquer) demandant un Nom Utilisateur et un Mot de passe pour reconnaître le compte utilisateur

(+)

Le mot de passe peut contenir jusqu'à **127 caractères**

Le nom utilisateur peut contenir jusqu'à **20 caractères**

Administrateur Mot de passe

N.B: le système fait la différence entre **Minuscules /Majuscules** et n'accepte pas les caractères suivant: " Λ :;=,+*?<>

L'écran de Verrouillage qui apparait lorsqu'aucune session inter-active n'est ouverte.

Des que l'on s'est loggué On tombe sur l'écran d'accueil

N.B : si la désactivation de l'écran de verouillage est demandée cela peut se gérer via les stratégies via **Gpedit.msc**



Configuration ordinateur / Modèles d'administration / Panneau de Configuration /Personnalisation

Par sécurité, utilisez un mot de passe d'au moins 7 caractères avec des lettres majuscules et minuscules, des nombres et de la ponctuation...



Winlogon.exe

Ouverture de session

Séquence authentifiée 1 Fermeture de session Ouverture de session Séquence authentifiée 2

Fermeture de session

Arrêt Poste

Lorsque l'on ferme une session, tous les travaux en cours ont terminés, et l'on doit pour pouvoir de nouveau travailler, ouvrir une nouvelle session

Connexion multiples Utilisateur

Sur un poste Windows 10 (comme XP) il est
possible de changer d'utilisateur connecté sur
e poste, sans fermer sa session (les travaux et
a tâches initiés continuent) c'est-à-dire que
'on peut autoriser sur un poste plusieurs
sessions en parallèle de différents utilisateurs

Il n'est plus nécessaire de fermer la • session d'un autre utilisateur pour ouvrir sa propre session....



Autrement dit deux utilisateurs peuvent ouvrir chacun une session et se passer la connexion sans arrêter leur travaux respectifs....

Winlogon.exe



Mais si l'Administrateur ouvre également une connexion, alors

l'impression d'être tout seul...

Système Windows Pro/Edu/Ent/LTSC https://www.cabare.net Page 70/139 - Michel Cabaré -





Sr10-11 – Système Cours - Ver 3.0

Arrêt Poste

recommence à jouer... il à Administrateur util Connecté

il verra toutes les autres connections en cours

P	Gestionnaire des tâches						×			
Fichier O	ptions Afficha	ige								
Processus	Performance	Historique d	es applications	Démarrage	Uti	ilisateurs	Détails	Services		
	*			1	%	43	%	7%	0%	
Utilisateur			Statut	Processe	ur	Mémo	ire	Disque	Réseau	
Ad P	ministrateur (6)		Déconnecté	C)%	12,3 N	/lo	0 Mo/s	0 Mbits/s	
⊳ 📮 uti	I (9)			c)%	42,2 N	/lo (),2 Mo/s	0 Mbits/s	

N.B: Cette fonctionnalité, extrêmement gourmande en ressource, pose certains problèmes avec des applications non spécifiquement dessinée pour Windows 8, et entraîne parfois des pertes de donnée ...

POUR TOUTES CES RAISONS LES CONNECTIONS RAPIDES NE SONT PAS **CONSEILLEES SUR UNE MACHINE A USAGE PROFESSIONNEL!**

Désactiver la bascule rapide Utilisateur

Pour faire disparaître Changer d'Utilisateur (sans fermer la session)

		Cerrouiller
Se déconnecter		Changer d'utilisateur
Modifier un mot de	passe	Se déconnecter
Gestionnaire des tâc	ches	Modifier un mot de passe
		Gestionnaire des tâches
Soit on utilise gpedit.msc	-	 Éditeur d'objets de stratégie de groupe Fichier Action Affichage ? A A R R R R R R R R R R R R R R R R R R
Configuration ordinate d'administration p∪is Système/Ouverture de sessi d'entrée pour le changemen	eur / Modèle ion/Masquer les poin ⁻ t rapide d'utilisateur	Stratégie Ordinateur local Configuration ordinateur Paramètres du logiciel Paramètres Windows Modèles d'administration Modèles d'administration Paramètres du logiciel Paramètres du logiciel Paramètres du logiciel Modèles d'administration
Système Accès au stockage amovible	📑 Ouwerture de session	

ou alors II faut passer par la base de registre



Regedt32.exe

💣 Édite	ur du Reg	istre		
Fichier	Edition	Affichage	Favoris	?
⊿.,™	Ordinateu	r		
⊳ - (HKEY_	CLASSES_RO	от	
⊳ - (HKEY_	CURRENT_U	SER	
▶ [HKEY_	LOCAL_MAC	HINE	

Et dans la clé

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Il faut créer la valeur DWORD : HideFastUserSwitching

HideFastUserSwitching REG_DWORD 0x00000000 (0)

Lorsque la valeur Dword vaut 1, alors les sessions multiples sont désactivées.

Modifier la valeur DWORD 32 bits				
Nom de la valeur :				
HideFastUserSwitching				
Données de la valeur : 1	Base			
	OK Annuler			

N.B : cette option est automatiquement activée si le poste fait partie d'un domaine. (par défaut la bascule entre utilisateurs locaux est activé sur un poste en workgroup)

SID Sécurity identifier :

Le **SID** est un numéro d'identification unique sur un poste Windows comportant 38 digits et représentant un compte utilisateur ou un nom de groupe.

Créé automatiquement à chaque déclaration de nouveau groupe ou utilisateur, il reste stocké dans la machine même si le groupe ou l'utilisateur qui en était à l'origine est supprimé. Ce qui fait que si on supprime puis on recrée un compte ayant le même nom, le SID attribué la deuxième fois sera différent de celui utilisé lors de la 1° création, et par conséquent on ne pourra réutiliser les ressources droits et permissions allouées lors de la première utilisation

Windows 10 se fonde sur les SID et pas sur les noms !

Utilisateur	s et groupes locaux	23
<u>^</u>	Chaque compte d'utilisateur a un identificateur unique en plus du nom d'utilisateur. La suppression d'un compte d'utilisateur supprime cet identificateur et il ne peut pas être restauré, même si vous créez un nouveau compte avec un nom d'utilisateur identique. Ceci peut empêcher l'utilisateur d'accéder à des ressources auxquelles il est actuellement autorisé à accéder. Voulez-vous vraiment supprimer l'utilisateur bob ?	
		_
	<u>O</u> ui <u>N</u> on	

PAR CONSÉQUENT IL EST IMPOSSIBLE DE RECRÉER UN COMPTE UTILISATEUR UNE FOIS QUE CELUI-CI A ÉTÉ EFFACÉ, MEME SI LE MEME NOM EST ATTRIBUÉ ON NE POURRA UTILISER LES RESSOURCES ANCIENNEMENT ALLOUÉES




Whoami:

En tant que quoi on est logué ? whoami (ou whoami /upn ou whoami /fqdn)

C:\Users\Administrateur>whoami ıtil-pc\administrateur

et le SID à titre d'information whoami /user

C:\Users\Administrateur>whoami /user		
Informations sur l'utilisateur		
	01D	
NOM a'utilisateur	51D	
win-8-ent-x64\administrateur	S-1-5-21-3539324183-3274001343-3598065848-500	

Comptes Visibles pré-définis :

Il y a un changement important par rapport aux versions précédentes, seuls deux comptes sont crées. Sous Windows 10 il existe 2 Comptes Utilisateurs prédéfinis

🜆 Gestion de l'ordinateur (local)	Nom	Nom complet	Description
✓ [™]	Numerical Administrateur		Compte d'utilisateur d'administration
> 🕑 Planificateur de tâches	DefaultAccount		Compte utilisateur géré par le système.
> 🛃 Observateur d'événeme	💀 Invité		Compte d'utilisateur invité
> 8 Dossiers partagés	WDAGUtilityAccount		Compte d'utilisateur géré et utilisé par le système
Vilisateurs et groupes l			compre a administrear gere et admine par le systeme i
Utilisateurs			

Le Compte Administrateur (celui d'origine):

C'est la personne qui aura le pouvoir maximal sur la station de travail, et pourra gérer la configuration du système

- Ce compte ne peut être supprimé, mais peut être renommé
- Ce compte par défaut est inactivé •

Le Compte Invité :

Pour des utilisateurs occasionnels ayant un minimum de droits

- Ce compte par défaut est inactivé
- **N.B:** dans la pratique, lors de l'installation d'un poste Windows 10 hors domaine, un assistant se déroule lors du premier démarrage, demandant les noms des "futurs" utilisateur du poste.... Cela a pour effet de créer des comptes utilisateur – administrateurs !

Ces comptes ayant donc des privilèges forts, puisqu'ils sont membre du groupe des administrateurs du poste.

Comptes Invisibles système :

Il existe aussi des comptes invisibles, essentiellement

NT AUTHORITE\LocalService Compte de

service

local

Un compte limité similaire au compte de service réseau mais qui se connecte au réseau en Anonyme.



NT

Compte

AUTHORITE\NetworkService service

réseau

Un compte de service beaucoup plus limité que le compte de Service local ou administrateurs mais qui peut accéder aux réseaux

AUTHORITE\LocalSystem ou	Compte
NT AUTHORITY	système
ou \LocalSystem	Local

Compte avec les privilèges les plus élevés sur Windows. Ce compte peut accéder aux réseaux comme n'importe quel utilisateur Windows local.

Utilisateurs locaux:

Il est possible de créer des comptes utilisateurs sur un poste **Windows** on parle alors de comptes locaux, qui n'ont de portée que la machine sur laquelle ils sont créés.

La meilleure façon pour faire cela se trouve dans le menu

Démarrer / Panneau de configuration (affichage classique) / Outils d'Administration/ Gestion de l'ordinateur

Ou plus rapidement par clic droit sur l'icône Ordinateur du bureau



Sur l'icône Ordinateur du bureau on demande clic droit gérer

🎥 Gestion de l'ordinateur	
Fichier Action Affichage ? Image: Section de l'ordinateur (local) Image: Section de l'ordinateur (local) Image: Section de l'ordinateur de tâches Image: Section de l'ordinateur de tâches Image: Section de l'ordinateur de tâches Image: Section de l'ordinateur d'événements <	Pour créer un nouvel utilisateur il suffit de demander clic droit sur le dossier Utilisateurs , Puis Nouvel utilisateur
Nouvel utilisateur Nom d'utilisateur : Nom complet : Description : Mot de passe : Confirmer le mot de passe : Vullisateur doit changer le mot de passe à la prochaine ouverture de L'utilisateur ne peut pas changer de mot de passe Le mot de passe n'expire jamais Le compte est désactivé	e session



Gestion des Comptes:

Le compte administrateur d'origine, est désactivé par défaut lors de l'installation. Comme on ne peut pas lui donner un mot de passe lors de l'installation, il faut impérativement lui en donner un lors de son activation !

	Propriétés de Adminis	trateur 🔋 💽
	Général Membre de	Profil
	Administrat	eur
	Nom complet :	
	Description :	Compte d'utilisateur d'administration
	L'utilisateur doit changer le mot de passe à la prochaine ouverture de session	
Administrateur	 ✓ Le mot de passe n'expire jamais ✓ Le compte est désactivé 	

c'est le seul qui ne subit pas par défaut l'UAC !

Re-définition de mot de passe

Si on en a les privilèges, on réinitialise le mot de passer d'un compte utilisateur en faisant clic-droit sur le compte à changer, puis on demande **Définir le mot de passe...**

Nom	Nom complet	Description
💭 Administrateur		Compte d'utilisateur d'administration
bob	Définir le mot o	de passe

Cacher le dernier Utilisateur

Pour cacher le nom du dernier utilisateur à s'être authentifié...

Stratégies de sécurité locales / Stratégies locales / Options de sécurité



N.B: pour ne pas proposer une liste des utilisateurs locaux existante, et demander un login – mot de passe, il suffit d'activer cette option



Notions de groupes :

On peut aussi définir l'appartenance d'un individu à un groupe (ou à plusieurs groupes) ayant des droits et des permissions biens définis, on dit alors que tel **compte utilisateur** est membre de tel ou tel **groupe**

Toute personne connectée sur le réseau, et à fortiori sur le serveur, est un utilisateur dont on aura forcément prédéfini les actions qu'il est censé faire, et celles qu'il ne peut pas faire, par conséquent toute action sur une machine est déterminée par ce que l'on appelle des "**droits**".

Les droits d'un utilisateur sont souvent déterminés par le groupe auquel il appartient, un **groupe** étant un ensemble d'utilisateur ayant les mêmes droits, ou mieux, un ensemble de droits et de permissions bien définis, dont on bénéficiera lorsque l'on en fait partie.

Un groupe possède un symbole qui est



Groupes Locaux Prédéfinis :

Il existe un certain nombre de **groupes prédéfinis** dans Windows, depuis le groupe Administrateurs (disposant de tous les droits) jusqu'au groupe Invité (ayant les droits les plus faibles, et ne disposant même pas d'un mot de passe...)

Ces groupes prédéfinis, l'administrateur lui même ne peut les détruire ni les renommer. Autrement dit **ce n'est pas vous qui gérez les groupe prédéfinis**, **mais vous pouvez vous en servir....**

Dans SEVEN on distingue trois types de comptes utilisateur

- Des comptes utilisateurs standards
- Des comptes utilisateurs administrateurs
- Des comptes utilisateurs invités



Liens Symboliques – Raccourcis – Jonctions :

Un lien symbolique c'est un alias avec le dossier/fichier sur lequel on se lie... (si on supprime le lien symbolique, le dossier/fichier n'est pas supprimé)

Un lien réel c'est un autre nom pour le même dossier/fichier (si on supprime le lien réel, le dossier/fichier est supprimé)

Différence entre liens symboliques et raccourcis:

- Un Raccourci est une redirection au niveau du système d'exploitation, SEVEN
- Un **Lien symbolique** est une redirection au niveau du système de fichier, NTFS

N.B: on peut lister les liens avec dir /a ou mieux dir /al

Le lien garde les propriétés du dossier-fichier vers lequel il pointe, ce n'est pas fichier Ink. Ce lien se comporte comme le dossier-fichier "original".

En effet dans les propriétés d'un "raccourci" est-ce utile de savoir que c'est un fichier **Ink** de 800 octets ?, alors qu'avec un lien symbolique, nous pourrons savoir combien pèse le dossier cible, géré son partage, ses accès... exactement comme si vous regardiez les propriétés du vrai dossier

Par exemple si certains dossiers sont perdus dans l'arborescence complexe de votre système et on veut les gérer depuis l bureau, il vous suffira de créer des liens symboliques sur le bureau avec ces dossiers.

N.B: Les jonctions de répertoire font "double emplois" avec les liens symboliques, simplement elles existent pour des raisons de compatibilité. Elles ne peuvent être données qu'avec des chemins absolus !

Objectif:

Les profils d'utilisateur présentent plusieurs avantages :

- Lorsque les utilisateurs ouvrent une session sur leur station de travail, ils reçoivent les paramètres du bureau tels qu'ils existaient à la fermeture de la dernière session.
- Plusieurs utilisateurs peuvent utiliser le même ordinateur et chacun reçoit un bureau personnalisable lorsqu'il ouvre une session.

Les profils permettent de mémoriser notamment les paramètres suivants:

Explorateur Windows NT Tous les paramètres définissables par l'utilisateur pour l'Explorateur Windows NT.



Barre des tâches	Tous les groupes de programmes personnels et leurs propriétés, tous les programmes et leurs propriétés, et tous les paramètres de la barre des tâches.
Paramètres d'imprimante	Connexions aux imprimantes du réseau.
Panneau de configuration	tout sauf polices / date-heure / affichage drivers / réseau /
Accessoires	Tous les paramètres d'application spécifiques à l'utilisateur qui affectent l'environnement Windows NT de l'utilisateur, tels que la Calculatrice, l'aspect de l'horloge, le Bloc-notes, Paint

Profil Local:

Le profil est crée automatiquement par défaut pour chaque utilisateur qui ouvre une session sur un poste. Il prend alors le nom de **Profil Local**.

Le profil local peut être créé à partir d'un profil local par défaut (modèle) stocké dans un dossier **Default** (depuis Windows 7) ou **Default User** (sous XP)

Emplacement Profils Locaux Seven:

Les Profils Windows 10 ne sont pas stockés comme les profils XP:

XP (Document and Settings)	Windows 10 8 -7 (Users ou " Utilisateurs ")
A (Document and Octings)	

• Le dossier <u>Racine des profils</u> devient « visuellement » le dossier **\Utilisateurs** (selon la régionalisation française) mais se trouve être le dossier **\Users** (anciennement **\Document and Settings)**

N.B : Avec la régionalisation de l'interface Windows, le dossier **Users** apparaît dans l'explorateur comme **Utilisateurs.** Mais on le retrouve en demandant

Clic-Droit / Ouvrir une fenêtre de commandes ici



Administrateur : C:\Windows\system32\cmd.exe
C:\Users>_





N.B: on ne peut plus «accéder» à **Documents and Settings**... ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **user**...

Emplacement non disponible	x
C:\Documents and Settings n'est pas accessible. Accès refusé.	La commande en invite dir /a ou mieux dir /al liste les jonctions
C:∖≻dir ∕al Le volume dans le lecteur C n'a pas de n Le numéro de série du volume est F2F4-F3 Répertoire de C:∖	10m. 37C
14/07/2009 05:53 <jonction> Docu 0 fichier(s)</jonction>	nents and Settings [C:\Users]

Structure des Profils Windows 10 :

Dans le dossier Utilisateurs (Racine des profils), on trouve désormais



N.B: on ne peut plus « accéder » à **Default Users**... ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **C:\Users\Default**...

Emplacement non disponible	×	
Accès refusé.		La commande en invite
		dir /a ou mieux dir /al liste le
(ОК	jonctions
Répertoire de C:\Users		
4/07/2009 05:53 〈SYMLINKD〉 All Users [C:\ProgramData] 4/07/2009 05:53 〈JONCTION〉 Default User [C:\Users\Default]		
0 fichier(s) 0 octets 2 Rép(s) 6 714 511 360 octets libres		
Système Windows Pro/Edu/Ent/LTSC https://www.cabare.net Page 79/139		

- Michel Cabaré -

Sr10-11 – Système Cours - Ver 3.0

Structure d'un profil Utilisateur

Les principaux changements Windows 10-7 par rapport aux profils XP sont:

XP (Document and Settings)	Windows 10-8-7 (Users ou "Utilisateurs")
Pour un compte Donné nommé " Administrateur " Tout se trouvait dans	Pour un compte Donné " Administrateur " désormais une partie se trouve sous C:\Users\Administrateur
Document and Settings \ Administrateur	Et une autre partie se trouve dans
	C:\Users\Administrateur \Appdata\Roaming\Microsoft\Windows

- Les préfixes **mes** et **ma** sont supprimés des dossiers 膭 Bureau • document ou musique (à la place de mes document ou ma musique
- Les dossiers document ou musique... ne sont plus des • sous-dossiers du dossier mes documents, mais sont directement crées à la racine du dossier profils (en quelque sorte remise à plat de l'arborescence...)
- 🔓 Contacts Favoris 🍺 Liens 🜗 Ma musique Mes documents 崖 Mes images 📔 Mes vidéos Parties enregistrées Recherches 🚺 Téléchargements
- 5 nouveaux dossiers apparaissent dans le profil 10 Seven •

	 Bureau Contacts Documents Favoris Images Liens Musique Objets 3D OneDrive Parties enregistrées Recherches 	N.B: Les noms des dossiers physiques ne correspondent pas forcément. Avec la "régionalisation", on peut dire que : Certaines entrées	Length Name 3D Obj Contac Deskto Downlo Favori Links Music OneDri Pictur Saved Search Securi Videos	ects ts p nts ads tes ve es Games es tyScans
	SecurityScans Féléchargements Vidéos	anciennement stockées sous XI profil utilisateur sont maintenant o un sous dossier du profil utilisateur \AppData\Roaming	P directement depuis Windov r Appdata	dans le vs 7 dans Local
		\AppData\Local		Roaming
		\AppData\LocalLow		
	comme par exen	nple AppData\Roaming\Microsoft\V	Vindows	
	Menu Démarrer	Appdata\Roaming\Microsoft\Wir	ndows\Start Me	enu
	Modèles	Appdata\Roaming\Microsoft\Wir	ndows\Templat	es
* * * * * * * * *	Application Data [Cookies [C:\Users\ Local Settings [C: Menu Démarrer [C:\ Mes documents [C:\ Modèles [C:\Users\ Recent [C:\Users\A SendTo [C:\Users\A Uoisinage d'impres Uoisinage réseau [C:\Users\Administrateur\AppData\Roamin Administrateur\AppData\Roaming\Microso \Users\Administrateur\AppData\Local] Users\Administrateur\AppData\Local] Users\Administrateur\Documents] Administrateur\AppData\Roaming\Microso dministrateur\AppData\Roaming\Microsof dministrateur\AppData\Roaming\Microsof sion [C:\Users\Administrateur\AppData\Roaming\Dicrosof c:\Users\Administrateur\AppData\Roaming\Dicrosof	ng] oft\Windows\Cook Microsoft\Window oft\Windows\Temp ft\Windows\Recen ft\Windows\SendT \Roaming\Microso ng\Microsoft\ <u>Win</u>	ies] s\Start Menu] lates] t] o] ft\Windows\Printer Sho dows\Network Sho <u>rtcuts</u>



Le dossier **AppData** contient 3 sous-répertoires nommés **Local, LocalLow et Roaming**, jouant chacun un rôle spécifique :

• **Roaming** : contient les données "itinérantes" de l'utilisateur, c'est-à-dire celle qui potentiellement le suivent d'une ordinateur à un autre, indépendamment de la machine utilisée.

• Local contient les données spécifiques à un ordinateur, c'est-à-dire des données que le développeur d'une application ne souhaite pas voir synchronisées entre différentes machines. Il peut s'agir de données de cache ou des paramètres purement locaux. Notez que si votre ordinateur n'appartient pas à un domaine, il n'y a pas de différence fondamentale entre Roaming et Local.

• LocalLow est similaire au dossier Local si ce n'est qu'il est destiné à des applications ayant uniquement besoin d'écrire des données, mais séparément du reste des données afin qu'elles n'aient pas accès à d'autres informations. C'est le cas par exemple du mode Privé de Internet Explorer.

Profil par Défault

Les principaux changements depuis Seven par rapport aux profils XP sont :

• Le dossier **Default** correspondant au dossier **Default User** sous XP contient le profil par défaut

C:\Users>dir ∕al Le volume dans le lecteur C n'a pas de nom. Le numéro de série du volume est 144A-3A67							
Répertoire	de C:\Us	ers					
19/01/2008 19/01/2008	15:23 15:23	<symlinkd> <jonction></jonction></symlinkd>	All Users [C:\ProgramData] Default_User [C:\Users\Default]				

Méthode Certifiée pour modifier le profil par défaut

Il n'est plus possible dans Windows 10 selon Microsoft de modifier le profil par défaut comme on le faisait dans XP ni avec windows enabled comme on pouvait encore le faire dans Seven.

Ceci car certains bug apparaissaient lorsque on copiait/collait brutalement le profil type dans Default user...

La solution désormais repose sur un fichier **Unattend.xml** contenant une instruction di genre **<copyProfile>true</copyProfile>**

Ce fichier devant être passé en paramètre à un sysprep de la machine...



Profil Public (ex-all users)

Les principaux changements par rapport aux profils XP sont les suivants :

 les dossiers ProgramData et Users\ Public correspondent en partie à l'ancien dossier All User sous Windows XP

C:∖Users>di Le volume Le numéro Répertoire	r ∕al dans le de série de C:∖U	lecteur C n'a y du volume est sers	pas de nom. 144A-3A67
19/01/2008	15:23	<symlinkd></symlinkd>	All Users [C:\ProgramData]
19/01/2008	15:23	<jonction></jonction>	Default_User [C:\Users\Default]

XP (Document & Settings)	Windows 10 (ProgramData et Users)	
All users	En partie dans C:\ProgramData plus exactement	
	C:\ProgramData\Microsoft\Windows\	
	Et l'autre partie dans C:\Users\Public	

Ce dossier ProgramData contient tous les liens pour compatibilité antérieure

Répertoire	e de C:\	ProgramData	
14/07/2009 18/02/2010	05:53 09:25	< JONCTION>	Application Data [C:\ProgramData] Bureau [C:\Isers\Public\Deskton]
14/07/2009	Ø5:53	<jonction></jonction>	Desktop [C:\Users\Public\Desktop]
14/07/2009	Ø5:53	< JONCTION>	Documents [C:\Users\Public\Documents]
18/02/2010	07:25 05:53	<junciiun></junciiun>	Favoris [G:\Users\Public\Favorites] Fauorites [G:\Users\Public\Fauorites]
18/02/2010	Ø9:25	<jonction></jonction>	Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010	09:25	<jonction></jonction>	Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009	05:53	<jonction></jonction>	Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009	05:53	<jonction></jonction>	Templates [C:\ProgramData\Microsoft\Windows\Templates]

Et on voit bien que la nouvelle structure de **All-Users** est donc découpée en 2 sections => **ProgramData & Users\Public**

<u>1° partie</u> : stockée en ProgramData\Microsoft\Windows

18/02/2010	09:25	<jonction></jonction>	Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010	09:25	<jonction></jonction>	Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009	05:53	<jonction></jonction>	Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009	05:53	<jonction></jonction>	Templates [C:\ProgramData\Microsoft\Windows\Templates]

- pour modifier le menu démarrer il faut aller en c:\ProgramData\Microsoft\Windows\Start Menu
- pour donner une modèle il faut aller en c:\ProgramData\Microsoft\Windows\Templates
- pour exécuter un programme à l'ouverture de session c:\ProgramData\Microsoft\Windows\Start Menu\Programs\startup

os-s	ysteme (C:) > ProgramData > Microsoft > \	Windows ⇒ Menu Dém	arrer > Programmes	› Démarrage
^	Nom	Modifié le	Туре	Taille
	📓 desktop.ini	16/07/2016 15:21	Paramètres de co	1 Ko

2° partie : stockée en Users\Public

18/02/2010 14/07/2009	09:25 05:53	<jonction> <jonction></jonction></jonction>	Bureau [C:\Users\Public\Desktop] Desktop [C:\Users\Public\Desktop]
14/07/2009	05:53	<jonction></jonction>	Documents [C:\Users\Public\Documents]
18/02/2010	09:25	<jonction></jonction>	Favoris [C:\Users\Public\Favorites]
14/07/2009	05:53	<jonction></jonction>	Favorites [C:\Users\Public\Favorites]

 pour poser des raccourcis ou dossiers ou documents sur le Bureau de tout le monde il faut aller en c:\Users\Public\Desktop



N.B: les autres entrées **users\public** correspondent à des fonctionnalités de partage réseau simplifié, en environnement personnel

Supprimer tous les profils locaux Windows 10: Par GPO

On peut passer par une GPO, ou bien Gpedit.msc

Configuration ordinateur \ modèles d'administration \ Système



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





Par base de registre

En effacant les entrées dans

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Profile List

Par utilitaire delprof2

Un nouvel utilitaire remplace l'ancien delprof obsolète depuis Seven

Delprof2 – User Profile Deletion Tool

Delprof2 is the unofficial successor to Microsoft's Delprof which does not work with operating systems newer than Windows XP. Here are the main facts:



Suivit de

C:\Users\Administrateur\Desktop\Delprof2 1.6.0\Delprof2 1.6.0>delprof2 /q





INTERFACE WINDOWS 10

Accès Paramètres Windows 10:

Le contenu s'étoffe de build en build

Sous 1511, 9 entrées

Système Affichage, notifications, applications, alimentation	Périphériques Bluetooth, imprimantes, souris	Réseau et Internet Wi-Fi, mode Avion, VPN	Personnalisation Arrière-plan, écran de verrouillage, couleurs	Comptes Comptes, adresse de messagerie, synchronisation, travail,
Heure et langue Voix, région, date	Options d'ergonomie Narrateur, loupe, contraste élevé	Confidentialité Emplacement, caméra	Mise à jour et sécurité Windows Update, récupération, sauvegarde	

Sous 1803, 12 entrées

Paramètres							-		×
			Paramètres	Wind	OWS				
			Rechercher un paramètre		٩				
旦	Système Affichage, son, notifications, puissance		Périphériques Bluetooth, imprimantes, souris		Téléphone Associer votre téléphone Android ou votre iPhone		Réseau et Internet Wi-Fi, mode Avion, VPN		
Ļ	Personnalisation Arrière-plan, écran de verrouillage, couleurs		Applications Désinstaller, valeurs par défaut, fonctionnalités facultatives	8	Comptes Comptes, e-mail, synchronisation, travail, autres	A A	Heure et langue Voix, région, date		
8	Jeux Barre de jeux, DVR, diffusion, mode jeux	Ģ	Options d'ergonomie Narrateur, loupe, contraste élevé	A	Confidentialité Emplacement, caméra	\mathbb{C}	Mise à jour et sécurité Windows Update, récupératio sauvegarde	n,	
Q	Recherche Langue, autorisations, historique								

Et les entrées sont de plus en plus complètes



Réseau et internet :

1511

🔅 RÉSEAU ET INTERNET	🖨 État 🔓
Consommation des données	🔛 Ethernet
Réseau privé virtuel	Accès à distance
Accès à distance	% VPN
Ethernet	Consommation des
Proxy	Proxy

Dans Ethernet une réinitialisation du réseau...

données

1803

Réseau et Internet

Mise à Jour et Sécurité

151

511	1803				
	Mise à jour et sécurité				
	C Windows Update				
	Sécurité de Windows				
🐯 MISE À JOUR ET SÉCURITÉ	→ Sauvegarde				
Windows Update	P Résoudre les problèmes				
Windows Defender	S Récupération				
Sauvegarde	 ⊘ Activation 				
Récupération	占 Localiser mon appareil				
Activation	H Pour les développeurs				
Pour les développeurs	😸 Programme Windows Insider				

Dans Résoudre les problèmes toute une multitude d'assistants



Panneau de Configuration style 7:

Microsoft veut à terme abandonner son panneau de configuration traditionnel

L'accès

Affichage Windows 10 par catégories Ajuster les paramètres de l'ordinateur Afficher par : Catégorie 🔻 Système et sécurité Comptes et protection des Consulter l'état de votre ordinateur utilisateurs Enregistrer des copies de sauvegarde de vos 🛞 Modifier le type de compte fichiers à l'aide de l'Historique des fichiers 🛞 Configurer le contrôle parental pour un Rechercher et résoudre des problèmes utilisateur Réseau et Internet Apparence et personnalisation Afficher l'état et la gestion du réseau Modifier le thème Choisir les options de groupe résidentiel et de Modifier l'arrière-plan du Bureau partage Modifier la résolution de l'écran Matériel et audio Horloge, langue et région Afficher les périphériques et imprimantes Ajouter une langue Ajouter un périphérique Modifier les méthodes d'entrée Modifier les formats de date, d'heure ou de Programmes nombre Désinstaller un programme Options d'ergonomie

Affichage Windows 10 par petites icones

Ajuster les paramètres de l'ordinateur

Afficher par : Petites icônes 🔻

💻 Affichage Barre des tâches et navigation 🔇 Centre de synchronisation 👯 Centre Réseau et partage Reference de lecteur BitLocker Clavier Courrier (32 bits) & Comptes d'utilisateurs 🐻 Connexions RemoteApp et Bureau à ... Pate et heure 📱 Dossiers de travail Espaces de stockage Exécution automatique Flash Player (32 bits) 💶 Gestion des couleurs Groupement résidentiel 📇 Gestionnaire de périphériques Gestionnaire d'identification listorique des fichiers 😪 Langue Options d'alimentation 🕑 Options d'ergonomie Options de l'Explorateur de fichiers 🔏 Options d'indexation 🔁 Options Internet Houtils d'administration 🛃 Panneau de configuration NVIDIA Pare-feu Windows Reriphériques et imprimantes 🚅 Personnalisation Programmes par défaut A Polices Programmes et fonctionnalités Reconnaissance vocale Récupération 🔊 Région Résolution des problèmes 🍓 Sauvegarder et restaurer (Windows 7) 🚩 Sécurité et maintenance 📢 Son Souris 🖳 Système Windows Defender I Téléphone et modem

Laisser Windows suggérer les paramètres

Optimiser l'affichage



L'explorateur Windows:

On lance l'explorateur soit via la recherche cortana



Soit clic / droit **Explorateur de fichier** dans la barre des tâches en bas à gauche sur l'icône Windows



Ce qui donne



par rapport à l'aspect par défaut de l'explorateur windows on peut modifier notamment dans Affichage / le Volet de navigation



Volets de Navigation Afficher tous les dossiers Pas de Favoris



Toujours dans Affichage / Option on demande Modifier les options des dossiers

les éléments oms de fichiers és sélectionnés	
Af Modifier les options des dossiers et de recherche	glet Affichage
Options des dossiers	
Général Affichage Rechercher	Affiche
Affichage des dossiers Vous pouvez appliquer le type d'affichage (Détails ou	Ne pa
lcônes, par exemple) de ce dossier à tous les dossiers du même type.	Ne pa
Appliquer aux dossiers Réinitialiser les dossiers	Ne pa
Paramètres avancés :	
Fichiers et dossiers	ne pu
 Afficher la bare d'état Afficher la bare d'état Afficher la tégende des dossiers et des éléments du Burez Afficher le chemin d'accès complet dans la barre de titre Afficher les dossiers et les fichiers NTFS chiffrés ou comp 	Ne pa

Afficher le chemin d'accès complet Ne pas masquer les extensions Ne pas masquer les fichiers cachés Ne pas masquer les lecteurs vides Ne pas masquer les fichiers systèmes Ne pas utiliser l'assistant partage

Ensuite pour le **Ruban** c'est une affaire de choix ...

🌆 l 💽 🚺 = l		C:\data		- • ×
Fichier Accueil	Partage Affichage			v 😮
€ ∋ - ↑ 🎚	▹ Ordinateur ▷ Disque local (C:) ▷ data ▷		✓ 🖒 Recherche	r dans : data 🕉
Bibliothèques	Nom	Modifié le	Type Tail	le
Þ 🤣 Groupe résident	iel	03/05/2013 12:01	Dossier de fichiers	
Crdinateur Grdinateur Grdinateur Grdinateur Disque local (0 Stecycle.Bin SysReset Grdinateur Grdinateur Grdinateur Grdinateur	e en			
Fichier Accueil	Partage Affichage			^ ()
Volet de navigation •	Très grandes icônes Icônes moyennes Icônes icônes ✓ Liste Image: Détails ✓	□ □ Cases à comparante Trier □ ✓ Extension par + □ ✓ Éléments	ocher des éléments is de noms de fichiers Masq masqués s	uer les éléments électionnés
Volets	Disposition	Affichage ac	Afficher/Masquer	

Interface Aero:

Les réglages dits « AERO » sont disponibles dans les **propriétés ordinateur**, dans **Paramètres systèmes avancés - Performances**



Propriétés système					
Nom de l'ordinateur		Matériel			
Paramètres système avancés	Protection du système	Utilisation à distance			
Vous devez ouvrir une session ces modifications.	n d'administrateur pour eff	ectuer la plupart de			
Performances					
Effets visuels, planification d mémoire virtuelle	u processeur, utilisation d	e la mémoire et Paramètres	donnant		
Options de performance	es				
Effets visuels Avance	Prévention de l'exécution	n des données		_	
Sélectionnez les parar de Windows sur cet o	nètres que vous voulez util rdinateur.	iser pour l'apparence et les	performances	Pour Désactiver A demande d'obte	ERO on enir les
Laisser Windows d	hoisi <mark>r l</mark> a meilleure configura	tion pour mon ordinateur		meilleures performa	nces
Ajuster afin d'obte	nir la meilleure apparence			(Sans offat 2D à ag	
Ajuster afin d'obte	nir les meilleures performa	nces		s (suns eller so a gog	JO)
Paramètres persor	nnalisés :				
 Activer la compos Activer l'affichage Afficher des minia 	sition du Bureau e transparent atures au lieu d'îcônes				

NB : ALT+TAB pour passer d'une application à l'autre gère désormais le bureau

Menu Contextuel / Accueil Win+X

En bas à gauche, sur l'icône Accueil (lorsqu'elle apparaît)

on retrouve quasiment à l'identique le menu Contextuel de l'ancien Menu Démarrer...

Ce Menu dit Win+X est modifiable selon une procédure particulière, cf chapitre suivant spécifique Menu Win-X





Evolution notables :

• Disparition de l'accès direct au Panneau de configuration

Qui reste accessible via executer control

💷 Exécu	ıter	×
	Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.	
Ouvrir :	control	\sim

• Invite Powershell à la place de l'invite de commande

l'invite	de co	mmande	e peu	t se	
redemo	redemander via Paramètres,				
Personr	nalisati	on / b	arre	des	I
tâches	dans	laquelle	on	va	(
trouver					

Remplacer Invite de commandes par Windows PowerShell dans le menu, lorsque je clique avec le bouton droit sur le bouton Démarrer ou que j'appuie sur la touche Windows+X

Compromis Performances – arrêt services:

Certaines fonctionnalités de Windows 10 sont « gourmandes », et par conséquent peuvent être désactivées si besoin, comme l'indexation automatique :

Activé

On peut arrêter le service : Windows Search

Nom	Description	État	Type de démarrage	Ouvrir une session en tant que
🙀 Windows Search	Fournit des	Dém	Automatique (débu	Système local
Propriétés de Windows Sea	rch (Ordinateur I	ocal)		
Général Connexion Récu	upération Dépen	dances		
Nom du service : WSeard	h			
Nom complet : Window	s Search			
Description : Fournit de mise	des fonctionnalités en cache des pro	s d'indexati priétés, de	on de contenu, 🔺 résultats de 🖕	
Chemin d'accès des fichier C:\Windows\system32\Se	s exécutables : archIndexer.exe /I	Embedding		
Type de démarrage : AL	tomatique (début (différé)	•	
Obtenir de l'aide pour confi	qurer les options d	le démarra	<u>ge des services.</u>	
État du service : Démarré	5			
Démarrer An	rêter Su:	spendre	Reprendre	
Vous pouvez spécifier les p service.	aramètres qui s'ar	opliquent a	u démarrage du	



Bureaux Virtuels:

On peut disposer de plusieurs bureaux virtuels pour segmenter les environnements (perso / boulot) :

Le point d'entrée des bureaux virtuels est la 3° icone ne partant de la gauche dans la barre des tâches



Cela permet de visualiser sur le haut (ou le bas) de l'écran

Bureau 1	Bureau 2	Nouveau bureau
		• +

- Accéder au menu des bureaux virtuels et aux programmes en cours d'exécution : **Touche Windows + TAB**
- Créer un bureau virtuel : « WIN + CTRL + D »
- Passer d'un bureau virtuel à un autre très facilement : « WIN + CTRL + flèches gauche et droite »

N.B: Vous pouvez supprimer un poste de travail virtuel à tout moment en cliquant sur le "X" en haut à droite du bureau que vous voulez fermer. Cela transférera tous les programmes et applications sur le bureau à gauche de son emplacement dans la vue des tâches.





Historique des Activités - Timeline - ospolicy.admx

Windows 10 build 1803 est capable en plus de gérer un historique des activité



Que l'on peut effacer ou interdire via l'interface graphique dans

Paramètres, Confidentialité puis Historique des activités (Historique de mes activités sur cet appareil)

← Paramètres	— — ×
 Accueil Rechercher un paramètre Confidentialité 	Historique des activités Revenez à ce que vous faisiez sur votre appareil en stockant l'historique de vos activités, y compris les informations sur les sites web que vous visitez et la façon dont vous utilisez les applications et les services.
Autorisations de Windows	Enregistrer l'historique de mes activités sur cet appareil
보다 Historique des activités	Revenez à ce que vous faisiez, même si vous changez d'appareil, en envoyant à Microsoft l'historique de vos activités, y compris les informations sur les sites web que vous visitez et sur l'utilisation des applications et des services.
Autorisations Windows	Envoyer l'historique de mes activités à Microsoft

2 GPO existent

Configuration Ordinateur / Modèle d'administration / Système / stratégies de système d'exploitation

Avec respectivement Autoriser la publication des activités de l'utilisateur et Autoriser le chargement des activités de l'utilisateur





Ici on autorise la gestion de l'historique localement sur la machine, mais on s'interdit le stockage sur le Cloud Microsoft (le cas échéant)

Historique des activités

*Certains paramètres sont masqués ou gérés par votre organisation.

Revenez à ce que vous faisiez sur votre appareil en stockant l'historique de vos activités, y compris les informations sur les sites Publication non configurée web que vous visitez et la façon dont vous utilisez les applications et (autorisée) les services. Enregistrer l'historique de mes activités sur cet appareil Revenez à ce que vous faisiez, même si vous changez d'appareil, en envoyant à Microsoft l'historique de vos activités, y compris les informations sur les sites web que vous visitez et sur l'utilisation des applications et des services. Chargement désactivé (interdit)

Envoyer l'historique de mes activités à Microsoft

Dans le doute, on peut désactiver les 2

Dans ce cas ne pas prêter attention au BUG d'affichage (case cochée mais grisée)



Envoyer l'historique de mes activités à Microsoft



MENU WIN-X



On perd le **panneau de** configuration

On perd le centre de mobilité Choix entre Cmd et Powershell

Forcément on peut avoir envie de retrouver toujours les même entrées, indépendamment des releases OS, par exemple :

- L'invite de commande(admin) •
- L'accès au panneau de configuration •





Structure Menu Windows-X

Les raccourcis sont stockés pour 1 utilisateur (ici dans l'exemple Administrateur) en C:\users\Administrateur\Appdata\Local\Microsoft\Windows\WinX

Correspondant à

os-systeme (C:) > Utili	sateurs > Administrateur	> AppData > Local >	Microsoft > Windows	> WinX
,	Nom	^	Modifié le	Туре
	Group1		16/07/2016 15:23	Dossier de fichiers
	Group2		16/07/2016 15:23	Dossier de fichiers
	Group3		16/07/2016 15:23	Dossier de fichiers

les groupes contiennent des Raccourcis + Ashcodes (non modifiables)

Nom	Modifié le	Туре
📻 04 - Disk Management	30/10/2015 08:18	Raccourci
🔚 Centre de mobilité Windows	30/10/2015 08:18	Raccourci
📊 Connexions réseau	30/10/2015 08:18	Raccourci
📄 desktop.ini	30/10/2015 08:21	Paramètres de
🎥 Gestion de l'ordinateur	30/10/2015 08:18	Raccourci
🗊 Gestionnaire de périphériques	30/10/2015 08:18	Raccourci
📷 Invite de commandes	30/10/2015 08:18	Raccourci
🔂 Invite de commandes	30/10/2015 08:18	Raccourci
腸 Observateur d'événements	30/10/2015 08:18	Raccourci
📰 Options d'alimentation	30/10/2015 08:18	Raccourci
📰 Programmes et fonctionnalités	30/10/2015 08:18	Raccourci
📰 Système	30/10/2015 08:18	Raccourci
🔁 Windows PowerShell	02/12/2017 15:31	Raccourci
🔁 Windows PowerShell	02/12/2017 15:31	Raccourci
Nom	Modifié le	Туре
🔄 desktop.ini	30/10/2015 08:21	Paramètres de co
📻 Exécuter	30/10/2015 08:18	Raccourci
🛼 Explorateur de fichiers	30/10/2015 08:18	Raccourci
📷 Gestionnaire des tâches	30/10/2015 08:18	Raccourci
寣 Panneau de configuration	30/10/2015 08:18	Raccourci
🛼 Rechercher	30/10/2015 08:18	Raccourci
	Nom Programmes et fonctionnalités Programmes et fonctionnali	NomModifié leImage: Od - Disk Management30/10/2015 08:18Image: Centre de mobilité Windows30/10/2015 08:18Image: Centre de périphériques30/10/2015 08:18Image: Centre de commandes30/10/2015 08:18Image:

Le raccourci du panneau de configuration (récupéré sur un **menu Win-x** d'un **windows 1511** par exemple) étant le suivant





Test Modification Menu Win-X windows 10 (1709 – 1803)

Sur un poste **Window**s pour lequel dans le **menu-X** le **panneau de configuration** à disparu (build majeur 1709-1803), on peut rajouter un 4° groupe,

:	>	AppData → Local	۶	Microsoft > Windows >	WinX
		Nom		^	Modifié le
		Group1			02/12/2017 15:19
		Group2			03/12/2017 16:32
/	١	Group3			02/12/2017 15:25
	ł	Group4			03/12/2017 16:45

Contenant le raccourci du panneau de configuration récupéré précedemment !

AppData	• >	Local \Rightarrow Microsoft \Rightarrow Windows \Rightarrow WinX \Rightarrow G	roup4
	^	Nom	Modifié le
		📓 desktop.ini	03/12/2017 16:45
		🗊 Panneau de configuration	30/10/2015 08:18

Ce qui devrait amener, après un re-démarrage, le menu Win-X modifié suivant

Panneau de configuration	←
Applications et fonctionnalités	
Centre de mobilité	
Options d'alimentation	
Observateur d'événements	
Système	
Gestionnaire de périphériques	
Connexions réseau	
Gestion du disque	
Gestion de l'ordinateur	
Windows PowerShell	
Windows PowerShell (admin)	
Gestionnaire des tâches	
Paramètres	
Explorateur de fichiers	
Rechercher	
Exécuter	
Arrêter ou se déconnecter	
Bureau	

N.B: <u>on ne peut pas ajouter des raccourcis classiques</u> pour étoffer les **Win-X menu**, il faut récupérer des raccourcis spéciaux ... Ceci car Microsoft à intégrer un **ahscode** sur les raccourcis de ce menu, pour que justement il ne soit pas modifiable facilement.

Ceci dit, maintenant que l'on a compris ou étaient stockées les entrées, on va pouvoir utiliser un petit Utilitaire **Win-X Editor**, pour générer ces raccourcis !





Utilitaire Win-x Editor 3.0

Récupérable sur le site de winaero et testé jusqu'à la version 1703

Win+X Menu Editor v3.0 is out

I released a new version of my freeware app, Win+X Menu Editor, which provides you a simple and useful way to edit Win+X menu without system file modification. It keeps your system integrity untouched. This version is compatible with Windows 10 Creators Update. Here is what's new in this version.

Download Win+X Menu Editor allows you to add or remove Win	1+X me	nu ite	ems			
Donate options for satisfied						
users:						
Donate						
VISA 🤐 💷 🕬						
On récupère la version 3	— P	ropr	iétés de : Win	XEditor.ex	e	
Microsoft.WindowsAPICodePack.dll	Gén	éral	Compatibilité	Sécurité	Dét 🔰	Versions précédente
Microsoft.WindowsAPICodePack.Shell.dll					*0	
readme.txt	P	roprié	ité	Valeur		
WinXEditor.exe		Desc	ription			
WinXMenuEditorRelease zin	D	Descri	ption du fichier	Win+X M	enu Edito	or
8 WINAWEITREBUICHTERBEIZEP	T	уре		Application	n	
	V	ersion/	n du fichier	3.0.0.0		
	N	lom d	u produit	Win+X M	enu Edito	or
Et an la lance via l'evecutable	V	/ersio	n du produit	3.0.0.0		
EI ON le lance via l'executable	C	Copyri	ght	Copyright	©http:/	/winaero.com 2012
WinxEditor.exe	T	aille		145 Ko		

Les entrées par groupe apparaissent, avec la possibilité

- de créer / gérer des groupes
- Ajouter un programme via un executable
- Ajouter un programme parmi ceux proposés





Ajouter un groupe

Win+X Menu Editor 3.0.0.0	_		×
Add a program 👻 Create a group Remove		Restore of	defaults
Group4			^
Group3			
Programmes et fonctionnalités			

Ajouter un executable

	Win+X Menu	Editor 3.0.0.0	
Add	a program 👻	Create a group	Remove
	Add a progr	am	Ins
	Add preset	6	+
	Add a Contr	ol Panel item	
ø	Add an Adm	inistrative Tools ite	em

on va chercher un executable, donne un nom

→ Ce F	PC → os-systeme (C	:) > Windows > S	System32 >	Rename	
Nouveau o	dossier			Please enter new name:	
Profile ^	Nom	^	1	panneau de configuration	
tate	📴 control.exe		-		
9	convert.exe		1		OK Cancel

Et on obtient



Ensuite, il n'est pas nécessaire de re-démarrer le poste pour voir les changements, il suffit de demander restart explorer



Ajouter un élement du panneau de configuration ou outil d'administration

	💶 Add a Control Panel Item	_	\times
Win+X Menu Editor 3.0.0.0	Filter items:		
Add a program Ins	Icon Item		^
Add preset	肩 Bibliothèques		
👰 Add a Control Panel item	📃 Ce PC		
ndd an Administrative Tools item	Centre de mobilité Windows		
	Add an Administrative Tools Item	— r	<
Win+X Menu Editor 3.0.0.0	Filter items:		
Add a program Create a group Remove			
Add a program Ins			 _
Add preset	Icon Item		^
Add a Control Panel item	Analyseur de performances		
Add an Administrative Tools item	Configuration du système		

Pour obtenir au final



Restaurer le menu initial

📃 Win+X Menu Editor 3.0.0.0	_		×
Add a program 👻 Create a group Remove		Restore of	defaults



ACCES RAPIDE EXPLORATEUR

Gestion accès rapide:

Par défaut sur windows 10... l'explorateur s'ouvre sur un accès rapide...



On peut supprimer des entrées avec le menu contextuel désépingler de l'Accès rapide

🗸 🖈 Accès rapide	Oossiers
📃 Bureau	* Bi
🕂 Téléchargemen	its 🕜 🗖 C
Documents	Développer
📰 Images	Ouvrir dans une nouvelle fenêtre
🛩 🛄 Bureau	Numeriser avec Windows Defender
> 🤱 Administrate	Désépingler de l'Accès rapide

On peut ajouter une entrée avec le menu contextuel épingler dans l'Accès rapide

Développer	
Numériser avec Windows De	efender
Ouvrir dans une nouvelle fer	nêtre
Épingler dans Accès rapide	



Ouverture Explorateur sur C: + pas d'accès rapide automatique

sur l'Accès rapide un cli droit Options

🗸 📌 Accès rapide	<u>^</u> ~
E. Bureau	Réduire
🚽 Téléchargen	Épingler le dossier actuel à Accès rapide
Documents	Options
Images	Épingler à l'écran de démarrage
	Ouvrir dans une nouvelle fenêtre

Qui amène directement à Affichage / Option / modifier les options des dossiers et de

on demande Ce Pc et on décoche

recherche

Par défaut on à

Général Affichage Rechercher	Général Af	fichage Rechercher
Ouvrir l'Explorateur de fichiers dans : Accès rapide Parcourir les dossiers	Ouvrir l'Exp de fichiers Parcourir	lorateur dans : les dossiers Ouvrir tous les dossiers dans la même fenêtre Ouvrir chaque dossier dans une fenêtre distincte
Cliquer sur les éléments de la manière suivante	Cliquer su	ur les éléments de la manière suivante Ouvrir les éléments par un simple clic (sélection par pointage) Souligner les titres d'icônes comme dans mon
Souligner les titres à loones comme dans mon navigateur Ne souligner les titres d'icônes que si le pointeu est sur eux Ouvrir les éléments par un double-clic (sélection pa		navigateur Ne souligner les titres d'icônes que si le pointeur est sur eux Ouvrir les éléments par un double-clic (sélection par simple clic)
Simple ciic) Déclaration de confidentialité Afficher les fichiers récemment utilisés dans Accès rapide	Déclarati	on de confidentialité Afficher les fichiers récemment utilisés dans Accès rapide
Afficher les dossiers récemment utilisés dans Accès rapide Effacer l'historique de l'Explorateur de fichiers		Arritorier les dossiers recemment utilises dans Acces rapide Effacer l'historique de l'Explorateur de fichiers
Paramètres par dé	t	Paramètres par défau



Désinstaller l'accès rapide:

Il faut vider d'abords l'accès rapide de tout son contenu, enlever les entrées automatique, et demander à l'explorateur Windows d'ouvrir sur Ce PC (et non pas sur l'accès rapide)

Puis Regedit, Rechercher la clé HKEY_CLASSES_ROOT\CLSID{679f85cb-0220-4080-b29b-

5540cc05aab6} Une fois sur la clé on change ses autorisations

1 1 1		L N	·
	> -	{679f85cb-0220-4080-b29b-5540cc05aab6}	
	>	{67A66362-050E-42ff-B241-82C1F51EA9B9}	Développer
	> -	{67CA7650-96E6-4FDD-BB43-A8E774F73A5	Nouveau
	>	{67EA3D48-83F2-408C-AD46-97F207D79DB	Rechercher
	>	{67F07E00-CCEF-11D2-9EF9-006008039E37	
	> -	{681FD532-7EC2-4548-9ECE-44AABCFBD25	Supprimer
	>	{682159d9-c321-47ca-b3f1-30e36b2ec8b9}	Renommer
<			
			Exporter
Ordinateu		_CLASSES_ROOT (CLSID)(0/9185CB-0220-408)	AutorisationsN
			1

Il faut en prendre possession en se donner les droits d'accès

Du coup dans le dossier on peut demander dans "ShellFolder", double-click

Attributes, et on change la clé de a0100000 à a0600000, et on valide par OK.

>	ab) (par défaut)	REG_SZ	(valeur non définie)
	왜 Attributes	REG DWORD	0xa0100000 (2685403136)
<pre></pre>	Refinitures FolderValueFlags Modifier la valeur Nom de la valeur : Attributes Données de la valeu a0100000	REG_DWORD DWORD 32 bits	décimale Annuler
	꽶 Attributes	REG_DWORD	0xa0600000 (2690646016)
	ሙ FolderValueFlags	REG_DWORD	0x00000001 (1)

Puis II faut redémarrer windows... **N.B** : Pour retrouver l'accès rapide il suffit de redonner la valeur **a010000** à la clé...

Modifier la valeur DWORD 3	2 bits ×
Nom de la valeur : Attributes	
Données de la valeur : a0600000	Base
	OK Annuler



Pour obtenir



DESINSTALLER ONEDRIVE

Icones points de lancement Onedrive:

Le lancement de Onedrive, espace de stockage sur le cloud à l'aide d'un identifiant

microsoft est présent à plusieurs endroits, notamment

• Dans la barre des tâches



Désactivation de Onedrive:



N.B : un redémarrage du poste est nécessaire !



INCLASSABLES WINDOWS 10

Menu étendus MAJ + clic droit:

On peut avoir des menus "contextuels" complets à l'aide de la touche MAJ

Menu contextuel

data				
Affichage	•			
Trier par	•			
Regrouper par	►			
Empiler par	►			
Actualiser				
Coller				
Coller le raccourci				
Nouveau	•			
Propriétés				
	Affichage Trier par Regrouper par Empiler par Actualiser Coller Coller le raccourci Nouveau Propriétés			

MAJ + Menu contextuel

Jata Prog Utilis Wind BOO	Explorer Ouvrir Ouvrir une fenêtre de commandes ici Rechercher	_
	Partager Restaurer les versions précédentes Copier en tant que chemin d'accès	
	Couper Copier	
	Créer un raccourci Supprimer Renommer	
	Propriétés	

Ouvrir une fenêtre de commande ici

Positionne le path local d'une invite de commande directement dans le dossier

Administrateur : C:\Windows\system32\cmd.exe _ 🗆 🗙 C:\data>_

Copier en tant que chemin d'accès

Permettant de récupérer la chaîne entre guillemet du chemin

"C:\data"

Ouvrir une fenêtre powershell ici (depuis 1803)

data		100
Doc		Ouvrir
expe		Ouvrir dans un nouveau processus
Inte		Ouvrir dans une nouvelle fenêtre
MSC		Épingler dans Accès rapide
Perf		Ouvrir la fenêtre PowerShell ici
Pro		Accorder l'accès à
Pro		Restaurer les versions précédentes
Pro	۲	Rechercher les menaces
Qua		
Rec		Inclure dans la bibliothèque
sysp		Épingler à l'écran de démarrage
Syst		Copier en tant que chemin d'accès



N.B : si on veut réobtenir l'invite de commande à la place de Powerschell on désactive dans Paramètres / Personnalisation / barre des tâches







Outils dxdiag:

Pour tester les pb directx, en ligne de commande dxdiag

😵 Outil de diagnostic DirectX 📃 🗉 💌
Système Affichage Son 1 Son 2 Entrée
Cet outil vous permet d'obtenir des informations détaillées sur les composants et pilotes DirectX installés sur votre système.
Si vous connaissez l'origine de ce problème, diquez sur l'onglet approprié. Sinon, diquez sur Page suivante ci-dessous pour afficher chaque page l'une après l'autre.
Informations système
Date/heure du jour : vendredi 19 mars 2010, 06:01:37
Nom de l'ordinateur : TEST-PC
Système d'exploitation : Windows 7 Professionnel 32 bits (6.1, version 7600)
Langue : français (Paramètres régionaux : français)
Fabricant du système : System manufacturer
Modèle du système : P5QL PRO
BIOS: BIOS Date: 07/01/09 17:37:27 Ver: 08.00.14
Processeur : Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz (4 CPUs), ~2.7GHz
Mémoire : 2048MB RAM
Fichier de pagination : 664 Mo utilisé(s), 3429 Mo disponible(s)
Version DirectX : DirectX 11
Rechercher les signatures numériques WHQL
DxDiag 6.01.7600.16385 32 bits Unicode Copyright © 1998-2006 Microsoft Corporation. Tous droits réservés.
Aide Page suivante Enregistrer toutes les informations Quitter

Outils shutdown:

En ligne de commande shutdown		
Shutdown /s /t 30	arrêt dans 30 secondes	
Shutdown /Is /t 0	fermeture de session immédiate	
Shutdown /m \\nomposte /t 0	arrêt du pc \\nomposte « immédiat »	
N.B : Les 2 options –r –f semblent obligatoires avec l'option –m		

Pour accéder au menu options de démarrage shutdown avec l'option /r/o

Shutdown /r /o	arrêt immédiat		
C:\Users\Administrateur>shu	tdown /r /o_		
Ou encore mieux			
Shutdown /r /o /f /t 0			

Une interface graphique est également disponible

Shutdown /i





Or <u>d</u> inateurs :	
	Ajout <u>e</u> r
	<u>S</u> upprimer
	Pa <u>r</u> courir
Quelles tâches voulez-vous que ces ordinateurs exécutent :	
Redémarrer 🗨	
Avertir les utilisateurs de l'action	
Afficher l'avertissement pendant 30 secondes	
Manihara d'érrénamente de avien hana terreira	
Moniteur d'évenements de mise nois tension	
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs.	le vous
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs. Option :	le vous <u>P</u> lanifié
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs. Option : Autre (planifié)	le vous
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs. Option : Autre (planifié) Un redémarrage ou un arrêt pour une raison inconnue	le vous
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs. Option : Autre (planifié) Un redémarrage ou un arrêt pour une raison inconnue	le vous
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs. Option : Autre (planifié) Un redémarrage ou un arrêt pour une raison inconnue Comm <u>e</u> ntaire : (obligatoire pour la raison que vous avez séle	le vous
Sélectionnez l'option qui décrit le mieux la raison pour laquel voulez arrêter les ordinateurs. Option : Autre (planifié) Un redémarrage ou un arrêt pour une raison inconnue Comm <u>e</u> ntaire : (obligatoire pour la raison que vous avez séle	le vous

Whoami / Runas:

En ligne de commande whoami permet de connaître son login

C:\Users\Administrateur>whoami test-pc\administrateur

N.B: à ce propos on peut lancer une tache avec un autre login (équivalent de RUNAS en ligne de commande) avec Pointer + SHIFT + Clic DROIT

Ainsi sur un executable, parfois sur certains raccourci, on peut faire apparaître Exécuter en tant qu'autre utilisateur



Forcément suivit de

	Sécurité Windows 🔘	×		
Exécuter en tant qu'autre utilisateur				
Entrez les informations d'identification à utiliser pour C: \Windows\system32\cmd.exe.				
	Nom d'utilisateur			
	Mot de passe			


Historique de fiabilité - Perfmon /rel :



Ou plus simple

Exécuter			
		Entrez le nom d'un progra Windows l'ouvrira pour ve	
	Ouvrir :	perfmon /rel	

On obtient

🏲 Panneau de configuration\Tous les Panneaux de configuration\Sécurité et maintenance\Moniteur de 🛛 🗕 🗌						
← → → ↑ 🏲 « Sécurité et maintenance → Moniteur de fiabilité	~	Ō	Rechercher			Q
Fichier Edition Affichage Outils ?						

Examiner l'historique de fiabilité et des problèmes de votre ordinateur

L'indice de stabilité indique la stabilité globale de votre système sur une échelle de 1 à 10. En sélectionnant une période spécifique, vous pouvez examiner les problèmes particuliers d'ordre matériel ou logiciel qui affectent votre système.



Détails de fiabilité pour : 10/07/2018

Source	Résumé	Date	Action	
🚫 Événements critiques (2) —————			· · ·	~
🖅 Autostart program viewer	Fonctionnement arrêté	10/07/2018 06:22	Rechercher une s	
🖅 Autostart program viewer	Fonctionnement arrêté	10/07/2018 06:23	Rechercher une s	
i Événements d'information (2)				~
9NBLGGH1Z8G6-Microsoft.NET.N	Windows Update a réussi	10/07/2018 05:35	Afficher les détail	
9NBLGGH1QWGC-Microsoft.Adve	Windows Update a réussi	10/07/2018 05:36	Afficher les détail	



Enregistreur d'action - psr.exe:

L'outil s	e lanc	e via psr.exe				
	Exécuter					
	۵	Entrez le nom d'un programme, dossier, Windows l'ouvrira pour vous.				
	Ouvrir :	psr.exe				
On ob	tient					
📑 Enr	egistreur	d'actions utilisateur	₽ ₽	_		×
Co <u>m</u>	mencer	l 'enregistrement O Arrêt <u>e</u> r l'enregistr	:ment 📑 Ajouter u	ın <u>c</u> omme	entaire	•

Il suffit simplement d'enregistrer l'endroit de stockage via le menu paramètres

strement 🛛 🛋 Ajoute	un <u>c</u> ommentaire	
Aide	F1	
Paramètres	N	
À propos de l'Enreg	istreur d'actions	c come choix
La localis	ation	le format de fichier
Paramètres d	l'Enregistreur d'actions utilisateur	×
Fichier de s	rtie ·	
\\nas-1\co	nmun\acces-salle-1\windows 10 administr	ration Parcourir Fichiers ZIP (*.zip)
Capture	écran	Fichiers XML (*.xml)
Activer l	capture d'écran :	\searrow
Nombre	Oui On Non Arcantures d'écran récentes à stocker :	
Hombre		23
<u>Aidez-moi a</u>	vec ces paramètres O	K Annuler

Et on démarre l'enregistrement

I Enregistreur d'actions utilisate	ur	- 🗆	×				
Commencer l'enregistrement	💿 Arrêt <u>e</u> r l'enregistrement 🛛 🛋 🧍	Ajouter un <u>c</u> ommentaire	•				
6	▼ X L						
On fait ce que l'on veut,							
et on arrête l'enreg	istrement						
Enregistreur d'actions	utilisateur - Enregistrement en cours	_					
Suspendre l'enregistre	ment 🛈 Arrêt <u>e</u> r l'enregistrement	■ Ajouter un <u>c</u> omme	ntaire 🔞				
	45	Y X IIII					



Recording_20180710_1256.mht

Qui est visualisable dans un navigateur:



Étapes enregistrées

Ce fichier contient toutes les étapes et informations enregistrées pour vous aider à les décrire aux autres. Avant de partager ce fichier, vérifiez les éléments suivants :

- Les étapes ci-dessous décrivent précisément l'enregistrement.
- Toutes les informations ci-dessous et les captures d'écran peuvent être dévoilées aux autres.

Les mots de passe et le texte tapé n'ont pas été enregistrés, à l'exception des touches de fonction et de raccourci utilisées. Vous pouvez procéder comme suit :

- Consulter les étapes enregistrées
- Consulter les étapes enregistrées sous forme de diaporama
- Consulter les détails supplémentaires

Étapes

Étape 1: (10/07/2018 12:56:05) Clic avec le bouton gauche par l'utilisateur sur « Démarrer (Bouton) »

Suivant



Détails supplémentaires

La section suivante contient les détails supplémentaires enregistrés.

Ces détails facilitent l'identification précise des programmes et de l'interface utilisateur employée dans cet enregistrement. Cette section peut contenir du texte interne aux programmes, compréhensible seulement par les utilisateurs chevronnés ou les programmeurs.

Consultez ces détails pour vérifier qu'ils ne contiennent aucune information à ne pas révéler aux autres.

```
Session d'enregistrement: 10/07/2018 12:56:04 - 12:56:16

Étapes enregistrées : 4, Actions manquées : 0, Autres erreurs : 0

Système d'exploitation: 10586.1176.amd64fre.th2_release_sec.170913-1848 10.0.0.0.2.48

Étape 1: Clic avec le bouton gauche par l'utilisateur sur « Démarrer (Bouton) »

Programme: Explorateur Windows, 10.0.10586.0 (th2_release.151029-1700), Microsoft Corporatior

Éléments d'interface: Démarrer, Start, Shell_TrayWnd

Étape 2: Clic avec le bouton gauche par l'utilisateur sur « Actualité

Macron se rend en Russie pour soutenir les Bleus (élément de liste) » dans « Début »

Programme: Windows Shell Experience Host, 10.0.10586.1106 (th2_release.170904-1742), Microsoft

Éléments d'interface: Actualité

Macron se rend en Russie pour soutenir les Bleus, TileListViewItem, en-tête de groupe Jouer e
```



Microsoft Management Console:

Dite plus couramment **MMC**, cette console d'administration n'est en fait qu'un coquille vide, ne faisant rien si ce n'est unifier et homogénéiser l'aspect des différents outils de gestion que l'on doit employer.

La MMC sert donc à fournir une interface commune pour tous les outils d'administrations sous Windows

Chaque MMC peut recevoir (ou on peut lui ôter) des outils d'administrations via ce que l'on appelle des «snap-in» ou encore des «composant logiciels enfichables ». Il existe un snap-in pour chaque outils de gestion.

Les consoles contiennent de manières générale un ou plusieurs snap-in et sont enregistrées dans des fichiers dotés de l'extension .msc stockés par défaut dans le dossier Outils d'Administration Winnt\System32

S'il est évident qu'il existe déjà un certain nombre de consoles prédéfinies, il est tout aussi évident que l'on peut se créer ses propres consoles personnalisées

Si on a besoin que d'une partie console (par seulement d'une gestionnaire exemple le de disques), peut donc être 11 avantageux de lancer uniquement partie intéressante, la en exécutant le fichier d'extension .msc associé

····· / · ·····	-
Fichier	Rôle
certmgr.msc	Certificats
ciadv.msc	Service d'indexation
devmgmt.msc	Gestionnaire de périphériques
dfrg.msc	Défragmenteur de disques
diskmgmt.msc	Gestion des disques
dnsmgmt.msc	Gestionnaire de DNS
eventvwr.msc	Observateur d'événements
faxserv.msc	Gestion du service de télécopie
fsmgmt.msc	Dossiers partagés
gpedit.msc	Stratégie de groupe
ias.msc	Service d'authentification Internet
lusrmgr.msc	Utilisateurs et groupes locaux
ntmsmgr.msc	Stockage amovible
ntmsoprq.msc	Demandes de l'opérateur de stockage amovible
perfmon.msc	Analyseur de performances
secpol.msc	Paramètres de sécurité locaux
services.msc	Services
wmimgmt.msc	Infrastructure de gestion Windows (WMI)
comexp.msc	Service de composants
iis.msc	Services Internet
msinfo32.msc	Informations système

Créer une console personnalisée:

Il faut demander **Executer /** Et taper mmc

Ou rechercher MMC



On obtient une **console1** vide prête à être personnalisée





🚡 Console1 - [Racine de la console]							
🚟 Fichier Action Affichage Favoris Fenêtre ?							
⇐ ➡ 🔲 🗟 🔽							
📔 Racine de la console	Actions						
	Aucun élément	Racine de la console 🛛 🔺					
		Autres actions					

En étant placé à la racine de la console, demander dans le menu

Fichier / Ajouter - Supprimer un composant logiciel enfichable

Ajouter ou supprimer des composants logiciels enfichables					
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.					
Composants logiciels enfichables disp	onibles :	Composants logiciels enfi. sélect	ionnés :		
Composant logiciel enfi Fournis	sseur	🔛 Racine de la console	Modifier les extensions		
S Analyseur de perfor Microso	oft Cor oft Cor		Supprimer		
Configuration du clie Microso	oft Cor E		Monter		
Contrôle WMI Microso	oft Cor Ajout	er >	Descendre		
Image: Second state Microson Image: Second state Image: Second state Microson	oft Cor oft Cor	<i>\</i> ∕3			
Gestion de l'impression Microso	oft Cor oft Cor				
Restion de la straté Microso	oft Cor				

Dans la liste des snap-in choisir « **gestion de l'ordinateur** » (par exemple) et demander de gérer l'ordinateur local

Ges	tion de l'ordinateur
:	Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable. - Ce composant logiciel enfichable gérera toujours :
	Cordinateur local (l'ordinateur sur lequel cette console s'exécute)
	C Un autre ordinateur : Parcourir

Et l'on voit que notre console se personnalise !

🖀 Console1 - [Racine de la console\Gestion de l'ordinateur (local)\Outils système\Utilisateurs et groupes locaux\Utilisat 👝 💿 💌					
🚟 Fichier Action Affichage Favoris F	enêtre ?			_ 8 ×	
📔 Racine de la console	Nom	Nom complet	Description	Actions	
Gestion de l'ordinateur (local)	admin	admin		Utilisateurs 🔺	
 Outris systeme Planificateur de tâches Observateur d'événements Observateur d'événements Observateur d'événements Observateur d'événements Utilisateurs et groupes locaux Utilisateurs 	Administrat Invité F test Invité Invité	test	Compte d'utilisa Compte d'utilisa	Autres actions 🕨	
Pour enregistrer cette Console / Enregistrer sous	console	il faut	demander	le menu	
Nom du fichier : michel.msc Type : Fichiers Microsoft	Management Consol	•	Et taper ici le console mr exemple « mic	nom de la nc, par hel »	



Pour peu que l'on ait placé le fichier .msc dans le bon dossier...



N.B: on peut placer le fichier sur le bureau... ou ailleurs...

Limiter les fonctions d'un composant logiciel :

Lorsque l'on crée une console avec un composant, celui-ci peut donner accès à plein de fonctionnalités différentes. Si on veut ce composant, mais avec moins de fonctionnalités, (en quelque sorte on veut le « brider ») Il suffit de :

- désactiver certaines extensions de la console
- enregistrer la console en mode utilisateur...

Désactiver des extensions de la console :

Au moment d'inclure le composant gestion de l'ordinateur

Ajouter ou supprimer des composants logiciels enfichables					
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.					
Composants logiciels enfichables disponibles :	Composants logiciels enfi. sélectionnés :				
Composant logiciel enfi Fournisseur Malyseur de perfor Microsoft Cor Certificats Microsoft Cor Configuration du clie Microsoft Cor Configuration et an Microsoft Cor Contrôle ActiveX Microsoft Cor Contrôle WMI Microsoft Cor	Racine de la console Gestion de l'ordinateur (local) Modifier les extensions Supprimer Monter Descendre				
	Extensions nour Gestion de l'ordinateur				
On demande Modifier les extensions pour obtenir alors	Vous pouvez indiquer quelles extensions doivent être activées afin d'ajouter ou de supprimer des fonctionnalités à votre console, composant logiciel enfichable ou extension. Si une extension n'est pas installée, vous pouvez l'Installer en la sélectionnant et en cliquant sur Installer. Toujours activer toutes les extensions disponibles Toutes les extensions disponibles, et toutes les extensions installées ultérieurement seront activées				
on demande de n'activer que les extensions sélectionnées	N'activer que les extensions sélectionnées Seules les extensions sélectionnées ci-dessous seront activées. Les extensions installées ultérieurement ne seront pas activées.				
et ensuite on faite sa sélection					
	Description :				



Enregistrer la console utilisateur :

Avant d'enregistrer la console, il faut dans le menu Flchier / Option

itions 🗾		
Ionsole Nettoyage de disque	1	
Console 1 Changer l'îcône		
Ces options prendront effet lorsque vous ouvrirez une nouvelle session MMC.		
Mode de console :		Mode de console :
Mode auteur		Mode utilisateur - accès total
		Description

Demander de passer en Mode utilisateur...

Empêche les utilisateurs d'ajouter ou de supprimer des o	omposants
logiciels enfichables ou de changer les options du fichier	de console de
composants enfichables. Les utilisateurs bénéficient d'u	n accès sans
limites à l'arborescence.	

Au prochain lancement, les composants enfichables de cette console ne sont plus modifiables... et son réduit à la gestion utilisateur





Secpol.msc - Rappel stratégies locales et GPo de domaine

Les stratégies locales se lancent depuis les outils d'administration, à travers stratégie de sécurité locale

ce qui donne ensuite accès aux paramètres suivants :

a Paramètres de sécurité locaux							
Action Affichage $4 \Leftrightarrow \Rightarrow 1 \textcircled{1} \times \textcircled{1} 2$							
Arbre	Stratégie 🛆	Paramètre local	Paramètre en cours				
Paramètres de sécurité	Conserver l'historique des mots de passe	0 mots de passe mémorisés	0 mots de passe mé				
E III Stratégies de comptes	BDurée de vie maximale du mot de passe	42 Jours	42 Jours				
庄 💼 Stratégie de mot de passe	BDurée de vie minimale du mot de passe	0 Jours	0 Jours				
🗄 📑 Stratégie de verrouillage du compte	Bles mots de passe doivent respecter des exigences de co	Désactivé	Désactivé				
🚊 💼 Stratégies locales	Blongueur minimale du mot de passe	0 Caractères	0 Caractères				
吏 👜 Stratégie d'audit	BS Stocker le mot de passe en utilisant le cryptage réversible	Désactivé	Désactivé				
🕀 📴 Attribution des droits utilisateur							
🕀 📴 Options de sécurité							
😑 🛄 Stratégies de clé publique							
Agents de récupération de données cryptées							
🗄 📲 🛃 Stratégies de sécurité IP sur Ordinateur local							

Les **GPO** ou **stratégies de domaine/réseaux** elles sont en général utilisées à travers le réseau (pour tout le domaine ou une partie à travers les UO...)

A ce stade, on ne confond plus les « réglages des stratégies locales » avec le fait de passer ces réglages localement via **secpol.msc** (ou **le panneau de configuration / stratégies locales**) ou via une **GPO** de **domaine**

Gpedit.msc - editeur de stratégie de domaine "locale" ! :

Il est cependant possible de modifier localement les stratégies d'une machine Windows avec les options normalement réservées aux stratégies de domaine /réseau, ARG !

Il faut passer par une console personnalisée **gpedit.msc** que l'on lance depuis **démarrer / executer**...

Éditeur de stratégie de groupe locale		
Fichier Action Affichage ?		
 Stratégie Ordinateur local Stratégie Ordinateur local Stratégie Ordinateur 	🚊 Stratégie Ordinateur local	
 Paramètres du logiciel Paramètres Windows Modèles d'administration Composants Windows Imprimantes Panneau de configuration Réseau Système Tous les paramètres Configuration utilisateur Paramètres du logiciel Paramètres Windows Modèles d'administration 	Sélectionnez un élément pour obtenir une description.	Nom

N.B: Evidemment on ne choisit pas sur qui cela s'applique...!



Liste de toutes les stratégies - Policysettings-1809.xls :

Microsoft publie des mises à jour dans un fichier Excel contenant le détail des paramètres de stratégies de groupe Pour les machines Windows 10. (et a chaque version, une version de ce fichier est disponible)

- Windows10andWindowsServer2016PolicySettings.xlsx
- Windows10andWindowsServer2016PolicySettings-1803.xlsx
- Windows10andWindowsServer2019PolicySettings--21H2.xlsx
- Windows10andWindowsServer2019PolicySettings--1809.xlsx
- Windows11andWindowsServer2019PolicySettings--21H2.xlsx

Pour chercher la version 1809 on peut faire une recherche du genre

Google	windows 10 1809 spreadsheet policies				Q			
_	Tous	Actualités	Images	Vidéos	Shopping	Plus	Paramètres	Outils
	Environ	199 000 résulta	its (0,49 seco	ondes)				

Group Policy Settings Reference Spreadsheet Windows 1809 ... https://techcommunity.microsoft.com/.../Windows-10...Policy...Spr... Traduire cette page Group Policy Settings Reference Spreadsheet Windows 1809 ... Windows 10 ... has been changed to reflect that the spreadsheet is the 1809 GPO settings now.

Download Group Policy Settings Reference Spreadsheet Windows ... https://www.microsoft.com/en-us/download/details.aspx?id... Traduire cette page 23 oct. 2018 - Group Policy Settings Reference Spreadsheet Windows 1809. Important! Selecting a language below will dynamically change the complete ...

Group Policy Settings Reference Spreadsheet Windows 1809

lr	nportant! Selecting a lan	guage below will dynamically change the complete page co	ntent to that language.
L	anguage:	English	Download

This spreadsheet lists the policy settings for computer and user configurations that are included in the Administrative template files delivered with the Windows operating systems specified. You can configure these policy settings when you edit Group Policy Objects.

amenant

Version:	Date Published:
1809	10/23/2018
File Name:	File Size:







Policysettings – 11-21H2.xls :

Google

windows 11 21H2 spreadsheet policies

Group Policy Settings Reference Spreadsheet for Windows 11 October 2021 Update (21H2)

Important! Selectir	ng a language below will dynamic	ally change the complete page content to that language.
Language:	English	Downloan

This spreadsheet lists the policy settings for computer and user configurations that are included in the Administrative template files delivered with for Windows 11 October 2021 Update (21H2) . You can configure these policy settings when you edit Group Policy Objects.



Voire les nouveautés par Branche :

Le fichier permet de faire le lien entre les définitions des paramètres dans les GPO et les clés de registre correspondantes. On peut faire plusieurs filtres sur ce fichier excel.

Filtre simple : Si on demande juste 1809 dans la colonne New in Windows 10 on obtiendra les 166 nouveaux réglages possibles (qui ne correspondent pas forcément à une nouvelle fonctionnalité 1809)

А	В	С	D	E	G
New in Windows 10 🕫	File name 💌	Policy Setting Name	Scope 🔻	Policy Path	Supported On
1809	apphvsi.admx	Allow Windows Defender Application Guard to use Root Cer	Machine	Windows Components\Windows Defender Application Gua	At least Windows 10 Enterprise
1809	apphvsi.admx	Allow camera and microphone access in Windows Defender	Machine	Windows Components\Windows Defender Application Gua	At least Windows 10 Enterprise
1809	apphvsi.admx	Allow users to trust files that open in Windows Defender Ap	Machine	Windows Components\Windows Defender Application Gua	At least Windows 10 Enterprise
1809	apphvsi.admx	Configure additional sources for untrusted files in Windows	Machine	Windows Components\Windows Defender Application Gua	At least Windows 10 Enterprise
1809	controlpanel.admx	Settings Page Visibility	User	Control Panel	At least Windows Server 2016, Windows 10 Version 1703
1809	datacollection.admx	Disable deleting diagnostic data	Machine	Windows Components\Data Collection and Preview Builds	At least Windows Server 2016, Windows 10 Version 1809

Filtre multiple : si on demande 1809 sur la colonne New in Windows 10 et at least windows server 2016 an windows 10 version 1809 sur la colonne Supported On

1	New in Windows 10 💌	File name	-
₽↓	Trier de <u>A</u> à Z	lservice.admx	Approved Installation Sites for ActiveX
Z L	Trier de Z à A	lservice.admx	Establish ActiveX installation policy for
	Trier par couleur	rograms.admx	Specify default category for Add New I
		rograms.admx	Hide the "Add a program from CD-RON
K	Effa <u>c</u> er le filtre de « New in Windows 10 »	rograms.admx	Hide the "Add programs from Microsof
	Filtrer par couleur 🕨	rograms.admx	Hide the "Add programs from your net
	Eiltres textuels	rograms.admx	Hide Add New Programs page
		rograms.admx	Remove Add or Remove Programs
	Rechercher 2	rograms.admx	Hide the Set Program Access and Defau
	(Sélectionner tout)	rograms.admx	Hide Change or Remove Programs page
	<u> </u> 1607	rograms.admx	Go directly to Components Wizard
		rograms.admx	Remove Support Information
	1803	rograms.admx	Hide Add/Remove Windows Compone
	2 1809	eview.admx	Toggle user control over Insider builds
			G

Supported On			
At least Windows Vista	Az↓	Trier de <u>A</u> à Z	
At least Windows Vista	Z L	Trier de Z à A	
Windows Server 2003, Windows XP, and Windows 2000 on	,	- Trier par couleur	
Windows Server 2003, Windows XP, and Windows 2000 on			
Windows Server 2003, Windows XP, and Windows 2000 on	K	Effacer le filtre de « Supported On »	
Windows Server 2003, Windows XP, and Windows 2000 on		Filtrer par couleur	
Windows Server 2003, Windows XP, and Windows 2000 on		Filtres textuels	
Windows Server 2003, Windows XP, and Windows 2000 on		Darah arah ar	
Windows Server 2003, Windows XP, and Windows 2000 on		Kechercher	
Windows Server 2003, Windows XP, and Windows 2000 on		At least Windows Server 2016 or Win	1
Windows Server 2003, Windows XP, and Windows 2000 on		At least Windows Server 2016, Windows	
Windows Server 2003, Windows XP, and Windows 2000 on		At least Windows Server 2016, Windows	
Windows Server 2003, Windows XP, and Windows 2000 on		At least Windows Server 2016, Wind	
Windows Server 2016, Windows 10 up to Version 1703			
At least Windows Server 2003		✓ At least Windows Server 2016, Wind	ł

Donc pour les nouveautés 1809 qui ne marchent que sur 1809, alors

New in Windows 10 耳	File name 💌	Policy Setting Name 💌
1809	datacollection.admx	Disable deleting diagnostic data
1809	datacollection.admx	Disable diagnostic data viewer.
1809	datacollection.admx	Configure Microsoft 365 Update Readiness upload endpoint
1809	oobe.admx	Don't launch privacy settings experience on user logon
1809	oobe.admx	Don't launch privacy settings experience on user logon
1809	windowsdefender.admx	Configure low CPU priority for scheduled scans
1809	windowsdefendersecuritycenter.admx	Disable the Clear TPM button
1809	windowsdefendersecuritycenter.admx	Hide the TPM Firmware Update recommendation.
1809	windowsdefendersecuritycenter.admx	Hide Windows Security Systray
1809	windowsupdate.admx	Remove access to "Pause updates" feature



Télécharger (installer) des ADMX modèle de GPO 10-1809 (sur un Serveur)

Téléchargeons un templates pour Windows 10 v1809 depuis le site de microsoft

Administrative Templates (.admx) for Windows 10 October 2018 Update (1809)

h	mportant! Selecting a lang	guage below will c	dynamically change the co	omplete page	content to that languag	e.	
L	anguage:	English			Downlo	ad	
This p 10 Oc	page provides the ctober 2018 Upda	e complete s ate (1809)	set of Administra	ative Temp	plates (.admx) fo	or Windows	
Θ	Details						
	Version:			Date	Published:		
	File Name:			File S	Size:		
	Administrative Template .msi	es (.admx) for Win	idows 10 October 2018 เ	Jpdate 13.8 I	vIB		
On té	lécharge le fic	hier					
	Ouverture de Admini	strative Template	s (.admx) for Windows 1	0 October	×		
	Vous avez choisi d'o []]e Template : qui est un fich à partir de : ht	uvrir : s (.admx) for Wir ier de type : Wind tps://download.r	ndows 10 October 2018 dows Installer Package (nicrosoft.com	8 Update.msi 13,8 Mo)			
	Voulez-vous enregis	trer ce fichier ?					
			Enregistrer le fichier	Annuler			
Nom					Туре	Modifié le	Taille
👸 Adm	inistrative Templates (.adı	mx) for Windows	10 October 2018 Update.	msi	Package Windows	26/11/2018 13:28	14 116 Ko
Et on	l'installe				- I		
	Administrative lempl	ates (.admx) for Wir	ndows 10 October 20	- L	×		
	for Windows 10	October 201	8 Update Setup W	/iz 🛋			
	The installer will guide you Windows 10 October 2018	through the steps req 3 Update on your com	uired to install Administrative To puter.	emplates (.admx) f	or		
	WARNING: This computer Unauthorized duplication of or criminal penalties, and w	r program is protected or distribution of this pro vill be prosecuted to th	by copyright law and internatic ogram, or any portion of it, may e maximum extent possible un-	nal treaties. result in severe ci der the law.	vil		
		(Cancel < Back	Next >			



en-U	S		17/05/2018 09:26	Dossier de fichiers
es-ES	3		17/05/2018 09:26	Dossier de fichiers
fi-Fl			17/05/2018 09:26	Dossier de fichiers
fr-FR			17/05/2018 09:26	Dossier de fichiers
hu-H	U		17/05/2018 09:26	Dossier de fichiers
📕 it-IT		2	17/05/2018 09:26	Dossier de fichiers
🗋 Activ	eXInstallService.admx		03/05/2018 14:56	Fichier ADMX
🗋 Add	RemovePrograms.admx		03/05/2018 14:56	Fichier ADMX
🗋 Allov	vBuildPreview.admx		03/05/2018 14:56	Fichier ADMX
🗋 Арр(Compat.admx		03/05/2018 14:56	Fichier ADMX

Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre Magasin Central



L'idée est que par rapport à un ebsemble de mises à jour disponibles, comme ici à la sortie d'une nouvelle version de l'OS windows 10 v1803, on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx...

On remplace donc juste un admx et son fichier de langue, tout en gardant l'ancien...

recup-totale-admx-PolicyDefinitions-windows-10-1809	^	Nom
en-US		fr-FR
📙 fr-FR		OOBE.admx
📙 remplacement-et-ajout-depuis-les-recup-dans-magasin-central		WindowsUpdate.admx
fr-FR		



Télécharger (installer) des ADMX modèle de GPO 10-21H2 (sur un Serveur)

Téléchargeons un templates pour Windows 10 v21H2 depuis le site de microsoft

Administrative Templates (.admx) for Windows 10 November 2021 Update [21H2]

Important! Selecting	a language below will dynamically change	the complete page content to that language.
Language:	English	Download

This page provides the complete set of Administrative Templates (.admx) for Windows 10 November 2021 Update [21H2]

⊖ Details

/ersion:	Date Published:
.0	11/19/2021
le Name:	File Size:
dministrative Templates (.admx) for Windows 10 November 2021 Updat .msi	13.1 MB

On télécharge le fichier

Nom	Туре	Modifié le	Taille
🛃 Administrative Templates (.admx) for Windows 10 October 2018 Update.msi	Package Windows	26/11/2018 13:28	14 116 Ko

Et on l'installe

🖟 Administrative Templates (.admx) for Windows 10 November... — 🛛 🛛 🗙



Welcome to the Administrative Templates (.admx) for Windows 10 November 2021 Update Setup Wizard

The Setup Wizard allows you to change the way Administrative Templates (.admx) for Windows 10 November 2021 Update features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central.** L'idée est que on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx...

On remplace donc 1 admx et son fichier de langue, tout en gardant l'ancien...

recup-totale-admx-PolicyDefinitions-windows-10-1809	^	Nom
en-US		fr-FR
📙 fr-FR		OOBE.admx
📙 remplacement-et-ajout-depuis-les-recup-dans-magasin-central		WindowsUpdate.admx
fr-FR		



Télécharger (installer) des ADMX modèle de GPO 11-21H2 (sur un Serveur)

Téléchargeons un templates pour Windows 11 v21H2 depuis le site de microsoft

ADMX Templates for Windows 11 October 2021 Update [21H2]

Important! Selecting a language below will dynamically change the complete page content to that language.

E

Language:

English

Download

This page provides the complete set of Administrative Templates (.admx) for Windows 11 October 2021 Update [21H2]



Version: 1.0	Date Published: 10/6/2021
File Name:	File Size:
Administrative Templates (.admx) for Windows 11 October 2021 Update. msi	13.2 MB

On télécharge le fichier

Nom	Modifié le	Туре	Taille
🙀 Administrative Templates (.admx) for Windows 11 October 2021 Update.msi	26/01/2022 14:53	Package Windows	13 564 Ko

Et on l'installe

d Administrative Templates (.admx) for Windows 11 October 2... — 🗌 🗙



Welcome to the Administrative Templates (.admx) for Windows 11 October 2021 Update Setup Wizard

The Setup Wizard will install Administrative Templates (.admx) for Windows 11 October 2021 Update on your computer. Click Next to continue or Cancel to exit the Setup Wizard.







Completed the Administrative Templates (.admx) for Windows 11 October 2021 Update Setup Wizard

Click the Finish button to exit the Setup Wizard.

Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central.** L'idée est que on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx...

GPO Windows 10 qui disparaissent (sous Windows 11):

https://techcommunity.microsoft.com/t5/core-infrastructure-andsecurity/windows-10-or-windows-11-gpo-admx-which-one-to-use-for-your/bap/3063322

https://4sysops.com/archives/group-policies-for-windows-11-and-10-21h2compared/

Dans le magasin, il ne peut y avoir qu'un fichier ADMX avec un nom donné

Fondamentalement il y a quelques **GPO** qui n'existent que sous **Windows 10** et d'autres qui sont apparues sous **windows 11**. Apriori cela semble normal que sous **windows 11** de nouvelles **GPO** apparaissent, mais le problème c'est que quelques anciennes **GPO** de **windows 10** disparaissent !

Ce qui fait que si on remplace les **ADMX** de 10 par les **ADMX** de 11, on peut risquer de perdre la main sur ces réglages !

Heureusement la liste est courte : est l'idée pour faire simple sera la suivante : si on n'utilisa pas les rares **GPO windows 10** « qui disparaissent » dans les **ADMX** de



windows 11, on peut sans problème installer ces ADMX, sinon il faut s'en passer, et rester avec les ADMX de windows 10!

N.B : il existe une procédure pour faire en sorte que l'on puisse administrer le même modèle **ADMX** en version 10 et version 11 mais.... Est-ce raisonnable ?

ADMX name	Scope	Setting	
DataCollection	Both	Allow Telemetry: Enhanced	
DeliveryOptimization	Computer	Download Mode: Bypass	
EAIME	User	Turn on Live Sticker	
EAIME	User	Turn on lexicon update	
InetRes	Both	Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects	
InetRes	Both	Reset zoom to default for HTML dialogs in Internet Explorer mode	
MicrosoftEdge	Both	Suppress the display of Edge Deprecation Notification	
Printing	Computer	Limit print driver installation to Administrators	
TerminalServer	Computer	Set the Remote Desktop licensing mode: AAD per User	
WindowsDefender	Computer	Scan packed executables	

Liste des ADMX windows 10 dans lesquels des réglages « disparaissent »



AppPrivacy Computer Let Windows apps take screenshots of various windows or displays AppPrivacy Computer Let Windows apps turn off the screenshot border AppxPackageManager Computer Archive infrequently used apps AppxPackageManager Computer Do not allow sideloaded apps to auto-update in the background AppxPackageManager Computer Do not allow sideloaded apps to auto-update in the background on a metered network CloudContent Computer Turn off cloud consumer account state content CloudContent User Turn off Spotlight collection on Desktop DataCollection Computer Prevent lock screen background motion DataCollection Computer Discovery Mode: Local Discovery DnsClient User Configure DNS over HTTPS (DoH) name resolution EAIME User Configure Korean IME version
AppPrivacy Computer Let Windows apps turn off the screenshot border AppxPackageManager Computer Archive infrequently used apps AppxPackageManager Computer Do not allow sideloaded apps to auto-update in the background AppxPackageManager Computer Do not allow sideloaded apps to auto-update in the background AppxPackageManager Computer Do not allow sideloaded apps to auto-update in the background on a metered network CloudContent Computer Turn off cloud consumer account state content CloudContent User Turn off Spotlight collection on Desktop DataCollection Computer Prevent lock screen background motion DataCollection Computer Discovery Mode: Local Discovery DnsClient User Configure DNS over HTTPS (DoH) name resolution EAIME User Configure Korean IME version
AppPrivacyComputerLet Windows apps turn off the screenshot borderAppxPackageManagerComputerArchive infrequently used appsAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local Discovery name resolutionEAIMEUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Local Discovery Control Panel Dk
AppPrivacyComputerLet Windows apps turn off the screenshot borderAppxPackageManagerComputerArchive infrequently used appsAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDataCollectionComputerDiscovery Mode: Local DiscoveryDnsClientUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
AppxPackageManagerComputerArchive infrequently used appsAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopDataCollectionComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerDiscovery Mode: Local DiscoveryDnsClientUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
AppxPackageManagerComputerArchive infrequently used appsAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopDataCollectionComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerDiscovery Mode: Local DiscoveryDnsClientUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
AppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the backgroundAppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerDiscovery Mode: Local DiscoveryDnsClientUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
AppxPackageManagerComputerauto-update in the background Do not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log Collection Discovery Mode: Local DiscoveryDeliveryOptimizationComputerDiscovery Mode: Local Discovery DnsClientEAIMEUserConfigure DNS over HTTPS (DoH) name resolution
AppxPackageManagerComputerDo not allow sideloaded apps to auto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
CloudContentComputerauto-update in the background on a metered networkCloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientUserConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
CloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDataCollectionComputerLimit Dump CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
CloudContentComputerTurn off cloud consumer account state contentCloudContentUserTurn off Spotlight collection on DesktopControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerDiscovery Mode: Local DiscoveryDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
CloudContentUserstate contentControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDataCollectionComputerDiscovery Mode: Local DiscoveryDataCollectionComputerDiscovery Mode: Local DiscoveryDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
CloudContent User Turn off Spotlight collection on Desktop ControlPanelDisplay Computer Prevent lock screen background motion DataCollection Computer Limit Diagnostic Log Collection DataCollection Computer Limit Dump Collection DeliveryOptimization Computer Discovery Mode: Local Discovery DnsClient Computer Configure DNS over HTTPS (DoH) name resolution EAIME User Configure Korean IME version
ControlPanelDisplayComputerDesktopDataCollectionComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
ControlPanelDisplayComputerPrevent lock screen background motionDataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
DataCollectionComputerImit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
DataCollectionComputerLimit Diagnostic Log CollectionDataCollectionComputerLimit Dump CollectionDeliveryOptimizationComputerDiscovery Mode: Local DiscoveryDnsClientComputerConfigure DNS over HTTPS (DoH) name resolutionEAIMEUserConfigure Korean IME version
DataCollection Computer Limit Dump Collection DeliveryOptimization Computer Discovery Mode: Local Discovery DnsClient Computer Configure DNS over HTTPS (DoH) name resolution EAIME User Configure Korean IME version
DeliveryOptimization Computer Discovery Mode: Local Discovery DnsClient Computer Configure DNS over HTTPS (DoH) name resolution EAIME User Configure Korean IME version
DnsClient Computer Configure DNS over HTTPS (DoH) name resolution EAIME User Configure Korean IME version
EAIME User Configure Korean IME version
EAIME User Configure Korean IME version
FileSys Computer Enable NIFS non-paged pool
usage
FileSysComputerNTFS parallel flush threshold
FileSysComputerNTFS parallel flush worker threads
FileSys Computer Configure NTFS default tier
Globalization Both Restrict Language Pack and
Language Feature Installation
InetRes Both Replace JScript by loading
JScript9Legacy in place of JScript
via MSHTML/WebOC.
NetlogonComputerUse lowercase DNS host names
when registering domain
controller SRV records
NewsAndInterests Computer Allow News and Interests
Sam Computer Configuration settings for the
Security Account Manager
Sensors Computer Force instant Wake
Sensors Computer Force instant Lock
Sensors Computer Configure Lock Timeout
StartMenu Both Locked Start Layout: Re-Apply
Layout at every logon
StartMenu Both Show or hide "Most used" list from
Start menu
Teel Der
Laskbar Computer Configure the Chat icon on the



TenantRestrictions	Computer	Configure Cloud Policy Details		
TerminalServer	Computer	Enable auto-subscription		
TerminalServer	Computer	Do not allow location redirection		
TerminalServer	Computer	Allow UI Automation redirection		
WindowsDefender	Computer	Configure scheduled task times randomization window		
WindowsDefender	Computer	Define the directory path to copy support log files		
WindowsDefender	Computer	Configure IP Address Exclusions		
WindowsDefender	Computer	Turn on script scanning		
WindowsDefender	Computer	Allow Microsoft Defender Antivirus to update and communicate over a metered connection		
WindowsDefender	Computer	Configure Network Protection to be allowed to be configured into block or audit mode on Windows Server		
WindowsDefender	Computer	Control datagram processing for network protection		
Sandbox	Computer	Allow vGPU sharing for Windows Sandbox		
Sandbox	Computer	Allow networking in Windows Sandbox		
Sandbox	Computer	Allow audio input in Windows Sandbox		
Sandbox	Computer	Allow video input in Windows Sandbox		
Sandbox	Computer	Allow printer sharing with Windows Sandbox		
Sandbox	Computer	Allow clipboard sharing with Windows Sandbox		
WindowsUpdate		<changes folder="" in="" structure=""></changes>		



SERVICES- NOMS LONG - COURTS

Services par noms courts

Classés par Noms courts

Noms court	LONG NAME	Noms Longs - Gestionnaire de Services	
AeLookupSvc	Application	Expérience d'application	
	Experience		
ALG	Application Layer	Service de la passerelle de la couche	
	Gateway Service	Application	
AppHostSvc	Application Host	Application Host Helper Service	
	Helper Service		
AppIDSvc	Application Identity	Identité de l'application	
Appinfo	Application	Informations d'application	
	Information		
AppMgmt	Application	Gestion d'applications	
	Management		
aspnet_state	ASP.NET State Service	Service d'état ASP.NET	
AudioEndpointBuilder	Windows Audio	Générateur de points de terminaison	
	Endpoint Builder	du service Audio Windows	
AudioSrv	Windows Audio	Audio Windows	
AxInstSV	ActiveX Installer	Programme d'installation ActiveX	
	(AxInstSV)	(AxInstSV)	
BDESVC	BitLocker Drive	Service de chiffrement de lecteur	
	Encryption Service	BitLocker	
BFE	Base Filtering Engine	Moteur de filtrage de base	
BITS	Background	Service de transfert intelligent en	
	Intelligent Transfer	arrière-plan	
	Service		
Browser	Computer Browser	Explorateur d'ordinateurs	
bthserv	Bluetooth Support Service	Service de prise en charge Bluetooth	
CertPropSvc	Certificate	Propagation du certificat	
	Propagation		
CISVC	Indexing Service	Service d'indexation	
clr_optimization_v2.0.5072 7	Microsoft .NET Framework NGEN v2.0.50727	Microsoft .NET Framework NGEN v2.0.x	
COMSysApp	COM+ System Application	Application système COM+	
CryptSvc	Cryptographic Services	Services de chiffrement	
CscService	Offline Files	Fichiers hors connexion	
DcomLaunch	DCOM Server	Lanceur de processus serveur DCOM	
	Process Launcher		
defragsvc	Disk Defragmenter	Défragmenteur de disque	
Diagtrack	Diagnostics	Gestions collecte des informations de	
	Tracking Service	diagnostic et télémtrie	



Dhcp	DHCP Client	Client DHCP	
Dnscache	DNS Client	Client DNS	
dot3svc	Wired AutoConfig	Configuration automatique de réseau câblé	
DPS	Diagnostic Policy Service	Service de stratégie de diagnostic	
EapHost	Extensible Authentication Protocol	Protocole EAP (Extensible Authentication Protocol)	
EFS	Encrypting File System (EFS)	Système de fichiers EFS (Encrypting File System)	
ehRecvr	Windows Media Center Receiver Service	Service de réception Windows Media Center	
ehSched	Windows Media Center Scheduler Service	Service de planification Windows Media Center	
EventLog	Windows Event Log	Journal d'événements Windows	
EventSystem	COM+ Event System	Système d'événement COM+	
Fax	Fax	Télécopie	
fdPHost	Function Discovery Provider Host	Hôte du fournisseur de découverte de fonctions	
FDResPub	Function Discovery Resource Publication	Publication des ressources de découverte de fonctions	
FontCache	Windows Font Cache Service	Service de cache de police Windows	
FontCache3.0.0.0	Windows Presentation Foundation Font Cache 3.0.0.0	Cache de police de Windows Presentation Foundation 3	
fsssvc	Windows Live Family Safety	Service Windows Live Contrôle parental	
ftpsvc	Microsoft FTP Service	Service FTP Microsoft	
gpsvc	Group Policy Client	Client de stratégie de groupe	
hidserv	Human Interface Device Access	Accès du périphérique d'interface utilisateur	
hkmsvc	Health Key and Certificate Management	Gestion des clés et des certificats d'intégrité	
HomeGroupListener	HomeGroup Listener	Écouteur HomeGroup	
HomeGroupProvider	HomeGroup Provider	Fournisseur HomeGroup	
idsvc	Windows CardSpace	Windows CardSpace	
IISADMIN	IIS Admin Service	Service d'administration IIS	
IKEEXT	IKE and AuthIP	Modules de génération de clés IKE et	



	IPsec Keying	AuthIP
IPBusEnum	Pop V IP Buc	Énumératour de bus IP Pop Y
	Enumerator	
iphlpsvc	IP Helper	Assistance IP
iprip	RIP Listener	RIP Listener
Keylso	CNG Key Isolation	Isolation de clé CNG
KtmRm	KtmRm for	Service KtmRm pour Distributed
	Distributed	Transaction Coordinator
	Transaction	
	Coordinator	
LanmanServer	Server	Serveur
LanmanWorkstation	Workstation	Station de travail
litdsvc	Link-Layer	Mappage de découverte de
	Discovery Mapper	ropologie de la couche de liaison
Imhosts	TCP/IP NetBIOS	Assistance NetBIOS sur TCP/IP
	Helper	
LPDSVC	LPD Service	Service LPD
Mcx2Svc	Media Center	Service Media Center Extender
	Extender Service	
MMCSS	Multimedia Class	Planificateur de classes multimédias
MpsSvc	Windows Firewall	Pare feu Windows
MSDTC	Distributed	Coordinateur de transactions
	Transaction	distribuées
	Coordinator	
MSISCSI	Microsoft iSCSI	Service Initiateur iSCSI de Microsoft
	Initiator Service	
msiserver MSMO	Windows Installer	Windows Installer
MSMQ	Message Queuing	Message Queuing
Momornggers	Triggers	Deciencheurs Message Queuing
napagent	Network Access	Agent de protection d'accès réseau
Notlogon	Protection Agent	
Netrogon	Neflogon	
Netman	Connections	Connexions resedu
NetMsmgActivator	Net.Msma Listener	Adaptateur d'écouteur Net.Msma
•	Adapter	
NetPipeActivator	Net.Pipe Listener	Adaptateur d'écouteur Net.Pipe
	Adapter	
netprotm	Network List	Service Liste des reseaux
NetTcpActivator	Net Ico Listener	Adaptateur d'écouteur Net Top
	Adapter	
NetTcpPortSharing	Net.Tcp Port	Service de partage de ports Net.Tcp
	Sharing Service	
NtsCint	Client for NFS	Client pour NFS
NIaSvc	Network Location	Connaissance des emplacements
	Awareness	reseau



nsi	Network Store	Service Interface du magasin réseau
n2nimevo	Interface Service	Costionnaire d'identité récord
	Identity Manager	homologue
p2psvc	Peer Networking	Groupement de mise en réseau de
	Grouping	pairs
PcaSvc	Program	Service de l'Assistant Compatibilité
	Compatibility	des programmes
	Assistant Service	
PeerDistSvc	BranchCache	BranchCache
pla	Performance Logs	Journaux & alertes de performance
PlugPlay	& amp; Alerts	Plug and Play
		Piug-ana-Piay
PNRFAutoReg	Name Publication	d'ardinatours PNPP
	Service	
PNRPsvc	Peer Name	Protocole PNRP
	Resolution Protocol	
PolicyAgent	IPsec Policy Agent	Agent de stratégie IPsec
Power	Power	Alimentation
ProfSvc	User Profile Service	Service de profil utilisateur
ProtectedStorage	Protected Storage	Emplacement protégé
QWAVE	Quality Windows	Expérience audio-vidéo haute qualité
	Audio Video	Windows
	Experience	
RasAuto	Remote Access	Gestionnaire de connexion
	Auto Connection	automatique d'accès distant
BasMan	Manager Romoto	Costionnairo do connovions d'accès
Nasivian	Connection	distant
	Manager	
RemoteAccess	Routing and	Routage et accès distant
	Remote Access	
RemoteRegistry	Remote Registry	Registre à distance
RpcEptMapper	RPC Endpoint	Mappeur de point de terminaison
	Mapper	RPC
RpcLocator	Remote Procedure	Localisateur d'appels de procedure
BpcSs	Remote Procedure	Appel de procédure distante (PPC)
Rpood	Call (RPC)	
SamSs	Security Accounts	Gestionnaire de comptes de sécurité
	Manager	
SCardSvr	Smart Card	Carte à puce
Schedule	Task Scheduler	Planificateur de tâches
SCPolicySvc	Smart Card	Stratégie de retrait de la carte à
	Removal Policy	puce
SDRSVC	Windows Backup	Sauvegarde Windows
SeaPort	SeaPort	SeaPort
seclogon	Secondary Logon	Ouverture de session secondaire
SENS	System Event	Service de notification d'événements
	Notification	système



	Service		
SensrSvc	Adaptive	Brillance adaptative	
	Brightness		
SessionEnv	Remote Desktop	Configuration des services Bureau à	
	Configuration	distance	
SharedAccess	Internet	Partage de connexion Internet (ICS)	
ShallHWDetection	Shall Uardware	Détection matérial novau	
Shein WDelection			
simptop	Simple TCP/IP	Services TCP/IP simples	
	Services		
SNMP	SNMP Service	Service SNMP	
SNMPTRAP	SNMP Trap	Interruption SNMP	
Spooler	Print Spooler	Spouleur d'impression	
sppsvc	Software	Protection logicielle	
	Protection		
sppuinotify	SPP Notification	Service de notification SPP	
	Service		
SSDPSRV	SSDP Discovery	Découverte SSDP	
SstpSvc	Secure Socket	Service SSTP (Secure Socket Tunneling	
	Tunneling Protocol) Protocol)	
	Service		
StiSvc	Windows Image	Acquisition d'image Windows (WIA)	
StorSvo	Acquisition (WIA)	Comico do sta alcana	
	Storage Service	Service de slockage	
Swprv	Microsoft Software	Fournisseur de cliche instantane de	
	Provider		
SysMain	Superfetch	Superfetch	
TabletInputService	Tablet PC Input	Service Panneau de saisie Tablet PC	
-	Service		
TapiSrv	Telephony	Téléphonie	
TBS	TPM Base Services	Services de base de module de	
	plateforme sécurisée		
TermService	Remote Desktop	Services Bureau à distance	
Therese			
TUDEADODDED	Themes	Themes	
THREADORDER	Ihread Ordering	Serveur de priorités des threads	
TIntSyr	Joinet	Tolpot	
TrkWks	Distributed Link	Client de quivi de lien distribué	
TIRWAS	Tracking Client		
TrustedInstaller	Windows Modules	Programme d'installation pour les	
		modules Windows	
UI0Detect	Interactive	Détection de services interactifs	
	Services Detection		
UmRdpService	Remote Desktop	Redirecteur de port du mode	
Services UserMode		utilisateur des services Bureau à	
	Port Redirector		
upnpnost	UPnP Device Host	Hote de periphèrique UPnP	



UxSms	Desktop Window	Gestionnaire de sessions du
	Manager Session	Gesnormalie de reneirage
VaultSvc	Credential	Gestionnaire d'informations
	Manager	d'identification
vds	Virtual Disk	Disque virtuel
VSS	Volume Shadow	Cliché instantané des volumes
	Сору	
W32Time	Windows Time	Temps Windows
W3SVC	World Wide Web Publishing Service	Service de publication World Wide Web
WAS	Windows Process Activation Service	Service d'activation des processus Windows
wbengine	Block Level	Service de moteur de sauvegarde en
	Backup Engine	mode bloc
	Service	
WbioSrvc	Windows Biometric Service	Service de biométrie Windows
wcncsvc	Windows Connect	Windows Connect Now - Registre de
	Now - Config	configuration
	Registrar	
WcsPlugInService	Windows Color	Système de couleurs Windows
WdiServiceHost	Diggnostic Sonvico	Sanvica hâta WDISanvica Hast
	Host	
WdiSystemHost	Diagnostic System	Hôte système de diagnostics
	Host	
WebClient	WebClient	WebClient
Wecsvc	Windows Event	Collecteur d'événements de Windows
wercplsupport	Problem Reports	Prise en charge de l'application
	and Solutions	Rapports et solutions aux problèmes
	Control Panel	du Panneau de configuration
	Support	
WerSvc	Windows Error	Service de rapport d'erreurs Windows
WinDefend	Reporting Service	Windows Doferndar
		Vindows Delender
WinnitipAdtoFT0XySVC	Proxy Auto-	de Provy Web pour les services HTTP
	Discovery Service	Windows
Winmgmt	Windows	Infrastructure de gestion Windows
	Management	
	Instrumentation	
WinRM	Windows Remote	Gestion à distance de Windows
	Management (WS-	(Gestion WSM)
Wlansvc		Sonvico do configuration
Widiisve	WLAN AUIOCONIIg	automatique WLAN
wmiApSrv	WMI Performance	Carte de performance WMI
	Adapter	
WMPNetworkSvc	Windows Media	Service Partage réseau du Lecteur
	THUYEN NETWORK	



	Sharing Service	
WMSVC	Web Manaaement	Service de gestion Web
	Service	
WPCSvc	Parental Controls	Parental Controls
WPDBusEnum	Portable Device Enumerator Service	Service Énumérateur d'appareil mobile
WSCSVC	Security Center	Centre de sécurité
WSearch	Windows Search	Windows Search
wuauserv	Windows Update	Windows Update
wudfsvc	Windows Driver Foundation - User- mode Driver Framework	Windows Driver Foundation - Infrastructure de pilote mode- utilisateur
WwanSvc	WWAN AutoConfig	Service de configuration automatique WWAN

Services par noms longs - fr

Classés par Noms longs français		
Noms Longs - Gestionnaire de	Nom court	LONG NAME
Services		
Accès du périphérique d'interface utilisateur	hidserv	Human Interface Device Access
Acquisition d'image Windows (WIA)	StiSvc	Windows Image Acquisition (WIA)
Adaptateur d'écouteur Net.Msmq	NetMsmqA ctivator	Net.Msmq Listener Adapter
Adaptateur d'écouteur Net.Pipe	NetPipeAct ivator	Net.Pipe Listener Adapter
Adaptateur d'écouteur Net.Tcp	NetTcpActi vator	Net.Tcp Listener Adapter
Agent de protection d'accès réseau	napagent	Network Access Protection Agent
Agent de stratégie IPsec	PolicyAgen t	IPsec Policy Agent
Alimentation	Power	Power
Appel de procédure distante (RPC)	RpcSs	Remote Procedure Call (RPC)
Application Host Helper Service	AppHostS∨ c	Application Host Helper Service
Application système COM+	COMSysAp p	COM+ System Application
Assistance IP	iphlpsvc	IP Helper
Assistance NetBIOS sur TCP/IP	Imhosts	TCP/IP NetBIOS Helper
Audio Windows	AudioSrv	Windows Audio
BranchCache	PeerDistSvc	BranchCache
Brillance adaptative	SensrSvc	Adaptive Brightness
Cache de police de Windows Presentation Foundation 3	FontCache 3.0.0.0	Windows Presentation Foundation Font Cache 3.0.0.0
Carte à puce	SCardSvr	Smart Card



Centre de sécuritéwscsvcSecurity CenterCliché instantané des volumesVSSVolume Shadow CopyClient de stratégie de groupegpsvcGroup Policy ClientClient de suivi de lien distribuéTrkWksDistributed Link Tracking ClientClient DNSDhcpDHCP ClientClient pour NFSNfsClntClient for NFSCollecteurdévénementsdeWecsvcWindows Event CollectorConfiguration automatiquede dot3svcA distanceSessionEnvRemote Desktop ConfigurationAdistanceConnaissance des emplacementsNIdSVcNetwork ConnectionsMSDTCDécencheurs Message QueuingMSMQTriggMécouverte SSDPSSDPSRVSSDPSRVSSDP DiscoveryDéfection de services interactifsUl/DetectDétection de services interactifsUl/DetectUiObetectNeeGrouDétection de services interactifsUl/DetectDisque virtuelvdsVirtual DiskProtectedSÉcouteur HomeGroupHomeGrouHomeGrouHomeGrouListenerVirtual DiskExpérience audio-vidéoNetworkQualité WindowsAudio VidecExpérience des utilisateursBrowserConditiesterApplication ExperienceVirtual DiskExpérienceEnglacement protégéProtectedSForageProtectedSFichiers hors connexionAeLookupSApplicationAeLookupSAeLookup	Carte de performance WMI	wmiApSrv	WMI Performance Adapter
Cliché instantané des volumes VSS Volume Shadow Copy Client de stratégie de groupe gpsvc Group Policy Client Client de suivi de lien distribué TrkWks Distributed Link Tracking Client Client DNS Dnscache DNS Client Client pour NFS NfsCInt Client for NFS Collecteur dévénements de Windows Wecsvc Windows Event Collector Configuration automatique de distance Configuration automatique dot3svc Connaissance des emplacements NtdSVc Network Location Awareness Connexions réseau Netman Network Location Awareness Connexions réseau Netman Network Connections Déciencheurs Message Queuing MSMQTrigg Message Queuing Triggers pérection de services interactifs UIDDetect Interactive Services Detection Détection matériel noyau ShellHWDet Shell Hardware Detection Détection de services interactifs UIDDetect Interactive Strage Disque virtuel vds Virtual Disk	Centre de sécurité	WSCSVC	Security Center
Client de stratégie de groupegpsvcGroup Policy ClientClient de suivi de lien distribuéTrkWksDistributed Link Tracking ClientClient DHCPDhcpDHCP ClientClient DNSDnscacheDNS ClientClient pour NFSNfsCIntClient for NFSCollecteurd'événementsdeWindowsConfigurationautomatiqueConfigurationautomatiquededot3svcWired AutoConfigréseau câbléSessionEnvA distanceSessionEnvConnaissance des emplacementsNlaSvcNetmanNetwork Location AwarenessréseauNetmanConraiteur de transactionsMSDTCDéclencheurs Message QueuingMSMQTriggMessage Queuing TriggersSSDP DiscoveryDéfargmenteur de disquedefragsvcDétection de services interactifsUIDDetectDétection matériel noyauShellHWDetShellHWDetShell Hardware DetectionDétecteur HomeGroupHomeGrouPlasement protégéProtectedSProtected StorageProtected StorageEnumérateur de bus IP PnP-XIPBusEnumEmplacement protégéProtectedSForageAeLookupSApplicationAeLookupSApplicationAeLookupSApplicationAeLookupSApplicationStorageExpérience de sutilisateursDiagTrackDiagrackDiagnostic Stotware Shadow CopyProviderOrdine FilesStorage	Cliché instantané des volumes	VSS	Volume Shadow Copy
Client de suivi de lien distribué TrkWks Distributed Link Tracking Client Client DHCP Dhcp DHCP Client Client DNS Dnscache DNS Client Client pour NFS NfsCInt Client for NFS Collecteur d'événements de Wecsvc Windows Event Collector Configuration automatique de dot3svc Wired AutoConfig réseau câblé SessionEnv Remote Desktop Configuration Connaissance des emplacements réseau Netman Network Location Awareness Coordinateur de transactions distribuées MSDTC Distributed Transaction Coordinator Découverte SSDP SSDPSRV SSDP Discovery Défargmenteur de disque defragsvc Disk Defragmenter Détection de services interactifs UI0Detect Interactive Services Detection Détection matériel noyau ShellHWDet Shell Hardware Detection Disque virtuel vds Virtual Disk Écouteur HomeGroup HomeGroup HomeGroup Listener pListener Reperience Audio Videc Expérience audio-vidéo haute qualité Windows QWAVE Quality Windows Audio Videc	Client de stratégie de groupe	gpsvc	Group Policy Client
Client DHCP Dhcp DHCP Client Client DNS Dnscache DNS Client Client pour NFS NfsCInt Client for NFS Collecteur d'événements de Wecsvc Windows Event Collector Configuration automatique dot3svc Wired AutoConfig Configuration des services Bureau SessionEnv Remote Desktop Configuration à distance Connaissance des emplacements NlaSvc Network Location Awareness Connaissance des emplacements NlaSvc Network Connections Coordinateur Connexions réseau Netman Network Connections Coordinator Déclencheurs Message Queuing MSMQTrigg Message Queuing Triggers ers SDP Discovery Défragmenter Détection de services interactifs Ul0Detect Interactive Services Detection Détection matériel noyau ShellHWDet Shell Hardware Detection Econe Disque virtuel vds Virtual Disk Ecouteur HomeGroup HomeGroup HomeGroup Listener Emplacement protégé ProtectedS Protected Storage	Client de suivi de lien distribué	TrkWks	Distributed Link Tracking Client
Client DNS Dnscache DNS Client Client pour NFS NfsCInt Client for NFS Collecteur d'événements de Wecsvc Windows Event Collector Configuration automatique dot3svc Wired AutoConfig Configuration automatique dot3svc Wired AutoConfig Connaissance des emplacements NlaSvc Network Location Awareness Connaissance de transactions MSDTC Distributed Transaction Coordinator Goteincheurs Message Queuing MSMQTrigg Message Queuing Triggers Découverte SSDP SSDPSRV SSDP Discovery Défragmenteur de disque Détection matériel noyau Shell Hordware Detection Shell Hordware Detection Détection matériel noyau Shell Hordware Detection Ecouteur HomeGroup HomeGroup HomeGrou HomeGroup Listener Eindét Windows QWAVE Quality Windows Audio Video Expérience audio-vidéo haute QWAVE Quality Windows Audio Video Expérience des utilisateurs DiagTrack Diagnostics Tracking Service <th>Client DHCP</th> <th>Dhcp</th> <th>DHCP Client</th>	Client DHCP	Dhcp	DHCP Client
Client pour NFS NtsClnt Client for NFS Collecteur d'événements de Wecsvc Windows Event Collector Configuration automatique de dot3svc Wired AutoConfig Configuration automatique de dot3svc Wired AutoConfig Configuration dessionEnv Remote Desktop Configuration Account à distance Connaissance des emplacements NldSvc Network Location Awareness Connexions réseau Netman Network Connections Coordinateur Condinateur de transactions MSDTC Distributed Transaction Coordinator distribuées MSMQTrigg Message Queuing Triggers ers Découverte SSDP SSDPSRV SSDP Discovery Défragmenter Détection de services interactifs Ul0Detect Interactive Services Detection Détection matériel noyau ShellHWDet Shell Hardware Detection ection Détectuer HomeGroup HomeGrou HomeGrou Listener Expérience audio-vidéo haute Quality Windows Audio Videce Expérience de	Client DNS	Dnscache	DNS Client
Collecteur Windowsd'événements windowsde WecsvcWindows Event CollectorConfiguration réseau câbléautomatique de dot3svcWired AutoConfigConnaissance distanceSessionEnvRemote Desktop Configuration a distanceConnaissance des emplacements réseauNlaSvcNetwork Location AwarenessConnexions réseauNetmanNetwork ConnectionsCornexions réseauNetmanNetwork ConnectionsCordinateur distribuéesde transactionsMSDTCDéclencheurs Message Queuing ersMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDétection de services interactifsUI0DetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskEcouteur HomeGroupHomeGrou pListenerHomeGroup ListenerEmplacement protégéProtectedS torageProtectedS torageEnumérateur de bus IP PnP-XIPBusEnum PnP-X IP Bus EnumeratorExpérience audio-vidéo haute qualité WindowsAeLookupS ApplicationApplication Experience vcExpérience des utilisateursBrowserComputer BrowserExpérience des utilisateursDiagrackDiagnostics Tracking ServiceFournisseur de cliché instantané é uspiciel MicrosoftSwprvMicrosoft Software Shadow Copy Provider	Client pour NFS	NfsCInt	Client for NFS
Mindows Configuration automatique réseau câblédot3svcWired AutoConfigConfiguration des services Bureau à distanceSessionEnvRemote Desktop Configurationà distanceConnaissance des emplacements réseauNlaSvcNetwork Location AwarenessConnaissance des emplacements réseauNlaSvcNetwork ConnectionsConnexions réseauNetmanNetwork ConnectionsCoordinateur distribuéesde transactions mSDTCDistributed Transaction CoordinatorDéclencheurs Message Queuing distribuéesMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disque defragsvcDisk DefragmenterDétection de services interactifsUIODetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup pListenerHomeGroup ListenerEmplacement protégé qualité WindowsProtectedS torageProtected StorageÉnumérateur de bus IP PnP-X ualité WindowsIPBusEnumPnP-X IP Bus EnumeratorExpérience qualité WindowsAeLookupS vcApplicationAeLookupS vcExpérience des utilisateurs connectés et télémétrieDiagTrackDiagnostics Tracking ServiceFournisseur de cliché instantané de logiciel MicrosoftSwprvMicrosoft Software Shadow Copy	Collecteur d'événements de Windows	Wecsvc	Windows Event Collector
Configuration des services Bureau à distanceSessionEnvRemote Desktop Configurationà distanceConnaissance des emplacements réseauNIaSvcNetwork Location AwarenessConnexions réseauNetmanNetwork ConnectionsCoordinateur distribuéesde transactions MSDTCDistributed Transaction CoordinatorDéclencheurs Message Queuing derageneteur de disqueMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disquedefragsvcDisk DefragmenterDétection de services interactifsUIODetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup ulistenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnum VCPnP-X IP Bus EnumeratorExpérience audio-vidéo hauteQWAVE VCQualityExpérience d'application connectés et télémétrieAeLookupS DiagTrackApplication Experience Diagnostics Tracking ServiceFournisseur de cliché instantané de logiciel MicrosoftSwprvMicrosoft Software Shadow Copy Provider	Configuration automatique de réseau câblé	dot3svc	Wired AutoConfig
Connaissance des emplacements réseauNlaSvcNetwork Location AwarenessConnexions réseauNetmanNetwork ConnectionsCoordinateur distribuéesMSDTCDistributed Transaction CoordinatorDéclencheurs Message Queuing Déclencheurs Message QueuingMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disquedefragsvcDisk DefragmenterDétection de services interactifsUlODetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup qualité WindowsHomeGrou plistenerProtectedS torageÉnumérateur de bus IP PnP-XIPBusEnum QWAVEPnP-X IP Bus EnumeratorExpérienceaudio-vidéo haute qualité WindowsAudio Video ExperienceExpérience des connectés et télémétrieBrowserComputer BrowserExpériencedes utilisateurs connectés et télémétrieDiagTrack swprvDiagnostics Tracking ServiceFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantané de logiciel MicrosoftSwprvMicrosoft	Configuration des services Bureau à distance	SessionEnv	Remote Desktop Configuration
Connexions réseauNetmanNetwork ConnectionsCoordinateur distribuéestransactionsMSDTCDistributed Transaction CoordinatorDéclencheurs Message QueuingMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disquedefragsvcDisk DefragmenterDétection de services interactifsUIODetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup 	Connaissance des emplacements réseau	NIaSvc	Network Location Awareness
Coordinateur distribuéesde transactions MSDTCMSDTCDistributed Transaction Coordinator Distributed Transaction CoordinatorDéclencheurs Message Queuing Découverte SSDPMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disque Détection de services interactifsdefragsvcDisk DefragmenterDécetton de services interactifsUIODetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup plistenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérience audio-vidéo qualité WindowsAeLookupS vcApplication ExperienceExpérience des connectés et télémétrieBrowserComputer BrowserExpérience de logiciel MicrosoftCscServiceOffline FilesFournisseur de cliché instantané de logiciel MicrosoftswprvMicrosoft Software Shadow Copy	Connexions réseau	Netman	Network Connections
Déclencheurs Message QueuingMSMQTrigg ersMessage Queuing TriggersDécouverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disquedefragsvcDisk DefragmenterDétection de services interactifsUI0DetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup pListenerHomeGrou pListenerHomeGroup ListenerÉnumérateur de bus IP PnP-XIPBusEnum QWAVEPnP-X IP Bus EnumeratorExpérienceaudio-vidéo haute vcQWAVEQuality Windows Audio VideoExpérience d'applicationAeLookupS vcApplication ExperienceExpérience des utilisateursBrowserComputer BrowserExpérience des utilisateursDiagTrackDiagnostics Tracking ServiceFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantané de logiciel MicrosoftswprvMicrosoft Software Shadow Copy Provider	Coordinateur de transactions distribuées	MSDTC	Distributed Transaction Coordinator
Découverte SSDPSSDPSRVSSDP DiscoveryDéfragmenteur de disquedefragsvcDisk DefragmenterDétection de services interactifsUI0DetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroupHomeGrou pListenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnum QWAVEPnP-X IP Bus EnumeratorExpérience audio-vidéo ualité WindowsAeLookupS vcApplication ExperienceExpérience d'applicationAeLookupS utilisateurs DiagTrackDiagnostics Tracking ServiceFournisseur de cliché instantané de logiciel MicrosoftStory WirvMicrosoft Software Shadow Copy Provider	Déclencheurs Message Queuing	MSMQTrigg ers	Message Queuing Triggers
Défragmenteur de disquedefragsvcDisk DefragmenterDétection de services interactifsUI0DetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroup pListenerHomeGroup pListenerHomeGroup ListenerÉmumérateur de bus IP PnP-XIPBusEnum 	Découverte SSDP	SSDPSRV	SSDP Discovery
Détection de services interactifsUI0DetectInteractive Services DetectionDétection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroupHomeGrou pListenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérienceaudio-vidéo haute qualité WindowsQWAVEQuality Windows Audio ExperienceExpérience d'applicationAeLookupS vcApplication ExperienceExpérience des connectés et télémétrieDiagTrack ServiceDiagnostics Tracking ServiceFournisseur de cliché de logiciel MicrosoftSwprvMicrosoft Software Shadow Copy Provider	Défragmenteur de disque	defragsvc	Disk Defragmenter
Détection matériel noyauShellHWDet ectionShell Hardware DetectionDisque virtuelvdsVirtual DiskÉcouteur HomeGroupHomeGrou pListenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérienceaudio-vidéo haute qualité WindowsQWAVE ReperienceQuality WindowsVideo ExpérienceExpérience d'applicationAeLookupS vcApplication ExperienceApplication ExperienceExpérience des connectés et télémétrieDiagTrack ServiceDiagnostics Tracking ServiceFournisseur de cliché instantané de logiciel MicrosoftSwprvMicrosoft Software Shadow Copy Provider	Détection de services interactifs	UI0Detect	Interactive Services Detection
Disque virtuelvdsVirtual DiskÉcouteur HomeGroupHomeGrou pListenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnum QWAVEPnP-X IP Bus EnumeratorExpérience qualité WindowsQWAVE VcQuality Windows ExperienceExpérience d'application connectés et télémétrieAeLookupS DiagTrackApplication ExperienceExpérience de logiciel MicrosoftUtilisateurs instantané swprvDiagnostics Tracking Service Microsoft Software Shadow Copy Provider	Détection matériel noyau	ShellHWDet ection	Shell Hardware Detection
Écouteur HomeGroupHomeGrou pListenerHomeGroup ListenerEmplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérience audio-vidéo haute qualité WindowsQWAVEQuality Windows Audio 	Disque virtuel	vds	Virtual Disk
Emplacement protégéProtectedS torageProtected StorageÉnumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérience audio-vidéo haute qualité WindowsQWAVEQuality Windows Audio Video ExperienceExpérience d'applicationAeLookupS vcApplication ExperienceExpérience des utilisateurs connectés et télémétrieBrowserComputer BrowserExpérience des utilisateurs connectés et télémétrieDiagTrackDiagnostics Tracking ServiceFournisseur de cliché instantané de logiciel MicrosoftSwprvMicrosoft Software Shadow Copy Provider	Écouteur HomeGroup	HomeGrou	HomeGroup Listener
Emplacement protegeProtecteds torageProtecteds torageÉnumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérienceaudio-vidéo haute qualité WindowsQWAVEQuality WindowsAudio Video ExperienceExpérience d'applicationAeLookupS vcApplication ExperienceExpériencedes utilisateurs connectés et télémétrieBrowserComputer BrowserFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantané de logiciel MicrosoftswprvMicrosoftSoftware Shadow Copy Provider	Emplocoment protégé	pListener	
Énumérateur de bus IP PnP-XIPBusEnumPnP-X IP Bus EnumeratorExpérienceaudio-vidéohauteQWAVEQualityWindowsAudioVideoqualité WindowsAudioAudioVideoExperienceAudioVideoExpérience d'applicationAeLookupSApplication ExperienceExpérienceBrowserComputer BrowserExpériencedes utilisateursDiagTrackDiagnostics Tracking ServiceFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantanéswprvMicrosoftSoftwareAugustical MicrosoftSwprvMicrosoftSoftwareKenderSoftwareSoftwareShadowCopyProviderSoftwareShadowCopy		torage	Protected Storage
Expérience qualité Windowsaudio haute qualité WindowsAudio Video ExperienceExpérience d'applicationAeLookupS vcApplication ExperienceExplorateur d'ordinateursBrowserComputer BrowserExpérience connectés et télémétrieDiagTrackDiagnostics Tracking ServiceFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantané de logiciel MicrosoftswprvMicrosoft Software Shadow Copy Provider	Énumérateur de bus IP PnP-X	IPBusEnum	PnP-X IP Bus Enumerator
Expérience d'application AeLookupS Application Experience vc Provider Provider Explorateur d'ordinateurs Browser Computer Browser Expérience des utilisateurs connectés et télémétrie DiagTrack Diagnostics Tracking Service Fichiers hors connexion CscService Offline Files Fournisseur de cliché instantané de logiciel Microsoft swprv Microsoft Software Shadow Copy Provider	Expérience audio-vidéo haute qualité Windows	QWAVE	Quality Windows Audio Video Experience
Explorateur d'ordinateursBrowserComputer BrowserExpériencedesutilisateursDiagTrackDiagnostics Tracking ServiceConnectés et télémétrieDiagTrackCscServiceOffline FilesFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantanéswprvMicrosoftSoftwareAle logiciel MicrosoftswprvProvider	Expérience d'application	AeLookupS vc	Application Experience
ExpériencedesutilisateursDiagTrackDiagnostics Tracking Serviceconnectés et télémétrieDiagTrackDiagnostics Tracking ServiceFichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantanéswprvMicrosoftSoftwarede logiciel MicrosoftSwprvProvider	Explorateur d'ordinateurs	Browser	Computer Browser
Fichiers hors connexionCscServiceOffline FilesFournisseur de cliché instantané de logiciel MicrosoftswprvMicrosoftSoftwareShadowCopyProvider	Expérience des utilisateurs connectés et télémétrie	DiagTrack	Diagnostics Tracking Service
Fournisseur de cliché instantanéswprvMicrosoftSoftwareShadowCopyde logiciel MicrosoftProvider	Fichiers hors connexion	CscService	Offline Files
	Fournisseur de cliché instantané de logiciel Microsoft	swprv	Microsoft Software Shadow Copy Provider
Fournisseur HomeGroup HomeGrou HomeGroup Provider pProvider Provider Provider	Fournisseur HomeGroup	HomeGrou pProvider	HomeGroup Provider
GénérateurdepointsdeAudioEndpWindows Audio Endpoint BuilderterminaisonduserviceAudioointBuilderWindows Audio Endpoint BuilderWindows	Générateur de points de terminaison du service Audio Windows	AudioEndp ointBuilder	Windows Audio Endpoint Builder
Gestion à distance de WindowsWinRMWindows Remote Management (WS-(Gestion WSM)Management)	Gestion à distance de Windows (Gestion WSM)	WinRM	Windows Remote Management (WS- Management)
Gestion d'applications AppMgmt Application Management	Gestion d'applications	AppMgmt	Application Management
Gestion des clés et des certificats hkmsvc Health Key and Certificate d'intégrité	Gestion des clés et des certificats d'intégrité	hkmsvc	Health Key and Certificate



		Management
Gestionnaire d'identité réseau homologue	p2pimsvc	Peer Networking Identity Manager
Gestionnaire d'informations d'identification	VaultSvc	Credential Manager
Gestionnaire de comptes de sécurité	SamSs	Security Accounts Manager
Gestionnaire de connexion automatique d'accès distant	RasAuto	Remote Access Auto Connection Manager
Gestionnaire de connexions d'accès distant	RasMan	Remote Access Connection Manager
Gestionnaire de sessions du Gestionnaire de fenêtrage	UxSms	Desktop Window Manager Session Manager
Groupement de mise en réseau de pairs	p2psvc	Peer Networking Grouping
Hôte de périphérique UPnP	upnphost	UPnP Device Host
Hôte du fournisseur de découverte de fonctions	fdPHost	Function Discovery Provider Host
Hôte système de diagnostics	WdiSystem Host	Diagnostic System Host
Identité de l'application	AppIDSvc	Application Identity
Informations d'application	Appinfo	Application Information
Infrastructure de gestion Windows	Winmgmt	Windows Management Instrumentation
Interruption SNMP	SNMPTRAP	SNMP Trap
Isolation de clé CNG	Keylso	CNG Key Isolation
Journal d'événements Windows	EventLog	Windows Event Log
Journaux & alertes de performance	pla	Performance Logs & amp; Alerts
Lanceur de processus serveur DCOM	DcomLaun ch	DCOM Server Process Launcher
Localisateur d'appels de procédure distante (RPC)	RpcLocato r	Remote Procedure Call (RPC) Locator
Mappage de découverte de topologie de la couche de liaison	lltdsvc	Link-Layer Topology Discovery Mapper
Mappeur de point de terminaison RPC	RpcEptMa	RPC Endpoint Mapper
Message Queuing	MSMQ	Message Queuing
Microsoft .NET Framework NGEN v2.0.x	clr_optimiz ation_v2.0. 50727	Microsoft .NET Framework NGEN v2.0.50727
Modules de génération de clés IKE et AuthIP	IKEEXT	IKE and AuthIP IPsec Keying Modules
Moteur de filtrage de base	BFE	Base Filtering Engine
Netlogon	Netlogon	Netlogon
Ouverture de session secondaire	seclogon	Secondary Logon
Pare-feu Windows	MpsSvc	Windows Firewall
Parental Controls	WPCSvc	Parental Controls
Partage de connexion Internet (ICS)	SharedAcc ess	Internet Connection Sharing (ICS)
Planificateur de classes multimédias	MMCSS	Multimedia Class Scheduler
Planificateur de tâches	Schedule	Task Scheduler



Plug-and-Play	PlugPlay	Plug and Play
Prise en charge de l'application Rapports et solutions aux problèmes du Panneau de configuration	wercplsup port	Problem Reports and Solutions Control Panel Support
Programme d'installation ActiveX (AxInstSV)	AxInstSV	ActiveX Installer (AxInstSV)
Programme d'installation pour les modules Windows	TrustedInsta ller	Windows Modules Installer
Propagation du certificat	CertPropSv c	Certificate Propagation
Protection logicielle	sppsvc	Software Protection
Protocole EAP (Extensible Authentication Protocol)	EapHost	Extensible Authentication Protocol
Protocole PNRP	PNRPsvc	Peer Name Resolution Protocol
Publication des ressources de découverte de fonctions	FDResPub	Function Discovery Resource Publication
Redirecteur de port du mode utilisateur des services Bureau à distance	UmRdpServ ice	Remote Desktop Services UserMode Port Redirector
Registre à distance	RemoteRe gistry	Remote Registry
RIP Listener	iprip	RIP Listener
Routage et accès distant	RemoteAc cess	Routing and Remote Access
Sauvegarde Windows	SDRSVC	Windows Backup
SeaPort	SeaPort	SeaPort
Serveur	LanmanSer ver	Server
Serveur de priorités des threads	THREADOR DER	Thread Ordering Server
Service d'activation des processus Windows	WAS	Windows Process Activation Service
Service d'administration IIS	IISADMIN	IIS Admin Service
Service de biométrie Windows	WbioSrvc	Windows Biometric Service
Service de cache de police Windows	FontCache	Windows Font Cache Service
Service de chiffrement de lecteur BitLocker	BDESVC	BitLocker Drive Encryption Service
Service de configuration automatique WLAN	Wlansvc	WLAN AutoConfig
Service de configuration automatique WWAN	WwanSvc	WWAN AutoConfig
Service de découverte automatique de Proxy Web pour les services HTTP Windows	WinHttpAut oProxySvc	WinHTTP Web Proxy Auto-Discovery Service
Service de gestion Web	WMSVC	Web Management Service
Service de l'Assistant Compatibilité des programmes	PcaSvc	Program Compatibility Assistant Service
Service de la passerelle de la couche Application	ALG	Application Layer Gateway Service
Service de moteur de sauvegarde en mode bloc	wbengine	Block Level Backup Engine Service



Service de notification	SENS	System Event Notification Service
Service de notification SPP	sppuinotify	SPP Notification Service
Service de partage de ports	NetTcnPort	Net Ico Port Sharing Service
Net.Tcp	Sharina	Nettrep Fort sharing service
Service de planification Windows	ehSched	Windows Media Center Scheduler
Media Center		Service
Service de prise en charge	bthserv	Bluetooth Support Service
Bluetooth	D	
Service de profil utilisateur	ProfSvc	User Profile Service
d'ordinateurs PNRP	PNRPAUTOR	PNRP Machine Name Publication
Service de publication World Wide		Service World Wide Web Publishing Service
Web	**55*C	wond wide web i ublishing service
Service de rapport d'erreurs	WerSvc	Windows Error Reporting Service
Windows		
Service de réception Windows	ehRecvr	Windows Media Center Receiver
Service de stockage	StorSuc	Service
Service de stockaye	310137C	Siologe Service
Service de strategie de diagnostic	DPS	Diagnostic Policy Service
arrière-plan	BI12	Service
Service d'état ASP.NET	aspnet_stat	ASP.NET State Service
	е	
Service d'indexation	CISVC	Indexing Service
Service Énumérateur d'appareil	WPDBusEnu	Portable Device Enumerator Service
Mobile Service ETD Microsoft	m the court	
Service FTP Microsoft	TTPSVC	MICROSOTT FIP Service
Service note wDIServiceHost	Waiservice	Diagnostic Service Host
Service Initiateur iSCSI de	MSISCSI	Microsoft iSCSL Initiator Service
Microsoft	101010001	
Service Interface du magasin	nsi	Network Store Interface Service
réseau Service Kamping neur Distributed		
Transaction Coordinator	KIMRM	KIMRM for Distributed Iransaction
Service Liste des réseaux	netorofm	Network List Service
Service I PD		
Service Media Center Extender	Mcx2Svc	Media Center Extender Service
Service Panneau de saisie Tablet	TabletInput	Tablet PC Input Service
PC	Service	
Service Partage réseau du Lecteur	WMPNetw	Windows Media Player Network
Windows Media	orkSvc	Sharing Service
Service SNMP	SNMP	SNMP Service
Service SSTP (Secure Socket	SstpSvc	Secure Socket Tunneling Protocol
Tunneling Protocol)		Service
Service Windows Live Contrôle parental	tsssvc	Windows Live Family Safety
Services Bureau à distance	TermServic	Remote Desktop Services
	е	
Services de base de module de	TBS	TPM Base Services
plateforme sécurisée		



Services de chiffrement	CryptSvc	Cryptographic Services
Services TCP/IP simples	simptcp	Simple TCP/IP Services
Spouleur d'impression	Spooler	Print Spooler
Station de travail	LanmanWo rkstation	Workstation
Stratégie de retrait de la carte à puce	SCPolicySv c	Smart Card Removal Policy
Superfetch	SysMain	Superfetch
Système d'événement COM+	EventSyste m	COM+ Event System
Système de couleurs Windows	WcsPlugInS ervice	Windows Color System
Système de fichiers EFS (Encrypting File System)	EFS	Encrypting File System (EFS)
Télécopie	Fax	Fax
Téléphonie	TapiSrv	Telephony
Telnet	TIntS∨r	Telnet
Temps Windows	W32Time	Windows Time
Thèmes	Themes	Themes
WebClient	WebClient	WebClient
Windows CardSpace	idsvc	Windows CardSpace
Windows Connect Now - Registre de configuration	wcncsvc	Windows Connect Now - Config Registrar
Windows Defender	WinDefend	Windows Defender
Windows Driver Foundation - Infrastructure de pilote mode- utilisateur	wudfsvc	Windows Driver Foundation - User- mode Driver Framework
Windows Installer	msiserver	Windows Installer
Windows Search	WSearch	Windows Search
Windows Update	wuauserv	Windows Update

