Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 31 janvier 2017

N° DAT-NT-36/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 19

Note technique

Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10

Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les « **Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10** ». Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
SDE, COSSI	SDE	SDE	31 janvier 2017

Évolutions du document :

Version	Date	Nature des modifications
1.0	20 janvier 2017	Première version publiée
1.1	31 janvier 2017	Correction de liens morts

Pour toute question :

Contact	Adresse	@mél
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	conseil.technique@ssi.gouv.fr

Table des matières

1 Introduction

Les préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10 font l'objet de nombreux articles depuis sa sortie. Beaucoup sont alarmistes et font germer l'idée que Microsoft dispose d'un accès élargi aux données et en collecte un certain nombre à l'insu de l'utilisateur, ce qui engendre de nombreuses critiques.

À la date d'écriture de cette note et selon les informations rendues publiques par Microsoft, des données sont collectées (et corrélées entre elles) sous Windows 10 par plusieurs biais :

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

Les données recueillies par Microsoft peuvent être stockées et traitées aux États-Unis ou dans tout autre pays dans lequel Microsoft, ses filiales ou prestataires de service sont implantés.

Bien entendu, il est du ressort de chaque entité d'apprécier son propre besoin en matière de confidentialité des données, idéalement par une analyse de risques (menée par exemple avec la méthode [EBIOS]) dont les conclusions doivent permettre de prendre une décision au plus haut niveau.

R1 - Adapter les recommandations de ce document

> Les recommandations du présent document sont à adapter afin d'obtenir un compromis entre les besoins métier à couvrir et les besoins en confidentialité des données. Lorsque certains mécanismes apportent un gain de productivité notable sur un périmètre restreint de postes de travail (comme par exemple l'agent personnel Cortana pour des équipes commerciales), il est dans ce cas pertinent de leur appliquer des politiques de sécurité spécifiques plutôt que d'abaisser le niveau de sécurité de la politique globale.

Windows 10 est par ailleurs amené à fortement évoluer au fur et à mesure des mises à jour du système, apportant leur lot de nouvelles fonctionnalités et de nouveaux paramétrages à effectuer. Contrairement à ses prédécesseurs qui faisaient l'objet de mises à jour majeures via des *Service Packs* facilement identifiables, Windows 10 évolue via des mises à jour mineures et majeures au fil de l'eau. Le niveau de version de Windows 10 n'est donc plus représenté par un Service Pack mais par un numéro de version ou son nom de code associé. L'historique des versions publiques à ce jour est :

- la version 1507 datée du 29 juillet 2015 (nom de code *Threshold 1*) ;
- la version 1511 datée du 12 novembre 2015 (nom de code *Threshold 2*) ;
- la version anniversaire 1607 datée du 2 août 2016 (nom de code *Redstone 1*).

Le présent document se base sur la version 1607 de Windows 10 (nom de code *Redstone 1*) et guide dans la mise en œuvre de mesures de sécurité dans un environnement *Active Directory*.

Enfin, pour un même sujet, plusieurs recommandations peuvent être proposées dans le document. Ces solutions se distinguent par leur niveau de sécurité. Elles doivent permettre au lecteur de retenir les recommandations offrant la meilleure protection au regard du contexte et des étapes nécessaires à leur mise en œuvre. Ainsi, les recommandations seront présentées de la manière suivante :

Rx	La recommandation offre un niveau de protection optimal.
Rx ⊖	Cette mesure propose un premier niveau dérogatoire à la recommandation précédente. Le niveau de protection atteint est plus faible.
Rx ⊖⊖	Cette dernière dérogation implique un niveau de sécurité plus faible que Rx ⊖. Le niveau de confiance est donc plus faible.

TABLE 1 – Priorisation des recommandations

2 Service de télémétrie

Le service de télémétrie du système est configurable de manière centralisée par stratégie de groupe (GPO ou *Group Policy Object*, voir page Technet [MSGPO]) via l'option « données de diagnostic et d'utilisation » et selon quatre niveaux ici listés par ordre croissant de quantité de données collectées :

- sécurité (option non disponible graphiquement, configurable dans la base de registre ou par GPO et uniquement sur les éditions « Entreprise », « Éducation » et « IoT Core » [1] de Windows 10) ;
- de base ;
- amélioré ;
- complet.

Les différents niveaux de collecte sont largement détaillés par Microsoft sur la page Technet [MSDTCK]. Il est important de retenir :

- qu'aux niveaux de collecte « amélioré » et « complet », des données sensibles et personnelles sont inévitablement collectées par Microsoft ;
- qu'aucun niveau ne permet de complètement bloquer l'envoi d'informations ;
- que ces niveaux de collecte ne concernent que le service de télémétrie du système d'exploitation lui-même. Les autres logiciels tels Microsoft Office ou ceux d'autres éditeurs ne tiennent pas compte de ce paramétrage, ils disposent généralement de leurs propres paramètres de télémétrie.

Au niveau « de base » de collecte de données, un poste de travail cherchera au minimum à transmettre :

- les informations du système d'exploitation et l'identifiant de l'appareil ;
- les données de configuration matérielle (type d'appareil, fabricant, modèle, nombre de processeurs, taille et résolution d'écran, date, paramètres régionaux et linguistiques, etc.) ;
- les logiciels, pilotes et micrologiciels installés ;
- les données de performance et de fiabilité (processus exécutés, durée d'exécution, rapidité de réponse aux entrées, nombre d'erreurs rencontrées, vitesses de transmission, etc.) ;
- la configuration réseau (adresses IP, nombre de connexions réseau, caractéristiques des réseaux auxquels le système se connecte, etc.).

1. Édition de Windows 10 pour les objets connectés et terminaux légers.

Ce niveau « de base » peut être jugé suffisamment intrusif pour être inacceptable en environnement professionnel. Dans ce cas, le niveau « sécurité » devrait être privilégié. Les données collectées et transmises peuvent ainsi être limitées au strict minimum :

- les informations du système d'exploitation (version, architecture, etc.) ;
- l'identifiant de l'appareil ;
- le type d'appareil (exemple : ordinateur de bureau).

Enfin, il reste possible de passer outre ce paramétrage en désactivant le service de télémétrie au niveau du système.

R2 - Désactiver le service de télémétrie

Il est recommandé de désactiver le service de télémétrie par une stratégie de groupe, de manière à ce qu'aucune information ne soit transmise à Microsoft par ce biais.

La désactivation du service de télémétrie n'est pas supportée officiellement par Microsoft, bien qu'aucun effet de bord ne soit connu à ce jour.

R2 ⊖ - Configurer la télémétrie au niveau « **sécurité** »

Il est recommandé de limiter les données transmises à Microsoft via le service de collecte de données de télémétrie, et ainsi éviter la fuite d'informations sensibles ou personnelles. À défaut de désactiver le service de télémétrie, il est donc recommandé de configurer le niveau de collecte du service de télémétrie au niveau « sécurité ».

R2 ⊖⊖ - Configurer la télémétrie au niveau « **de base** »

À défaut d'avoir déployé Windows 10 en édition Entreprise, Éducation ou *IoT Core*, le niveau « de base » de collecte du service de télémétrie est recommandé.

Les adresses IP et enregistrements DNS des serveurs de collecte de Microsoft sont sujets à modification sans information préalable. Il n'est donc pas recommandé de chercher à bloquer les flux réseau de télémétrie en sortie (via le pare-feu Windows ou les pare-feux de défense périmétrique) à moins que cette mesure de sécurité vienne en complément des précédentes et dans un objectif de défense en profondeur.

R3 - Désactiver l'envoi de rapports par MSRT et Windows Defender

Pour limiter la collecte au strict minimum, il est également nécessaire de désactiver l'envoi de rapports par l'outil de suppression de logiciels malveillants (MSRT) et par l'antivirus *Windows Defender* (également appelé *EndPoint Protection*) qui sont transmis via le service de télémétrie du système.

L'application de ces recommandations se traduit par la mise en œuvre d'une GPO telle qu'illustrée dans l'annexe I.

3 Assistant personnel Cortana et composant *Desktop Search*

L'assistant personnel Cortana est un agent logiciel qui aide l'utilisateur à accomplir ses tâches. Cortana peut par exemple :

- envoyer des courriels ou des messages ;
- faire des recherches sur Internet ;
- exécuter des applications ;
- transmettre des rappels en fonction de l'heure, des rendez-vous et de la géolocalisation de l'utilisateur.

L'agent Cortana est utilisable par reconnaissance vocale ou via l'utilisation du champ de recherche intégré à la barre de tâches Windows (le composant *Windows Desktop Search*), ces deux composants sont donc liés.

Pour être efficace, l'agent Cortana doit accéder aux informations personnelles de l'utilisateur, utiliser les données de l'appareil, des services en ligne, etc. L'utilisation de Cortana pose donc beaucoup de problèmes concernant la divulgation d'informations sensibles ou personnelles. En environnement professionnel, il est recommandé de désactiver Cortana.

R4 - Désactiver l'agent personnel Cortana

> Pour éviter la divulgation d'informations sensibles ou personnelles en environnement professionnel, il est recommandé de désactiver l'agent personnel Cortana.

R5 - Restreindre l'utilisation de *Windows Desktop Search*

> Pour éviter la divulgation d'informations sensibles ou personnelles en environnement professionnel, il est recommandé de restreindre l'utilisation du composant *Windows Desktop Search* à de la recherche locale sur l'appareil. L'utilisation d'un navigateur maîtrisé reste à privilégier pour les recherches sur Internet.

Les problématiques de maîtrise des navigateurs Internet Explorer, Google Chrome et Mozilla Firefox sur les postes de travail sont abordées dans les notes [IE], [CHROME] et [MOZFF] de l'ANSSI.

L'application de ces recommandations se traduit par la mise en œuvre d'une GPO telle qu'illustrée dans l'annexe II.

4 Les paramètres de personnalisation de l'expérience utilisateur

Un certain nombre de données sont par défaut envoyées aux services de Microsoft à des fins de personnalisation et d'amélioration de l'expérience utilisateur. Cela peut présenter un intérêt pour un usage personnel de l'équipement informatique, mais n'est généralement pas souhaitable en environnement professionnel pour des questions de confidentialité. Ces données peuvent comprendre par exemple :

- des données de saisies clavier ou manuscrites ;
- des coordonnées et informations de calendriers ;
- les carnets d'adresses et de contacts.

R6 - Durcir les paramètres de personnalisation de l'expérience utilisateur

Il est recommandé de désactiver :
– la personnalisation des saisies clavier, vocales et manuscrites ;
– l'envoi de rapports d'erreurs et de diagnostic à Microsoft ;
– le programme d'amélioration de l'expérience utilisateur.

R7 - Désactiver la géolocalisation

Il est possible de désactiver la géolocalisation au niveau du système (voire de désactiver le service Windows « lfsvc »), de sorte que ni Windows ni les applications ne soient en mesure de récupérer la position géographique de l'équipement. Si cette fonctionnalité n'est nécessaire à aucune des applications utilisées dans le contexte professionnel, voire si elle est jugée indésirable, sa désactivation au niveau système est dans ce cas recommandée.

En cas d'utilisation des navigateurs Internet Explorer ou Edge, des données telles que les sites Web visités ou les fichiers téléchargés peuvent être transmises à Microsoft. Pour des raisons de confidentialité, il peut être intéressant de :
– désactiver les filtres *SmartScreen* dès lors que l'entité met en œuvre des fonctions de sécurité anti-maliciel et anti-hameçonnage sur ses propres serveurs mandataires ;
– désactiver la fonction *d'avance rapide avec prédiction de page*.
La mise en œuvre de ces recommandations est détaillée dans la note technique [IE] de l'ANSSI.

L'application de ces recommandations se traduit par la mise en œuvre d'une GPO telle qu'illustrée dans l'annexe III.

5 Applications universelles

Cette étape consiste à créer les règles permettant aux utilisateurs d'exécuter les applications universelles (également appelées *Packaged Apps*, applications empaquetées, *Windows Apps*, *Metro style apps*, applications immersives ou bien encore *Modern Apps*) autorisées dans une organisation. Il est en premier lieu important de distinguer les applications universelles sous windows 10, les applications universelles sous windows 8 et les applications de bureau classiques.

De manière synthétique, les applications universelles Windows 10 sont développées pour la plateforme *Universal Windows Platform (UWP)* tandis que les applications universelles Windows 8 utilisent spécifiquement l'interface de programmation WinRT (*Windows Runtime*). Ces deux types d'applications portent le même nom mais sont pourtant bien différentes, une application universelle Windows 8 ne s'exécutera pas sur Windows 10 et inversement. En revanche, la plateforme UWP est fortement inspirée de son prédécesseur, ce qui facilite le portage des applications universelles Windows 8 vers Windows 10.

Les applications universelles, empaquetées en un seul et unique fichier au format `.AppX`, sont généralement moins complexes que les applications de bureau classiques. De par leur cadre d'exécution

contrôlée, elles présentent moins de risques de sécurité pour le système que les applications de bureau classiques. Les applications universelles peuvent d'ailleurs être installées avec un simple compte utilisateur non privilégié et sont publiables et téléchargeables via un magasin d'applications (*Windows Store* ou magasin privé déployé en interne). Enfin, elles sont utilisables sur une large gamme d'équipements (tablettes, ordiphones, ordinateurs, etc.).

Plusieurs dizaines d'applications universelles sont pré-installées sous Windows 10 (actualités, météo, cartes, finances, Skype, etc.). Ces applications peuvent accéder à des ressources potentiellement sensibles du système, comme la géolocalisation, les carnets d'adresse ou les calendriers et utilisent des services en ligne auxquels ces informations sont transmises. Les utilisateurs non privilégiés sont par ailleurs en capacité d'en installer d'autres, qui peuvent présenter des risques plus ou moins importants pour la confidentialité.

Il est donc recommandé de contrôler les applications universelles déployées et utilisables sur les postes de travail, au même titre que les applications de bureau classiques. Ce contrôle peut passer par la mise en œuvre de règles de restriction logicielle [APPLOCKER] uniquement pour les éditions « Entreprise » et « Éducation » de Windows 10, ou avec toute autre solution commerciale alternative) spécifiques aux applications universelles, la désinstallation des applications indésirables, le paramétrage des droits d'accès aux magasins d'applications, etc.

Seule la problématique de la confidentialité des données est traitée dans cette section. Les autres problématiques liées aux applications universelles seront abordées dans d'autres documents de sécurisation de Windows 10 en environnement professionnel.

R8

Désactiver l'identifiant unique de publicité, utilisé par les développeurs, éditeurs et réseaux publicitaires pour partager des informations collectées sur l'utilisateur entre applications et donc utilisable pour corréler des informations sur ce dernier.

R9 - Bloquer ou désinstaller les applications universelles

Si l'usage des applications universelles n'est pas nécessaire dans le contexte professionnel, il est dans ce cas préférable de complètement désactiver le magasin d'applications (éditions « Entreprise » et « Éducation » de Windows 10 uniquement depuis la version 1511 de Windows 10). La majeur partie des applications universelles pré-installées peuvent être désinstallées par script, et des règles de stratégies de restriction logicielle peuvent également être mises en œuvre en complément dans une démarche de défense en profondeur.

Des exemples de commandes de désinstallation des applications universelles pré-installées figurent dans l'annexe IV.

R9 ⊖ - Maîtriser les applications universelles et leurs accès

Si des applications universelles sont utilisées en contexte professionnel, il est dans ce cas important :
- de définir une liste précise d'applications autorisées et de bloquer les autres à l'aide de stratégies de restriction logicielle ;
- de restreindre précisément les accès octroyés aux applications universelles autorisées (données de géolocalisation, calendrier, contacts, webcam, microphone, etc.) en applicant le principe de moindre privilège.

L'application de ces recommandations se traduit par la mise en œuvre d'une GPO telle qu'illustrée dans l'annexe IV.

Pour les GPO AppLocker, se référer à la note technique [APPLOCKER] de l'ANSSI.

6 Services dans le nuage (Cloud)

Avec Windows 10, plusieurs services dans le nuage de Microsoft sont intégrés au système de manière à en généraliser l'usage.

L'utilisation de services dans le nuage en environnement professionnel doit faire l'objet d'une stratégie de gouvernance au plus haut niveau, qui intègre entre autres des risques de confidentialité, d'intégrité et de disponibilité des données que l'entité est prête à accepter. Pour aider dans cette démarche, l'ANSSI a publié un guide [INFOGER] sur l'externalisation ainsi qu'un référentiel [CLOUD] d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage . Les recommandations de cette section visent à interdire les services dans le nuage intégrés par défaut au système. Si l'entité décide de recourir à ces services après appréciation des risques que présentent leur utilisation, les recommandations qui suivent peuvent dans ce cas être adaptées voire ignorées.

6.1 Comptes Microsoft d'ouverture de session

Avec Windows 8 sont apparus les comptes Microsoft. Il s'agit d'un service d'authentification unique dans le nuage, utilisé pour accéder à certains services de Microsoft (Office, Skype, OneDrive, etc.) mais également comme compte d'ouverture de session sous Windows. Cela revient donc à déporter l'authentification locale vers une infrastructure de service d'annuaire centralisé dans le nuage (c'est-à-dire un type d'*IaaS* ou *Infrastructure As A Service*). Utiliser ce service permet, par exemple, de synchroniser des paramètres entre différents ordinateurs.

En utilisant ce service, divers paramètres d'ordinateur (historique de navigation, mots de passe Wi-Fi, etc.) sont stockés sur les serveurs de Microsoft ainsi que les secrets d'authentification de l'utilisateur et ses clés de chiffrement BitLocker (voir page Technet [MSBTLK]).

R10 - Ne pas utiliser de compte Microsoft pour l'ouverture de session utilisateur sous Windows 10

Bloquer l'utilisation de comptes Microsoft pour l'ouverture de session utilisateur sous Windows 10.

6.2 OneDrive

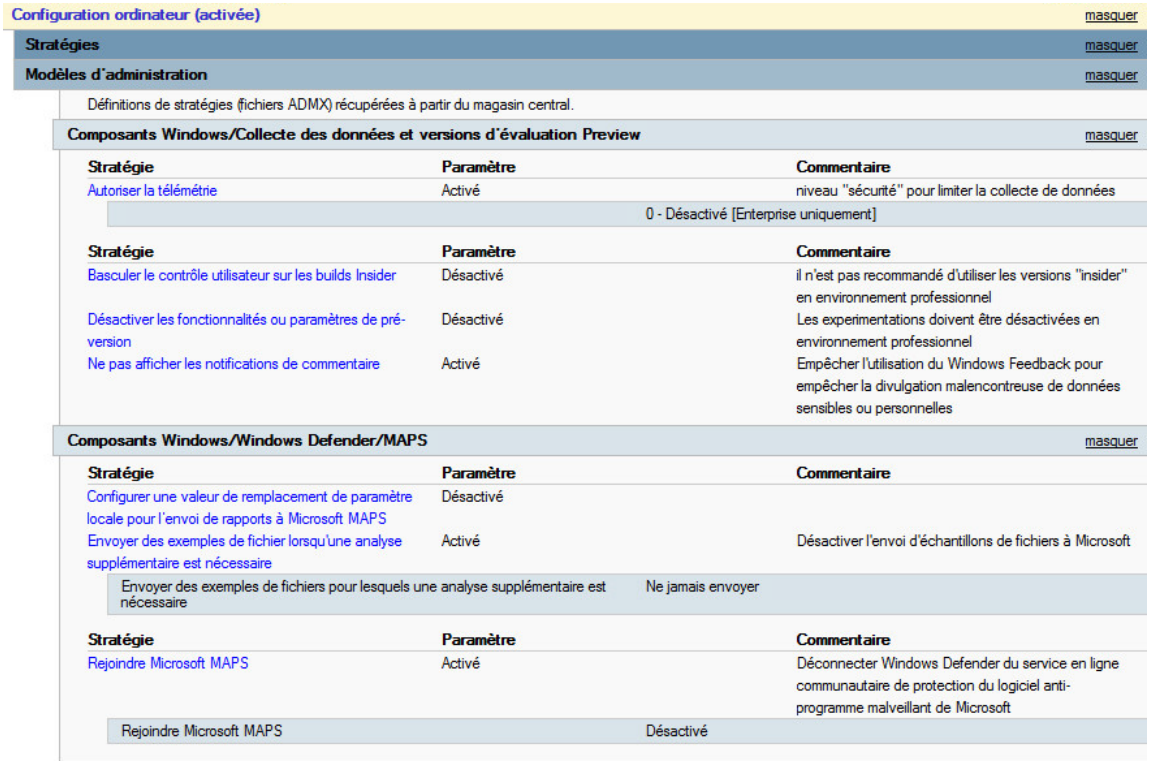
OneDrive est un service de stockage de données dans le nuage (c'est-à-dire du « STaaS » ou *STorage As A Service*). Un espace de stockage limité en volume est disponible gratuitement, et l'application OneDrive intégrée à Windows 10 permet de synchroniser des arborescences locales avec les espaces de stockage en ligne. L'utilisation aisée du service représente une tentation forte pour les utilisateurs d'y stocker des données professionnelles. Par mesure de sécurité pour la confidentialité des données, il est alors préférable de désactiver l'accès au service.

R11 - Désactiver OneDrive

Désactiver le service de stockage dans le nuage OneDrive.

L'application des recommandations concernant les services dans le nuage se traduit par la mise en œuvre d'une GPO telle qu'illustrée dans l'annexe V.

Annexe I : GPO de mise en œuvre des recommandations relatives au service de télémétrie



Configuration ordinateur (activée) — masquer

Stratégies — masquer

Modèles d'administration — masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Composants Windows/Collecte des données et versions d'évaluation Preview — masquer

Stratégie	Paramètre	Commentaire
Autoriser la télémétrie	Activé	niveau "sécurité" pour limiter la collecte de données
	0 - Désactivé [Enterprise uniquement]	

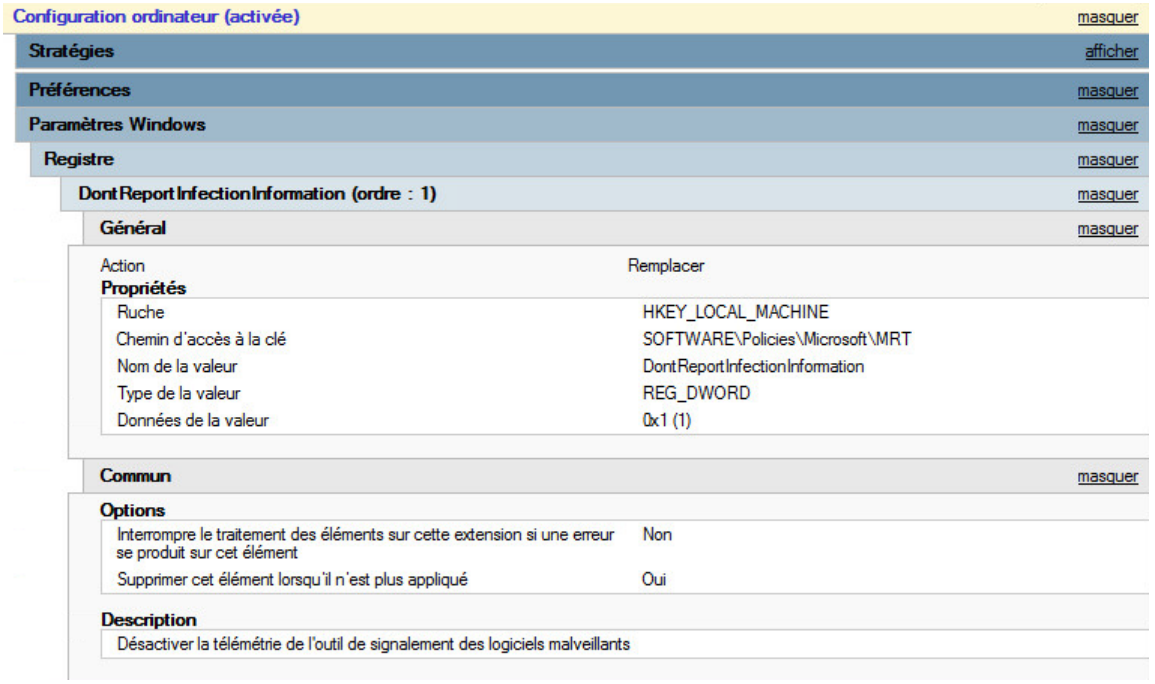
Stratégie	Paramètre	Commentaire
Basculer le contrôle utilisateur sur les builds Insider	Désactivé	il n'est pas recommandé d'utiliser les versions "insider" en environnement professionnel
Désactiver les fonctionnalités ou paramètres de pré-version	Désactivé	Les experimentations doivent être désactivées en environnement professionnel
Ne pas afficher les notifications de commentaire	Activé	Empêcher l'utilisation du Windows Feedback pour empêcher la divulgation malencontreuse de données sensibles ou personnelles

Composants Windows/Windows Defender/MAPS — masquer

Stratégie	Paramètre	Commentaire
Configurer une valeur de remplacement de paramètre locale pour l'envoi de rapports à Microsoft MAPS	Désactivé	
Envoyer des exemples de fichier lorsqu'une analyse supplémentaire est nécessaire	Activé	Désactiver l'envoi d'échantillons de fichiers à Microsoft
Envoyer des exemples de fichiers pour lesquels une analyse supplémentaire est nécessaire	Ne jamais envoyer	

Stratégie	Paramètre	Commentaire
Rejoindre Microsoft MAPS	Activé	Déconnecter Windows Defender du service en ligne communautaire de protection du logiciel anti-programme malveillant de Microsoft
Rejoindre Microsoft MAPS	Désactivé	

FIGURE 1 – GPO de mise en œuvre des recommandations relatives au service de télémétrie



Configuration ordinateur (activée) — masquer

Stratégies — afficher

Préférences — masquer

Paramètres Windows — masquer

Registre — masquer

DontReportInfectionInformation (ordre : 1) — masquer

Général — masquer

Action	Remplacer
Propriétés	
Ruche	HKEY_LOCAL_MACHINE
Chemin d'accès à la clé	SOFTWARE\Policies\Microsoft\MRT
Nom de la valeur	DontReportInfectionInformation
Type de la valeur	REG_DWORD
Données de la valeur	0x1 (1)

Commun — masquer

Options	
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément	Non
Supprimer cet élément lorsqu'il n'est plus appliqué	Oui

Description

Désactiver la télémétrie de l'outil de signalement des logiciels malveillants

FIGURE 2 – GPP de désactivation de la télémétrie de l'outil de signalement des logiciels malveillants

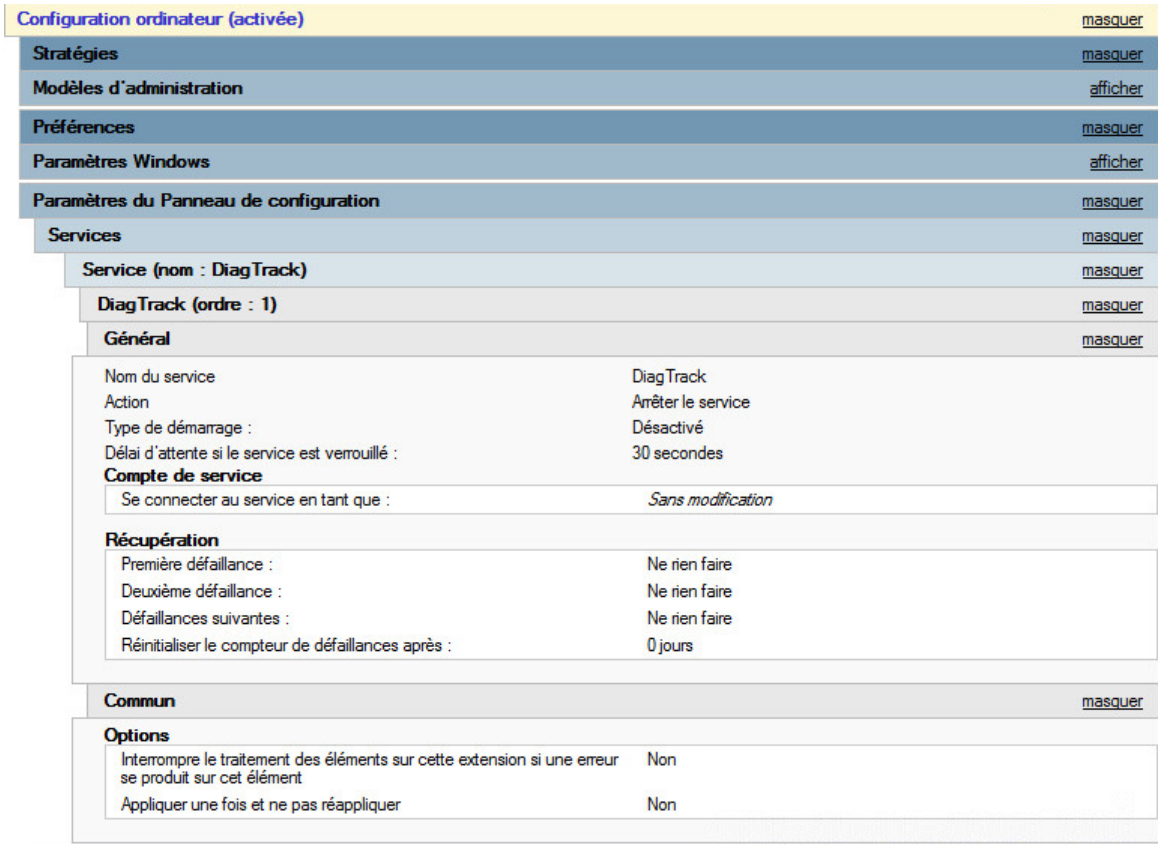
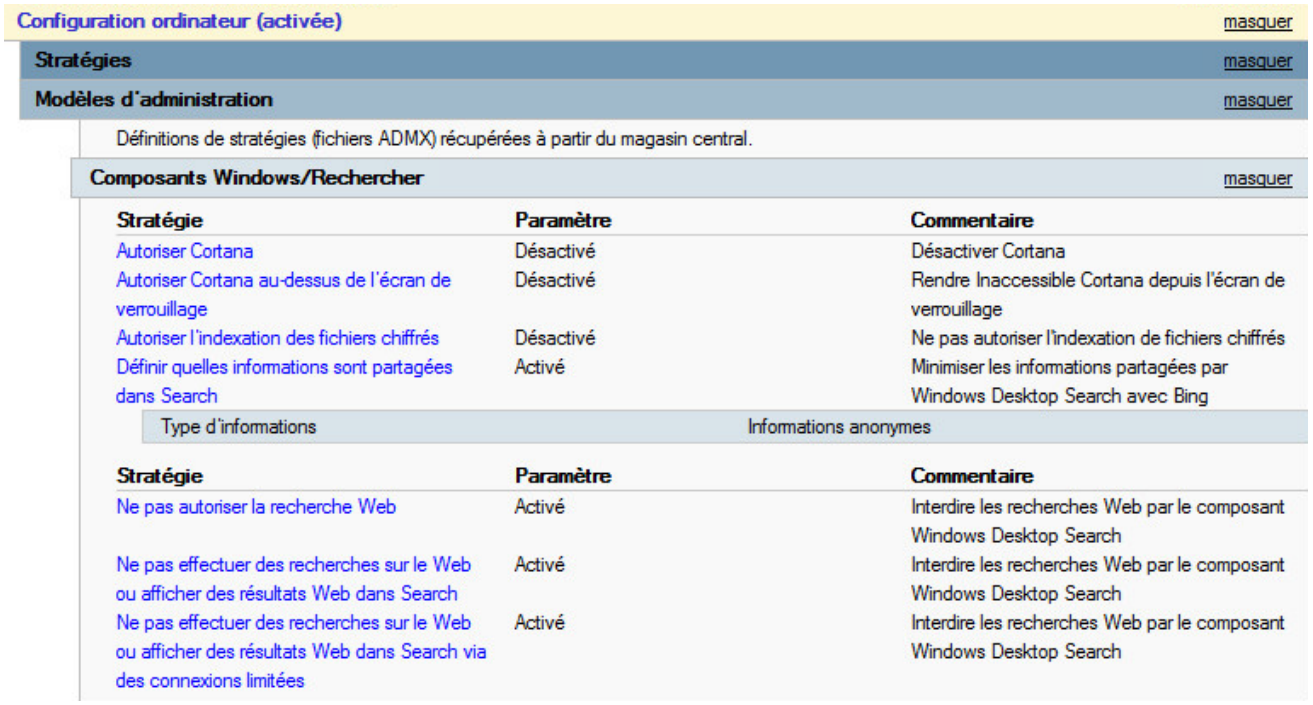


FIGURE 3 – GPP de désactivation du service de télémétrie (*DiagTrack*)

Annexe II : GPO de mise en œuvre des restrictions d'utilisation de Cortana et du composant *Windows Desktop Search*



Configuration ordinateur (activée) — masquer

Stratégies — masquer

Modèles d'administration — masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Composants Windows/Rechercher — masquer

Stratégie	Paramètre	Commentaire
Autoriser Cortana	Désactivé	Désactiver Cortana
Autoriser Cortana au-dessus de l'écran de verrouillage	Désactivé	Rendre Inaccessible Cortana depuis l'écran de verrouillage
Autoriser l'indexation des fichiers chiffrés	Désactivé	Ne pas autoriser l'indexation de fichiers chiffrés
Définir quelles informations sont partagées dans Search	Activé	Minimiser les informations partagées par Windows Desktop Search avec Bing
Type d'informations	Informations anonymes	

Stratégie	Paramètre	Commentaire
Ne pas autoriser la recherche Web	Activé	Interdire les recherches Web par le composant Windows Desktop Search
Ne pas effectuer des recherches sur le Web ou afficher des résultats Web dans Search	Activé	Interdire les recherches Web par le composant Windows Desktop Search
Ne pas effectuer des recherches sur le Web ou afficher des résultats Web dans Search via des connexions limitées	Activé	Interdire les recherches Web par le composant Windows Desktop Search

FIGURE 4 – GPO de mise en œuvre des restrictions d'utilisation de Cortana et du composant *Windows Desktop Search*

Annexe III : GPO de paramétrage des éléments de personnalisation de l'expérience utilisateur

Configuration ordinateur (activée) masquer

Stratégies masquer

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Composants Windows/Emplacement et capteurs masquer

Stratégie	Paramètre	Commentaire
Désactiver l'emplacement	Activé	Si cette fonctionnalité n'est nécessaire à aucune des applications utilisées dans le contexte professionnel, voir si elle est jugée indésirable, sa désactivation peut alors être envisagée.

Composants Windows/Rapport d'erreurs Windows masquer

Stratégie	Paramètre	Commentaire
Désactiver Rapport d'erreurs Windows	Activé	N'envoyer aucune information de rapport d'erreurs à Microsoft
Envoyer automatiquement des images mémoire pour les rapports d'erreurs générés par le système d'exploitation	Désactivé	Ne pas envoyer les dumps mémoire à Microsoft
Ne pas envoyer de données complémentaires	Activé	Ne pas envoyer de données complémentaires à Microsoft

Panneau de configuration/Options régionales et linguistiques masquer

Stratégie	Paramètre	Commentaire
Autoriser la personnalisation de la saisie	Désactivé	Ne pas personnaliser la saisie

Panneau de configuration/Options régionales et linguistiques/Personnalisation de l'écriture manuscrite masquer

Stratégie	Paramètre	Commentaire
Désactiver l'apprentissage automatique	Activé	Ne pas personnaliser la saisie manuscrite

Système/Gestion de la communication Internet/Paramètres de communication Internet masquer

Stratégie	Paramètre	Commentaire
Désactiver le contenu « Le saviez-vous ? » du Centre d'aide et de support	Activé	Désactiver la section "Le saviez vous ?" du centre d'aide
Désactiver le partage des données de personnalisation de l'écriture manuscrite	Activé	Ne pas partager les informations de personnalisation de la saisie manuscrite
Désactiver le Programme d'amélioration de l'expérience utilisateur Windows	Activé	Désactiver le programme d'amélioration de l'expérience utilisateur.
Désactiver le signalement d'erreurs de la reconnaissance de l'écriture manuscrite	Activé	Ne pas envoyer les erreurs de reconnaissance de saisie manuscrite
Désactiver Rapport d'erreurs Windows	Activé	Dasactiver le rapport d'erreurs à Microsoft

FIGURE 5 – GPO de paramétrage des éléments de personnalisation de l'expérience utilisateur

Annexe IV : GPO de paramétrage des applications universelles

GPO de paramétrage

Paramètres généraux :

Configuration ordinateur (activée) — masquer

Stratégies — masquer

Modèles d'administration — masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Composants Windows/Confidentialité de l'application — afficher

Composants Windows/Windows Store — masquer

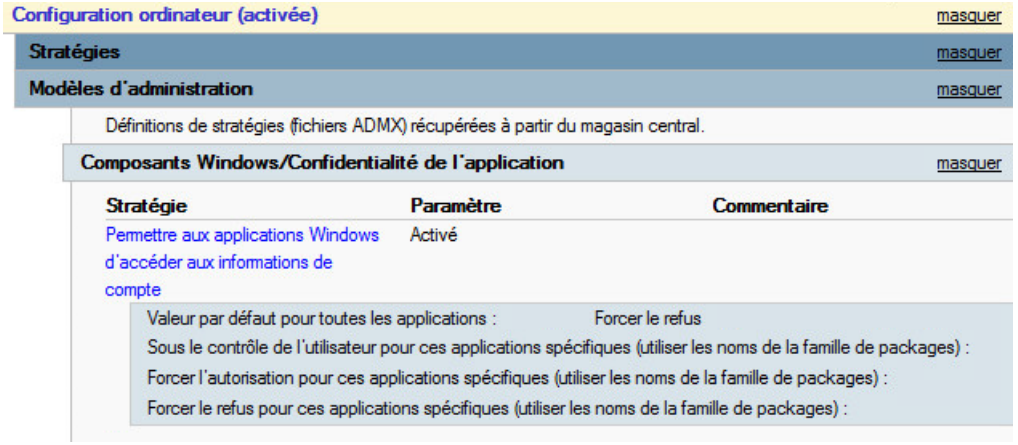
Stratégie	Paramètre	Commentaire
Afficher uniquement le magasin privé dans l'application du Windows Store	Activé	
Désactiver l'application du Windows Store	Activé	Désactiver le magasin d'applications
Désactiver toutes les applications du Windows Store	Activé	Désactiver le magasin d'applications ainsi que les applications du Windows Store pré-installés ou téléchargées.

Système/Profils utilisateur — masquer

Stratégie	Paramètre	Commentaire
Désactiver l'ID de publicité	Activé	Désactiver l'identifiant publicitaire

FIGURE 6 – GPO de paramétrage des applications universelles

Concernant les accès octroyés aux applications universelles autorisées, il faut procéder comme suit pour les quinze types d'accès (informations du compte, contacts, courriel, géolocalisation, etc.). L'action par défaut est de forcer l'interdiction d'accès, puis de créer des exceptions pour des applications autorisées. Dans l'exemple ci-après, aucune exception n'est configurée pour les droits d'accès aux informations du compte :



Configuration ordinateur (activée) — masquer

Stratégies — masquer

Modèles d'administration — masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.

Composants Windows/Confidentialité de l'application — masquer

Stratégie	Paramètre	Commentaire
Permettre aux applications Windows d'accéder aux informations de compte	Activé	

Valeur par défaut pour toutes les applications : Forcer le refus

Sous le contrôle de l'utilisateur pour ces applications spécifiques (utiliser les noms de la famille de packages) :

Forcer l'autorisation pour ces applications spécifiques (utiliser les noms de la famille de packages) :

Forcer le refus pour ces applications spécifiques (utiliser les noms de la famille de packages) :

FIGURE 7 – GPO de paramétrage des applications universelles

Commande PowerShell de désinstallation

La commande PowerShell suivante permet la désinstallation d'une application universelle (l'application fictive « Editeur.Meteo » dans cet exemple) sur le système en cours d'exécution et pour l'utilisateur courrant uniquement. Cette commande est utilisable dans un script d'ouverture de session ou en tâche planifiée par exemple :

```
Get-AppxPackage -AllUsers -Name Editeur.Meteo | Remove-AppxPackage
```

DISM

La commande suivante permet la désinstallation d'une application universelle directement dans l'image Windows (donc pour tous les utilisateurs) sur le système en cours d'exécution via DISM. Elle est utilisable dans un script de démarrage ou en tâche planifiée exécutée avec des privilèges élevés par exemple :

```
DISM.exe /Online /Remove-ProvisionedAppxPackage /Package-Name NomDePackage
```

Dans la ligne de commande ci-dessus, `NomDePackage` est le nom long du package à désinstaller. Il peut, par exemple, être récupéré via la commande suivante qui permet de lister les applications universelles :

```
DISM.exe /Online /Get-ProvisionedAppxPackages
```

La commande suivante permet la désinstallation d'une application universelle dans une image Windows hors ligne :

```
DISM.exe /Image:C:\DISM\offline /Remove-ProvisionedAppxPackage /Package-Name
NomDePackage
```

Dans la ligne de commande ci-dessus, `C:\DISM\offline` est le dossier de montage d'une image Windows au format `.vim` prélablement montée par DISM. Le nom long du package à désinstaller est récupéré par exemple via la commande suivante qui permet de lister les applications universelles présentes dans l'image montée par DISM :

```
DISM.exe /Image:C:\DISM\offline /Get-ProvisionedAppxPackages
```

Annexe V : GPO de paramétrage des éléments relatifs aux services dans le nuage

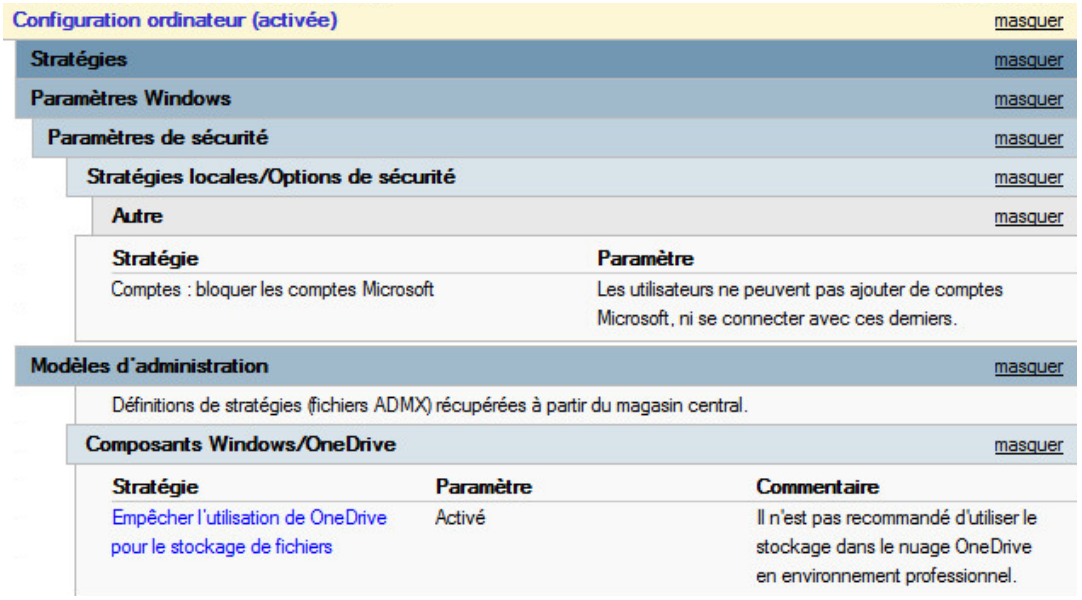


FIGURE 8 – GPO de paramétrage des services dans le nuage

Références

[APPLOCKER] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous windows.*
Note technique DAT-NT-013/ANSSI/SDE/NP, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/windows-restrictions-logicielles.

[CHROME] *Recommandations pour le déploiement sécurisé du navigateur Google Chrome sous Windows.*
Note technique DAT-NT-016/ANSSI/SDE/NP, ANSSI, août 2015.
https://www.ssi.gouv.fr/guide/recommandations-pour-le-deploiement-securise-du-navigateur-google-chrome-sous-windows.

[IE] *Recommandations pour le déploiement sécurisé du navigateur Microsoft Internet Explorer.*
Note technique DAT-NT-018/ANSSI/SDE/NP, ANSSI, août 2014.
https://www.ssi.gouv.fr/guide/recommandations-pour-le-deploiement-securise-du-navigateur-microsoft-internet-explorer.

[MOZFF] *Recommandations pour le déploiement sécurisé du navigateur Mozilla Firefox sous Windows.*
Note technique DAT-NT-020/ANSSI/SDE/NP, ANSSI, février 2015.
https://www.ssi.gouv.fr/guide/recommandations-pour-le-deploiement-securise-du-navigateur-mozilla-firefox-sous-windows.

[EBIOS] *Expression des besoins et identification des objectifs de sécurité.*
Guide Version 1.1, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/ebios/.

[INFOGER] *Externalisation et sécurité des systèmes d'information - Un guide pour maitriser les risques.*
Guide Version 1.0, ANSSI, janvier 2013.
https://www.ssi.gouv.fr/infogerance.

[CLOUD] *Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage – Référentiel d'exigences.*
Referentiel Version 1.3, ANSSI, jul 2014.
https://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestataires-de-services-securises-dinformatique-en-nuage.

[MSBTLK] *Vue d'ensemble du chiffrement de lecteur BitLocker.*
Technet, MICROSOFT, décembre 2016.
https://technet.microsoft.com/fr-fr/library/cc732774(v=ws.11).aspx.

[MSGPO] *Stratégie de groupe pour les débutants.*
Technet, MICROSOFT, avril 2011.
https://technet.microsoft.com/fr-fr/library/hh147307(v=ws.10).aspx.

[MSDTCK] *Configurer la télémétrie Windows dans votre organisation.*

Technet, MICROSOFT, décembre 2016
https://technet.microsoft.com/fr-fr/itpro/windows/manage/configure-windows-telemetry-in-your-organization