# RECOMMANDATIONS DE SÉCURITÉ POUR LA JOURNALISATION DES SYSTÈMES MICROSOFT WINDOWS EN ENVIRONNEMENT ACTIVE DIRECTORY

## GUIDE ANSSI

ANSSI-PB-090
18/07/2022

**PUBLIC VISÉ :**

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

# Informations

## Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [10].

Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles 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.

## Évolutions du document :

| VERSION | DATE | NATURE DES MODIFICATIONS |
|---|---|---|
| 1.0 | 28/01/2022 | Version initiale |
| 1.1 | 18/07/2022 | Changement de politique d'audit du partage de fichiers détaillé |

# Table des matières

# 1
# Introduction

Tout système d'information (SI), qui contribue à la réalisation d'un service ou d'une mission, est exposé à un certain nombre de menaces cyber. Celles-ci traduisent les motivations des différents acteurs souhaitant lui nuire, de quelque manière que ce soit (modification, destruction, compromission, etc.) ou procéder à des actions d'espionnage ou d'intelligence économique. L'interconnexion croissante des réseaux et les besoins de dématérialisation augmentent cette exposition aux cyberattaques de manière substantielle. Les points d'interconnexion avec l'extérieur et en particulier avec Internet sont autant d'accès qu'un attaquant peut tenter d'exploiter pour s'introduire et se maintenir au sein d'un SI.

Qu'il s'agisse d'attaques opportunistes par rançongiciels [3], ou bien d'attaques ciblant des SI spécifiques, la détection et l'analyse des incidents de sécurité sont des activités essentielles qui concourent à la défense des SI face aux menaces de cyberattaques. Elles sont complémentaires aux actions primordiales visant à sécuriser le SI et traitées au travers notamment des analyses de risques, des travaux d'architecture, de configurations adaptées et d'audits de sécurité. La supervision de la sécurité ne peut être la seule mesure de sécurité envisagée pour se prémunir d'une attaque. Les journaux d'évènements étant des sources d'information indispensables à ces activités, leur disponibilité et leur centralisation sont primordiales pour en assurer le séquestre et en permettre l'analyse avec une vue d'ensemble du SI. Cette analyse peut alors être opérée selon différentes temporalités, que ce soit en quasi temps réel pour détecter des attaques en cours, ou bien *a posteriori* pour étudier des scénarios de compromissions passées.

## 1.1 Objectifs du guide

L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) travaille étroitement avec les différentes autorités administratives ainsi que de nombreux acteurs du secteur privé. Certaines de ces missions concernent la détection et l'analyse des incidents de sécurité. L'ANSSI est ainsi amenée à proposer des recommandations de journalisation des SI, avec pour objectif que les différents acteurs puissent les appliquer et ainsi disposer du socle minimum nécessaire au bon déroulement de ces missions.

L'ANSSI a publié le guide [6] qui présente ses recommandations de sécurité pour la mise en œuvre d'un système de journalisation. Ce dernier est volontairement générique en traitant de la mise en œuvre d'un système de journalisation indépendamment des technologies déployées. L'objectif du présent document est quant à lui de décliner ces concepts et ces recommandations génériques, pour des SI reposant sur des technologies Microsoft Windows ; il s'agit donc d'un complément qui ne se substitue pas au guide [6]. Certaines entités sont par exemple soumises à des contraintes règlementaires ou juridiques qui imposent un niveau minimum de journalisation ; ces aspects sont traités dans le guide [6] et non pas dans le présent guide.

Pour finir, ce guide a pour objectif de traiter cette thématique avec un niveau de granularité suffisamment précis, quelle que soit la stratégie de journalisation envisagée. En fonction des besoins de sécurité et des moyens de chaque entité, cette dernière peut consister à simplement disposer d'un socle minimum de journalisation à moindre coût, ou au contraire de procéder à des configurations avancées et adaptées à des menaces de haut niveau. De la même manière, la centralisation des évènements peut être mise en œuvre de manière sommaire ou bien opérée au sein d'un SI de détection des incidents de sécurité. Ce dernier permet alors d'assurer la collecte des journaux, leur stockage temporaire pour analyse et corrélation, puis leur archivage, entre autres. Il peut également faire partie intégrante d'un centre opérationnel de cybersécurité (SOC) [1].

## 1.2 Périmètre du guide

Le référentiel d'exigences des prestataires de détection des incidents de sécurité (PDIS) [7] précise les notions de conception d'un service de détection et d'analyse des incidents de sécurité. Il y est notamment indiqué que la détection des incidents de sécurité se compose de trois activités distinctes :

- la gestion des évènements, correspondant à l'ensemble des moyens techniques et organisationnels assurant le recueil et le stockage des évènements de sécurité du SI ;
- la gestion des incidents, correspondant à l'ensemble des moyens techniques et organisationnels permettant d'identifier et de qualifier un incident de sécurité sur la base d'évènements collectés. Le stockage et la capitalisation des incidents de sécurité dans un but d'amélioration du service font aussi partie de cette activité ;
- la gestion des notifications, correspondant à l'ensemble des moyens techniques et organisationnels permettant d'informer le commanditaire sur les incidents de sécurité détectés et de stocker ces notifications.

Le référentiel PDIS [7] précise par ailleurs les éléments qui composent l'architecture d'un SI dédié à la fourniture d'un service de détection. Il y est notamment indiqué que les évènements générés sur un périmètre supervisé sont centralisés vers des collecteurs situés dans une enclave de collecte du SI interne du commanditaire. Cette dernière regroupe ainsi l'ensemble des dispositifs impliqués dans le processus de collecte. Ces évènements peuvent ensuite être transférés vers le SI d'un service de détection des incidents de sécurité, qu'il soit par exemple opéré dans un SOC interne, ou externalisé auprès d'un PDIS. L'architecture globale ici décrite est représentée par la figure 1 ci-après. Le périmètre du présent guide se limite toutefois à couvrir :

- les aspects relatifs à une journalisation locale des évènements sur les systèmes Windows ;
- la centralisation des évènements dans une enclave de collecte du SI interne de l'entité, qui reste dans son périmètre de responsabilité y compris en cas d'externalisation du service de détection des incidents de sécurité.

1. Un SOC est un SI qui concentre les moyens humains, techniques et organisationnels dédiés au traitement des incidents de sécurité. En fonction des enjeux, des besoins et des ressources du commanditaire, ce centre peut être interne ou externalisé. Dans ce dernier cas, la mutualisation peut avoir des effets vertueux dans le partage de la connaissance de la menace et l'optimisation des règles de détection.

Le périmètre de ce guide est également représenté par un cadre rouge dans la figure 1.

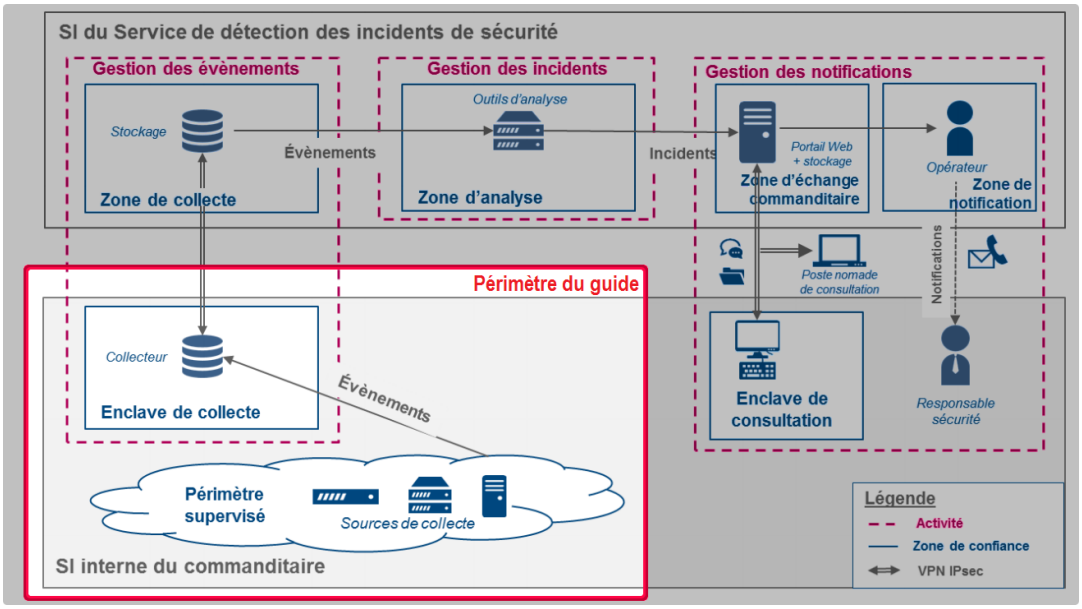


FIGURE 1 – Périmètre du présent guide dans la représentation simplifiée d'une architecture type de service de détection des incidents de sécurité du référentiel PDIS [7]

Dans le présent document, seules les fonctionnalités natives des systèmes Windows sont mises en œuvre ainsi que tout outil gratuitement mis à disposition par Microsoft. Il est notamment pris comme hypothèse que la gestion des systèmes Windows repose sur un annuaire Active Directory (AD). L'utilisation de solutions logicielles alternatives tierces n'est toutefois pas découragée ; elle nécessite dans ce cas un effort d'adaptation des recommandations de ce guide.

### Active Directory

AD est un service d'annuaire introduit par Microsoft sous Windows 2000 Server. Son implémentation permet de centraliser des informations relatives aux utilisateurs et aux ressources d'un SI en fournissant des mécanismes d'identification, d'authentification et d'autorisation. C'est donc un service d'annuaire au sens large, qui inventorie et gère un ensemble d'objets que sont les comptes et groupes utilisateurs de l'entité mais également les serveurs, postes de travail, imprimantes, etc. Il a vocation, entre autres, à permettre aux utilisateurs de trouver et d'accéder aux ressources connues de l'annuaire.

Enfin, ce guide couvre uniquement les cas d'usage des serveurs et des postes de travail qui sont en permanence connectés au SI ou qui s'y connectent fréquemment (systèmes en situation de nomadisme par exemple). Ces systèmes peuvent dès lors joindre les services de collecte des évènements de sécurité qui sont déployés sur le SI. Les systèmes utilisés hors du SI et sans connectivité régulière avec ce dernier sont hors périmètre du présent document ; ils doivent faire l'objet de dispositifs de journalisation spécifiques.

## 1.3 Organisation du guide

Ce guide présente en chapitre 2 des recommandations de mise en œuvre d'une stratégie de journalisation locale des systèmes Windows adaptée aux besoins de sécurité et à l'état de la menace. Sont ainsi traités divers aspects liés au paramétrage des capacités de journalisation natives des systèmes et à l'utilisation d'un utilitaire de journalisation avancée.

Le chapitre 3 traite quant à lui des aspects liés à la centralisation des journaux d'évènements Windows dans une enclave de collecte. Dans cette optique, il détaille les modalités de mise en œuvre du service « Collecteur d'évènements de Windows » (`WECSvc`) nativement présent sur les systèmes Windows. Sont notamment abordés les aspects liés à sa sécurisation, à son intégration dans des architectures de journalisation centralisée, ainsi qu'à la sélection des évènements qui devraient être transférés.

Plusieurs annexes complètent ce guide en précisant la mise en œuvre technique des recommandations présentées dans ces chapitres ou en transmettant des informations complémentaires qui peuvent être utiles à certains lecteurs.

- l'annexe A détaille les aspects techniques de la synchronisation d'horloge en environnement AD ;
- l'annexe B dresse une liste des journaux Windows les plus utiles aux activités de détection et d'analyse des évènements de sécurité, certains devant être explicitement activés ou rendus plus verbeux ;
- l'annexe C détaille comment configurer le stockage local et la rotation des journaux Windows sur les systèmes ;
- l'annexe D précise la recommandation de configuration des stratégies d'audit de Windows ;
- l'annexe E détaille les aspects techniques du déploiement et de la configuration centralisés de *sysmon*.
- l'annexe F est un guide didactique pour la compréhension des règles *sysmon*, destiné à des lecteurs qui ne sont pas familiers avec ce type de fichiers structurés ;
- l'annexe G précise les recommandations de mise en œuvre d'un service de collecte des évènements Windows ;
- l'annexe H donne une méthode permettant de créer un arborescence personnalisée de journaux pour les serveurs collecteurs d'évènements. Cela n'est généralement pas nécessaire lorsque les évènements ne font que transiter par des serveurs de collecte pour être ensuite ingérés dans des outils de détection et d'analyse des incidents de sécurité. Cela peut en revanche s'avérer pratique en l'absence de tels outils ou pour répondre à des besoins particuliers (pour répartir les évènements centralisés sur plusieurs volumes de stockage, répondre à des besoins des administrateurs en octroyant des droits de lecture à certains journaux, etc.).

## 1.4 Convention de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*.

Pour certaines recommandations de ce guide, il est proposé plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

### Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

La mise en place des recommandations associées conduit uniquement à préparer le terrain à une réponse à incident sans analyse ni détection proactive. Sur un SI peu complexe, elle nécessite généralement une semaine de travail ponctuelle pour un unique administrateur à temps plein.

R -

### Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

### Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

### Recommandation renforcée

Cette recommandation permet de mettre en œuvre un niveau de sécurité renforcée. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

La mise en place des recommandations associées conduit à la collecte des journaux de sécurité spécifique aux besoins de l'entité avec une amélioration continue. En général et d'après les retours d'expérience des bénéficiaires de l'ANSSI, la charge du maintien dans le temps de ce niveau de recommandation nécessite au minimum deux ingénieurs en détection à temps plein qui seraient spécialisés dans l'amélioration de la journalisation et de la détection. La charge de la supervision proactive (qualification des alertes) n'est toutefois pas incluse dans cette évaluation.

La liste récapitulative des recommandations est disponible en page 91.

# 2
# Mise en œuvre de la journalisation sur les systèmes Windows

### Objectif

Si satisfaire aux prérequis de base pour la journalisation des systèmes Windows est souvent une simple formalité, tendre vers un niveau de journalisation avancé requiert en revanche un certain effort. L'objectif de ce chapitre est de proposer un ensemble de recommandations sur l'environnement de journalisation des systèmes Windows de manière à faciliter ensuite la détection et l'analyse des incidents de sécurité.

## 2.1 Synchronisation des horloges

Les serveurs et les postes de travail disposent d'horloges internes utilisées, entre autres, pour horodater les évènements. Les horloges de tous les équipements dérivent naturellement dans le temps. Ces écarts peuvent se mesurer en secondes voire en minutes après quelques semaines de dérive. Or, la compréhension de l'enchaînement précis d'évènements issus de plusieurs journaux est plus difficile lorsque les équipements qui produisent ces journaux ne disposent pas du même temps de référence.

Il est par conséquent crucial de disposer d'équipements synchronisés sur la même source de temps, sans quoi des évènements pourraient ne pas être pris en compte dans l'analyse, rendant celle-ci moins efficace. Il est ainsi recommandé de disposer de sources de temps fiables et utilisées par l'ensemble des équipements qui composent le SI.

NTP est le protocole le plus fréquemment utilisé pour la synchronisation des horloges des équipements avec des sources de temps.

### NTP

Le protocole NTP (*Network Time Protocol*) est largement utilisé pour synchroniser les équipements sur une ou plusieurs sources de temps. Il est disponible pour la plupart des systèmes d'exploitation, quel que soit le type d'équipement. Une architecture NTP type comprend généralement un ou plusieurs serveurs NTP internes sur lesquels se synchronisent les machines du SI. Ces serveurs référents peuvent, quant à eux, calibrer leurs horloges à l'aide de matériel spécifique (intégrant une horloge atomique ou utilisant les signaux radio ou satellitaires par exemple) ou bien se syn-

chroniser avec des serveurs NTP publics. Une source de temps peut ainsi avoir une précision plus ou moins importante par rapport au temps universel.

Les serveurs NTP de référence du SI peuvent synchroniser leurs horloges auprès de serveurs de temps reconnus et accessibles publiquement sur Internet [2]. Dans des contextes spécifiques, l'utilisation d'une source de temps matérielle autonome peut également être envisagée. Pour les besoins de journalisation, seule la cohérence des horloges au sein du SI est nécessaire. La recherche d'une précision accrue vis-à-vis du temps universel sera motivée uniquement par des besoins métier spécifiques.

R1

### Veiller à la synchronisation des horloges

Les horloges des équipements doivent être synchronisées sur plusieurs sources de temps internes cohérentes entre elles. Ces dernières peuvent elles-mêmes être synchronisées sur plusieurs sources de temps externes fiables, sauf dans le cas particulier de réseaux physiquement isolés.

En environnement AD, les systèmes Windows synchronisent par défaut leurs horloges avec celles des contrôleurs de domaine (DC, *Domain Controllers*). Il est donc recommandé de rester dans cette configuration par défaut. En revanche, la source de temps de la forêt AD doit être synchronisée avec les serveurs NTP de référence du SI.

La mise en œuvre technique de cette recommandation est traitée en annexe A.

### Information

Il est à noter que la synchronisation des horloges des systèmes a un intérêt qui va au-delà de la seule journalisation. Dans un environnement AD, une cohérence temporelle (avec un écart maximal de quelques minutes par défaut) est un prérequis indispensable au bon fonctionnement de certains protocoles d'authentification comme Kerberos.

## 2.2 Activation des journaux utiles

Les évènements des systèmes d'exploitation Windows sont enregistrés dans les fichiers de journaux. Ceux-ci sont répartis dans deux rubriques, « journaux Windows » et « journaux des applications et des services ». Tous ces journaux sont visualisables, par exemple, à l'aide de la console *Microsoft Management Console* [28] (MMC) « observateur d'évènements » (`eventvwr.msc`) et sont stockés par défaut à l'emplacement `%WINDIR%\System32\winevt\Logs`.

Les journaux Windows sont répartis en quatre fichiers : « Application », « Installation », « Sécurité » et « Système », chacun servant à l'écriture des évènements liés à ces quatre types d'évènements. Il s'agit de journaux importants du système et qui sont utiles aux activités de détection et d'analyse.

2. Le site Web de RENATER propose par exemple une liste [9] de serveurs de temps français.

Les « journaux des applications et des services », apparus avec Windows 7, sont des journaux secondaires qui peuvent être créés par divers fournisseurs d'évènements ; des journaux de ce type existent nativement sous Windows (depuis Windows Vista) pour le stockage des évènements spécifiques à certains fournisseurs (*Windows Defender*, *Windows PowerShell*, etc.). Certains de ces journaux présentent un réel intérêt pour les activités de détection et d'analyse, mais d'autres n'en présentent que pour de l'analyse de dysfonctionnements ou du débogage. Leur utilité dépend ainsi des solutions logicielles déployées et utilisées, des fonctionnalités et mécanismes de sécurité mis en œuvre, etc. Seule l'analyse de risques de l'entité et la stratégie de détection qui en découle peuvent permettre d'éclairer les administrateurs et les équipes de sécurité sur la nécessité de collecter tout ou partie de ces journaux.

**R2**

### Identifier et activer les journaux Windows utiles aux activités de détection et d'analyse

Pour pouvoir mener les activités de détection et d'analyse dans des conditions optimales, il est nécessaire au préalable d'activer les journaux d'évènements spécifiés à l'annexe B et de configurer les compléments de journalisation qui figurent en section B.4. Bien que ces journaux ne fassent pas nécessairement l'objet d'une centralisation, leur présence sur les système reste utile en cas de réponse à incident.

**R3 +**

### Réviser régulièrement les journaux Windows à collecter en fonction de l'évolution du SI et des menaces

Comme les SI évoluent, ainsi que les menaces et les risques qui pèsent sur eux, la stratégie de détection doit évoluer en conséquence.

En complément de la recommandation R2, il est ainsi recommandé de continuellement identifier tout journal, ou complément de journalisation (tels que ceux mentionnés en section B.4) qui pourraient s'avérer pertinents pour la mise en œuvre de règles de détection avancées.

## 2.3 Fonctionnalités de journalisation des applications tierces

Si les systèmes Windows incluent nativement des fonctionnalités de journalisation avancées, cela n'est pas forcément le cas pour des applications tierces installées sur ces systèmes. Comme indiqué par le guide générique sur la journalisation [6], il s'agit d'un point de vigilance à prendre en compte au plus tôt.

Ces applications tierces devraient idéalement écrire leurs évènements dans des journaux gérés par le système Windows plutôt que dans des formats propriétaires qui complexifieraient leur collecte et leur traitement. Il est par ailleurs préférable qu'elles n'utilisent pas le journal « Application » générique du système mais créent un ou plusieurs journaux qui leurs soient propres dans les « journaux des applications et des services » de Windows. Leur niveau de journalisation, qu'il soit configurable ou figé dans le code, devrait par ailleurs permettre d'écrire au minimum tout évènement essentiel à la détection et l'analyse des incidents de sécurité.

R4 +

### Veiller à la journalisation des applications tierces

Il est recommandé de privilégier les applications tierces qui disposent nativement d'une fonctionnalité de journalisation pertinente et qui écrivent leurs évènements dans des journaux gérés par le système Windows tout en respectant un format de données structuré (écriture des informations dans des champs distincts et exploitables, renseignement d'une version du format de données, etc.). La prise en compte de ce besoin devrait se faire au plus tôt pour éviter que des solutions logicielles inappropriées ne soient déployées sur le SI.

Enfin, si les évènements journalisés par ces applications tierces sont susceptibles de contenir des éléments à caractère personnel, il est dans ce cas nécessaire de satisfaire aux contraintes réglementaires exposées en annexe D du guide générique sur la journalisation [6].

## 2.4 Stockage local et rotation des journaux sur les systèmes

Pour que toute information essentielle aux activités de détection et d'analyse soit en permanence disponible, une politique de rétention des journaux d'évènements doit être formalisée et mise en œuvre sur l'ensemble des équipements journalisés. Sur les systèmes Windows, la stratégie de rétention ne permet pas directement de spécifier une durée de rétention des évènements. Elle consiste en revanche à configurer une taille maximale pour chacun des fichiers de journaux (journaux Windows et journaux des services et applications).

Trois paramètres de configuration sont alors disponibles pour préciser le comportement adopté par le système lorsqu'un fichier atteint sa taille maximale :

- **ne plus journaliser les nouveaux évènements**. Cette option est déconseillée car les nouveaux évènements sont ainsi perdus ;
- **remplacer les évènements les plus anciens par les nouveaux**. Cette rotation automatique est pertinente lorsque la taille du journal permet la rétention des évènements pendant une durée suffisante. Il s'agit de l'option à privilégier car c'est la plus facilement maintenable ;
- **archiver le journal et le vider**. Cette option nécessite un certain effort de maintenance étant donné que l'exportation locale des journaux peut, à terme, se traduire par une grande volumétrie de journaux stockés sur les systèmes et donc à une saturation de l'espace disque local. Elle présente un intérêt si le besoin d'auditabilité du système est important mais que les évènements ne sont ni sauvegardés ni centralisés.

La stratégie de rétention locale des journaux sur les systèmes journalisés devient néanmoins accessoire dès lors que leur collecte pour centralisation est mise en œuvre. En effet, la problématique de leur archivage et de leur rétention est dans ce cas déplacée sur les serveurs de collecte et plus généralement au sein de l'infrastructure de journalisation (les aspects relatifs à la collecte des journaux pour centralisation dans une infrastructure de journalisation sont abordés au chapitre 3). Les systèmes n'ont ainsi plus nécessairement besoin de stocker eux-mêmes les journaux pendant plusieurs mois ou années.

La centralisation porte toutefois rarement sur l'intégralité des journaux, il reste donc nécessaire de les stocker suffisamment longtemps sur les systèmes journalisés de manière à permettre une analyse en cas de réponse à incident. La taille idéale de chaque journal dépend ainsi essentiellement de leur centralisation complète ou non. En cas de centralisation complète, la taille idéale d'un journal dépend de la fréquence de collecte des journaux puis, dans une moindre mesure, d'éventuelles contraintes telles que les situations de nomadisme où des équipements d'accès distant peuvent potentiellement rester sans connexion au serveur de collecte pendant une période de temps longue. En cas de centralisation partielle ou inexistante d'un journal, sa taille idéale dépend du volume d'évènements inscrits dans ce dernier et de la réglementation en termes de durée de conservation (se référer au guide générique sur la journalisation [6]). Dans la plupart des cas, la stratégie de rotation automatique par effacement des évènements les plus anciens s'avère adaptée dès lors que la taille des journaux est correctement configurée.

R5

### Paramétrer les stratégies de stockage local et de rétention des journaux d'évènements

Les évènements journalisés sur les systèmes doivent être disponibles pour permettre leur analyse en local ou leur centralisation. Il est ainsi recommandé :

- de configurer une rotation automatique des journaux par effacement des évènements les plus anciens (configuration par défaut), sauf exception découlant d'un besoin spécifique ;
- de configurer des tailles de journaux Windows permettant la rétention des évènements sur les systèmes pendant une durée suffisante et adaptée au contexte de chaque entité. Il est pour cela recommandé d'appliquer les configurations spécifiées en annexe C, et ce pour tous les journaux d'évènements utiles aux activités de détection et d'analyse (cf. recommandation R2 de la section 2.2) ;
- de s'assurer que les partitions système des équipements aient un espace disque suffisant pour la bonne application de cette stratégie de stockage local et de rétention des journaux d'évènements.

## 2.5 Configuration des stratégies d'audit natives

Les systèmes Windows – depuis Windows Vista et Windows Server 2008 – intègrent nativement plus d'une cinquantaine de stratégies d'audit dont l'activation va avoir pour effet de générer des évènements de sécurité de différentes catégories. Ces évènements sont écrits dans le journal « Sécurité » de Windows.

### Information

Il est à noter que, dans Windows ainsi que dans la documentation de Microsoft, la journalisation est souvent désignée par le terme « audit ». Bien que le terme « journalisation » soit privilégié dans le présent document, le terme « audit » reste néanmoins utilisé lorsqu'il s'agit de faire référence à des éléments du système ayant cet intitulé.

Chacune de ces stratégies d'audit concerne un comportement spécifique dont il est possible de journaliser les échecs et succès. Cette granularité permet de sélectionner finement les évènements

à journaliser en fonction des besoins de sécurité. L'enjeu du paramétrage de ces stratégies d'audit est d'obtenir un bon équilibre entre :

- la volumétrie d'information obtenue, qui, lorsqu'elle est trop importante, complexifie sa centralisation, son stockage et son traitement tout en nuisant potentiellement à la performance des systèmes ;
- la pertinence des informations journalisées, de sorte que toute information essentielle soit réellement disponible et permette de mener à bien les activités de détection et d'analyse.

R6

### Paramétrer les stratégies d'audit avancées des systèmes Windows

Les évènements journalisés dans la configuration par défaut des stratégies d'audit des systèmes Windows sont insuffisants pour détecter ou analyser des incidents de sécurité. Il est donc recommandé de modifier cette configuration par défaut de manière à tendre autant que possible vers un bon équilibre entre volumétrie et pertinence des informations journalisées. Ce paramétrage doit s'appuyer sur l'analyse des risques du SI et la stratégie de détection qui en découle. La mise en œuvre technique de cette recommandation est traitée en annexe D.

Dans ce contexte, les paramètres de stratégie d'audit recommandés par l'ANSSI sont à considérer comme un niveau de journalisation minimum à appliquer. Ils figurent en annexe D. Il convient toutefois de préciser que tous les évènements journalisés ne font pas nécessairement l'objet d'une centralisation ; ce sujet est traité en section 3.3.

## 2.6 Journalisation avancée reposant sur sysmon

Les stratégies d'audit natives de Windows, basiques ou avancées, restent insuffisantes dès qu'il s'agit de journaliser des comportements très spécifiques ou des informations additionnelles souvent utiles aux activités de détection et d'analyse des incidents de sécurité. Ce besoin de journalisation avancée concerne principalement les entités exposées à un fort niveau de menace ou pour lesquelles les impacts d'un incident de sécurité sur leur activité métier seraient critiques, que ce soit sur l'intégralité de leur SI ou sur des sous-ensembles qui se démarquent de par leur exposition aux menaces ou leur sensibilité.

Lorsque les limites des stratégies d'audit natives sont atteintes (c'est-à-dire lorsque la détection requiert l'application de règles de journalisation complexes ou qu'elle requiert la journalisation d'évènements qui ne sont pas journalisés nativement), il est possible de recourir à des utilitaires complémentaires qui offrent des capacités de journalisation supplémentaires et une meilleure granularité de configuration. En l'occurrence, *System Monitor* [39] (*sysmon*) est un utilitaire qui fait souvent référence en complément des stratégies d'audit natives. Cet utilitaire a été développé par *Winternals* [3] et fait partie de la suite d'outils *Sysinternals*. Tout comme plusieurs dizaines d'autres outils *Sysinternals* très connus des administrateurs système, *sysmon* reste à ce jour gracieusement mis à disposition par Microsoft. Il continue d'être développé et fait l'objet de mises à jour régulières, qui lui apportent de nouvelles capacités de configuration ou de supervision [4].

3. *Winternals* est une entreprise rachetée par Microsoft en 2006.
4. La page de téléchargement de *sysmon* [39] dresse une liste des évènements journalisables par l'utilitaire.

### Attention

Bien que *sysmon* fasse l'objet d'un développement régulier de Microsoft, il est en revanche proposé par l'éditeur sans aucun support logiciel. Des problèmes de stabilité du système peuvent être rencontrés sur des systèmes obsolètes ou en cohabitation avec des solutions logicielles inhabituelles. Son déploiement rapide et généralisé est donc déconseillé sur des systèmes dont la disponibilité est critique ; il doit faire l'objet d'une phase de test préalable.

Il est par ailleurs préférable de ne pas déployer en production de toutes nouvelles versions majeures de *sysmon* car elles présentent généralement quelques *bugs*. Il est donc plus sage d'attendre que des mises à jour mineures soient publiées et corrigent les bugs constatés.

### Information

*Sysmon* peut être exécuté à la demande ou installé comme un service Windows. Dans ce cas, *sysmon* peut démarrer automatiquement avec le système – le pilote de *sysmon* étant par ailleurs chargé très tôt dans la chaîne de démarrage – et apporte alors une supervision persistante du système.

R7 +

### Mettre en œuvre sysmon sur les systèmes

Il est recommandé de déployer *sysmon* sur les systèmes des entités exposées à un niveau de risque accru du fait de leurs activités métier. Pour apporter une capacité de journalisation avancée et persistante, *sysmon* doit être installé sous forme de service Windows exécuté au démarrage.

L'annexe E aborde différents points d'attention techniques relatifs au déploiement centralisé et sécurisé de *sysmon* et à sa configuration, puis à sa mise à jour. Il est recommandé de les prendre en compte en s'inspirant du déploiement par stratégies de groupes (GPO, *Group Policy Object* [18]) illustré dans cette annexe.

Contrairement aux stratégies d'audit natives, *sysmon* requiert un certain effort de paramétrage sous la forme d'un fichier de configuration au format XML. C'est ce dernier qui indique, à travers un ensemble de règles à écrire soi-même, quels comportements *sysmon* journalisera.

### Attention

S'engager dans la voie d'une journalisation avancée reposant sur *sysmon* nécessite les compétences adéquates et requiert un investissement de temps notable, tant pour son déploiement initial que pour son maintien en conditions opérationnelles (MCO) ou de sécurité (MCS).

Chaque règle *sysmon* se construit autour :

- d'un type d'évènement (création de processus, requête DNS, pilote chargé, etc.) ;
- d'un ensemble de champs spécifiques à l'évènement (port réseau de destination, hôte distant, ligne de commande, signature, etc.) ;

- de conditions sur les champs (contient telle valeur, est égal à, commence par, à l'exception de, etc.).

Le fichier de configuration XML de *sysmon* se compose d'un ensemble de règles et de quelques paramètres globaux ; il peut facilement atteindre plusieurs centaines de lignes. L'utilisation de fichiers de configuration *sysmon* génériques comme source d'inspiration est conseillée, mais leur adaptation au SI est nécessaire pour que les règles configurées soient pertinentes au regard du contexte d'emploi. Comme la compréhension des règles *sysmon* est un prérequis souhaitable à leur mise en œuvre sur le SI, l'annexe F explique leur construction d'une manière simple et illustrée.

Différents sites Web proposent des modèles de fichiers de configuration de *sysmon*. Deux d'entre eux sont particulièrement intéressants :

- `sysmon-config` [53] de *SwiftOnSecurity* ;
- `sysmon-modular` [52] d'Olaf Hartong.

### Attention

Attention à ne pas mettre en production des fichiers de configuration de *sysmon* trop volumineux. Au delà de 2000 lignes, il est généralement constaté des problèmes de stabilité.

Un autre cas d'usage de *sysmon* concerne les secteurs d'activités sensibles qui font l'objet de campagnes d'attaques ciblées et parfois très sophistiquées. Dans une démarche de recherche d'indicateurs de compromission, les administrateurs système et experts en SSI de ces entités devraient être capables de déployer rapidement des règles *sysmon* spécifiques (transmises par des partenaires de *Threat intelligence* par exemple) sur leur parc informatique. Cela implique que les équipes soient formées à la configuration de *sysmon* et que les systèmes Windows soient configurés pour rendre possible l'application rapide des nouvelles configurations de l'utilitaire.

R8 +

### Élaborer et maintenir la configuration de sysmon

Lorsque *sysmon* est déployé sur le SI (recommandation R7+), il est recommandé de dédier les moyens humains nécessaires à sa configuration soignée, celle-ci nécessitant une bonne connaissance du SI ainsi que des compétences minimales en système Windows et en SSI.

Les équipes doivent par ailleurs être en mesure de rapidement déployer une nouvelle configuration de *sysmon* sur les systèmes lorsque cela s'avère nécessaire (pour améliorer la détection de nouvelles menaces, pour prendre en charge de nouveaux types d'évènements, etc.).

L'annexe F explique le fonctionnement des règles *sysmon* pour les lecteurs qui ne sont pas familiers avec ce type de fichier structuré et propose des bonnes pratiques pour leur maintenabilité.

# 3
# Collecte des journaux d'évènements Windows

Le guide de recommandations de sécurité pour la mise en œuvre d'un système de journalisation [6] intègre des recommandations visant à renforcer la résilience du système de journalisation. Il recommande notamment de déplacer les journaux sur des machines différentes de celles qui les ont générés et de les centraliser sur des serveurs dédiés. Il propose à cette occasion différentes architectures de journalisation centralisée.

Force est de constater que certaines entités n'exploitent pas les évènements de sécurité et n'ont pas d'activité de détection ni d'analyse. Dans ce cas, elles ont généralement pour projet – et y sont parfois contraintes – de centraliser leurs journaux pour permettre des analyses *a posteriori* en cas de survenue d'un incident de sécurité. D'autres, plus matures en termes de SSI, disposent en interne ou par l'intermédiaire de PDIS [7] des moyens nécessaires à l'exploitation et la corrélation des évènements du SI.

Dans tous les cas, il est à noter que la compromission d'un SI est généralement une question de temps et de moyens. Les attaquants procèdent selon une logique de retour sur investissement. Lorsque l'enjeu financier est élevé, ils peuvent mobiliser d'importants moyens et par exemple recourir à l'exploitation de vulnérabilités encore non connues et non corrigées. Le principe de défense en profondeur vise donc à entraver et ralentir suffisamment les attaquants – quels que soient leurs moyens – dans l'optique de pouvoir les détecter avant que leurs attaques n'aient des conséquences graves. Cette capacité de réaction est principalement rendue possible par les moyens d'analyse et de détection des évènements de sécurité. De tels moyens permettent ainsi de prévenir des incidents de sécurité graves, ou d'en limiter les conséquences, en rendant possibles des actions de remédiation rapides et qui peuvent par exemple être menées par des prestataires de réponse aux incidents de sécurité (PRIS [8]) qualifiés. En l'absence de tels moyens, l'intérêt des événements journalisés se limitera aux investigations numériques. Ces journaux sont en effet primordiaux pour les équipes de réponse à incident, qui cherchent à comprendre la cinématique d'une compromission pour y remédier au mieux. Dans cette situation, la compromission a déjà eu lieu. C'est la raison pour laquelle la centralisation et l'analyse en continu des évènements de sécurité sont importantes : pour permettre une réaction rapide avant que des conséquences graves ne soient à déplorer.

En environnement Microsoft, la centralisation des évènements peut reposer sur deux services Windows nativement intégrés au système d'exploitation depuis Windows Vista et Windows Server 2008 :

- le WEC – « *Windows Event Collector* » – du service du même nom (ou « Collecteur d'évènements de Windows » en français) et qui a pour nom court `WECSvc` : il remplit une fonction de cen-

tralisation des évènements du SI en collectant les évènements journalisés par les systèmes. Le service `WECSvc` est ainsi exécuté sur un ou plusieurs serveurs de collecte ;

- le WEF – « *Windows Event Forwarding* » – porté par le service « *Windows Event Log* » (ou « Journal d'évènements de Windows » en français) qui a pour nom court `EventLog` : il transfère les évènements aux serveurs de collecte configurés. Chaque système du SI, qu'il soit un poste de travail ou un serveur, est donc considéré comme un client WEF dès lors qu'il transfère ses évènements à un ou plusieurs serveurs WEC.

L'articulation entre WEC et WEF et illustrée par la figure 2.

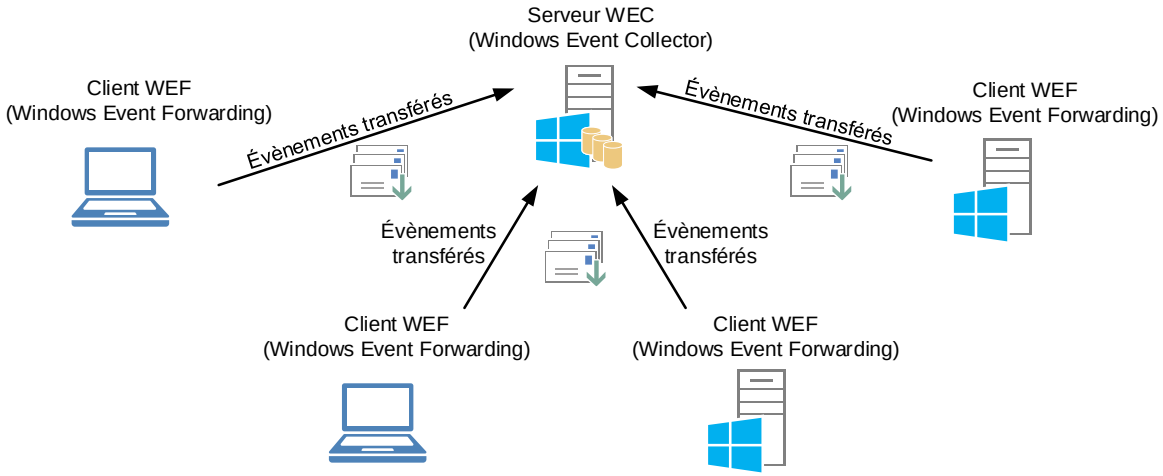


FIGURE 2 – Représentation de l'articulation entre WEC et WEF

La configuration du service `WECSvc` repose sur un principe d'abonnements (*subscriptions*). Chaque abonnement configuré sur un serveur collecteur précise une sélection d'évènements ciblés : depuis quels journaux (journaux Windows historiques et journaux des services et applications), de quelles sévérités, fournisseurs, ID d'évènements, etc. Ils peuvent donc réceptionner une large sélection d'évènements (p. ex. tous les évènements du journal de sécurité) ou au contraire une sélection très restreinte (p. ex. l'évènement 4625 du journal de sécurité, qui caractérise un échec d'ouverture de session). Chaque abonnement permet également de préciser quels sont les ordinateurs dont les évènements doivent être centralisés, ainsi que divers paramètres de configuration liés à leur transfert. Les évènements qui répondent aux critères ciblés sont ainsi transférés selon une fréquence paramétrée dans chaque abonnement.

Pour la bonne compréhension de la suite du guide, il convient de rappeler que son périmètre se limite à la centralisation des évènements dans une enclave de collecte du SI interne de l'entité. Bien que les recommandations soient formulées de manière générale et applicables à toute solution logicielle de centralisation des évènements, ce guide n'aborde que les aspects liés au déploiement de serveurs collecteurs d'évènements Windows reposant sur le service `WECSvc`, quels que soient leurs rôles dans l'architecture plus globale d'un centre opérationnel de cybersécurité ou d'un SI dédié à la détection des incidents de sécurité (cf. référentiel PDIS [7]). Il couvre différentes problématiques ayant trait au déploiement de ces serveurs de collecte et propose des bonnes pratiques de configuration.

Pour finir, il est également rappelé que les problématiques d'architecture globale – et notamment celles ayant trait au cloisonnement du système de journalisation – sont abordées dans le guide générique sur la journalisation [6].

## 3.1 Déploiement de serveurs collecteurs d'évènements

Diverses contraintes sont à prendre en compte pour définir une architecture de centralisation des journaux d'évènements au sein d'une ou plusieurs enclaves de collecte : répartition géographique du SI, bande passante des liens entre sites, volumétrie journalière des évènements, nombre de systèmes journalisés, besoins de sécurité (SI classifiés de défense ou SIIV par exemple), etc. Il est donc naturel que les besoins en matière d'architecture de journalisation varient d'une entité à l'autre.

Ces besoins et contraintes hétérogènes se traduisent par différentes modalités de déploiement des serveurs collecteurs d'évènements Windows. Certaines entités peuvent ainsi se contenter d'un seul serveur de collecte où les évènements sont stockés mais ne font pas l'objet d'une analyse continue par une équipe dédiée à la supervision de sécurité. Pour d'autres entités en revanche, le service collecteur d'évènements Windows est fonctionnellement trop limité pour être un lieu de stockage définitif des évènements à des fins de détection et d'analyse voire d'archivage. Dans ce cas, les serveurs collecteurs d'évènements des systèmes Windows sont positionnés dans des enclaves de collecte et ne sont que des intermédiaires de centralisation des évènements. Ils sont ainsi de simples collecteurs de proximité, où ne font que transiter les évènements avant d'être centralisés dans un SI de détection des incidents de sécurité ou dans un centre opérationnel de cybersécurité, ces derniers exploitant notamment des solutions spécialisées de type SIEM [5].

Le déploiement de multiples serveurs de collecte permet de répondre à ces nombreuses contraintes d'architecture et entre autres :

- offrir de la haute disponibilité, en configurant les clients pour transférer leurs évènements à plusieurs serveurs de collecte (comme précisé en section G.2.4);
- répartir la charge sur plusieurs serveurs, ce qui est particulièrement important lorsque le SI supervisé est constitué de milliers d'équipements. Cela peut être fait en ayant plusieurs serveurs de collecte dont les abonnements ciblent chacun un sous-ensemble du parc informatique;
- chaîner des serveurs de centralisation dans une architecture étendue, avec des serveurs de collecte qui transfèrent leurs évènements à d'autres serveurs de collecte (ce qui est d'ailleurs le cas entre les serveurs de collecte de l'enclave de collecte interne d'un commanditaire et ceux de la zone de collecte d'un PDIS, comme représenté par la figure 1);
- répondre à des considérations géographiques et de bande passante d'interconnexion réseau;
- gérer différentes durées de conservation légale.

5. Un SIEM (*Security Information and Event Management*) est un système de supervision centralisée de la sécurité.

### Information

Il est à noter que la configuration d'un WEF pour l'envoi des évènements vers plusieurs serveurs WEC se traduit par l'envoi redondant de ses évènements à chacun des serveurs WEC.

R9

### Déployer des serveurs de collecte

Il est recommandé de centraliser les évènements des systèmes Windows. Cette centralisation peut se faire à l'aide d'un ou plusieurs serveurs collecteurs d'évènements Windows. Ces derniers ne sont pas nécessairement la destination finale des évènements Windows. Ils peuvent n'être que des intermédiaires de centralisation dans une enclave de collecte interne au SI de l'entité, en amont de leur transfert vers un SI de détection des incidents de sécurité ou un centre opérationnel de cybersécurité.

Il est recommandé d'appliquer les bonnes pratiques de mise en œuvre sécurisée du service `WECSvc` détaillées en annexe G.

Les limitations de volumétrie [47] du service collecteur d'évènements Windows devraient toutefois être consultées préalablement à toute conception d'architecture. Microsoft recommande notamment de ne pas dépasser 10 000 systèmes clients actifs par service `WECSvc`, ainsi que 10 000 évènements transférés par seconde.

R10 +

### Centraliser les évènements dans leur format brut

Le séquestre des journaux au format brut (c'est-à-dire sans que ce format ait été transformé) peut s'avérer utile en cas d'investigation car il conserve toutes les informations et peut servir de source à d'autres outils de traitement. Pour les entités exposées à un niveau de risque accru du fait de leurs activités métier, il est ainsi recommandé de les centraliser sans les transformer, que ce soit dans l'enclave de collecte ou par la suite au sein d'un SI de détection des incidents de sécurité.

Bien que le service `WECSvc` préserve le format brut des évènements centralisés, il convient en revanche de s'assurer que l'utilisation de solutions logicielles alternatives ou complémentaires dans la chaîne de centralisation et de traitement des évènements de sécurité respecte cette recommandation.

Enfin, et pour satisfaire aux différentes recommandation de ce chapitre, il apparaît essentiel de disposer d'une capacité de stockage adaptée à la volumétrie des évènements générés par les équipements du SI.

R11

### Veiller au bon dimensionnement et à la disponibilité du stockage centralisé des évènements

Il est recommandé de dimensionner les capacités de stockage des serveurs collecteurs ou du SI de détection des incidents de sécurité de manière à ce qu'ils ne soient pas un frein au bon déroulement des activité de détection et d'analyse. Par ailleurs, ce stockage devrait être redondé et sauvegardé de manière à assurer la disponibilité des

évènements centralisés.

## 3.2 Sécurisation du transfert des évènements

Le transfert d'évènements entre systèmes clients et serveurs collecteurs d'évènements de Windows se fait par `WinRM` (*Windows Remote Management*), un protocole de gestion des systèmes à distance lui aussi nativement intégré aux systèmes Windows. Le trafic réseau échangé par `WinRM` est encapsulé dans le protocole HTTP, dont le mécanisme de chiffrement TLS n'est pas activé par défaut. Il est néanmoins à noter que l'authentification des ordinateurs auprès des contrôleurs de domaine de l'AD aboutit à la génération de clés de session qui sont uniques entre chaque client et chaque serveur collecteur d'évènements. Ces clés de session sont réutilisées pour assurer la confidentialité, l'intégrité et l'authentification du trafic réseau échangé par `WinRM`, sans recourir à TLS. Ce fonctionnement apporte donc nativement une authentification mutuelle et permet d'assurer un transfert fiable et sécurisé des évènements.

### Information

Le transfert d'évènements par `WinRM` en HTTPS n'est utile que pour la collecte d'évènements depuis des équipements non membres de l'AD. L'authentification par certificat sur laquelle HTTPS repose vient alors pallier l'absence de secrets partagés (gérés par les DC en environnement AD) entre les clients et les serveurs collecteurs. Dans ce cas, des certificats doivent être générés puis installés sur chaque client et serveur collecteur d'évènements. La mise en œuvre de `WinRM` en HTTPS est hors périmètre du présent guide et le lecteur est invité à consulter la documentation détaillée de Microsoft [43] si nécessaire.

**R12**

### Sécuriser le transfert d'évènements

La méthode de transfert des évènements doit être configurée de sorte à garantir l'intégrité et la confidentialité des évènements transférés, tout en contrôlant la surface d'attaque qu'elle représente pour les systèmes clients et les serveurs collecteurs d'évènements.

Lorsque la centralisation des évènements vers des serveurs collecteurs repose sur l'utilisation du service `WECSvc`, il est recommandé que `WinRM` repose exclusivement sur une authentification Kerberos afin de garantir un chiffrement approprié des paquets échangés. Une attention particulière doit par ailleurs être portée à la restriction fonctionnelle de `WinRM` au strict transfert d'évènements, cela afin de réduire autant que possible la surface d'attaque que sa mise en œuvre représente pour les systèmes.

Les paramètres de configuration et de durcissement de `WinRM` recommandés sont précisés en section G.1.2. La restriction fonctionnelle de `WinRM` au strict transfert d'évènements est plus particulièrement abordée en sous-section G.1.3.3.

### Information

Concernant la sécurité des authentifications des systèmes membres du domaine AD – et sur laquelle repose la sécurité du transfert d'évènements par `WinRM` – l'utilisation de Kerberos doit être fortement privilégiée et les systèmes devraient par ailleurs accepter exclusivement un chiffrement Kerberos en AES128 minimum [25].

Quant aux authentifications NTLM qui continueraient néanmoins d'être utilisées, l'utilisation de NTLMv2 [29] avec négociation d'un chiffrement 128 bits [30] devrait être requise.

## 3.3 Sélection des évènements à centraliser

De manière pragmatique, une entité qui n'exploite pas ses journaux d'évènements peut être tentée de les centraliser sans sélection personnalisée, de manière à simplement permettre une investigation numérique après incident. En revanche, une entité qui souhaite procéder à de la détection et de l'analyse des incidents de sécurité (en mettant par exemple en œuvre un SIEM) doit généralement s'attacher à configurer des abonnements qui ciblent une sélection d'évènements plus adaptée à son contexte.

Par ailleurs, la fréquence de transfert de chaque abonnement au service `WECSvc` est configurable et permet d'ajuster les délais de transmission des évènements. Un transfert n'est pas possible en temps réel mais l'utilisation de fréquences courtes permet de s'en approcher. Il est techniquement possible de configurer une fréquence de transmission d'une seconde. Cela ne signifie pas que les systèmes clients se connectent au serveur collecteur d'évènements toutes les secondes, mais qu'ils vérifient chaque seconde si des évènements ciblés se sont produits au cours de la seconde écoulée et les transfèrent au serveur de collecte le cas échéant. Pour des questions de performance système et réseau, il n'est toutefois pas recommandé d'utiliser des intervalles de temps si courts.

**R13**

### Centraliser une liste standard d'évènements Windows

Il est recommandé de réaliser une sélection standard d'évènements Windows transférés à des serveurs de collecte, afin de disposer d'un minimum d'informations utiles pour les activités de détection ou de réponse à incident. Il est à noter que cette sélection standard requiert l'activation de journaux utiles (recommandation R2) ainsi que le paramétrage des stratégies d'audit avancées (recommandation R6).

L'annexe A du guide générique sur la journalisation [6] précise quels sont les évènements qui doivent être centralisés en priorité pour constituer un « socle minimal de journalisation ». Lorsque la centralisation des évènements vers des serveurs de collecte repose sur l'utilisation du service `WECSvc`, il est recommandé de configurer les abonnements et la sélection d'évènements tels que proposés en section G.1.4.

**R14 +**

### Centraliser une liste personnalisée d'évènements Windows

Pour les entités exposées à un niveau de risque accru du fait de leurs activités métier, et en complément de la recommandation R13, il leur est recommandé de réaliser une centralisation d'évènements additionnels en fonction des besoins de sécurité

qui leurs sont propres, des spécificités de leurs SI et de leurs capacités de détection et d'analyse. Cette sélection additionnelle d'évènements collectés est généralement le fruit d'une analyse des scénarios de compromission redoutés et des évènements qu'ils génèrent, appelée également stratégie de détection. Elle doit donc évoluer en continu en s'appuyant sur une veille de l'état de la menace.

Lorsque *sysmon* est mis en œuvre en application de la recommandation R7+, il est par ailleurs recommandé de centraliser les évènements générés par l'utilitaire (son fichier de journal étant listé dans le tableau 2).

### Information

Appliquer la recommandation R14+ peut s'accompagner d'une forte augmentation de la volumétrie des évènements collectés, ce qui peut nécessiter le déploiement de serveurs de collecte dédiés à un ensemble de systèmes journalisés (p. ex. des serveurs de collecte dédiés aux contrôleurs de domaine AD lorsqu'un audit avancé des tickets Kerberos est configuré pour détecter des anomalies dans leur utilisation).

## 3.4 Mode Push, mode Pull

Le transfert des évènements entre les systèmes clients et les serveurs de collecte peut se faire selon deux modes :

- le mode *Push* (*Source Initiated Subscription*) concerne les cas où les évènements sont poussés par les systèmes clients vers les serveurs de collecte. Les flux réseau sont donc initiés par les clients et à destination des serveurs de collecte selon une fréquence définie ;
- le mode *Pull* (*Collector Initiated Subscription*) concerne les cas où ce sont les serveurs de collecte qui vont chercher les évènements sur les systèmes clients. Les flux réseau sont dans ce cas initiés par les serveurs de collecte à destination des systèmes clients selon une fréquence définie.

Entre les systèmes clients et les serveurs collecteurs d'évènements, il est conseillé d'utiliser le mode *Push* qui présente différents avantages :

- il ne nécessite pas de compte de service, au contraire du mode *Pull* qui requiert un compte disposant de droits de lecture sur les journaux d'évènements de tous les systèmes abonnés ;
- il ne contraint pas à maintenir une liste précise de systèmes clients abonnés ;
- il limite la charge pesant sur les serveurs collecteurs d'évènements. Cela est d'autant plus vrai lorsque les serveurs avec des abonnements en mode *Pull* doivent se connecter à des systèmes clients qui ne sont pas en ligne 24h/24, ce qui consomme des ressources système et réseau pour tenter de s'y connecter en vain ;
- il minimise les connexions réseau. En effet, les serveurs avec des abonnements en mode *Pull* se connectent aux systèmes abonnés sans savoir s'ils ont des évènements à transférer, occasionnant des connexions inutiles qui sont un frein à la réduction du délai de transmission des évènements ;
- il minimise la surface d'exposition des clients, car la configuration de leur service `WinRM` en écoute sur le réseau n'est dans ce cas pas nécessaire.

R15

### Privilégier les abonnements configurés en mode Push

Lorsque la centralisation des évènements vers des serveurs collecteurs repose sur l'utilisation du service `WECSvc`, il est recommandé de privilégier la configuration d'abonnements en mode *Push*. L'application de cette recommandation est d'autant plus importante sur les ressources les plus sensibles du SI (les contrôleurs de domaine AD, entre autres), dans la mesure où leur exposition doit être limitée au strict minimum nécessaire (se référer aux recommandations de la section 3.5).

Les paramètres de configuration et de durcissement de `WinRM` recommandés pour l'utilisation du mode *Push* sont précisés en section G.2 de l'annexe G.

Le mode *Pull*, en revanche, présente l'avantage que le transfert d'évènements Windows ne nécessite aucune connexion réseau entrante sur les serveurs de collecte, ce qui est souvent perçu comme un atout pour leur surface d'attaque. Ce mode augmente en revanche la surface d'attaque des clients. Cet atout est à relativiser dans la mesure où une vulnérabilité dans le service `WinRM` présenterait des désagréments plus importants pour la sécurité des ressources les plus sensibles du SI qu'une compromission des serveurs de collecte d'évènements ; et ce d'autant plus que l'usage de `WinRM` a tendance à se généraliser pour l'administration distante des serveurs Windows.

R16 -

### Prêter attention aux risques induits par les abonnements configurés en mode Pull

Si des abonnements `WECSvc` en mode *Pull* sont toutefois utilisés, il est recommandé de porter une attention tout particulière aux comptes de service employés : le non-respect du principe de moindre privilèges pourrait permettre des rebonds de compromission depuis les serveurs de collecte et vers leurs clients (les ressources journalisées du SI dont les évènements sont centralisés). Il est également recommandé de porter attention aux spécificités de configuration que le mode *Pull* implique sur le service `WinRM` et le filtrage des flux réseau.

Pour appliquer cette recommandation, les spécificités de configuration du mode *Pull* sont détaillées en section G.3 de l'annexe G.

## 3.5 Sécurité des ressources journalisées et cloisonnement des serveurs de collecte

La mise en œuvre d'une collecte d'évènements ne doit pas affaiblir la sécurité du SI, et en priorité la sécurité des ressources les plus sensibles, c'est à dire celles qui portent les valeurs métier de l'entité (au sens de la méthode EBIOS RM [4]) et celles qui permettent le contrôle de l'AD (les contrôleurs de domaine par exemple). De ce point de vue, il est à noter que les serveurs WEC ne sont pas considérés comme faisant partie des ressources les plus sensibles du SI, dans la mesure où leur compromission est certes dommageable mais n'est pas censée entrainer une prise de contrôle des valeurs métier ni du reste du SI.

R17

### Cloisonner les serveurs de collecte

Les bonnes pratiques d'administration et d'utilisation des accès privilégiés [33] doivent permettre d'assurer un cloisonnement (se référer au guide d'administration sécurisée des SI [5]) des serveurs de collecte d'évènements Windows vis-à-vis des autres ressources du SI. Les serveurs de collecte doivent ainsi être administrés en respectant les politiques de sécurité applicables à leur niveau de sensibilité. Ce cloisonnement est d'autant plus important vis-à-vis des ressources les plus sensibles du SI car la sécurité de ces dernières ne doit en aucun cas être mise en péril dans l'hypothèse d'une compromission des serveurs de collecte (d'où l'importance de la recommandation R15 pour ces ressources).

### Accès privilégié

Un accès est dit *privilégié* dès lors qu'il permet des actions sensibles qui sont interdites aux utilisateurs. C'est notamment le cas des accès octroyés à des comptes d'administration du domaine AD ou à des comptes d'administration fonctionnelle d'une application métier.

Par ailleurs et quel que soit leur niveau de sensibilité pour le SI ou les valeurs métier de l'entité, la sécurité des serveurs de collecte reste à assurer étant donné la nature des informations qu'ils centralisent. En effet, ces informations peuvent s'avérer utiles pour un attaquant, que ce soit en phase de reconnaissance ou de compromission des ressources du SI. Un attaquant tente généralement d'effacer ses traces pour rendre plus difficile la compréhension de son action. Il est par conséquent nécessaire de protéger ces informations, en procédant au durcissement et au maintien à jour des serveurs de collecte, comme cela est recommandé par le guide générique sur la journalisation [6].

## 3.6 Solutions tierces de collecte

Certains SI mettent en œuvre des solutions tierces de collecte en remplacement des composants logiciels WEF et WEC nativement intégrés à Windows. Chaque solution logicielle tierce présente des risques de sécurité qui lui sont propres et qui différent des risques que présentent les WEF et les WEC.

R18

### Proscrire les solutions logicielles tierces de collecte sur les ressources sensibles de l'AD

Il est recommandé de proscrire l'installation de solutions logicielles tierces de collecte ou de centralisation d'évènements sur les ressources journalisées les plus sensibles du SI (les contrôleurs de domaine AD, entre autres), car ces dernières peuvent en augmenter la surface d'attaque.

R19 -

## Protéger les ressources sensibles de l'AD en cas d'utilisation de solutions logicielles tierces de collecte

Si des solutions tierces de collecte venaient toutefois à être déployées sur des ressources sensibles du SI, une analyse doit dans ce cas être menée pour identifier les éventuels chemins de compromission que ces solutions engendrent.

Si la solution fonctionne en mode *Pull*, il est probable que des chemins de compromission existent depuis les serveurs de collecte et vers les agents installés sur les ressources journalisées. Si tel est le cas, un filtrage réseau doit garantir que ces agents ne peuvent recevoir des connexions réseau que depuis des serveurs de collecte d'un niveau de sensibilité équivalent ou supérieur au leur.

Si la solution fonctionne en mode *Push*, il peut arriver que des chemins de compromission existent depuis les agents installés sur les ressources journalisées et vers les serveurs de collecte (tout service en écoute réseau sur ces serveurs pouvant présenter des vulnérabilités). En cas de doute sur le niveau de sécurité des services de collecte, un filtrage réseau doit garantir qu'ils ne soient joignables que depuis les ressources journalisées d'un niveau de sensibilité équivalent ou supérieur au leur.

## Chemin de compromission

Un chemin de compromission est une cheminement logique et reproductible qui exploite une ou plusieurs défaillances humaines, matérielles ou logicielles permettant de réaliser une ou plusieurs élévations de privilèges successives, localement ou depuis une ressource du SI vers une autre.

## Élévation de privilèges

Lorsqu'un attaquant élève ses privilèges, il devient en capacité de mener des actions qui lui sont normalement interdites par un mécanisme de sécurité mais qui sont autorisées à des personnes ou tâches logicielles qui disposent de droits et privilèges supérieurs.

R20

## MCS des solutions tierces de collecte

Les solutions tierces de collecte doivent faire l'objet d'un maintien en condition de sécurité (MCS) assidu et spécifique dans la mesure où elles sont hors-périmètre des mises à jour automatiques de Windows. Ce MCS est primordial pour protéger les ressources journalisées contre toute vulnérabilité connue de ces solutions.

# Annexe A
# Synchronisation NTP des systèmes Windows

Il est recommandé que l'ensemble des équipements d'un SI soit configuré pour prendre leur référence horaire sur un serveur NTP. En environnement AD, les systèmes membres synchronisent par défaut leurs horloges avec celles de leurs contrôleurs de domaine [6] (DC). Par défaut, le DC qui possède le rôle FSMO [22] de *PDC Emulator* dans le domaine racine est la source de temps de référence pour la forêt AD. Les autres DC se synchronisent avec le *PDC Emulator* de leur domaine ou avec un DC du domaine parent.

Dans le cas où des équipements du SI seraient répartis géographiquement sur des fuseaux horaires différents, le fuseau horaire configuré localement sur chaque système leur permet d'assurer automatiquement une cohérence temporelle lors de la synchronisation des horloges. Lorsque deux serveurs échangent des données horodatées, l'horodatage se base ainsi sur le temps UTC (temps universel coordonné). C'est également le cas des évènements qui sont enregistrés à l'heure UTC.

Lorsqu'un système Windows synchronise son horloge avec la hiérarchie du domaine AD, cette synchronisation se fait de manière sécurisée grâce à la clé de session Kerberos issue de l'authentification mutuelle entre les comptes d'ordinateur et les DC. Il est recommandé de rester dans cette configuration par défaut. Sur le périmètre des annuaires AD, il est par conséquent nécessaire de s'assurer de deux aspects détaillés dans les sections de cette annexe :

1. les systèmes Windows membres d'un domaine AD synchronisent leurs horloges avec celles des DC de ce domaine, selon la configuration par défaut. Cette configuration par défaut est également applicable aux DC qui ne portent pas le rôle FSMO [22] de *PDC Emulator*, pour qu'ils synchronisent leurs horloges avec le DC qui le porte ;
2. le DC ayant le rôle FSMO [22] de *PDC Emulator* du domaine racine d'une forêt AD synchronise son horloge avec celles des serveurs NTP internes de référence, ces derniers étant quant à eux synchronisés sur d'autres sources fiables (recommandation du guide sur la journalisation [6]).

## A.1 Configuration NTP des systèmes Windows membres de l'AD

Pour s'assurer que les systèmes Windows membres de domaines AD synchronisent leurs horloges avec celles de leurs DC et que ces derniers synchronisent leurs horloges entre eux, les points d'at-

6. Les informations techniques de référence sur le service de temps Windows peuvent être consultées dans l'article [31] de Microsoft.

tention qui suivent sont à contrôler.

### A.1.1 Démarrage du service de temps de Windows

Le service Windows « Temps Windows » (de nom court `W32Time`) est le service chargé de synchroniser l'horloge du système. Il doit donc être démarré sur tous les systèmes (postes de travail et serveurs) afin de remplir sa fonction. Bien que ce service Windows soit en démarrage automatique par défaut, cela peut avoir été modifié à l'installation du système ou par la suite. Dans certains contextes, il peut donc être utile de s'assurer de son démarrage automatique. Cela peut par exemple se faire de manière centralisée à l'aide d'une GPO appliquée à tous les ordinateurs du domaine AD (incluant les DC). La stratégie à utiliser est précisée par le listing 1.

```
Configuration Ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Services
    systèmes\Temps Windows
```

Listing 1 – Stratégie de démarrage du service de temps Windows

### A.1.2 Règles de pare-feu

Le service de temps de Windows utilise le protocole NTP pour synchroniser son horloge avec ses serveurs de temps. Ce protocole nécessite que le port UDP 123 soit ouvert en connexion entrante sur les serveurs fournisseurs de temps et en connexion sortante sur les clients NTP. Des règles de pare-feu autorisant ces flux doivent donc être créées sur les pare-feux logiciels des systèmes membres de l'AD.

Sur les clients NTP, tout trafic sortant est par défaut autorisé sur le pare-feu Windows. Il n'y a dans ce cas aucune règle de pare-feu à créer. En revanche, si la configuration a été durcie et que le trafic sortant est par défaut interdit, il convient alors de créer une règle explicite autorisant le protocole NTP (UDP à destination du port 123) pour le service `W32Time` et à destination des DC de l'AD.

Sur les DC :

- pour le trafic entrant, il suffit d'activer la règle de pare-feu prédéfinie « Contrôleur de domaine Active Directory - W32Time (NTP-UDP-entrant) ». Elle autorise le protocole NTP (UDP entrant sur le port 123) pour le service `W32Time` ;
- pour le trafic sortant (là encore, uniquement si la configuration a été durcie et que le trafic sortant y est par défaut interdit), il convient de créer une règle autorisant le protocole NTP (UDP à destination du port 123) pour le service `W32Time` et à destination des autres DC. Sur le DC ayant le rôle de *PDC Emulator* du domaine racine de la forêt (voir section A.2), le protocole NTP doit également être autorisé à destination des fournisseurs de temps de référence (mais non membres de l'AD).

Des règles autorisant ces flux NTP doivent également être créées sur les éventuels équipements de filtrage déployés sur le réseau du SI.

La configuration des règles de filtrage du pare-feu intégré de Windows peut par exemple se faire par configuration centralisée à l'aide des GPO. La stratégie à utiliser est précisée par le listing 2.

```
Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Pare-feu Windows
     avec fonctions avancées de sécurité
```

Listing 2 – Stratégie de configuration du pare-feu Windows

### A.1.3 Configuration du service de temps Windows

La configuration par défaut du service de temps Windows est appropriée dans la mesure où elle consiste à synchroniser les horloges à partir de la hiérarchie du domaine AD. Néanmoins, cette configuration peut avoir été modifiée à l'installation du système ou par la suite. Dans certains contextes, il peut donc être utile de s'assurer qu'elle reste bien celle appliquée. Cela peut par exemple se faire par configuration centralisée à l'aide d'une GPO appliquée aux ordinateurs du domaine (incluant les DC et à l'exclusion de celui portant le rôle de *PDC Emulator*, sa configuration spécifique étant abordée en section A.2). Les stratégies à activer sont précisées par le listing 3.

```
Configuration ordinateur\Modèles d'administration\Système\Service de temps Windows\Fournisseurs
     de temps\Activer le client NTP Windows
Configuration ordinateur\Modèles d'administration\Système\Service de temps Windows\Fournisseurs
     de temps\Configurer le client NTP Windows
```

Listing 3 – Stratégie de configuration du service de temps Windows

Les paramètres recommandés pour la configuration du client NTP Windows sont indiqués par le tableau 1 (à l'exception du DC ayant le rôle FSMO de *PDC Emulator*, qui fait l'objet de la section A.2).

| Paramètre | Valeur |
|---|---|
| `NtpServer`[a] | |
| `Type` | NT5DS |
| `CrossSiteSyncFlags` | 2 |
| `ResolvePeerBackoffMinutes` | Au choix de l'entité |
| `ResolvePeerBackoffMaxTimes` | Au choix de l'entité |
| `SpecialPollInterval` | Au choix de l'entité |
| `EventLogFlags`[b] | 0x2 |

[a] Pour les ordinateurs membres d'un domaine AD, ce paramètre est ignoré lorsque la valeur `Type` est définie à NT5DS.

[b] Le paramètre `EventLogFlags` peut être modifié pour ne rien journaliser (valeur `0x0`) ou pour journaliser les décalages d'horloge (valeur `0x1`, sachant que les décalages notables restent quoi qu'il en soit journalisés sous forme d'avertissement), les changements de source de temps (valeur `0x2`) ou bien les deux (valeur `0x3`). Les évènements du service de temps Windows sont journalisés dans le journal système depuis la source « Time-Service ».

Tableau 1 – Paramètres par défaut et recommandés de la stratégie de configuration du client NTP Windows

## A.2 Configuration du PDC Emulator du domaine racine de la forêt

En environnement AD, le DC ayant le rôle FSMO [22] de *PDC Emulator* du domaine racine d'une forêt AD devrait être le seul à synchroniser son horloge avec les serveurs NTP de référence, qu'il s'agisse de serveurs NTP internes au SI ou publics sur Internet.

La procédure de configuration à suivre sur le *PDC Emulator* est documentée dans l'article [32] de Microsoft. La commande *batch* du listing 4 permet par exemple de configurer le DC ayant le rôle FSMO de *PDC Emulator* pour l'utilisation des serveurs NTP ayant pour noms `0.fr.pool.ntp.org` et `1.fr.pool.ntp.org` (des adresses IP peuvent également être renseignées si nécessaire).

```
w32tm /config /manualpeerlist:"0.fr.pool.ntp.org 1.fr.pool.ntp.org" /syncfromflags:MANUAL
/reliable:yes /update
```

Listing 4 – Commande de configuration d'une liste de serveurs NTP

Le statut de synchronisation NTP peut ensuite être interrogé avec la commande du listing 5.

```
w32tm /query /status
```

Listing 5 – Commande de vérification de la synchronisation d'horloge

### Information

Si la synchronisation NTP doit *in fine* se faire auprès de serveurs NTP publics sur Internet, la liste de serveurs NTP français proposée par le réseau RENATER [9] est dans ce cas fortement recommandée : `0.fr.pool.ntp.org`, `1.fr.pool.ntp.org`, `2.fr.pool.ntp.org` et `3.fr.pool.ntp.org`.

S'il est préféré de procéder à la configuration NTP du *PDC Emulator* par GPO pour faciliter tout transfert ultérieur de ce rôle FSMO, il est à noter que le filtre WMI du listing 6 permet de cibler spécifiquement le DC portant ce rôle. Cette GPO ne doit être liée qu'à l'unité organisationnelle des DC.

```
Select * from Win32_ComputerSystem where Domainrole=5
```

Listing 6 – filtre WMI de ciblage du DC portant le rôle de *PDC Emulator*

Dans le cas spécifique des réseaux isolés, il n'est pas possible de synchroniser les serveurs avec des sources de temps sur Internet. En revanche, il est indispensable que les équipements soient synchronisés sur les mêmes sources de temps internes cohérentes entre elles. L'utilisation de sources de temps autonomes (de type GPS par exemple) est alors à envisager.

# Annexe B
# Journaux Windows utiles aux activités de détection et d'analyse

## B.1 Service de journal d'évènements Windows

En prérequis, il est à noter que le service Windows « Journal d'évènements Windows » (de nom court `EventLog`) est chargé de la journalisation des évènements de certains programmes et composants du système. Bien que ce service Windows soit en démarrage automatique par défaut, cela peut avoir été modifié à l'installation du système ou par la suite. Dans certains contextes, il peut donc être utile de s'assurer de son démarrage automatique. Cela peut par exemple se faire de manière centralisée à l'aide d'une GPO appliquée à tous les ordinateurs du domaine AD (incluant les DC). La stratégie à utiliser est précisée par le listing 7.

```
Configuration Ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Services
    systèmes\Journal d'évènements Windows
```

Listing 7 – Stratégie de démarrage du service « Journal d'évènements Windows »

## B.2 Liste des journaux utiles

À la date de rédaction de ce guide, les journaux Windows et des services et applications listés dans le tableau 2 présentent une importance pour les activités de détection et d'analyse. Leur intégrité et leur disponibilité devraient donc être assurées conformément aux recommandations du présent guide. Cette liste n'est pas exhaustive et chaque entité devrait identifier les autres journaux qui sont pertinents pour la sécurité de ses SI, qu'il s'agisse de journaux de Microsoft ou de tout autre éditeur de solution logicielle tierce déployée sur les systèmes (antivirus, contrôle des périphériques amovibles, etc.). Il est par ailleurs à noter que si la majorité de ces journaux sont activés par défaut sous Windows 10 (21H2 à date de publication de ce guide) et Windows Server 2019, quelques-uns ne le sont pas et devraient être expressément activés afin que les évènements associés soient journalisés ; cette précision est indiquée par des appels de note dans le tableau 2. L'activation des journaux désactivés est quant à elle abordée en section B.3.

| Journal | Systèmes cibles |
|---|---|
| Journaux historiques | |
| Application | Tous les systèmes |
| Installation | Tous les systèmes |
| Sécurité | Tous les systèmes |
| Système | Tous les systèmes |
| Journaux des services et applications | |
| Microsoft-Windows-Application-Experience/Program-Inventory | Tous les systèmes où le *Software Inventory Logging* [38] est mis en œuvre |
| Microsoft-Windows-AppLocker/* | Tous les systèmes sur lesquels une stratégie AppLocker est active |
| Microsoft-Windows-Authentication/*-DomainController[a] | Tous les serveurs contrôleurs de domaine AD |
| Microsoft-Windows-Authentication/ProtectedUser-Client[a] | Tous les systèmes |
| Microsoft-Windows-Bits-Client/Operational | Tous les systèmes |
| Microsoft-Windows-CodeIntegrity/Operational | Tous les systèmes |
| Microsoft-Windows-DeviceGuard/Operational | Tous les systèmes |
| Microsoft-Windows-DriverFrameworks-UserMode/*Operational[a] | Tous les systèmes |
| Microsoft-Windows-Kernel-PnP/Configuration | Tous les systèmes |
| Microsoft-Windows-NetworkProfile/Operational | Tous les systèmes qui peuvent se trouver en situation de nomadisme |
| Microsoft-Windows-NTLM/Operational | Tous les systèmes |
| Microsoft-Windows-PowerShell/Operational | Tous les systèmes |
| Microsoft-Windows-PrintService/Operational[a] | Tous les systèmes |
| Microsoft-Windows-Security-Mitigations/* | Tous les systèmes |
| Microsoft-Windows-SmartCard-Audit/Authentication | Tous les systèmes utilisant des cartes à puce |
| Microsoft-Windows-SMBClient/Operational | Tous les systèmes |
| Microsoft-Windows-SMBClient/Security | Tous les systèmes |
| Microsoft-Windows-SMBServer/Audit | Tous les systèmes |
| Microsoft-Windows-SMBServer/Security | Tous les systèmes |
| Microsoft-Windows-TaskScheduler/Operational | Tous les systèmes |
| Microsoft-Windows-TerminalServices-*/*[b] | Tous les systèmes exécutant les services *Terminal Services* |

Ce tableau se poursuit sur la page suivante

| Journal | Systèmes cibles |
|---|---|
| Microsoft-Windows-VPN-Client/Operational | Tous les systèmes utilisant le client VPN intégré de Windows ou d'éditeurs tiers qui utilisent ce journal |
| Microsoft-Windows-Wired-AutoConfig/Operational | Lorsque du 801.1x est mis en œuvre sur le réseau filaire |
| Microsoft-Windows-WLAN-AutoConfig/Operational | Tous les systèmes équipés d'une interface WiFi |
| Microsoft-Windows/Win32k/Operational | Tous les systèmes |
| Microsoft-Windows-Windows Defender/* | Tous les systèmes |
| Microsoft-Windows-Windows Firewall With Advanced Security/Firewall | Tous les systèmes utilisant le pare-feu intégré à Windows |
| Microsoft-Windows-WindowsUpdateClient/Operational | Tous les systèmes |
| Microsoft-Windows-WMI-Activity/Operational | Tous les systèmes |
| Microsoft Office Alerts (OAlerts) | Tous les systèmes sur lesquels la suite logicielle Microsoft Office est déployée |
| Windows PowerShell | Tous les systèmes |
| Journaux des services et applications reposant sur des utilitaires non-natifs | |
| Autoruns | Tous les systèmes sur lesquels s'applique une stratégie de journalisation reposant sur l'utilitaire *Autoruns* (si utilisé) |
| Microsoft-Windows-sysmon/Operational | Tous les systèmes sur lesquels s'applique une stratégie de journalisation reposant sur l'utilitaire *sysmon* (si utilisé) |

[a] Journaux non activés par défaut et dont l'activation est abordée en section B.3.

[b] Cette ligne fait référence à tous les journaux du service « `Terminal Services` », incluant « `LocalSessionManager` », « `RemoteConnectionManager` », etc.

Tableau 2 – Journaux Windows utiles aux activités de détection et d'analyse

## B.3 Activation des journaux désactivés par défaut

L'activation d'un journal peut se faire par commande *batch* à l'aide de l'outil `WEVTUtil` [49] comme indiqué par le listing 8 ci-dessous. Ces commandes peuvent être exécutées sur les images système avant leur déploiement.

```
# Renseigner le nom du journal à activer
wevtutil sl "Microsoft-Windows-DNS-Client/Operational" /enabled:true
```

Listing 8 – Activation d'un journal par commande *batch*

L'activation d'un journal peut également se faire à l'aide de l'outil de gestion de parc interne ou par GPP (*Group Policy Preferences* [23]) en utilisant la clé de registre du listing 9, de type `REG_DWORD` et qui doit dans ce cas être configurée avec la valeur `1` comme illustré par la figure 3.

```
HKLM:\Software\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-DNS-Client/Operational\Enabled
```

Listing 9 – Activation d'un journal par GPP

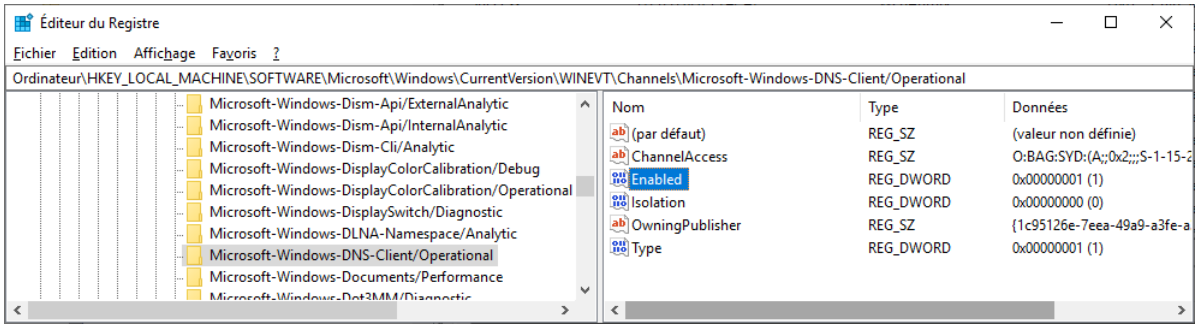


FIGURE 3 – Valeur de clé de registre pour l'activation d'un journal

Enfin, un script PowerShell est proposé au téléchargement sur GitHub [17] pour, entre autres, automatiser l'activation des journaux du tableau 2.

# B.4 Compléments de journalisation utiles

## B.4.1 Entrées de scripts PowerShell

La journalisation de toutes les entrées de scripts PowerShell est un complément d'information utile aux activités de détection et d'analyse. L'activation du paramètre de GPO indiqué par le listing 10 permet de journaliser les entrées de scripts PowerShell dans le journal des événements `Microsoft-Windows-PowerShell/Operational` (qui figure dans le tableau 2). Windows PowerShell enregistrera alors le traitement des commandes, les blocs de scripts, les fonctions et les scripts – qu'ils soient appelés de manière interactive ou par le biais de l'automatisation.

```
Configuration Ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows
    Powershell\Activer la journalisation de blocs de scripts Powershell
```

Listing 10 – Stratégie d'activation de la journalisation des entrées de scripts Powershell

### Attention

Les informations journalisées par ce biais devraient être considérées comme sensibles dans la mesure où des scripts PowerShell exécutés sur les systèmes peuvent contenir des informations sensibles. Il convient dans ce cas de modifier le descrip-

teur de sécurité du journal `Microsoft-Windows-PowerShell/Operational` pour empêcher sa lecture par tout le monde.

Pour ce faire, il est recommandé d'appliquer le descripteur de sécurité (au format SDDL [37]) du journal de sécurité au journal `Microsoft-Windows-PowerShell/Operational`. Cela peut se faire par PowerShell tel qu'illustré par le listing 11.

Il convient toutefois de préciser que cela pourrait ne pas suffire si des scripts PowerShell exécutés sur les systèmes sont susceptibles de contenir des informations qui permettraient de réaliser des élévations de privilèges sur le SI (ie : des secrets d'authentification privilégiés). La journalisation de toutes les entrées de scripts PowerShell ne doit donc être activée qu'en cas de certitude que cette mauvaise pratique n'a pas cours et après évaluation du risque.

```
# Chemin du journal Microsoft-Windows-PowerShell/Operationnal
$Path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\winevt\Channels\Microsoft-Windows-PowerShell/Operational'
# Copie du SDDL du journal de sécurité
$Sddl = ((wevtutil gl security) -like 'channelAccess*').Split(' ')[1]
# Application au SDDL du journal Microsoft-Windows-PowerShell/Operational
Set-ItemProperty -Path $Path -Name ChannelAccess -Value $Sddl
```

Listing 11 – Modification du descripteur de sécurité d'un journal

Le script PowerShell du listing 11 pour la modification du descripteur de sécurité du journal `Microsoft-Windows-PowerShell/Operational` est également proposé au téléchargement sur GitHub [16].

## B.4.2 Événements spécifiques à l'exécution de nouveaux processus

Il est utile de compléter les évènements 4688 du journal de sécurité – qui sont spécifiques à l'exécution de nouveaux processus – en incluant la ligne de commande de leur création. Cela peut se faire en activant le paramètre de GPO indiqué par le listing 12.

```
Configuration Ordinateur\Stratégies\Modèles d'administration\Système\Auditer la création
     de processus\Inclure la ligne de commande dans les événements de création de processus
```

Listing 12 – Stratégie d'activation de la journalisation des lignes de commande dans les événements de création de processus

### Attention

La journalisation des lignes de commande de création de nouveaux processus peut parfois journaliser des informations sensibles. C'est le cas par exemple lorsque les administrateurs exécutent des commandes contenant des mots de passe en clair : en cas d'élévation locale de privilèges, un attaquant gagnant l'accès en lecture au journal de sécurité pourrait ainsi trouver dans les évènements 4688 des informations lui permettant de réaliser des élévations de privilèges sur le SI. La journalisation des lignes de commande de création de nouveaux processus ne doit donc être activée qu'en cas de certitude que cette mauvaise pratique n'a pas cours et après évaluation du risque.

### B.4.3 Fichiers potentiellement malveillants détectés par Microsoft Windows Defender

Lorsque *Microsoft Windows Defender* est utilisé sur les systèmes, il est utile de compléter les évènements de détection des fichiers potentiellement malveillants de manière à ce que soient également journalisées leurs empreintes (conformément aux recommandations du guide générique sur la journalisation [6]). Cela peut se configurer par le registre sur les systèmes journalisés à l'aide de l'outil de gestion de parc interne ou par GPP. La clé de registre du listing 13, de type `REG_DWORD`, doit dans ce cas être configurée avec la valeur `1` [40].

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\ThreatFileHashLogging
```

Listing 13 – Valeur de clé de registre pour la journalisation des empreintes par Microsoft Windows Defender

# Annexe C
# Configuration des journaux Windows

## C.1 Journaux Windows historiques

Les paramètres de GPO permettant l'application de la recommandation R5 pour la rotation des journaux Windows sont situés à l'emplacement précisé par le listing 14. Les valeurs minimales recommandées par l'ANSSI, pour le stockage des journaux sur les systèmes Windows, sont quant à elles indiquées dans le tableau 3.

```
Configuration ordinateur\Modèles d'administration\Composants Windows\Service Journal des
    évènements\
```

Listing 14 – Emplacement des stratégies de configuration du service Journal des évènements

| Stratégies du service « Journal des évènements » | Recommandation |
|---|---|
| Application | |
| Contrôler le comportement du journal des évènements lorsque le fichier journal atteint sa taille maximale | Désactivé[a] (valeur par défaut) |
| Spécifier la taille de fichier journal maximale (Ko) | 51200 (50 Mo) |
| Sécurité | |
| Contrôler le comportement du journal des évènements lorsque le fichier journal atteint sa taille maximale | Désactivé (valeur par défaut) |
| Spécifier la taille de fichier journal maximale (Ko) | 409600 (400 Mo) sur les PC<br>1048576 (1 Go) sur les serveurs |
| Système | |
| Contrôler le comportement du journal des évènements lorsque le fichier journal atteint sa taille maximale | Désactivé (valeur par défaut) |
| Spécifier la taille de fichier journal maximale (Ko) | 51200 (50 Mo) |

[a] La désactivation de ce paramètre indique que les nouveaux évènements remplacent les anciens lorsque le fichier journal a atteint sa taille maximale.

Tableau 3 – Paramètres recommandés des stratégies de configuration du service Journal des évènements

### Information

Les tailles de fichiers de journaux Windows indiquées par le tableau 3 sont volontairement grandes pour être amplement suffisantes et adaptées à la plupart des contextes. Ces tailles permettent généralement de stocker au moins 6 mois de journaux sur les systèmes, serveurs ou postes de travail. Une revue régulière devrait toutefois être faite pour adapter les stratégies d'audit et la taille des journaux à l'activité réellement constatée des systèmes journalisés, dans l'optique de les rendre cohérentes avec la vitesse de remplissage.

Lorsqu'une centralisation des évènements vers des serveurs de collecte est mise en œuvre, une telle durée de rétention n'est pas nécessaire sur les systèmes puisque la problématique de stockage des évènements est déportée vers les équipements qui les centralisent.

Les serveurs assurant les rôles de DC, ADFS, *Microsoft Exchange* ou de serveur de fichiers sont la cible d'un volume d'authentifications bien supérieur aux autres serveurs. Une attention spécifique à la durée de rétention des journaux de ces machines devra être accordée si leurs journaux ne sont pas centralisés.

### Information

Il est recommandé par le guide générique sur la journalisation [6] de dédier une partition aux journaux lorsque la taille de ces derniers n'ont pas une taille maximale fixée. Lorsque la stratégie de rotation configurée sous Windows est celle par défaut, les journaux ont une taille fixe avec écrasement des évènements les plus anciens et cette recommandation n'est donc pas applicable.

## C.2 Journaux des services et applications

La taille par défaut des journaux de services et applications est généralement de 1 Mo, ce qui est suffisant lorsqu'une centralisation complète des évènements journalisés est mise en œuvre. Dans le cas contraire, il est généralement préférable d'augmenter la taille de certains d'entre eux. Par simplicité et pour éviter de configurer des tailles au cas par cas, tous les journaux qui figurent dans le tableau 2 devraient idéalement avoir une taille de 20 Mo. Pour ce faire, il n'existe toutefois aucune stratégie de groupe similaire à celle du listing 14 de redimensionnement des journaux Windows historiques.

Il est néanmoins possible de procéder par commandes *batch* sur chaque système, comme illustré par le listing 15 à l'aide de l'outil `WEVTUtil` [49].

```
# Renseigner le nom du journal à redimensionner
# Ici l'argument ms (maxsize) indique une taille de 20 MB (exprimée en octets).
wevtutil sl "Microsoft-Windows-Windows Defender/Operational" /ms:20971520
```

Listing 15 – Redimensionnement d'un journal par commande *batch*

Ces commandes peuvent être exécutées sur les images système avant leur déploiement. Cela peut aussi bien être fait *a posteriori* à l'aide, par exemple, d'une tâche planifiée ou à exécution immédiate créée par GPO (pour plus de détails sur l'exécution de scripts sur les systèmes d'une manière

centralisée par GPO, se référer aux exemples de l'annexe E). Une autre méthode peut consister à configurer des valeurs de registre par l'outil de gestion de parc interne ou par GPP ; la valeur `MaxSize` de type `REG_DWORD` prend dans ce cas une valeur en octets, comme illustré par la figure 4. Ces méthodes sont équivalentes, il convient de privilégier celle qui est la plus maîtrisée par les administrateurs.

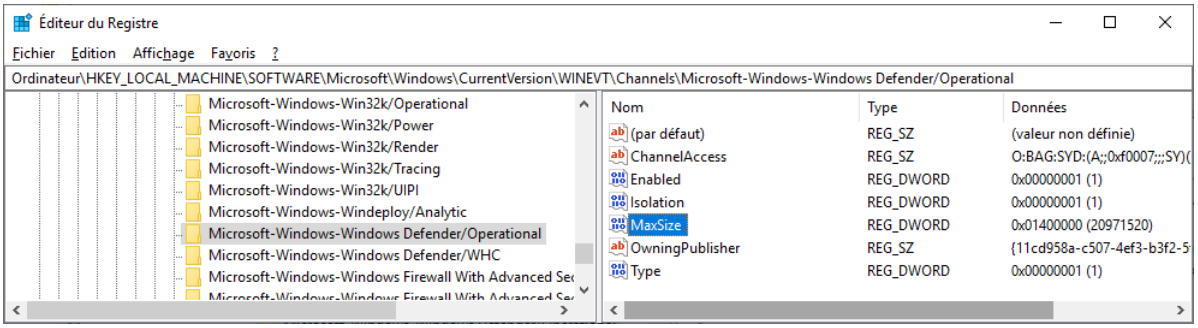


FIGURE 4 – Valeur de registre `MaxSize` d'un fichier de journal

Pour finir, un script PowerShell est proposé au téléchargement sur GitHub [17] pour, entre autres, automatiser le redimensionnement des journaux du tableau 2.

# Annexe D
# Configuration des stratégies d'audit de Windows

## D.1 Configuration centralisée des stratégies d'audit de Windows

Les stratégies d'audit peuvent se configurer par GPO :

- de manière simple à l'aide des stratégies d'audit de base qui existent depuis Windows 2000 (à l'emplacement indiqué par le listing 16) ;
- de manière plus fine et de la manière recommandée dans ce guide, à l'aide des stratégies d'audit avancées introduites dans Windows Vista et Windows Server 2008 (à l'emplacement précisé par le listing 17).

```
Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\
     Stratégie d'audit
```

Listing 16 – Stratégies d'audit de base

```
Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Configuration
     avancée de la stratégie d'audit\Stratégies d'audit système - Objet Stratégie de groupe
```

Listing 17 – Stratégies d'audit avancées

Il est à noter que les journaux générés par ces stratégies d'audit sont enregistrés dans le journal de sécurité des évènements Windows.

### Information

Lorsque des paramètres de stratégie d'audit sont appliqués par GPO, les paramètres de stratégie d'audit de l'ordinateur local de même catégorie sont effacés avant que les paramètres spécifiés par la GPO ne soient appliqués. Les stratégies d'audit appliquées par GPO, qu'elles soient de base ou avancées, remplacent alors les stratégies d'audit de l'ordinateur local.

Comme indiqué par l'article [20] de Microsoft, les stratégies d'audit de base et les stratégies d'audit avancées sont similaires et se recouvrent.

Les stratégies d'audit de base sont au nombre de neuf depuis Windows 2000. Depuis Windows Vista, chacune est également divisée en sous-catégories d'audit avancées, afin de pouvoir sélectionner plus finement quels évènements doivent être générés. L'utilisation des stratégies d'audit avancées apportent donc une finesse de configuration que les stratégies d'audit de base n'apportent pas.

### Attention

Le paramétrage conjoint de stratégies d'audit de base et de stratégies d'audit avancées est déconseillé : il peut se traduire par des résultats inattendus. Pour l'éviter, il est recommandé d'activer le paramètre de GPO précisé par le listing 18.

```
Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\
    Options de sécurité\Audit: force les paramètres de sous-catégorie de stratégie d'audit
    (Windows Vista ou ultérieur) à se substituer aux paramètres de catégorie de stratégie d'audit
```

Listing 18 – Stratégies d'audit avancées

## D.2 Paramètres recommandés de configuration des stratégies d'audit de Windows

La granularité des stratégies d'audit avancées est nécessaire pour mettre en œuvre les recommandations de journalisation de l'ANSSI. Ces dernières figurent dans le tableau 4. Pour des questions de maintenabilité, il est recommandé d'appliquer la même stratégie d'audit avancée sur les différentes catégories de systèmes, qu'il s'agisse de postes de travail ou de serveurs membres d'un domaine AD, ou bien de contrôleurs de domaine.

Ces recommandations minimales peuvent être étendues si cela s'avère pertinent au regard des objectifs de sécurité fixés sur des systèmes ayant des rôles très spécifiques, comme par exemple sur des systèmes dédiés à l'administration du SI. Il reste néanmoins recommandé de tester toute stratégie d'audit avant sa mise en production, afin de s'assurer que les journaux ne soient pas saturés trop rapidement.

| Stratégie d'audit avancée | Recommandation |
|---|---|
| Connexion de compte | |
| Auditer la validation des informations d'identification | Réussite[a] et échec |
| Auditer le service d'authentification Kerberos | Réussite et échec |
| Auditer les opérations de ticket de service Kerberos | Réussite et échec |
| Auditer d'autres évènements d'ouverture/fermeture de session | Réussite et échec |
| Gestion du compte | |
| Auditer la gestion des groupes d'applications | Pas d'audit |

Ce tableau se poursuit sur la page suivante

| Stratégie d'audit avancée | Recommandation |
|---|---|
| Auditer la gestion des comptes d'ordinateur | Réussite et échec |
| Auditer la gestion des groupes de distribution | Pas d'audit |
| Auditer d'autres évènements de gestion des comptes | Réussite et échec |
| Auditer la gestion des groupes de sécurité | Réussite et échec |
| Auditer la gestion des comptes d'utilisateur | Réussite et échec |
| Suivi détaillé | |
| Auditer l'activité DPAPI | Réussite et échec |
| Auditer l'activité Plug-and-Play (PNP) | Réussite |
| Auditer la création du processus | Réussite et échec |
| Auditer la fin du processus | Pas d'audit |
| Auditer les évènements RPC | Pas d'audit |
| Jeton d'audit ajusté à droite[b] | Pas d'audit[c] |
| Accès au service d'annuaire | |
| Auditer la réplication du service d'annuaire détaillé | Réussite et échec |
| Auditer l'accès au service d'annuaire | Réussite et échec |
| Auditer les modifications du service d'annuaire | Réussite et échec |
| Auditer la réplication du service d'annuaire | Réussite et échec |
| Connexion/déconnexion | |
| Auditer le verrouillage du compte | Réussite et échec |
| Auditer les revendications utilisateur/de périphérique | Pas d'audit |
| Auditer le mode étendu IPsec | Pas d'audit |
| Auditer l'appartenance à un groupe | Pas d'audit |
| Auditer le mode principal IPsec | Pas d'audit |
| Auditer le mode rapide IPsec | Pas d'audit |
| Auditer la fermeture de session | Réussite |
| Auditer l'ouverture de session | Réussite et échec |
| Auditer le serveur NPS (*Network Policy Server*) | Réussite et échec |
| Auditer d'autres évènements d'ouverture/fermeture de session | Réussite et échec |
| Auditer l'ouverture de session spéciale | Réussite |
| Accès aux objets | |
| Auditer l'application générée | Pas d'audit |
| Auditer les services de certification | Réussite et échec |
| Auditer le partage de fichiers détaillé | Réussite |

Ce tableau se poursuit sur la page suivante

| Stratégie d'audit avancée | Recommandation |
|---|---|
| Auditer le partage de fichiers | Réussite et échec |
| Auditer le système de fichiers | Échec |
| Auditer la connexion de la plateforme de filtrage | Échec |
| Auditer le rejet de paquet par la plateforme de filtrage | Pas d'audit |
| Auditer la manipulation de *handle* | Pas d'audit |
| Auditer l'objet de noyau | Pas d'audit |
| Auditer d'autres évènements d'accès à l'objet | Réussite et échec |
| Auditer le Registre | Pas d'audit |
| Auditer le stockage amovible | Réussite et échec |
| Auditer SAM | Pas d'audit |
| Auditer la stratégie d'accès centralisée intermédiaire | Pas d'audit |
| Modification de la stratégie | |
| Auditer la modification de la stratégie d'audit | Réussite et échec |
| Auditer la modification de la stratégie d'authentification | Réussite et échec |
| Auditer la modification de la stratégie d'autorisation | Réussite et échec |
| Auditer la modification de la stratégie de plateforme de filtrage | Réussite et échec |
| Auditer la modification de la stratégie de niveau règle MPSSVC | Échec |
| Auditer d'autres évènements de modification de stratégie | Pas d'audit |
| Utilisation des privilèges | |
| Auditer l'utilisation des privilèges non sensibles | Pas d'audit |
| Auditer l'utilisation de privilèges sensibles | Pas d'audit |
| Auditer d'autres évènements d'utilisation de privilèges | Réussite et échec |
| Système | |
| Auditer le pilote IPSEC | Réussite et échec |
| Auditer d'autres évènements système | Réussite et échec |
| Auditer la modification de l'état de la sécurité | Réussite |
| Auditer l'extension du système de sécurité | Réussite et échec |
| Auditer l'intégrité du système | Réussite et échec |

[a] Attention : sur un contrôleur de domaine AD, il n'est pas recommandé de journaliser les authentifications réussies, sauf de manière exceptionnelle, car cela génère un important volume d'évènements.

[b] Il s'agit d'une mauvaise traduction de Microsoft pour « l'ajustement des privilèges d'un jeton d'authentification ».

[c] Journaliser les réussites est intéressant mais s'avère trop verbeux au regard de la valeur ajoutée de ces évènements.

Tableau 4 – Stratégies d'audit avancées recommandées par l'ANSSI pour les systèmes Windows

## D.3 Particularités concernant l'audit de l'accès global aux objets

Une catégorie particulière de stratégies d'audit avancées doit être considérée à part : la catégorie « Audit de l'accès global aux objets » (n'apparaissant pas dans le tableau 4) qui permet de configurer des stratégies d'audit pour l'ensemble du système de fichiers ou du registre.

### Attention

L'audit de l'accès global aux objets est un outil puissant mais extrêmement verbeux. Son activation et la collecte subséquente ne doivent être entreprises que dans un environnement de détection mature incluant une connaissance des volumétries générées et un test de charge.

Ces stratégies fonctionnent différemment des autres stratégies d'audit avancées dans la mesure où elles se configurent en créant des règles explicites, sous forme d'ACE (*Access Control Entry*), chacune spécifiant un triplet :

- *principal* de sécurité (un compte utilisateur en particulier, un groupe d'utilisateurs, un compte d'ordinateur, etc.) ;
- type d'accès : réussite, échec ou les deux ;
- autorisations à journaliser (lire, écrire, changer le propriétaire, supprimer, etc.).

Il est toutefois important de préciser que l'intérêt de ces stratégies réside dans leur application à l'ensemble du système de fichiers et/ou du registre. Une vigilance toute particulière doit donc être portée aux règles créées de sorte qu'elles ne génèrent pas une trop importante volumétrie d'évènements (ce serait par exemple le cas d'une règle d'audit des accès en lecture sur le registre pour tout le monde) et soient suffisamment précises pour ne fournir que des informations essentielles. Ces règles d'audit de l'accès global aux objets sont donc généralement utilisées de manière ponctuelle pour du débogage, de l'analyse système ou dans le cadre d'un audit par exemple.

### Information

Pour que les règles d'audit de l'accès global aux objets soient réellement appliquées, il est nécessaire que les stratégies d'audit avancées « Auditer le système de fichiers » ou « Auditer le registre » de la catégorie « Accès aux objets » soient activées elles aussi.

Les règles d'audit d'accès global au système de fichiers sont illustrées par la figure 5 tandis que les règles d'audit d'accès global au registre sont illustrées par la figure 6.

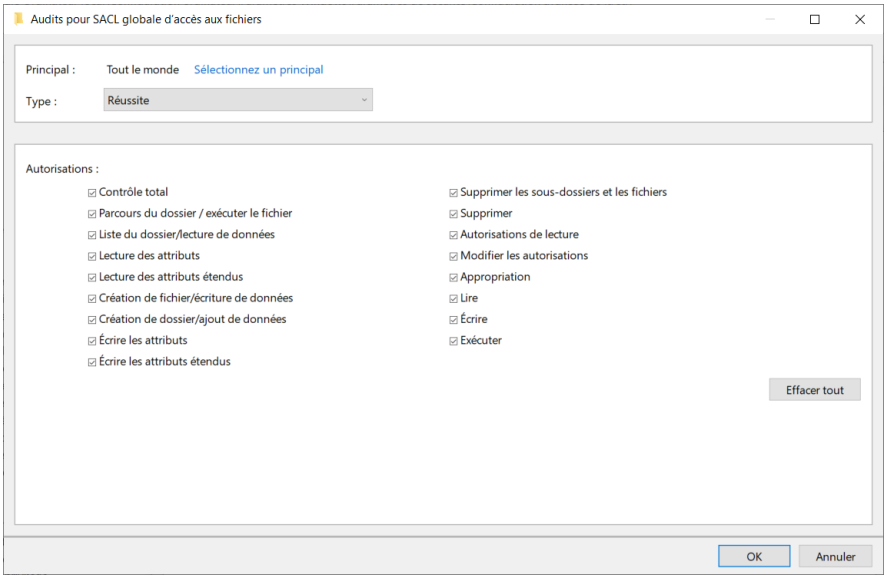


FIGURE 5 – Règle d'audit d'accès global au système de fichiers

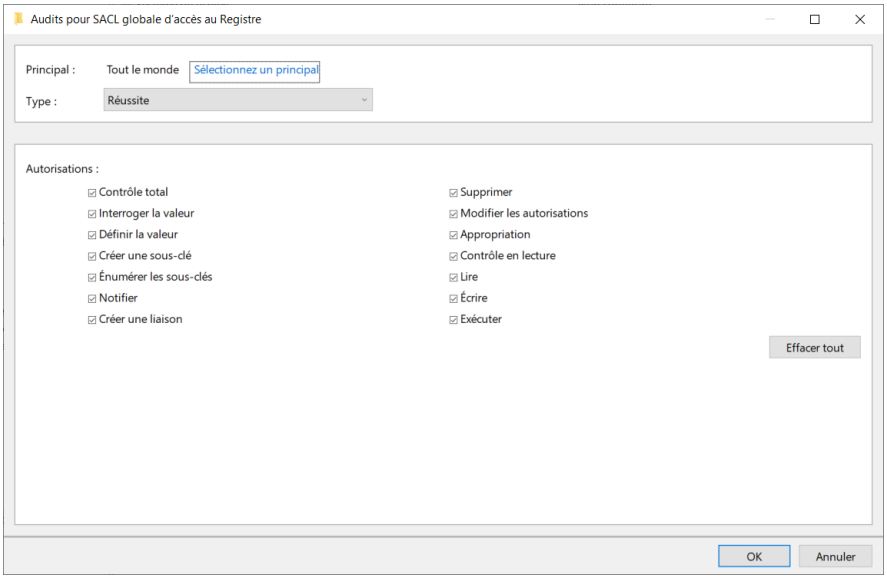


FIGURE 6 – Règle d'audit d'accès global au registre

Comme les stratégies d'audit d'accès global manquent de finesse, il est rare qu'elles soient activées de manière permanente sur un système. La configuration de différentes SACL [19] (*System Access Control List*) d'audit sur des dossiers, fichiers ou clés de registre à surveiller explicitement reste dans ce cas une alternative souvent préférable. Cette alternative permet de limiter davantage la volumétrie des évènements générés et de ne collecter que les informations strictement essentielles. Des SACL d'audit peuvent ainsi tout-à-fait être utilisées de manière permanente afin de journaliser des accès spécifiques. Chaque SACL se compose alors d'un ensemble d'entrées (les ACE mentionnées en section D.3).

## Information

Les SACLs d'audit se configurent directement dans les propriétés des objets à surveiller (fichier, dossier, clé de registre, etc.) et non pas via les stratégies d'audit par GPO. Néanmoins, il est nécessaire que les stratégies d'audit avancées « Auditer le système de fichiers » ou « Auditer le registre » de la catégorie « Accès aux objets » soient activées sinon les SACL configurées n'enregistrent aucun évènement d'accès.

L'utilisation des SACL est intéressante à plusieurs égards. Elle permet notamment de journaliser des accès autorisés à des fichiers considérés comme sensibles d'un point de vue métier. Un cas de figure récurrent concerne par exemple les fichiers de gestion de ressources humaines qui contiennent des informations sensibles sur les salariés. En positionnant des SACL en lecture sur ces fichiers, il est ainsi possible de contrôler les accès qui y sont faits et d'en vérifier l'adéquation avec le besoin d'en connaître à un moment donné. Par un traitement automatisé des journaux, il est ensuite envisageable de générer des rapports d'accès pouvant être envoyés par courriel aux responsables de leur revue. Dans une certaine mesure, l'utilisation des SACL peut s'inscrire dans une démarche globale de prévention des fuites de données (DLP, *Data Leakage Prevention*). Il convient toutefois de préciser que l'utilisation des SACL peut générer une grande quantité d'évènements. La figure 7 représente une SACL positionnée sur un fichier, composée d'une seule ACE qui configure la journalisation des accès en lecture ou en exécution réalisés par un compte utilisateur quelconque (compte du domaine ou compte local). Une SACL génère un évènement 4663 lors de toute tentative d'accès qui correspond aux ACE définies. L'évènement 4663 est détaillé dans la documentation [36] de Microsoft.

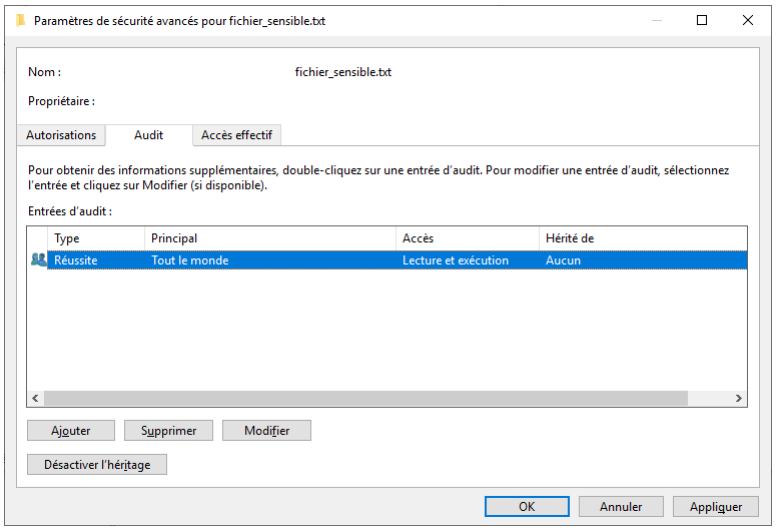


FIGURE 7 – SACL pour journaliser les accès en lecture à un fichier

# Annexe E
# Déploiement et configuration de sysmon par GPO

*Sysmon* est un utilitaire mis à disposition par Microsoft comme simple binaire au format `.exe`. Sans solution tierce de télé-déploiement de logiciels (SCCM [7], WAPT [8], etc.), il ne peut pas être déployé aussi simplement qu'un paquet d'installation au format `.msi`.

Il est fortement recommandé de s'appuyer sur l'outillage interne de télé-déploiement pour un déploiement de *sysmon*. En effet, ce dernier permet de disposer d'un suivi des déploiements et une intégration dans les processus standards du SI. La procédure ci-dessous, reposant sur les GPO nativement disponibles en environnement AD, n'a vocation qu'à illustrer les problématiques ayant trait à son télé-déploiement dans un format accessible à tous.

Pour un télé-déploiement par GPO en environnement AD, il est nécessaire de recourir à un script en langage « batch » ou « PowerShell ». Ce script peut alors être exécuté au démarrage du système ou par tâche planifiée ou à exécution immédiate.

Aucun modèle d'administration (fichier `.admx`) ne facilite par ailleurs la configuration centralisée de *sysmon* par GPO, obligeant ainsi les administrateurs à recourir à différentes méthodes de déploiement de sa configuration. L'objectif de cette annexe est de couvrir ces deux aspects : déploiement et mise à jour du service *sysmon* sur les systèmes, puis déploiement et mise à jour de sa configuration.

## E.1 Déploiement du service sysmon sur les systèmes

Il existe de nombreuses manières de procéder au déploiement de *sysmon* par GPO. Celle illustrée dans cette section en est une parmi d'autres, reposant sur une GPP de création de tâche à exécution immédiate (sous-section E.1.1). Cet exemple de tâche est chargé d'exécuter un script PowerShell de déploiement de *sysmon* depuis un partage réseau (sous-section E.1.2). Pour exécuter cette tâche uniquement sur les systèmes qui le nécessitent, des éléments de ciblage de la GPP sont également proposés (sous-section E.1.3). Il est à noter que l'outil de gestion de parc interne déployé sur le SI est à utiliser de préférence s'il permet d'implémenter les subtilités de déploiement et de configuration de *sysmon* détaillées dans cette section.

7. *System Center Configuration Manager* de Microsoft.
8. *Windows Advanced Packaging Tool* de Tranquil IT Systems.

### E.1.1 Tâche à exécution immédiate

La tâche proposée comme exemple dans cette annexe s'exécute dans le contexte du compte utilisateur intégré `NT AUTHORITY\SYSTEM` avec les privilèges les plus élevés sur le système local. Il exécute le programme `powershell.exe` avec pour argument un lien vers le script ici stocké dans le partage réseau `SYSVOL` de l'AD. Le choix du partage `SYSVOL` permet de s'assurer que les droits d'écriture sont limités aux administrateurs du domaine, et que le script est accessible en lecture seule à tous les utilisateurs du domaine. Le partage `SYSVOL` est par ailleurs automatiquement répliqué sur tous les contrôleurs de domaine de l'AD, grâce aux mécanismes de réplication intégrés.

#### Attention

Il est imprudent de créer une tâche planifiée ou à exécution immédiate configurée pour s'exécuter avec un compte utilisateur à privilèges du domaine. Le mot de passe de ce dernier se trouve enregistré sur les systèmes et il est trivialement récupérable par un attaquant. Lorsque l'exécution de cette tâche nécessite des privilèges d'administration locaux ainsi qu'un accès à un partage réseau, ce qui est le cas pour le déploiement de *sysmon*, l'utilisation du compte `NT AUTHORITY\SYSTEM` est une bonne pratique à laquelle il convient de ne pas déroger.

#### Attention

Les emplacements des scripts de démarrage ainsi que des scripts exécutés par tâche planifiée ou à exécution immédiate (de même que tous les autres scripts et contenus exécutables que eux-mêmes appellent) dans un contexte de compte `NT AUTHORITY\SYSTEM` doivent être choisis avec vigilance. Seuls les comptes à plus hauts privilèges de l'AD doivent y avoir des droits d'accès en écriture. L'accès en écriture à ces emplacements par un individu malveillant aurait pour conséquence une possibilité d'exécution de code arbitraire privilégié sur les systèmes.

Bien que l'exécution du script d'installation de *sysmon* soit généralement rapide, l'avantage d'une tâche par rapport à un script de démarrage est que cette exécution n'est pas bloquante pour l'utilisateur et ne ralentira donc pas le démarrage du système ni l'ouverture de session utilisateur. Cette tâche peut être exécutée :

- dès que possible (mode par défaut) ;
- une fois que l'ordinateur est inactif ;
- après plusieurs secondes ou minutes d'attente, de manière à ne pas réaliser immédiatement les opérations susceptibles d'impacter les performances du système.

#### Information

Idéalement, une bonne pratique consiste à signer les scripts PowerShell [34]. Il n'est dans ce cas pas nécessaire de contourner la politique de sécurité par défaut de Windows pour l'exécution de scripts PowerShell (argument « `-ExecutionPolicy bypass` » utilisé dans l'action de la tâche à exécution immédiate décrite ci-dessous), les politiques d'exécution `RemoteSigned` ou `AllSigned` peuvent ainsi être utilisées.

> La signature des scripts PowerShell étant hors périmètre de ce guide, la tâche à exécution immédiate illustrée ci-dessous se contente de contourner la politique d'exécution par facilité. Pour plus d'informations sur la procédure de signature des scripts PowerShell, le lecteur est invité à consulter l'article [34] de Microsoft.

La tâche à exécution immédiate prise comme exemple dans cette annexe est créée avec les caractéristiques suivantes :

- elle s'exécute sous le compte `NT AUTHORITY\System` avec les privilèges les plus élevés, même si l'utilisateur n'est pas connecté ;
- elle ne démarre qu'à la condition que l'ordinateur soit relié au secteur ;
- elle s'arrête si elle s'exécute plus de 15 minutes ;
- elle a pour action de démarrer le programme `powershell` avec pour argument :
  `-ExecutionPolicy bypass -File \\ad.lan\SYSVOL\ad.lan\scripts\sysmon\GPO_C_sysmon_deployment.ps1`
  (le chemin et le nom du script PowerShell étant à personnaliser) ;
- elle est créée uniquement sur les systèmes qui requièrent son exécution (les éléments de ciblage qui permettent de réduire la portée de cette activation sont détaillés en sous-section E.1.3).

Cet exemple de tâche à exécution immédiate pour l'exécution de scripts PowerShell sur les systèmes est disponible au téléchargement sur GitHub [13] sous forme de fichier au format XML. Il peut être utilisé pour créer une tâche par simple import, à l'aide de la commande du listing 19.

```
schtasks /create /xml "un_fichier.xml" /tn "un nom de tâche"
```

Listing 19 – Commande *batch* d'import de tâche planifiée au format XML

## E.1.2 Script PowerShell de déploiement et de mise à jour

La tâche à exécution immédiate proposée en sous-section E.1.1 n'a qu'une seule action : exécuter un script PowerShell mis à disposition sur un partage réseau. Le script du listing 20 proposé comme exemple dans cette annexe permet de procéder à l'installation et la mise à jour du service *sysmon* sur les systèmes.

Ce script se décompose en plusieurs étapes :

1. initialiser les fonctions de journalisation (fonctions optionnelles mais recommandées) ;
2. vérifier si un service *sysmon* est déjà installé et le désinstaller le cas échéant ;
3. installer la version à jour de *sysmon* en tant que service, à partir des binaires mis à disposition sur un partage réseau (dans cet exemple, le partage `SYSVOL` est utilisé pour les mêmes raisons de sécurité et de réplication que le script PowerShell) et avec la configuration par défaut de *sysmon* (c'est-à-dire sans spécifier de fichier de configuration) ;
4. demander une nouvelle application des GPO, afin que la stratégie de déploiement centralisé de la configuration de *sysmon* (traitée en section E.2) soit appliquée dans la foulée.

```
# Ici, renseigner le partage contenant Sysmon :
$SysmonShare = "\\ad.LAN\SYSVOL\ad.lan\TOOLS\Sysmon"
# Ici, préciser une source pour les journaux générés par le script
$LogSource = "ANSSI.Sysmon"
# Ici, préciser un EventId de départ pour les évènements journalisés
$LogEventId = 64210

# Initialisation de la journalisation
New-EventLog -LogName System -Source $LogSource -ErrorAction SilentlyContinue
Write-EventLog -LogName System -Source $LogSource -EntryType Information -Message "Running Sysmon Service Deployment Script" `
  -EventId $LogEventId
# Si un service Sysmon est déjà installé
$RegKey = "Registry::HKLM\SYSTEM\CurrentControlSet\Services\Sysmon"
# Si l'option -d a été utilisée à l'installation de sysmon pour renommer le pilote, modifier la clé de registre ci-dessus
$RegKey64ImagePath = (Get-ItemProperty -Path ($RegKey + "64") -Name ImagePath).ImagePath
$RegKey32ImagePath = (Get-ItemProperty -Path $RegKey -Name ImagePath).ImagePath
$SysmonShareVersion = (get-Item ($SysmonShare + "\Sysmon.exe")).VersionInfo.FileVersion
if ($RegKey64ImagePath)
{
    # Si Sysmon est déjà à jour, l'exécution du script se termine
    # Si cela arrive, c'est que le filtre WMI de la GPP n'est pas bon car ce script n'aurait pas dû s'exécuter
    $SysmonLocalVersion = (Get-Item ($RegKey64ImagePath)).VersionInfo.FileVersion
    if ($SysmonShareVersion -eq $SysmonLocalVersion){
        Write-EventLog -LogName System -Source $LogSource -EntryType Error -Message "Sysmon64 is already up to date" `
           -EventId ($LogEventId + 1)
        exit
    }

    # Obtention du nom de pilote
    $RegKey64DriverName = (Get-ItemProperty -Path ($RegKey + "64\Parameters") -Name DriverName).DriverName

    # Désinstallation
    $UninstallOutput = & $RegKey64ImagePath -u force 2>&1
    # (NB : Si le format de sortie de Sysmon change, l'argument match ci-dessous doit être changé en conséquence)
    if (($UninstallOutput -match ('.*(' + $RegKey64DriverName + ' removed\.|Sysmon64 removed\.)')).count -eq 2)
    {
        Remove-Item $RegKey64ImagePath
        Write-EventLog -LogName System -Source $LogSource -EntryType Information -Message ("Sysmon64 v" + $SysmonLocalVersion `
            + " has been uninstalled successfully") -EventId ($LogEventId + 2)
    }
    else
    {
        Write-EventLog -LogName System -Source $LogSource -EntryType Error -Message ("Sysmon64 v" + $SysmonLocalVersion `
            + " uninstall failed") -EventId ($LogEventId + 3)
        exit 1
    }
}
elseif ($RegKey32ImagePath)
{
    # Si Sysmon est déjà à jour l'exécution du script se termine
    # Si cela arrive, c'est que le filtre WMI de la GPP n'est pas bon car ce script n'aurait pas dû s'exécuter
    $SysmonLocalVersion = (Get-Item ($RegKey32ImagePath)).VersionInfo.FileVersion
    if ($SysmonShareVersion -eq $SysmonLocalVersion){
        Write-EventLog -LogName System -Source $LogSource -EntryType Error -Message "Sysmon is already up to date" `
            -EventId ($LogEventId + 1)
        exit
    }

    # Obtention du nom de pilote
    $RegKey32DriverName = (Get-ItemProperty -Path ($RegKey + "\Parameters") -Name DriverName).DriverName

    # Désinstallation
    $UninstallOutput = & $RegKey32ImagePath -u force 2>&1
    # (NB : Si le format de sortie de Sysmon change, l'argument match ci-dessous doit être changé en conséquence)
    if (($UninstallOutput -match ('.*(' + $RegKey32DriverName + ' removed\.|Sysmon removed\.)')).count -eq 2)
    {
        Remove-Item $RegKey32ImagePath
        Write-EventLog -LogName System -Source $LogSource -EntryType Information -Message ("Sysmon v" + $SysmonLocalVersion `
            + " has been uninstalled successfully") -EventId ($LogEventId + 2)
    }
    else
    {
        Write-EventLog -LogName System -Source $LogSource -EntryType Error -Message ("Sysmon v" + $SysmonLocalVersion `
            + " uninstall failed") -EventId ($LogEventId + 3)
        exit 1
    }
}
# Installation du Sysmon à jour, sans configuration spécifiée (car appliquée ensuite par GPP de registre)
$if64 = if($env:PROCESSOR_ARCHITECTURE -like "*64*"){"64"}else{""}
$SysmonPath = $SysmonShare + "\Sysmon" + $if64 + ".exe"
$InstallOutput = & $SysmonPath -accepteula -i 2>&1
# (NB : Si le format de sortie de Sysmon change, l'argument match ci-dessous doit être changé en conséquence)
if (($InstallOutput -match '.*(installed\.|started\.)').count -eq 4)
{
    Write-EventLog -LogName System -Source $LogSource -EntryType Information -Message ("Sysmon" + $if64 + " v" `
        + $SysmonShareVersion + " has been installed successfully") -EventId ($LogEventId + 4)
}
else
{
    Write-EventLog -LogName System -Source $LogSource -EntryType Error -Message ("Sysmon" + $if64 + " v" `
        + $SysmonShareVersion + " install failed") -EventId ($LogEventId + 5)
}
# Application des GPO (pour mise à jour, dans la foulée, de la configuration de Sysmon par GPP de registre)
& gpupdate /target:computer
```

Listing 20 – Script PowerShell d'installation ou de mise à jour de *sysmon*

L'exemple de script PowerShell du listing 20 pour le déploiement automatisé de *sysmon* est également disponible au téléchargement sur GitHub [12].

### E.1.3 Ciblage de systèmes

Il est préférable de cibler précisément les systèmes qui nécessitent l'exécution de cette tâche à exécution immédiate, c'est-à-dire ceux qui n'ont pas de service *sysmon* ou qui en ont une ancienne version nécessitant une mise à jour. Sans cela, la tâche sera créée à chaque application des GPO (au démarrage du système puis toutes les deux heures par défaut) et le script PowerShell associé se trouvera exécuté de nombreuses fois sans nécessité. Il est à noter que cette problématique est la même pour une entité qui recourt à un outil de télé-déploiement tiers plutot que de procéder par GPO.

Cette sélection de systèmes non équipés du service *sysmon* ou qui nécessitent une mise à jour du binaire peut se faire par ciblage de la GPP. Pour ce ciblage, il est par exemple possible de considérer que :

1. *sysmon* est installé si la clé de registre de son service – indiquée par le listing 21 – existe ;
2. l'installation de *sysmon* se caractérise notamment par la copie du binaire `sysmon.exe` (version 32 bits) ou `sysmon64.exe` (version 64 bits) dans le dossier `C:\Windows\`. La propriété *FileVersion* de ce binaire permet de connaître la version de *sysmon* installée.

```
Pour la version 32 bits de sysmon :
HKLM\SYSTEM\CurrentControlSet\Services\sysmon
Pour la version 64 bits de sysmon :
HKLM\SYSTEM\CurrentControlSet\Services\sysmon64
```

Listing 21 – Clés de registre de configuration du service *sysmon* par défaut

#### Information

Si l'installation de *sysmon* a été réalisée en spécifiant l'argument « `-d` » pour renommer le nom de son pilote (ce qui a très peu de valeur ajoutée du point de vue de la sécurité), alors les clés de registre indiquées par le listing 21 ne portent plus le nom de *sysmon* mais celui donné au pilote.

Le ciblage de la GPP de création de tâche à exécution immédiate peut donc être configuré comme indiqué en pseudo-code par le listing 22 et tel qu'illustré par la figure 8.

```
Aucun service sysmon n'est installé
OU
(
  La référence à un service sysmon est présente dans le registre
  ET la version du binaire sysmon est >= 0.0.0.0 et < 11.0.0.0
)
```

Listing 22 – Pseudo-code de ciblage pour le déploiement de *sysmon* par GPP de création de tâche à exécution immédiate

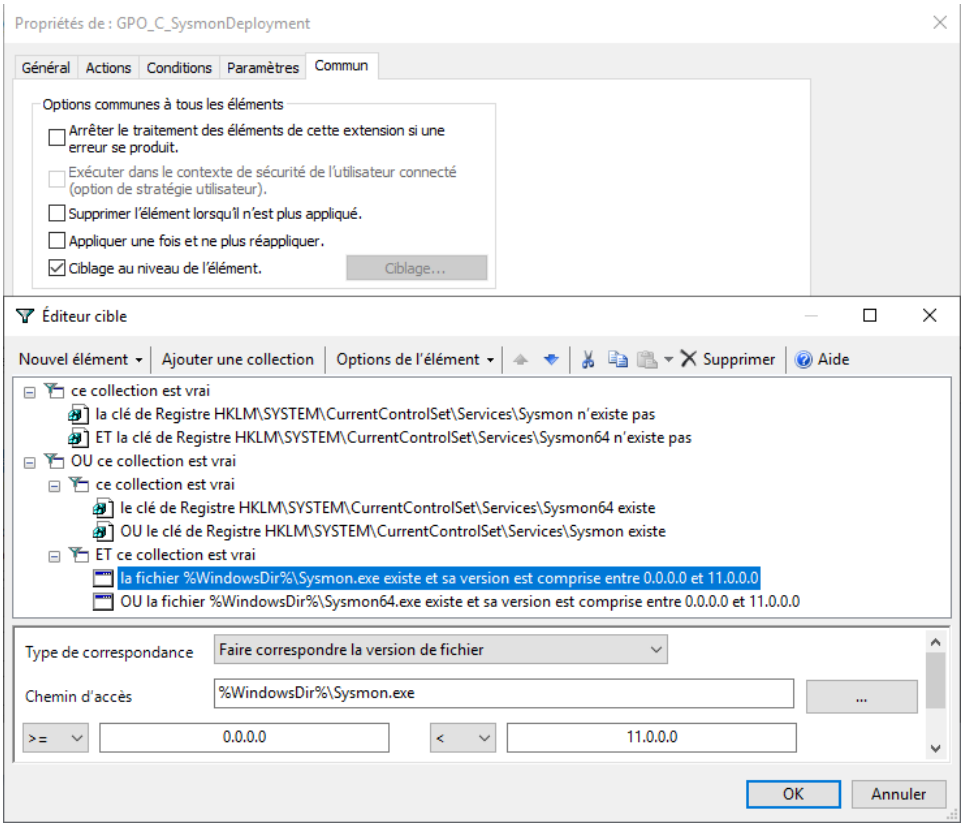


FIGURE 8 – Configuration d'un ciblage au niveau élément pour la GPP de création de tâche à exécution immédiate de déploiement de *sysmon*

## Information

Dans ce ciblage illustré par la figure 8 il est important de bien faire attention aux subtilités concernant :

- les collections (c'est-à-dire les sous-ensembles logiques entre parenthèses) ;
- les opérateurs logiques « ET » et « OU » ;
- l'opérateur de comparaison « < » pour ne cibler que les versions strictement inférieures à 11.0.0.0.

Par ailleurs, la version doit impérativement être précisée dans son format complet (« 11.0.0.0 » dans le cas présent) et non dans un format raccourci (« 11 »).

Chaque fois qu'une nouvelle version de *sysmon* doit être déployée, il suffit alors de mettre à jour les binaires `sysmon.exe` et `sysmon64.exe` sur le partage où l'utilitaire est mis à disposition, puis de modifier la version du binaire indiquée dans les éléments de ciblage de la GPP de création de tâche à exécution immédiate. Ainsi, cette tâche sera de nouveau créée sur les systèmes et le script PowerShell de déploiement s'exécutera par son intermédiaire.

# E.2 Déploiement et mise à jour de la configuration de sysmon sur les systèmes

## E.2.1 Déploiement de la configuration de sysmon par le registre

Le service *sysmon* présente l'avantage de stocker sa configuration dans différentes valeurs de la clé de registre de son pilote de périphérique. Cette clé de registre est indiquée par le listing 23 et son contenu est illustré par la figure 9.

```
HKLM\SYSTEM\CurrentControlSet\Services\sysmonDrv\Parameters
```

Listing 23 – Clé de registre de configuration de *sysmon*

### Information

*sysmon* repose sur un pilote de périphérique (*driver*) pour intercepter les évènements à journaliser. Le nom de ce pilote peut être modifié par l'option de configuration `DriverName` (`sysmonDrv` étant son nom par défaut), dans ce cas le chemin de la clé de registre illustrée par la figure 9 est modifié en conséquence. Ce changement de nom reste toutefois peu utile dans la mesure où la signature cryptographique du pilote reste la même, ce qui permet de facilement l'identifier quel que soit son nom.

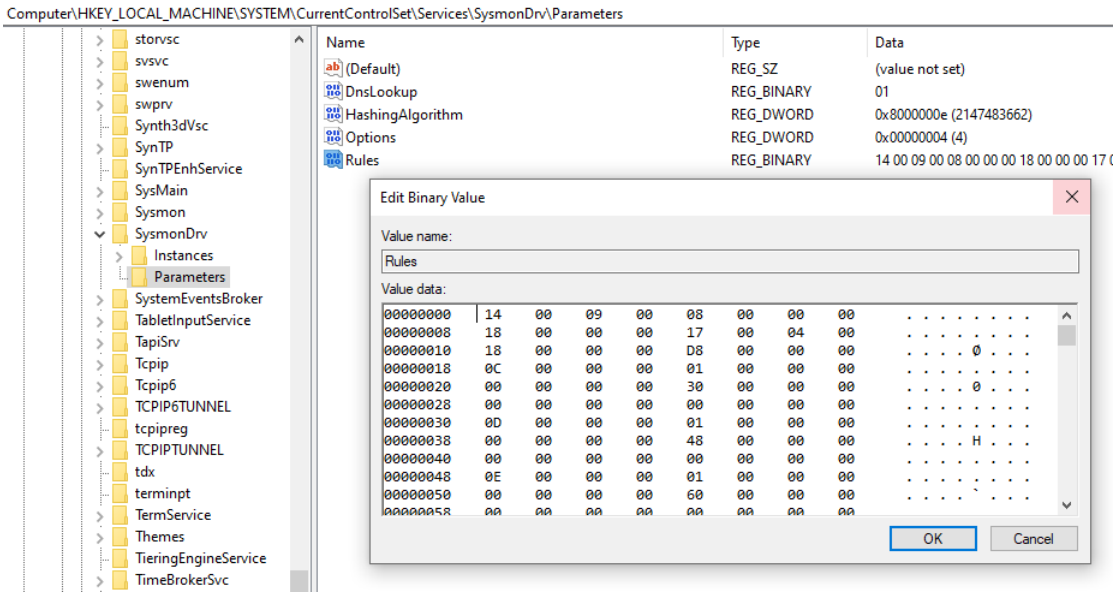


FIGURE 9 – Valeurs de clé de registre utilisées pour stocker la configuration de *sysmon*

Plus précisément, la valeur binaire `Rules` contient les règles de filtrage définies dans la balise `<EventFiltering>` du fichier de configuration de *sysmon* dans un format binaire. Les autres valeurs (`DNSLookup` ou `HashingAlgorithm` par exemple) stockent quant à elles des options de configuration générale. Il est à noter que la liste exhaustive des options disponibles figure dans la balise `<options>` du schéma XML de configuration de *sysmon*. La valeur binaire `Rules` contient ainsi potentiellement plusieurs kilo-octets de données.

Déployer la configuration de *sysmon* de cette manière présente deux avantages :

- aucun fichier de configuration de *sysmon* n'a besoin d'être stocké – ni localement sur chaque système ni de manière centralisée sur un partage réseau – ce qui évite sa consultation aisée par un attaquant qui chercherait à la contourner ;
- elle est réalisable sans script, par simple utilisation d'une GPP.

### Attention

Le déploiement des configurations par clé de registre nécessite un suivi de gestion des versions important dans la mesure où le contenu de la clé de registre est spécifique à la version de `sysmon` et que plusieurs versions peuvent coexister au sein d'un SI.

Le service Windows de *sysmon* surveille tout changement de ces valeurs de clé de registre. Il suffit de changer les données de ces valeurs sur les systèmes pour qu'une nouvelle configuration soit instantanément appliquée, automatiquement et sans besoin de redémarrage du service. Suite à l'installation du service *sysmon* avec une configuration par défaut réalisée par le script PowerShell 20, l'application d'une GPP de registre qui met à jour les valeurs de la clé de registre de *sysmon* permet ainsi de lui appliquer la configuration souhaitée.

### Information

Il est à noter qu'un changement de configuration de cette manière ne déclenche pas l'évènement *sysmon config state changed*, qui en revanche est généré lorsque la configuration est changée à l'aide d'un fichier XML. Il reste néanmoins possible de journaliser un évènement similaire en créant une règle *sysmon* qui surveille toute modification de la clé de registre du pilote de périphérique de *sysmon* ; dans ce cas, le rafraîchissement régulier de la GPO entraînera l'inscription de l'évènement.

Une bonne pratique de déploiement centralisé de la configuration de *sysmon* consiste ainsi :

1. à configurer *sysmon* sur un système dit « de référence », manuellement à l'aide d'un fichier de configuration au format XML ;
2. à exporter les différentes valeurs de la clé de registre de *sysmon* depuis ce système de référence ;
3. à les ajouter à la GPP de registre qui sera appliquée à tous les systèmes pourvus d'un service *sysmon* à jour, ce qui aura pour conséquence de copier ces valeurs de clé de registre à l'identique sur tous ces systèmes.

Chaque valeur de clé de registre peut ainsi être créée et mise à jour par GPP, telle qu'illustré par la figure 10, cela jusqu'à avoir configuré toutes les valeurs de registre nécessaires à la configuration de *sysmon*, comme illustré par la figure 11.

Les valeurs de clé de registre `Rules`, `HashingAlgorithm` et `Options`, ainsi que toutes celles qui concernent des paramètres de configuration spécifiques (comme `CheckRevocation` ou `DNSLookup` par exemple) doivent être créées ou mises à jour de cette manière pour déployer intégralement la configuration de *sysmon* sur les systèmes.

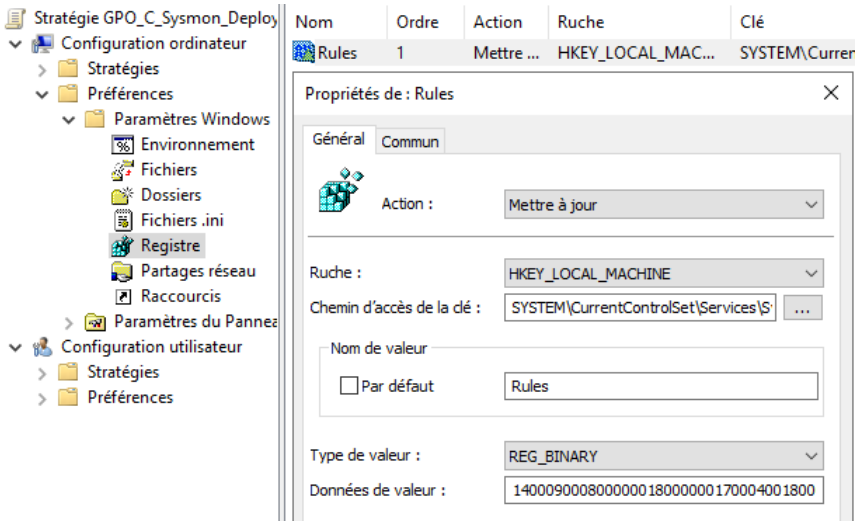


FIGURE 10 – Interface de création d'un élément de registre par GPP pour la configuration centralisée de *sysmon*

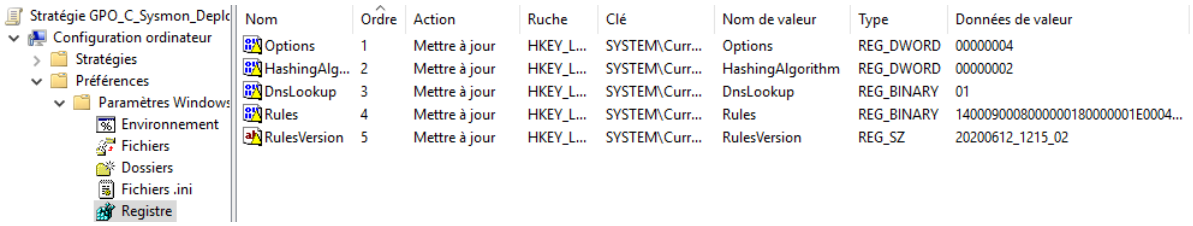


FIGURE 11 – Liste des valeurs créées et mises à jour par la GPP de registre de configuration centralisée de *sysmon*

Il est possible de créer ou modifier cette GPP de registre à l'aide des RSAT (*Remote Server Administration Tools*) « `Rsat.GroupPolicy.Management.Tools` » depuis le système de référence sur lequel la dernière version de *sysmon* est installée et configurée par fichier XML. Cela présente l'avantage de pouvoir sélectionner graphiquement la valeur binaire de clé de registre `Rules` (qui sera généralement celle à mettre à jour puisque les paramètres généraux de *sysmon* sont quant à eux rarement modifiés) en parcourant la ruche locale. L'assistant peuple alors automatiquement les champs « Ruche », « Chemin d'accès de la clé », « Nom de valeur », « Type de valeur » et « Données de valeur » (cf. figure 10) lors de la création ou de la mise à jour de l'élément de registre à déployer.

## Attention

Si la GPP de registre est configurée par RSAT depuis un système de référence *sysmon*, des bonnes pratiques de gestion des comptes à privilèges doivent dans ce cas être suivies :

- le système de référence doit être considéré comme étant d'un niveau de sensibilité et de sécurité équivalent à une station d'administration. Le niveau de sécurité approprié correspond par ailleurs au périmètre d'application le plus sensible des GPP qui y sont modifiées (par exemple, si une GPP s'applique à des contrôleurs de

domaine AD, alors le système de référence depuis lequel cette GPP est modifiée est d'un très haut niveau de sensibilité) ;

- il est préférable d'exécuter le RSAT avec un compte d'administration du domaine AD disposant uniquement d'une délégation de droits sur les GPP de configuration du *sysmon*, plutôt qu'un compte disposant de privilèges étendus (administrateurs du domaine, etc.). Ce compte d'administration ne doit être utilisé que sur ce système de référence et être considéré comme étant du même niveau de sensibilité.

Si la GPP n'est en revanche pas modifiée à l'aide des RSAT depuis le système de référence, il reste possible de simplement exporter les données des valeurs de clé de registre depuis ce dernier. Cet export peut ensuite être transféré vers une ressource d'administration par l'intermédiaire d'une copie de texte brut. Comme il n'est pas possible de simplement faire un copier/coller d'une valeur de clé de registre de type `REG_BINARY` (ce qui est le cas de la valeur `Rules`), l'utilisation d'une invite de commandes PowerShell avec élévation de privilèges est recommandée. La ligne de code proposée dans le listing 24 permet de réaliser cet export dans un format directement utilisable par copier-coller vers le champs « Données de valeur » des propriétés de l'élement de registre de type `REG_BINARY` illustré par la figure 10.

```
((Get-ItemProperty -Path
     HKLM:\SYSTEM\CurrentControlSet\Services\sysmonDrv\Parameters).Rules
     | ForEach-Object ToString X2) -join '' > un_fichier_texte.txt
# Ici c'est la valeur binaire "Rules" de sysmon qui est exportée.
```

Listing 24 – Script PowerShell d'export de valeur de clé de registre de type `REG_BINARY` dans un format adapté à la création d'une GPP de registre

### E.2.2 Gestion des mises à jour et ciblage des systèmes

D'une version à l'autre de *sysmon*, la version de son schéma change. Elle est indiquée par l'attribut `schemaversion` de la balise racine `<manifest>` en première ligne du schéma exporté. Cet attribut `schemaversion` se retrouve de la même manière dans la balise racine `<sysmon>` du fichier de configuration, indiquant alors quelle est la version du schéma utilisée dans le fichier de configuration (par exemple, `<sysmon schemaversion="4.30">` correspond à la version 11.0.0.0 de *sysmon*), ce qui lui permet de l'interpréter en conséquence. À chaque mise à jour de l'utilitaire et du fichier de configuration, il est donc nécessaire de mettre à jour cet attribut dans le fichier de configuration sans quoi de nouvelles options de configuration de *sysmon* pourraient ne pas être prises en compte.

Par ailleurs, une configuration de *sysmon* n'est pas nécessairement rétro-compatible avec d'anciennes versions de l'utilitaire, de même qu'une ancienne configuration n'est pas nécessairement compatible avec une version récente de l'utilitaire. Il est par conséquent souhaitable de ne mettre à jour la configuration de *sysmon* que sur les systèmes équipés de la dernière version de *sysmon*.

Cette sélection des systèmes équipés de la dernière version de *sysmon* peut se faire par ciblage, comme pour la tâche à exécution immédiate proposée en sous-section E.1.3. Puisque l'installation du service *sysmon* se caractérise notamment par la copie du binaire `sysmon.exe` (version 32 bits) ou `sysmon64.exe` (version 64 bits) dans le dossier `C:\Windows\`, la propriété *FileVersion* de ce binaire permet encore une fois de configurer le ciblage approprié. Le ciblage qui en résulte est proposé sous forme de pseudo-code dans le listing 25 et illustrée par la figure 12 (il est à noter que contrairement

à la tâche à exécution immédiate, les systèmes cibles sont cette fois-ci ceux ayant la version à jour de *sysmon*). Ce ciblage doit être appliqué à chaque valeur de clé de registre déployée par GPP de registre.

```
La version du binaire sysmon est >= 11.0.0.0 ou <= 11.0.0.0
```

Listing 25 – Élément de ciblage pour le déploiement de la configuration de *sysmon* par GPP de registre

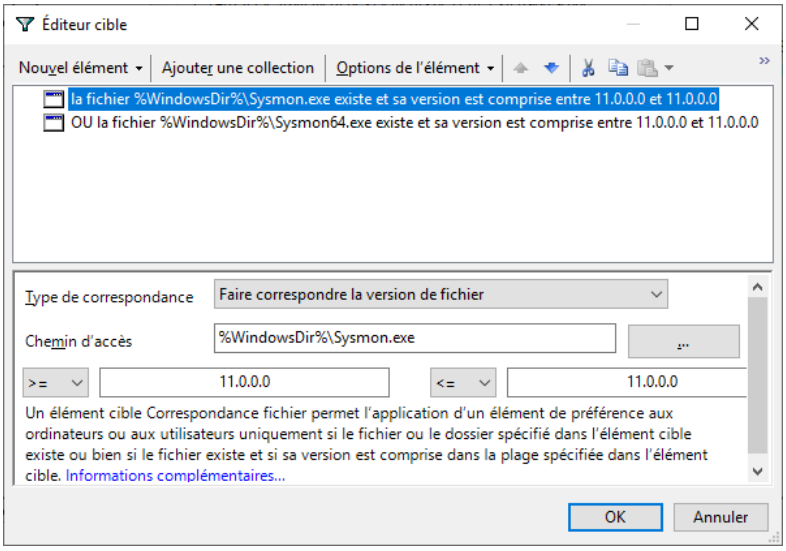


FIGURE 12 – Configuration d'un ciblage au niveau élément pour la GPP de registre

Ainsi, lorsqu'un système ne dispose pas de la dernière version de *sysmon* (celle mise à disposition sur le partage réseau), sa configuration n'est plus mise à jour. Dans ce cas, la GPP de création de tâche à exécution immédiate se charge de mettre à jour *sysmon* puis la GPP de registre appliquera alors ensuite toute nouvelle configuration destinée à cette version à jour de *sysmon*.

Pour finir, il est à noter qu'une seule et même GPO peut être utilisée pour le déploiement et la mise à jour de *sysmon* par GPP de tâche à exécution immédiate, ainsi que pour la mise à jour de la configuration de *sysmon* par GPP de registre ou à l'aide de l'outil de gestion de parc interne.

Le lecteur est invité à consulter l'annexe F pour une introduction à la création de règles *sysmon* afin de construire le fichier de configuration XML à utiliser sur le système de référence.

# Annexe F
# Aide à la compréhension des règles sysmon

Il est souhaitable de bien comprendre les règles *sysmon* avant leur déploiement sur le SI lorsqu'elles proviennent de sources tierces et pour être en mesure de les adapter au contexte de l'entité. Comme prérequis à la compréhension d'un fichier de configuration *sysmon*, il est nécessaire de connaître les rudiments du langage XML. La structure XML du fichier de configuration de *sysmon* restant néanmoins relativement simple, cette lacune peut être rapidement comblée à l'aide des nombreux tutoriels disponibles sur Internet. Cette annexe prend comme hypothèse que la connaissance du langage XML est un acquis du lecteur.

## F.1 Schéma XML du fichier de configuration

Pour comprendre les règles d'un fichier de configuration *sysmon*, il est préférable de connaître le schéma XML de ce dernier. Ce schéma indique assez précisément quels sont les types d'évènements journalisables, les champs spécifiques à chaque type d'évènement, les options générales prises en charge par l'utilitaire, les différentes conditions implémentées, etc. Le schéma de *sysmon* peut être affiché à l'aide de la commande *batch* du listing 26 ou par exemple exporté dans un fichier texte à l'aide de la commande *batch* du listing 27.

```
sysmon.exe -s
```

Listing 26 – Commande *batch* d'affichage du schéma de sysmon

```
sysmon.exe -s > schema.txt
```

Listing 27 – Commande *batch* d'export du schéma de sysmon

Ce schéma permet notamment de consulter les différents types d'évènements journalisables. Pour la version 11 de *sysmon*, il est le suivant :
`ProcessCreate`, `FileCreateTime`, `NetworkConnect`, `ProcessTerminate`, `DriverLoad`, `ImageLoad`,`CreateRemoteThread`, `RawAccessRead`, `ProcessAccess`, `FileCreate`, `RegistryEvent`,`FileCreateStreamHash`, `PipeEvent`, `WmiEvent`, `DNSQuery` et `FileDelete`.

Il permet également de remarquer que la journalisation des requêtes DNS, par exemple, se fait à l'aide de règles de type `DNSQuery` et que ces dernières, en version 11 de *sysmon*, sont personnalisables à l'aide des champs :

- `UtcTime`, qui correspond au temps UTC de l'évènement ;

- `ProcessGUID`, `ProcessId` et `Image` qui correspondent respectivement au GUID, au numéro et au chemin complet du binaire du processus qui est à l'origine de la requête DNS ;
- `QueryName`, `QueryStatus` et enfin `QueryResults` qui correspondent respectivement à la requête DNS, son statut (0 en cas de succès, 1 en cas d'échec) et son résultat (la réponse du serveur DNS).

Enfin, le schéma XML permet aussi de prendre connaissance des différentes conditions logiques implémentées et utilisables dans le fichier de configuration. En version 11 de *sysmon*, elles sont les suivantes : *is, is not, contains, contains any, contains all, excludes, excludes any, excludes all, begin with, end with, less than, more than* et *image*.

## F.2 Exemples didactiques

À l'aide des informations du schéma, il est possible de rapidement comprendre des règles simples en sachant :

- qu'une règle ne peut concerner qu'un unique type d'évènement (`DNSQuery`, `NetworkConnect`, `ProcessCreate`, etc.) ;
- qu'elles se composent d'un ensemble de conditions logiques optionnelles (`condition="is not"` par exemple) applicables aux différents champs disponibles pour le type d'évènement considéré (`QueryName`, `QueryResults`, etc.) ;
- que ces conditions peuvent être inclusives ou exclusives, ce qui est précisé à l'aide de l'attribut de type d'évènement `onmatch` indiquant si un évènement est journalisé lorsqu'une ou plusieurs conditions formulées sont vraies (`onmatch="include"`) ou si au contraire tout est journalisé sauf les évènements qui correspondent aux exceptions formulées (`onmatch="exclude"`).

### Information

Si l'attribut `onmatch="include"` est précisé mais qu'aucune condition n'est formulée alors aucune condition ne peut être vraie et aucun évènement de ce type n'est par conséquent journalisé. Au contraire, si l'attribut `onmatch="exclude"` est précisé mais qu'aucune exception n'est formulée alors tous les évènements de ce type sont dans ce cas journalisés. Ces deux utilisations de l'attribut `onmatch` sont illustrées par le listing 28.

En réalité, l'attribut `onmatch` est optionnel pour certains types d'évènements lorsque le schéma XML lui précise une valeur par défaut (attribut `ruledefault="include"` ou `ruledefault="exclude"`). Pour des questions de lisibilité et de maintenabilité de la configuration, il est néanmoins recommandé de toujours faire figurer explicitement l'attribut `onmatch` sans tenir compte de sa valeur par défaut.

```
<!-- Journaliser toutes les créations de processus -->
<ProcessCreate onmatch="exclude">
</ProcessCreate>
```

```
<!-- Ne journaliser aucune terminaison de processus -->
<ProcessTerminate onmatch="include">
</ProcessTerminate>
```

Listing 28 – *sysmon* – utilisation de l'attribut `onmatch`

Les exemples didactiques qui suivent dans cette annexe n'ont d'autre utilité que d'illustrer la logique de création de règles dans *sysmon* pour aider à leur compréhension. Ces exemples sont volontairement simplistes et ne présentent aucun intérêt en matière de sécurité.

Soit un premier exemple didactique de création d'une règle qui consiste à journaliser les requêtes DNS terminant par « .ssi.gouv.fr ». Dans cet exemple :

- le type d'évènement doit être indiqué par la balise `<DNSQuery>` ;
- la condition sur le champ `QueryName` doit être indiquée par la balise du même nom sous la forme `<QueryName condition="end with">.ssi.gouv.fr</QueryName>`.
- l'attribut `onmatch` de l'évènement doit avoir pour valeur `"include"` puisque la condition précédente indique les évènements à journaliser (*a contrario*, la proposition « journaliser toutes les requêtes DNS sauf celles terminant par « .ssi.gouv.fr » » aurait été exprimée par la même condition mais avec l'attribut `onmatch="exclude"`).

La règle *sysmon* qui traduit cet exemple figure dans le listing 29, tandis que sa règle contraire est illustrée par le listing 30.

```
<!-- Exemple 1 : journaliser les requêtes DNS terminant par ".ssi.gouv.fr" -->
<DnsQuery onmatch="include">
     <QueryName condition="end with">.ssi.gouv.fr</QueryName>
</DnsQuery>
```

Listing 29 – Règle *sysmon* – exemple 1

```
<!-- Exemple 2 : journaliser toutes les requêtes DNS sauf celles terminant
par ".ssi.gouv.fr" -->
<DnsQuery onmatch="exclude">
     <QueryName condition="end with">.ssi.gouv.fr</QueryName>
</DnsQuery>
```

Listing 30 – Règle *sysmon* – contraire de l'exemple 1

Des conditions inclusives (`onmatch="include"`) et exclusives (`onmatch="exclude"`) peuvent par ailleurs cohabiter dans une même règle *sysmon* ; elles sont dans ce cas complémentaires mais les règles d'exclusion l'emportent sur les règles d'inclusion. Ce principe de priorisation donnée à l'exclusion est illustré par l'exemple du listing 31.

```
<!-- Exemple 3 : journaliser les requêtes DNS terminant par ".ssi.gouv.fr" à l'exception de
celles qui concernent spécifiquement "www.ssi.gouv.fr" -->
<DnsQuery onmatch="include">
     <QueryName condition="end with">.ssi.gouv.fr</QueryName>
</DnsQuery>
<DnsQuery onmatch="exclude">
     <QueryName condition="is">www.ssi.gouv.fr</QueryName>
</DnsQuery>
```

Listing 31 – Règle *sysmon* – exemple 3

Lorsqu'une règle contient plusieurs conditions, elles doivent être lues de cette manière :

- si plusieurs conditions portent sur le même champ (`QueryName` par exemple), la règle s'applique si l'une ou l'autre des conditions est remplie ou si les deux conditions sont remplies : il y a donc un opérateur « OU » implicite entre champs identiques ;
- si une règle contient des conditions qui portent sur différents champs (`QueryName` et `Image` par exemple), alors chacune doit être vraie pour que la règle s'applique : il y a dans ce cas un opérateur « ET » implicite entre champs différents.

Ce principe d'opérateur implicite pour la formulation des conditions est illustré par les listings 32 et 33 ci-après.

```
<!-- Exemple 4 : journaliser les requêtes DNS terminant par ".ssi.gouv.fr" OU ".sgdsn.gouv.fr".
Il y a un "OU" implicite entre les deux conditions "QueryName" -->
<DnsQuery onmatch="include">
     <QueryName condition="end with">.ssi.gouv.fr</QueryName>
     <QueryName condition="end with">.sgdsn.gouv.fr</QueryName>
</DnsQuery>
```

Listing 32 – Règle *sysmon* – exemple 4

```
<!-- Exemple 5 : journaliser les requêtes DNS terminant par ".ssi.gouv.fr" ET provenant
d'un binaire "ping.exe" OU "iexplore.exe".
Il y a donc :
- un "OU" implicite entre les deux conditions "Image" ;
- un "ET" implicite entre les conditions "QueryName" et "Image". -->
<DnsQuery onmatch="include">
     <QueryName condition="end with">.ssi.gouv.fr</QueryName>
     <Image condition="end with">\ping.exe</Image>
     <Image condition="end with">\iexplore.exe</Image>
</DnsQuery>
```

Listing 33 – Règle *sysmon* – exemple 5

## F.3 Bonnes pratiques de structure du fichier de configuration de sysmon

Pour assurer la maintenabilité du fichier de configuration de *sysmon* dans le temps, il est recommandé de suivre certaines bonnes pratiques. Pour commencer, il est préférable de nommer les règles et de les placer systématiquement dans des groupes à l'aide de la balise `RuleGroup`, y compris lorsqu'une règle est seule dans son groupe. Cette pratique présente plusieurs avantages :

- un `RuleGroup` se compose d'une ou plusieurs règles (balise `Rule`). Lui-même, ainsi que chacune des règles qu'il contient, peut être nommé à l'aide de l'attribut `name="Un nom de règle ou de groupe de règles"`. En étant structuré en règles séparées et nommées, le fichier de configuration gagne en lisibilité et en maintenabilité. Les noms de règles figurent par ailleurs dans les informations des évènements journalisés, ce qui facilite leur traitement au sein d'un SIEM. Il est à noter que cet attribut accepte une taille maximale de 128 caractères depuis la version 10.42 de *sysmon* ;
- à l'aide de l'attribut `groupRelation` d'une balise `RuleGroup` (qui prend pour valeur `or` ou `and`) il est possible de spécifier explicitement la relation logique qui lie les champs différents entre eux

dans tout le `RuleGroup`, outrepassant ainsi l'opérateur « ET » implicite. Il est donc recommandé de toujours préciser explicitement le `groupRelation` d'une balise `RuleGroup` ;

- à l'aide de l'attribut `groupRelation` d'une balise `Rule` (qui prend pour valeur `or` ou `and`) il est possible de spécifier explicitement la relation logique qui lie les champs identiques entre eux dans le `Rule`, outrepassant ainsi l'opérateur « OU » implicite. Il est donc recommandé de toujours préciser explicitement le `groupRelation` d'une balise `Rule`. Néanmoins, l'enchaînement de plusieurs balises `Rule` portant sur les mêmes champs mais avec des `groupRelation` différents est à proscrire car elle peut aboutir à un résultat dénué de sens du fait d'une implémentation partielle de ces logiques dans *sysmon*.

Le listing 34 illustre l'utilisation des balises `Rule` et `RuleGroup`.

```
<!-- Exemple 6 : journaliser toutes les requêtes DNS provenant d'un binaire situé dans C:\Users\*
OU à destination de www.ssi.gouv.fr ou www.sgdsn.gouv.fr quel que soit le chemin du binaire -->
<RuleGroup name="Exemple 6" groupRelation="or">
     <DnsQuery onmatch="include">
          <Rule name="Exemple 6 - requête depuis C:\Users\*">
               <Image condition="begin with">C:\Users\</Image>
          </Rule>
          <Rule name="Exemple 6 - requête vers sites supervisés" groupRelation="or">
               <QueryName condition="is">www.ssi.gouv.fr</QueryName>
               <QueryName condition="is">www.sgdsn.gouv.fr</QueryName>
          </Rule>
     </DnsQuery>
</RuleGroup>
```

Listing 34 – Règle *sysmon* – exemple 6

Le nom de règle retenu pour un évènement journalisé n'est pas intuitif et dépend en réalité de plusieurs critères :

- les conditions formulées dans les règles sont évaluées par ordre d'apparition du champ dans le schéma de *sysmon* et non pas par ordre d'apparition dans le fichier de configuration. C'est-à-dire que pour un évènement de type `<DNSQuery>`, les conditions sur le champ `<QueryName>` sont toujours évaluées avant les conditions sur le champ `<Image>` ;
- dans le cas où la relation logique du `RuleGroup` est `groupRelation="or"`, le nom de règle de la première condition évaluée vraie est retenu ;
- dans le cas où la relation logique du `RuleGroup` est `groupRelation="and"`, le nom de règle de la dernière condition évaluée vraie est retenu.

Dans le cas de l'exemple 6 précédemment illustré par le listing 34, une requête DNS pour le nom de domaine « www.ssi.gouv.fr » réalisée par le binaire `C:\Users\malveillant.exe` sera ainsi journalisée avec l'information « Rulename="Exemple 6 - requête vers sites supervisés" » et non pas avec l'information « Rulename="Exemple 6 - requête depuis C :\Users*" ».

Il est par ailleurs particulièrement recommandé d'ajouter des commentaires dans le fichier XML de configuration (« `<!--` » marquant le début d'un commentaire sur une ou plusieurs lignes et « `-->` » en marquant la fin, comme illustré par les différents listings de cette annexe), de sorte qu'un tiers puisse facilement comprendre l'utilité de chaque règle ainsi que les raisons expliquant chaque condition ou exception formulée.

Tenir un registre des modifications (*changelog*) par l'utilisation d'outils de gestion de versions (« Git » par exemple) est également une bonne pratique qui facilite le travail en équipe et permet de savoir quelles ont été les modifications successives de la configuration de *sysmon*. Idéalement, le numéro de version de cette configuration devrait figurer sous forme de commentaire en début de fichier de configuration XML.

Enfin, il est d'usage de ne déployer que des configurations de *sysmon* qui ont été préalablement revues et testées. Cette bonne pratique permet de limiter les faux positifs ou négatifs, la saturation des journaux avec des évènements inappropriés, voire un dysfonctionnement général de l'outil. Pour faciliter le test d'un fichier de configuration, il est à noter que *sysmon* peut être exécuté en mode *debug*. La commande à utiliser est indiquée par le listing 35.

```
sysmon.exe -t -i c:\un_dossier\un_fichier_de_configuration.xml
```

Listing 35 – Commande *batch* d'utilisation de *sysmon* en mode *debug*

# Annexe G
# Mise en œuvre d'un service de collecte des évènements Windows

Cette annexe donne des recommandations pour le déploiement du service « Collecteur d'évènements de Windows » qui est nativement intégré aux systèmes Windows. Il couvre différents aspects ayant trait à sa mise en œuvre et à sa sécurisation, côté serveur WEC (*Windows Event Collector*) en section G.1 et côté clients WEF (*Windows Event Forwarding*) en section G.2. Le déploiement de ce service est abordé sous l'angle d'une utilisation exclusivement en mode *Push* (à privilégier) mais les spécificités de déploiement relatives au mode *Pull* sont néanmoins abordées en section G.3.

La figure 13 illustre une vision globale des configurations à réaliser pour la mise en œuvre du service de collecte des évènements Windows, ainsi que leurs sections correspondantes dans cette annexe.

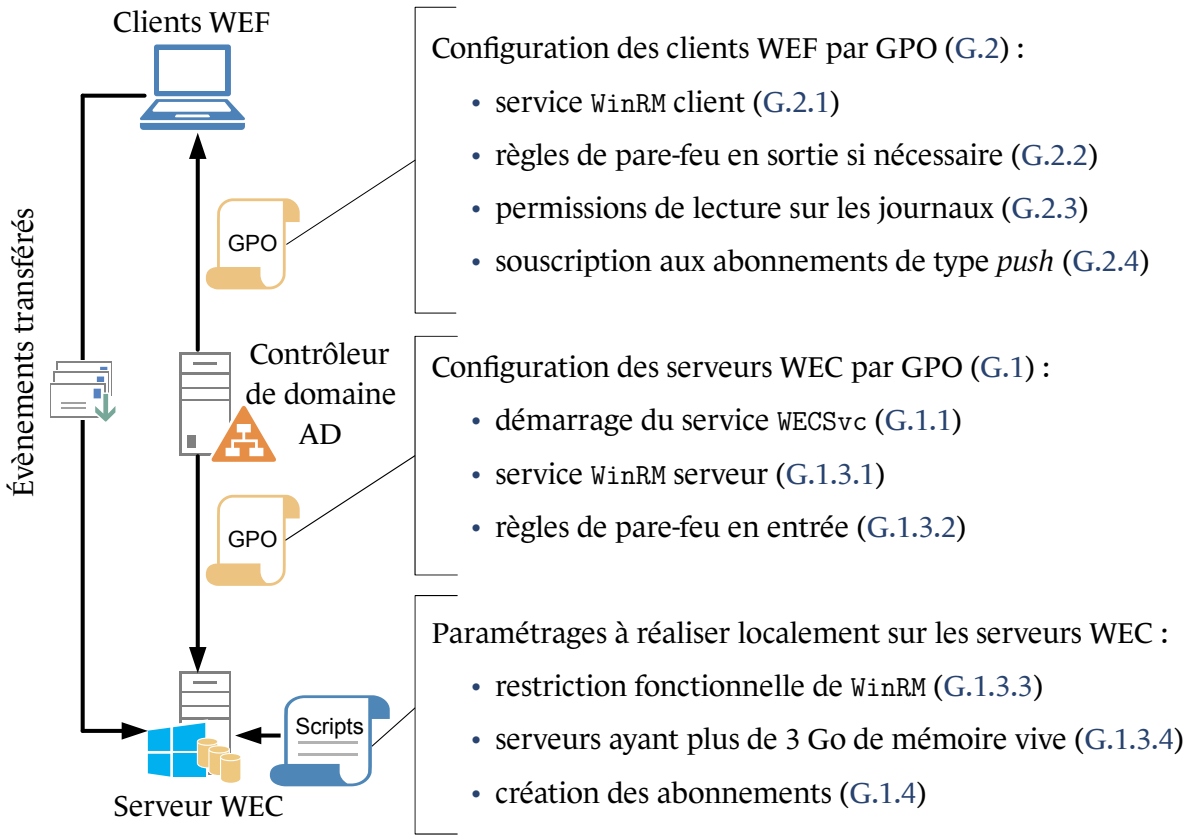


FIGURE 13 – Représentation synthétique des configurations à réaliser pour le déploiement d'un service de collecte des évènements Windows

Pour finir, la section G.4 propose quelques pistes de dépannage pour résoudre les problèmes de fonctionnement courants du service de collecte ou du transfert d'évènements.

# G.1 Configuration des serveurs collecteurs d'évènements

Le service Windows « Collecteur d'évènements de Windows » (`WECSvc`) est un service natif (depuis 2008 avec Windows Vista et Windows Server 2008) pour la collecte des évènements à des fins de centralisation. Il repose sur le service *Windows Remote Management* (`WinRM`) pour le transfert des journaux à travers le réseau depuis les systèmes clients vers le service collecteur d'évènements.

La configuration d'un serveur collecteur d'évènements se décompose en plusieurs étapes détaillées ci-après :

- démarrage automatique du service `WECSvc` (sous-section G.1.1) ;
- configuration du service `WinRM` (sous-section G.1.2) et mise en œuvre des compléments de configurations recommandés (sous-section G.1.3) ;
- création des abonnements (sous-section G.1.4).

En complément, l'annexe H indique une méthode permettant de créer un arborescence personnalisée de journaux pour les serveurs collecteurs d'évènements.

## G.1.1 Démarrage automatique du service `WECSvc`

Microsoft recommande de configurer le service collecteur d'évènements (`WECSvc`) en démarrage automatique avec début différé (le service `WinRM` est, quant à lui, déjà en démarrage automatique par défaut depuis Windows Server 2012). Cela peut notamment se faire sur chaque serveur collecteur d'évènements à l'aide de la commande *batch* du listing 36 (avec les privilèges d'administration locaux) ou bien par une GPP de services tel qu'illustré par la figure 14.

```
wecutil qc
```

Listing 36 – Commande *batch* de configuration rapide du service `WECSvc`

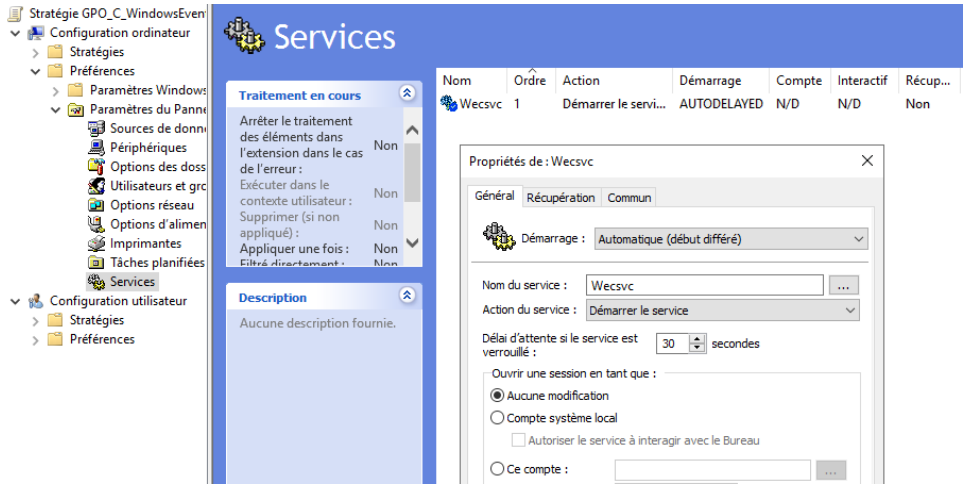


FIGURE 14 – GPP de service pour le démarrage automatique de `WECSvc` avec début différé

### G.1.2 Configuration rapide du service `WinRM`

`WinRM` repose sur le protocole standard HTTP pour ses communications réseau. Le service `WinRM` côté serveur nécessite donc une interface d'écoute HTTP à laquelle les systèmes clients `WinRM` vont se connecter. `WinRM` ne repose toutefois pas sur un service Web complexe comme Microsoft IIS (*Internet Information Services*) mais utilise en réalité le composant `HTTP.sys` natif du système.

Le service `WinRM` dispose lui aussi d'une commande de configuration rapide : elle est indiquée par le listing 37.

```
winrm qc
```

Listing 37 – Commande *batch* de configuration rapide du service `WinRM`

Cette commande de configuration rapide réalise plusieurs opérations :

- configurer le service `WinRM` en démarrage automatique ;
- configurer une interface d'écoute `WinRM` par défaut sur toutes les interfaces réseau ;
- activer les règles de pare-feu nécessaires aux trafic réseau de `WinRM` ;
- désactiver les restrictions d'UAC sur le réseau [35]. Cette désactivation n'est pas souhaitable pour l'utilisation de `WinRM` à des fins de seule centralisation des journaux, comme expliqué ci-dessous.

#### Attention

La question « ***Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users*** » posée lors de l'exécution de cette commande est dimensionnante en termes de sécurité et il convient d'y répondre par **NON** afin que les restrictions d'UAC sur le réseau restent activées. En cas de mauvaise manipulation ou pour réctifier une installation déjà réalisée, consulter l'article [35] pour réactiver les restrictions d'UAC sur le réseau.

Pour éviter tout risque d'erreur de manipulation, il est possible d'utiliser cette commande de configuration rapide de `WinRM`. En environnement AD, les opérations réalisées par cette dernière peuvent être réalisées par GPO :

- le démarrage automatique d'un service Windows par GPP est illustré en sous-section G.1.1 et cette même méthode peut être utilisée pour le service `WinRM` ;
- la configuration des interfaces d'écoute de `WinRM` est illustrée en sous-section G.1.3.1 ;
- l'activation de règles de pare-feu est illustrée en sous-section G.1.3.2 ;
- les restrictions d'UAC sur le réseau [35] sont déjà activées par défaut et doivent le rester.

Quelle que soit la méthode utilisée (commande de configuration rapide ou GPO), plusieurs compléments de configuration du service `WinRM` sont ensuite recommandés ; ils sont détaillés en sous-section G.1.3.

## G.1.3 Compléments de configuration du service `WinRM`

### G.1.3.1 Configuration fine du service `WinRM`

Plutôt que de laisser la configuration par défaut réalisée par la commande de configuration rapide du listing 37, une configuration idéale du service `WinRM` sur les serveurs collecteurs d'évènements consiste à mettre le service `WinRM` en écoute HTTP sur les seules interfaces réseau souhaitées, puis à désactiver les méthodes d'authentification trop faibles et interdire le trafic non chiffré. Si `WinRM` est toutefois utilisé pour d'autres besoins que le transfert des journaux au service de collecte d'évènements, la configuration du service `WinRM` doit dans ce cas être adaptée en conséquence. Bien qu'une configuration par défaut de `WinRM` soit déjà faite sous Windows Server 2019 ou par la commande de configuration rapide du listing 37, il est souhaitable d'en redéfinir la configuration de manière plus fine. Pour cela, les stratégies de groupe permettant la configuration de `WinRM` se situent à l'emplacement indiqué par le listing 38 et les paramètres de configuration qu'il est recommandé de définir sont quant à eux indiqués par le tableau 5.

```
Configuration ordinateur\Modèles d'administration\Composants Windows\Gestion à distance de
Windows (WinRM)\Service WinRM\
```

Listing 38 – Stratégie de configuration du service `WinRM` sur les serveurs collecteurs d'évènements

| Paramètre | Valeur |
|---|---|
| Autoriser la gestion de serveurs à distance via `WinRM` | Activé[a] |
| Autoriser l'authentification de base | Désactivé (valeur par défaut) |
| Autoriser l'authentification CredSSP | Désactivé (valeur par défaut) |
| Autoriser le trafic non chiffré | Désactivé (valeur par défaut) |
| Ne pas autoriser l'authentification Kerberos | Désactivé (valeur par défaut) |
| Ne pas autoriser l'authentification par négociation | Désactivé[b] (valeur par défaut) |

[a] Il convient de spécifier les interfaces réseau et adresses IP strictement nécessaires au service `WinRM`. L'interface IPv6 étant généralement inutilisée, il est préférable de la désactiver en laissant le filtre IPv6 vide.

[b] L'authentification par négociation utilise Kerberos pour les comptes de domaine et l'authentification NTLM pour les comptes locaux ou comme solution de repli lorsque l'authentification par Kerberos n'est pas possible. Il est toutefois possible d'imposer Keberos en activant ce paramètre. Sur les serveurs de collecte, il convient néanmoins de préciser que l'utilisation de `WinRM` par la boucle locale (127.0.0.1) implique une authentification par négociation (`NTLMSSP_NEGOCIATE`). Ainsi, les commandes `WinRM` de gestion du service de collecte doivent être exécutées avec l'argument « `-remote:FQDN_DU_SERVEUR` » pour éviter la boucle locale et permettre une authentification par ticket de service Keberos pour le SPN « `HTTP/FDQN_DU_SERVEUR` ». Il en va de même pour qu'un serveur de collecte s'abonne à lui-même : le FQDN est de mise. En revanche, la gestion des abonnements (cf. sous-section G.1.4) à l'aide de la console MMC n'est plus possible.

Tableau 5 – Paramètres de configuration du service `WinRM`

### Information

L'activation du paramètre « Autoriser la gestion de serveurs à distance via `WinRM` » (tableau 5) – tout comme la commande de configuration rapide du listing 37 – ont pour conséquence de créer un *listener* (interface d'écoute) `WinRM` en HTTP sur le port 5985. La configuration de ce *listener* peut être affichée à l'aide de la commande illustrée par la figure 15, cette dernière mentionnant le fait que le *listener* a été créé par GPO lorsque c'est le cas. Il n'est donc pas censé y avoir d'autres *Listeners* actifs sur le système, sauf si `WinRM` est utilisé par ailleurs pour d'autres besoins.

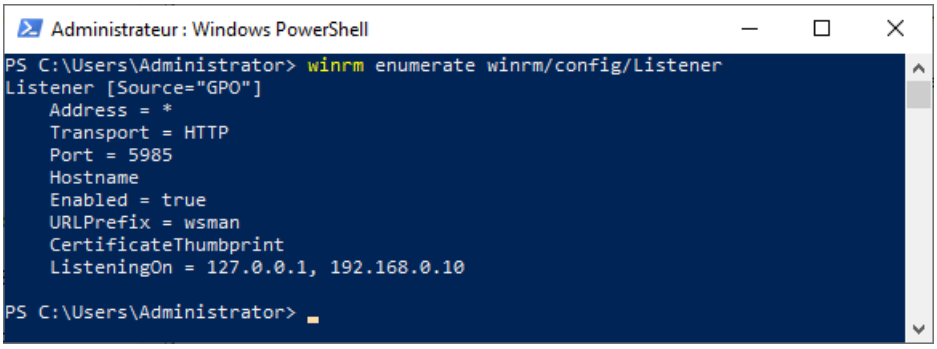


FIGURE 15 – Énumération des *Listeners* `WinRM`

Cette configuration de `WinRM` permet aux systèmes clients de se connecter à l'interface `WinRM` des serveurs collecteurs d'évènements via une authentification Kerberos ou NTLM. Bien qu'encapsulé dans HTTP, le trafic échangé par `WinRM` est chiffré à l'aide des clés de session d'authentification de comptes d'ordinateurs auprès des DC de l'AD, elles sont ainsi uniques par session entre chaque couple client et collecteur d'évènements. Ce fonctionnement apporte nativement une authentification mutuelle.

### Information

L'utilisation d'un *listener* `WinRM` en HTTPS n'est utile que pour la collecte d'évènements depuis des équipements non membres de l'AD. Comme précisé en section 3.2, elle est hors périmètre du présent guide.

#### G.1.3.2 Activation des règles de pare-feu pour le service `WinRM`

Par défaut, le pare-feu intégré à Windows bloque les flux entrants. Deux règles prédéfinies existent pour autoriser le trafic entrant du service `WinRM` (actives par défaut depuis Windows Server 2012 ou après exécution de la commande de configuration rapide du listing 37. Ces deux règles peuvent également être activées via la console d'administration du pare-feu Windows (`wf.msc`), en ligne de commande *batch* (listing 39) ou par GPO (figure 16). Pour ce faire, il convient d'utiliser la règle de trafic entrant prédéfinie intitulée « Gestion à distance de Windows » (ou *Windows Remote Management (HTTP-In)* en ligne de commande).

Ces règles n'autorisent que le protocole HTTP sur le port 5985. Lorsque des *listeners* HTTPS sont utilisés, des règles similaires doivent être créées pour le port 5986. Si par ailleurs des *listeners* de

compatibilité sont utilisés sur les ports 80 ou 443, les règles de trafic entrant pour `WinRM` doivent être adaptées en conséquence. Dans une démarche de défense en profondeur, il est souhaitable de personnaliser ces règles de pare-feu en spécifiant des interfaces réseau et en précisant des ensembles d'adresses IP sources (sous-réseaux, plages IP, etc.) autorisées à communiquer avec le serveur collecteur d'évènements par `WinRM`. Ces ensembles d'adresses IP correspondent dans ce cas aux systèmes autorisés à transférer des évènements au collecteur.

```
netsh advfirewall firewall set rule name="Windows Remote Management (HTTP-In)" new enable=yes
```

Listing 39 – Activation des règles de pare-feu prédéfinies pour le service `WinRM` par commande *batch*

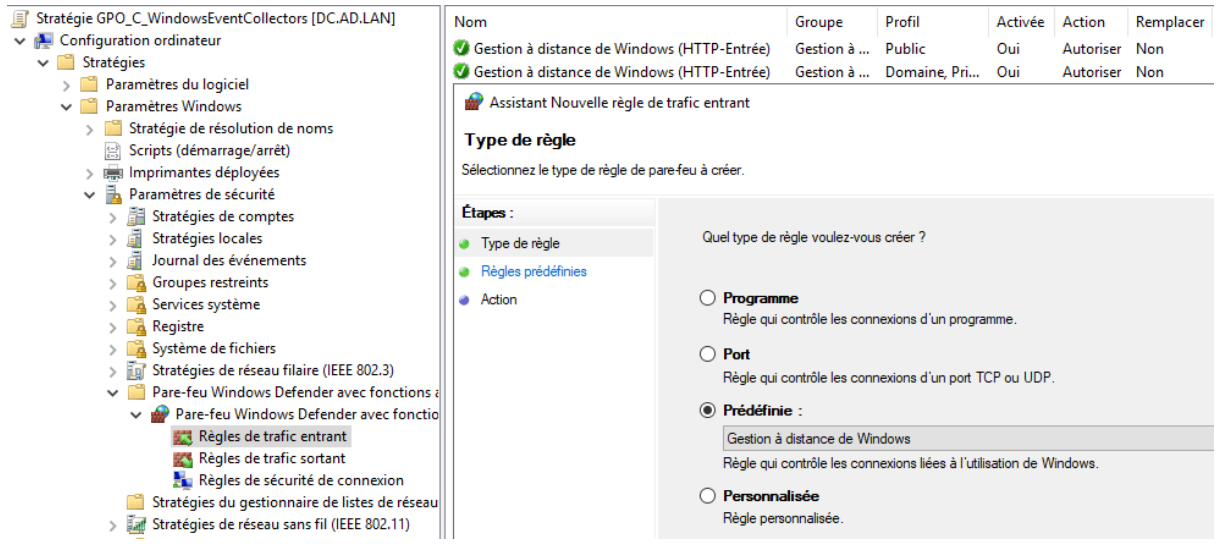


FIGURE 16 – Activation des règles de pare-feu prédéfinies pour le service `WinRM` par GPO

### G.1.3.3 Restriction fonctionnelle de `WinRM` au strict transfert d'évènements

L'activation du service `WinRM` sur un serveur est souvent perçue comme une porte d'entrée dangereuse car elle permet l'exécution de commandes à distance en PowerShell. Il est toutefois à noter que les différents *plugins* configurés par défaut dans `WinRM` (c'est le cas par exemple du *plugin Microsoft.PowerShell* pour le Shell distant) ne sont accessibles que par des utilisateurs privilégiés : groupe des administrateurs locaux (incluant donc les administrateurs du domaine AD), membres du groupe *Remote Management Users* et utilisateurs en session interactive sur les serveurs (SID `S-1-5-4`).

#### Information

`WinRM` expose différents *plugins* par défaut. L'*Event Forwarding Plugin* n'en est qu'un parmi d'autres, de même qu'il existe un *plugin* pour faire du WMI sur `WinRM` (*WMI Provider*), un autre qui expose une console *PowerShell* sur `WinRM` (*Microsoft.PowerShell*), etc.

Les descripteurs de sécurité au format SDDL des différents *plugins* peuvent être affichés à l'aide de la commande *batch* du listing 40 (balises « `<Security>` », attribut « `Sddl=` »), ce qui permet de s'assurer que les permissions effectives soient bien celles attendues (le SDDL par défaut du *plugin* `microsoft.powershell` est par exemple illustré à travers le listing 41).

```
winrm enumerate winrm/config/plugin /f:pretty
```

Listing 40 – Commande *batch* de consultation de la configuration des *plugins* `WinRM` au format XML

```
Sddl="O:NSG:BAD:P(A;;GA;;;BA)(A;;GA;;;IU)(A;;GA;;;RM)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)"
```

Listing 41 – Exemple de SDDL par défaut pour le *plugin* `microsoft.powershell`

Lorsqu'il est fonctionnellement envisageable de restreindre l'usage de `WinRM` sur les serveurs de collecte à la seule collecte des évènements, il est recommandé de désactiver tous les *plugins* de PowerShell à l'exception de celui nommé *Event Forwarding Plugin* puisqu'il est requis pour le transfert d'évènements. Cette désactivation peut se faire par PowerShell comme illustré par le listing 42.

### Attention

La désactivation des *plugins* PowerShell à l'aide du listing 42 ne doit être faite qu'après en avoir bien évalué l'impact en production : l'administration distante des serveurs par PowerShell ne sera plus possible.

Il est par ailleurs à préciser que le *plugin WMI Provider* est nécessaire au fonctionnement de certaines *Cmdlets* PowerShell comme *Get-ComputerInfo*.

```
 # Lister les plugins
$Plugins = dir WSMAN:\localhost\Plugin\
# Pour chaque plugin, sauf le "Event Forwarding Plugin"
foreach ($Plugin in $Plugins.Name){
  if ($Plugin -ne "Event Forwarding Plugin"){
    # Désactivation du plugin
    # Attention, il convient de s'assurer que le plugin désactivé n'est
    # pas utilisé par ailleurs pour d'autres besoins opérationnels
    set-item "WSMAN:\localhost\Plugin\$Plugin\enabled" -value False
  }
}
# Redémarrage du service WinRM
Restart-Service winrm

# Affichage du SDDL de chaque plugin (pour information seulement)
# Lister les plugins
$Plugins = dir WSMAN:\localhost\Plugin\
# Pour chaque plugin
foreach ($Plugin in $Plugins.Name){
  Write-Host "Plugin $Plugin :"
  $Resources = (dir "WSMAN:\localhost\Plugin\$Plugin\Resources").PSPath
  # Pour chaque ressource du plugin
  foreach ($Resource in $Resources){
    Write-Host "`tResource Uri = " (Get-Item ("$Resource\ResourceUri")).value
    $Security = (dir ($Resource + "\Security")).PSPath
    Write-Host "`tSDDL = " $(dir ($Security + "\sddl")).value
    }
}
```

Listing 42 – Désactivation des *plugins* `WinRM` non nécessaires au transfert d'évènements

Le script PowerShell du listing 42 pour la désactivation des *plugins* `WinRM` non nécessaires au transfert d'évènements est également disponible au téléchargement sur GitHub [15].

En revanche, chercher à restreindre l'usage de `WinRM` en désactivant les sessions PowerShell distantes (par la commande « `Disable-PsRemoting` » notamment) n'a pas vraiment de sens puisque ces utilisateurs privilégiés restent en capacité d'exécuter des commandes à distance à travers

d'autres *plugins* de `WinRM` (notamment *WMI Provider* et *Microsoft.PowerShell*) et sont donc en capacité de réactiver les sessions PowerShell distantes. La désactivation des *plugins* de `WinRM` est donc nécessaire pour restreindre fonctionnellement ce dernier au strict transfert d'évènements.

#### G.1.3.4 serveurs disposant de plus de 3 Go de mémoire vive

Lorsqu'un serveur collecteur d'évènements dispose de plus de 3 Go de mémoire vive, les services `WinRM` et `WECSvc` ne s'exécutent pas dans le même hôte de service (processus `svchost.exe`) et cela nuit au bon fonctionnement de la collecte. Cela peut se vérifier en comparant le PID des deux services dans le gestionnaire de tâches. Si leurs PIDs sont différents alors il est nécessaire d'octroyer la permission `GENERIC EXECUTE` au SID du service `WECSvc` sur les URLs `http://+:5985/wsman/` et `http://+:5986/wsman/` gérées par le composant `HTTP.sys` (ou sur `http://+:80/wsman/` ou sur `http://+:443/wsman/` si des écouteurs de compatibilité ont été configurés), tel qu'indiqué dans l'article de support [21]. Cette opération devrait également être faite sur des serveurs disposant de moins de 3 Go de mémoire vive, en anticipation d'une future augmentation de leurs capacités.

### G.1.4 Création des abonnements

La dernière étape de configuration d'un serveur de collecte d'évènements consiste à créer un ou plusieurs abonnements. Un abonnement va indiquer quels évènements transférer au serveur de collecte, comment les transférer, à quelle fréquence, vers quel journal de destination, etc. Un abonnement peut être créé à l'aide de l'assistant graphique de l'observateur d'évènements, cette méthode ne donne alors accès qu'à un ensemble restreint de paramètres de configuration.

Il est préférable d'utiliser l'assistant graphique afin d'assurer la maintenabilité de la configuration dans le temps, à moins qu'une forte expertise des administrateurs ou des besoins spécifiques justifient de créer ou modifier les abonnements en ligne de commande à l'aide de l'outil `WECUtil` [44] ou au format XML, méthodes qui permettent de définir l'ensemble des paramètres de configuration possibles et d'automatiser la configuration d'un serveur de collecte.

Un abonnement créé graphiquement à travers l'observateur d'évènements produit une configuration XML automatiquement générée. Elle peut alors être éditée directement en XML via l'assistant graphique ou bien être exportée (commande *batch* indiquée par le listing 43). Par facilité, mais aussi pour éviter les erreurs – notamment dans la sélection des systèmes clients pouvant rejoindre les abonnements, exprimée par une chaîne SDDL [37] – il est préférable de configurer les différents abonnements graphiquement puis d'en éditer le XML automatiquement généré si nécessaire.

```
wecutil get-subscription "Nom_Abonnement" /f:XML > Nom_Abonnement.xml
```

Listing 43 – Export d'abonnement de collecte d'évènements au format XML

La sous-section G.1.4.1 porte sur les requêtes de sélection des évènements à transférer, tandis que la sous-section G.1.4.2 détaille la configuration des modalités de transfert et que la sous-section G.1.4.3 s'attache au redimensionnement du journal de destination.

#### G.1.4.1 Sélection des évènements à collecter

Différentes documentations sur Internet proposent des sélections d'évènements à collecter.

Microsoft propose des configurations d'abonnements types en annexes E et F de l'article « *Use Windows Event Forwarding to help with intrusion detection* » [47]. Cette sélection standard d'évènements est généralement suffisante pour appliquer la recommandation R13. L'ANSSI en propose toutefois une version légèrement modifiée sur GitHub [14].

Pour les entités exposées à un niveau de risque accru du fait de leurs activités métier, cette sélection standard d'évènements est insuffisante. C'est pourquoi il est leur recommandé (recommandation R14+) de réaliser une centralisation d'évènements additionnels en fonction des besoins de sécurité qui leurs sont propres, des spécificités de leurs SI et de leurs capacités de détection et d'analyse.

Microsoft propose également un tableau [46] qui répertorie les événements à surveiller plus particulièrement sur les contrôleurs de domaine AD ; il correspond aux recommandations du guide « *Monitoring Active Directory for Signs of Compromise* » [45]. Différentes entités publient également des exemples de sélections spécifiques de journaux dont il est utile de s'inspirer. C'est le cas par exemple de l'agence nationale de cyber sécurité australienne [1] ou du groupe Palantir [51].

### G.1.4.2 Modalités de transfert

Le tableau 6 indique les paramètres de configuration XML les plus utiles à renseigner pour la configuration d'un abonnement, ainsi que leurs valeurs recommandées. Il est à noter que les balises de configuration XML n'ont pas le même nom que les arguments qui leurs correspondent en ligne de commande de l'outil `WECUtil` [44]. Un abonnement peut également être modifié *a posteriori* par ligne de commande [44] afin de modifier ou préciser des paramètres de configuration complémentaires, comme illustré par le listing 44.

| Paramètres | Valeurs |
|---|---|
| `ConfigurationMode` | La valeur `Normal` est généralement un bon compromis, tandis que la valeur `Custom` permet de spécifier des valeurs personnalisées pour les paramètres de configuration `MaxLatencyTime`, `MaxItems`, `Heartbeat` et `Delivery`. |
| `ContentFormat` | La valeur `Events` indique aux clients de transférer les évènements sans leurs informations de localisation linguistique, ce qui est préférable pour réduire la volumétrie des évènements centralisés. La valeur `RenderedText` (valeur par défaut) permet de spécifier l'inverse. |
| `Delivery` | `<Delivery Mode="Push">` indique que les évènements transférés sont « poussés » par les systèmes clients (chacun initialisant régulièrement des connexions réseau vers le serveur collecteur) alors que `<Delivery Mode="Pull">` indique que les évènements transférés sont « tirés » par le service de collecte lui-même (c'est alors ce dernier qui initialise régulièrement des connexions vers les systèmes abonnés). |
| `Heartbeat` | Fréquence des signes de vie des clients lorsqu'aucun évènement n'est transféré, exprimé en millisecondes. La valeur par défaut de 15 minutes (900 000 millisecondes) est un bon compromis. |

Ce tableau se poursuit sur la page suivante

| Paramètres | Valeurs |
|---|---|
| `LogFile` | Le nom du journal de destination sur le serveur collecteur (le journal « Évènements transférés » ou tout autre journal personnalisé). |
| `MaxItems` | Une vague de transfert est déclenchée lorsque ce nombre maximum d'évènements en attente de transfert au serveur collecteur est atteint. Si la valeur est de 1, une vague de transfert est déclenchée dès qu'un évènement est journalisé, ce qui risque de générer de nombreuses connexions réseau vers le serveur collecteur. Il n'est généralement pas nécessaire de changer la valeur par défaut (50 000 évènements). |
| `MaxLatencyTime` | Temps maximum d'attente entre chaque vague de transfert d' évènements au serveur collecteur, exprimé en millisecondes. La valeur par défaut de 15 minutes (900 000 millisecondes) est généralement un bon compromis. |
| `ReadExistingEvents` | La valeur `false` indique au client de seulement transférer les futurs évènements, tandis que la valeur `true` indique de transférer tous les évènements passés[a] et futurs. |
| `SubscriptionType` | Le type d'abonnement doit correspondre au `Deliverymode` configuré :<br>- `SourceInitiated` pour le `<Delivery Mode="Push">`;<br>- `CollectorInitiated` pour le mode `<Delivery Mode="Pull">`. |

[a] Le transfert des évènements passés peut induire une charge réseau importante lorsque de nombreux systèmes rejoignent l'abonnement dans un court laps de temps.

Tableau 6 – Paramètres de configuration utiles pour les abonnements de collecte d'évènements

```
REM Le mode de configuration "custom" est nécessaire pour modifier certains paramètres.
wecutil set-subscription "Nom_Abonnement" /cm:custom
REM Définir la fréquence de transfert des évènements au serveur collecteur (ici: 60 secondes).
wecutil set-subscription "Nom_Abonnement" /dmlt:60000
```

Listing 44 – Modification d'un abonnement par ligne de commande

### G.1.4.3 Taille du journal de destination

Une fois l'abonnement créé sur un serveur collecteur d'évènements, il convient de modifier la taille de son journal de destination (c-à-d. le journal « Évènements transférés » par défaut) de manière à ce qu'il occupe autant d'espace que possible et tout en respectant la recommandation R5. Ce journal peut ainsi aisément occuper plusieurs centaines de gigaoctets. Les méthodes de redimensionnement d'un fichier de journal sont détaillées en section C.2.

Un abonnement créé est directement prêt à recevoir des évènements transférés, il ne reste alors plus qu'à configurer les systèmes clients pour le transfert des évènements (section G.2).

## G.2 Configuration des systèmes clients pour le transfert d'évènements en mode Push

La configuration des postes clients pour le transfert d'évènements vers un serveur collecteur d'évènements nécessite peu de paramétrage et peut entièrement se faire par GPO. Les différentes stratégies de groupes à utiliser sont détaillées dans les sous-sections G.2.1 à G.2.4. Elles peuvent toutes être regroupées au sein d'une seule et même GPO à appliquer aux systèmes clients.

### G.2.1 Configuration du client `WinRM`

Le client `WinRM` est nécessaire sur les systèmes pour transférer les évènements aux serveurs collecteurs d'évènements. Comme côté serveur, le client `WinRM` requiert que le service *Windows Remote Management* (`WinRM`) soit configuré en démarrage automatique. Cela peut se faire à l'aide d'une GPP de Service appliquée aux systèmes clients de manière identique à la GPP de Service appliquée aux serveurs collecteurs d'évènements (cf. figure 14 en sous-section G.1.1).

La configuration du service `WinRM` réalisée côté serveur de collecte d'évènements impose le chiffrement du trafic et limite les méthodes d'authentification acceptées. Ces paramètres définis côté serveur s'imposant dans la négociation client-serveur, il n'est pas nécessaire de réaliser une quelconque configuration côté client `WinRM`. Néanmoins, une entité qui souhaiterait préciser sa configuration explicite (par soucis de cohérence ou en suivant le principe de défense en profondeur) le ferait en configurant certains paramètres figurant dans le tableau 7 à l'aide de la stratégie de groupe indiquée par le listing 45.

| Paramètre | Valeur |
|---|---|
| Autoriser l'authentification de base | Désactivé (valeur par défaut) |
| Autoriser l'authentification CredSSP | Désactivé (valeur par défaut) |
| Autoriser le trafic non chiffré | Désactivé (valeur par défaut) |
| Ne pas autoriser l'authentification Digest | Activé |
| Ne pas autoriser l'authentification Kerberos | Désactivé (valeur par défaut) |
| Ne pas autoriser l'authentification par négociation | Activé[a] (valeur par défaut : Désactivé) |

[a] Sur les clients `WinRM`, il est recommandé de n'autoriser que Kerberos en activant ce paramètre. Se reporter aux avantages et inconvénients mentionnés en note de bas de page de la section G.1.3.1.

Tableau 7 – Paramètres de configuration des clients `WinRM`

```
Configuration ordinateur\Modèles d'administration\Composants Windows\Gestion à distance de
Windows (WinRM)\Client WinRM\
```

Listing 45 – Stratégie de configuration du client `WinRM` sur les systèmes clients

Dans le prolongement de cette démarche, il est également recommandé de s'assurer que les systèmes clients n'aient aucun *listener* `WinRM` actif. Cette restriction peut s'appliquer à l'aide de la stratégie de groupe du listing 46.

```
Configuration ordinateur\Modèles d'administration\Composants Windows\Gestion à distance de
Windows (WinRM)\Service WinRM\Autoriser la gestion de serveurs à distance via WinRM : Désactivé
```

Listing 46 – Stratégie de configuration du service `WinRM` sur les systèmes clients

### Information

Si des *listeners* `WinRM` sont toutefois utilisés sur les ressources du SI pour répondre à d'autres besoins (d'administration distante notamment), alors il est dans ce cas recommandé d'en restreindre l'accès par des règles de parefeu local (les *listeners* `WinRM` sont en écoute sur les ports 5985 et 5986 par défaut) en limitant les adresses distantes autorisées au strict minimum nécessaire (c'est à dire les adresses réseau des postes d'administration par exemple).

## G.2.2 Configuration des règles de pare-feu pour le client `WinRM`

Par défaut, le pare-feu intégré à Windows ne bloque pas les flux sortants. Si néanmoins ce comportement par défaut a été modifié et que le pare-feu les bloque, alors l'ajout de règles autorisant le trafic sortant du client `WinRM` est nécessaire. Ces règles peuvent être créées via la console d'administration du pare-feu Windows (`wf.msc`), en ligne de commande *batch* (listing 39) ou par GPO. Comme aucune règle prédéfinie n'existe pour autoriser ce flux en sortie, leur création doit se faire par règles de filtrage personnalisées (cf. figure 17).

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-Out)" dir=out
action=allow protocol=TCP remoteport=5985 remoteip=[liste des IP des collecteurs] service=WinRM
profile=domain,private enable=yes
```

Listing 47 – Ajout d'une règle de pare-feu en sortie pour le client `WinRM` par commande *batch*

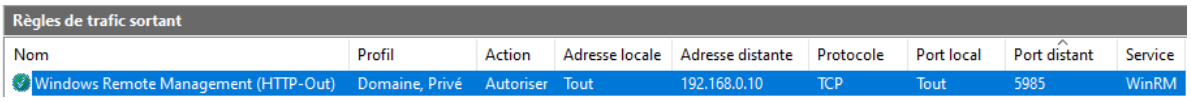


FIGURE 17 – Règle de pare-feu personnalisée pour autoriser le trafic sortant du client `WinRM` à destination d'un serveur de collecte d'évènements

### Information

Lorsque des *listeners* HTTPS sont utilisés sur les serveurs de collecte d'évènements, des règles similaires doivent être créées pour le port distant 5986. Si par ailleurs des *listeners* de compatibilité sont utilisés sur les ports 80 ou 443, les règles de trafic sortant pour `WinRM` doivent être adaptées en conséquence.

### G.2.3 Permissions de lecture sur les journaux

Le service `WinRM` est le service Windows chargé de transférer les évènements aux serveurs collecteurs d'évènements, c'est donc le service `WinRM` qui lit les journaux d'évènements locaux afin d'en extraire les évènements à transférer. Par défaut, le service `WinRM` s'exécute dans le contexte du compte « `NT AUTHORITY\NETWORK SERVICE` » (ou « `Autorité NT\Service réseau` » sur un système d'exploitation en langue française) de SID *S-1-5-20*. Ce compte ne dispose pas de droits de lecture sur l'ensemble des journaux d'évènements locaux. Le journal de sécurité, par exemple, ne lui est donc pas accessible. Cela peut également être le cas de certains journaux de services et applications et notamment du journal *sysmon*.

Une étape de configuration des systèmes clients consiste alors à octroyer les permissions de lecture au compte `NT AUTHORITY\NETWORK SERVICE` sur l'ensemble des journaux sources depuis lesquels des évènements doivent être transférés aux serveurs collecteurs d'évènements.

Octroyer ces permissions peut par exemple se faire de deux manières :

- en ajoutant le compte `NT AUTHORITY\NETWORK SERVICE` au groupe local intégré `Event Log Readers` de SID `S-1-5-32-573`, car ce dernier a les droits de lecture sur tous les journaux de l'ordinateur. Il s'agit de la méthode à privilégier mais elle nécessite un redémarrage des systèmes clients pour être prise en compte. Une stratégie de groupe appliquée à tous les systèmes journalisés peut être utilisée pour configurer l'appartenance à un groupe utilisateur local par GPO, elle est indiquée par le listing 48 et illustrée par la figure 18 ;
- en octroyant explicitement un droit de lecture au compte `NT AUTHORITY\NETWORK SERVICE` sur chaque journal d'évènements. Cette méthode est à retenir uniquement en cas de besoin de n'octroyer les droits que sur certains journaux bien spécifiques. Cela peut se faire en modifiant leur descripteur de sécurité, par la concaténation du descripteur existant (cf. commandes du listing 50) et de la chaîne de caractères « `(A;;0x1;;;S-1-5-20)` ». Pour les journaux Windows historiques, cela peut se faire par GPO à l'aide de la stratégie figurant dans le listing 49 et comme illustré par la figure 19 ou par GPP. Pour les journaux des services et applications, il est possible de procéder par script (à l'aide des commandes du listing 50) ou par clés de registre (à l'aide des clés de registre du listing 51).

```
Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Groupes restreints\
```

Listing 48 – Stratégie de restriction des membres d'un groupe

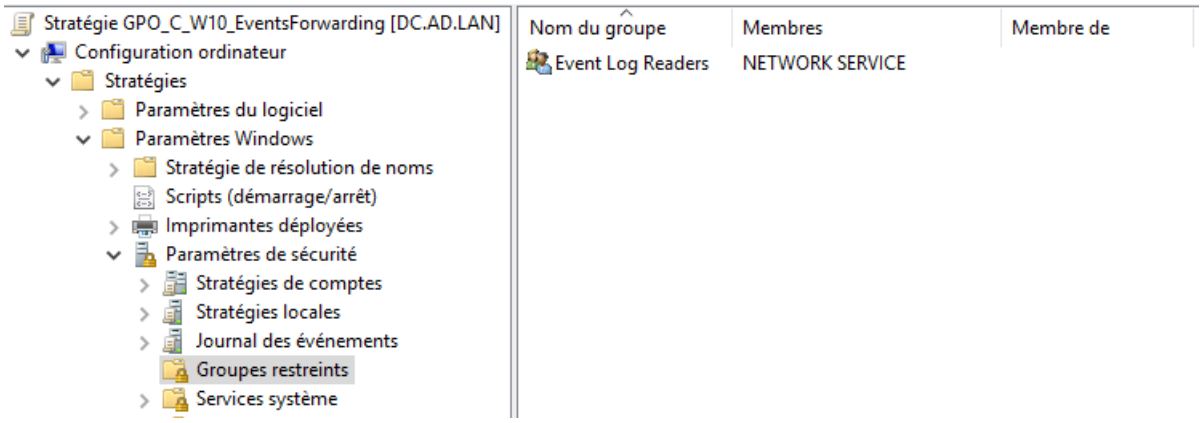


FIGURE 18 – Restriction de l'appartenance au groupe intégré *Event Log Readers*

## Attention

La stratégie de groupe illustrée par la figure 18 a pour effet de restreindre l'appartenance au groupe *Event Log Readers* aux seuls comptes explicitement listés. Si, sur certains systèmes, des comptes utilisateurs sont déjà membres de ce groupe pour d'autres besoins, alors ils s'en trouvent retirés. Dans ce cas, il convient soit de préciser explicitement l'appartenance de ces autres comptes au groupe *Event Log Readers* par la même stratégie de groupe, soit de préférer l'usage d'une GPP d'utilisateurs et de groupes locaux. Cette dernière permet de simplement ajouter une appartenance à un groupe, sans supprimer ses membres actuels.

```
Configuration ordinateur\Modèles d'administration\Composants Windows\Service Journal des
évènements\Sécurité\Configurer l'accès au journal
```

Listing 49 – Stratégie de configuration des droits d'accès aux journaux Windows

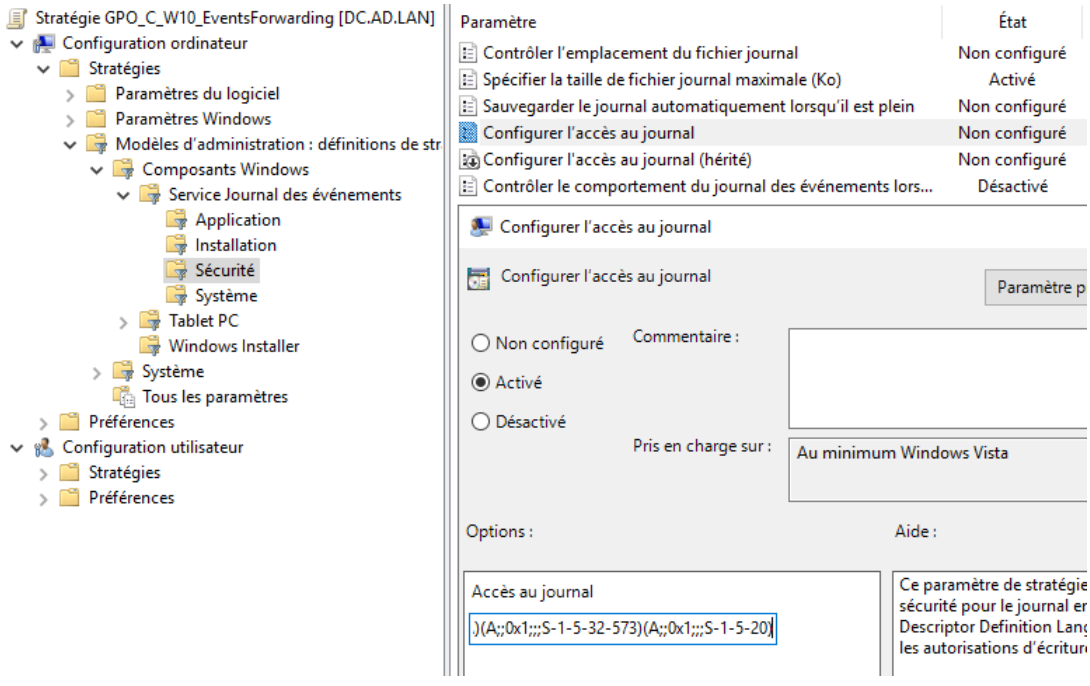


FIGURE 19 – Stratégie de configuration du descripteur de sécurité du journal Windows de sécurité

```
REM Affichage du descripteur de sécurite d'un journal d'évènements (channelAccess)
wevtutil get-log <nom de journal>
REM Modification du descripteur de sécurité d'un journal d'évènements
wevtutil set-log <nom de journal> /ca:"<descripteur de sécurité>"
```

Listing 50 – Lignes de commande *batch* pour la manipulation des descripteurs de sécurité des journaux d'évènements

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\<nom de journal>\ChannelAccess
```

Listing 51 – Clés de registre pour la manipulation des descripteurs de sécurité des journaux d'évènements

### Information

L'utilisation du compte virtuel [41] `NT SERVICE\WINRM` (de SID *S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970*) est sensiblement préférable à l'utilisation du compte `NT AUTHORITY\NETWORK SERVICE` car elle octroie les droits spécifiquement au service WinRM plutôt qu'à l'ensemble des services Windows. Dans certains cas, la MMC peut toutefois dysfonctionner lors de la manipulation de stratégies de groupe qui utilisent ce compte virtuel, il est donc conseillé de procéder par script.

Un script PowerShell est proposé au téléchargement sur GitHub [17] pour, entre autres, automatiser l'octroi des permissions de lecture adéquates au compte virtuel `NT SERVICE\WINRM` sur les journaux du tableau 2.

## G.2.4 Souscription aux abonnements de type push

Le rattachement des systèmes clients à un serveur collecteur d'évènements se configure par une URL en indiquant :

- le protocole (HTTP dans le cas présent, ou HTTPS si un *listener* HTTPS a été configuré) ;
- le serveur collecteur d'évènements (il est recommandé de le renseigner au format FQDN pour le bon fonctionnement de l'authentification Kerberos) ;
- le port (5985 en HTTP par défaut) ;
- optionnellement, la fréquence de rafraîchissement [9] ;
- optionnellement, l'empreinte du certificat serveur lorsque le protocole HTTPS est utilisé.

La stratégie de groupe indiquée par le listing 52 permet d'indiquer aux systèmes clients l'URL de leur gestionnaire d'abonnements de rattachement selon la syntaxe décrite par le listing 53 et comme illustré par la figure 20. Il est par ailleurs à noter que plusieurs URLs de serveurs de collecte peuvent être renseignés, il suffit pour cela de renseigner plusieurs valeurs, ligne par ligne. Il est toutefois rappelé que la configuration d'un WEF pour l'envoi des évènements vers plusieurs serveurs WEC se traduit par l'envoi redondant de ses évènements à chacun des serveurs WEC.

9. La fréquence de rafraîchissement, exprimée en secondes, est la fréquence à laquelle les systèmes clients vont lire la configuration des abonnements et vont ainsi appliquer toute nouvelle directive de transfert d'évènements. Si la configuration des abonnements change rarement, un rafraîchissement toutes les heures ou moins souvent est suffisant (se reporter aux recommandations de Microsoft [48]).

```
Configuration ordinateur\Modèles d'administration\Composants Windows\Transfert
d'évènements\Gestionnaire d'abonnements cible
```

Listing 52 – Stratégie de configuration du gestionnaire d'abonnements cible

```
Syntaxe attendue (valeurs entre crochets à remplacer) :
Server=[PROTO]://[FQDN]:[PORT]/wsman/SubscriptionManager/WEC,Refresh=[TEMPS],IssuerCA=[EMPREINTE]

Exemple :
Server=HTTP://WEC01.AD.LAN:5985/wsman/SubscriptionManager/WEC,Refresh=3600
Server=HTTP://WEC02.AD.LAN:5985/wsman/SubscriptionManager/WEC,Refresh=3600
```

Listing 53 – Syntaxe de configuration du gestionnaire d'abonnements cible

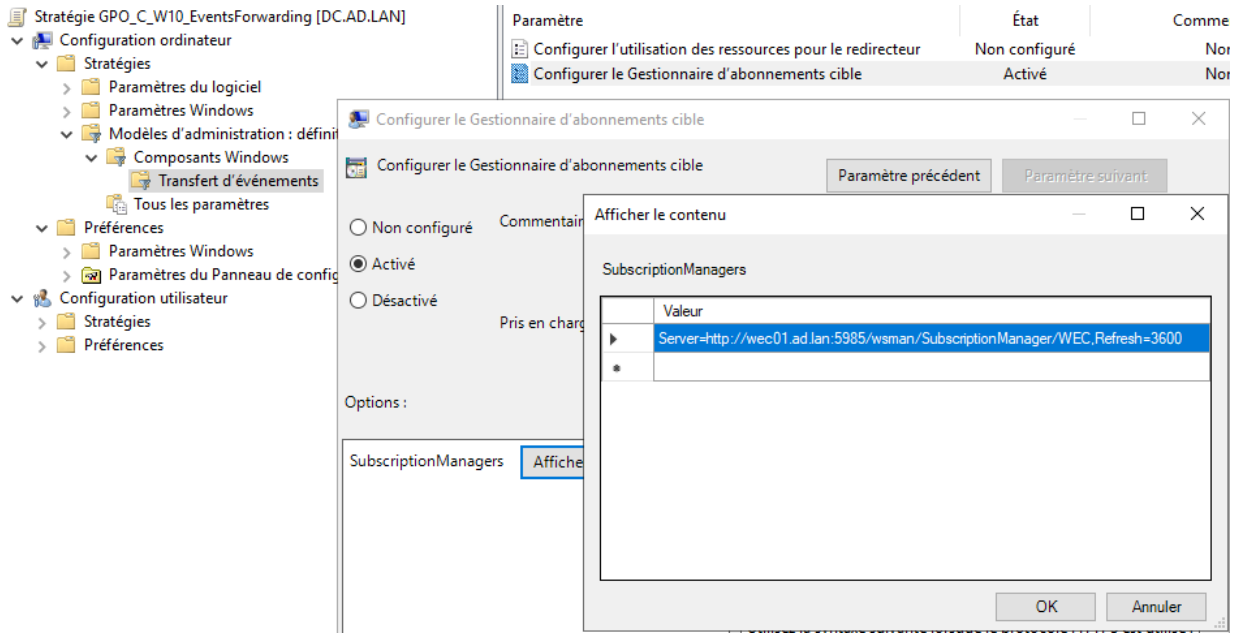


FIGURE 20 – Stratégie de configuration du gestionnaire d'abonnements cible

Une fois cette stratégie appliquée, les clients WEF souscrivent aux abonnements qui les concernent.

En cas de dysfonctionnement du transfert d'évènements vers les serveurs de collecte, la section G.4 aide à la résolution des problèmes les plus courants.

## G.3 Spécificités du mode Pull

L'utilisation d'abonnements en mode *Pull* modifie quelque peu le déploiement illustré dans cette annexe. En mode *Pull*, il n'est plus question de systèmes clients abonnés car le client devient une source d'évènements (c'est-à-dire les systèmes auxquels le service de collecte se connecte pour aller chercher des évènements).

Dans cette configuration, le serveur collecteur devient un client `WinRM` et les sources d'évènements sont des serveurs `WinRM`. La configuration du service `WinRM` serveur – abordée en section G.1 – devient donc recommandée sur les systèmes sources d'évènements et la configuration du service `WinRM` client (section G.2) devient quant à elle recommandée sur chaque serveur de collecte.

En conséquence, les règles de pare-feu nécessaires au service `WinRM` serveur (section G.1.3.2) doivent dans ce cas être configurées sur les systèmes sources d'évènements avec une restriction d'adresses IP sources qui correspondent aux IP des serveurs collecteurs d'évènements. Réciproquement, les règles nécessaires sur les systèmes clients abonnés en mode *Push* (section G.2.2) deviennent nécessaires sur les serveurs collecteurs d'évènements (avec une restriction d'IP sources qui correspondent dans ce cas et si possible aux plages d'adresses IP des systèmes sources d'évènements).

Par ailleurs, les systèmes sources d'évènements des abonnements en mode *Pull* n'ont pas besoin d'être configurés pour s'abonner au transfert d'évènements. La configuration réalisée en section G.2.4 est alors inutile puisqu'il revient au service collecteur d'évènements d'aller chercher les évènements par lui-même selon les paramètres de configuration des abonnements.

Enfin, comme indiqué en section 3.4, le mode *Pull* requiert un compte disposant de droits en lecture sur les journaux d'évènements de tous les systèmes sources d'évènements de ses abonnements.

### Attention

Il est recommandé d'utiliser le compte d'ordinateur (*machine account*) du serveur de collecte et de proscrire l'utilisation d'un compte utilisateur. Un compte d'ordinateur présente l'avantage d'avoir un mot de passe très complexe, aléatoire et renouvelé automatiquement, tandis que l'utilisation d'un compte utilisateur implique une gestion régulière par les administrateurs pour présenter les mêmes caractéristiques. Par ailleurs, l'utilisation d'un compte utilisateur est davantage exposée à des mauvaises pratiques ; il peut ainsi plus facilement servir de moyen de déplacement latéral à un attaquant, voire de moyen d'élévation de privilèges vers des ressources du SI s'il s'agit d'un compte disposant d'accès privilégiés (le compte administrateur du domaine par exemple).

### Déplacement latéral

Au cours d'une attaque, la phase de déplacement latéral représente le déplacement d'un attaquant d'un système à un autre qui lui est équivalent (entre postes de travail de bureautique par exemple).

Pour le bon fonctionnement de cette configuration, les comptes d'ordinateur des différents serveurs collecteurs d'évènements doivent alors se voir octroyer le droit de lecture des journaux sur les systèmes sources d'évènements. Pour cela, un groupe « WindowsEventCollectors » contenant les comptes d'ordinateur des serveurs collecteurs d'évènements peut par exemple être créé dans l'AD. Il suffit ensuite de le rendre membre du groupe `Event Log Readers` sur les systèmes sources d'évènements, de la même manière qu'illustré pour le compte `NT AUTHORITY\NETWORK SERVICE` en section G.2.3 par la figure 18.

## G.4 Dépannage

En cas de dysfonctionnement du transfert d'évènements vers les serveurs de collecte, cette section aide à la résolution des problèmes les plus courants.

En cas de défaut de réception d'évènements par un serveur de collecte, la démarche de vérification suivante peut être menée sur ce dernier :

1. vérifier que les services `WinRM`, et `WECSvc` sont démarrés (la configuration de ces services sur un serveur de collecte est abordée en sections G.1.1 et G.1.2) ;
2. vérifier que le service `WinRM` écoute sur les interfaces attendues (la commande PowerShell du listing 54 peut être utilisée et cette dernière doit indiquer les bons adresse IP et port d'écoute du service) ;
3. consulter le journal `Microsoft-Windows-EventCollector/Operational` du serveur de collecte. Un évènement d'identifiant 5 indique l'activation réussie d'un abonnement et dans ce cas l'erreur est plutôt à rechercher sur les postes clients. En revanche :
   a) un évènement d'identifiant 1 indique un possible problème de communication avec le serveur de collecte. Vérifier dans ce cas que les ports du pare-feu sont ouverts pour `WinRM` (port 5985 par défaut, comme précisé en section G.1.3.2) ;
   b) un évènement d'identifiant 6 indique un possible problème d'écriture dans le journal de destination de l'abonnement : vérifier dans ce cas l'exactitude du nom de journal et les droits d'accès à ce dernier ;
4. vérifier la configuration des abonnements. L'apparition d'évènements d'identifiant 101 dans le journal `Microsoft-Windows-Forwarding/Operational` des postes clients abonnés signifie généralement que la requête XPath de sélection des évènements collectés est incorrecte.

En cas de dysfonctionnement du transfert d'évènements par un poste client, la démarche de vérification suivante peut être menée sur ce dernier :

1. vérifier que le service `WinRM` est bien démarré (la configuration du service `WinRM` sur les postes clients est abordée en section G.2.1) ;
2. s'assurer que l'URL du collecteur est configurée et qu'elle est joignable depuis les postes clients. Pour cela :
   a) vérifier que la valeur de clé de registre indiquée par le listing 55 est correctement renseignée et qu'elle indique le FQDN et le numéro de port attendus (se référer à la section G.2.4 pour la construction de l'URL du serveur de collecte) ;
   b) utiliser la commande du listing 56 pour vérifier la connectivité avec le serveur de collecte ;
   c) consulter les évènements du journal `Microsoft-Windows-Forwarding/Operational` du poste client pour prendre connaissance des erreurs de communication avec le serveur de collecte (évènements d'identifiant 105) ou au contraire constater la bonne connectivité (évènements d'identifiant 104). Les évènements d'identifiant 105 peuvent révéler différentes erreurs :
      i. le code d'erreur 2150859027 peut indiquer que le serveur de collecte dispose de plus de 3 Go de RAM. Dans ce cas, vérifier la configuration indiquée en section G.1.3.4 et s'assurer que le serveur ait redémarré depuis cette modification ;
      ii. un message d'accès refusé indique généralement un problème d'authentification. Vérifier dans ce cas que les configurations de `WinRM` côté client (tableau 7) et côté serveur (tableau 5)

autorisent l'authentification Kerberos. Vérifier également que le client dispose d'un ticket Kerberos permettant de se connecter au collecteur (la commande du listing 57 devrait indiquer la présence d'un ticket Kerberos pour le serveur de collecte de type « `HTTP/[SERVEUR DE COLLECTE].[DOMAINE]@[DOMAINE]` »). Dans le cas contraire, un simple redémarrage du poste client peut suffire, sinon il est probable qu'il y ait des problèmes de configuration de l'AD causant des erreurs d'authentification Kerberos au sein du domaine. Des tickets Kerberos trop gros [26] peuvent également causer de tels dysfonctionnements ;

iii. un problème de nom du serveur qui ne peut pas être résolu indique que la résolution DNS du serveur de collecte par le poste client n'est pas possible, auquel cas soit l'adresse du collecteur est erronée (cf. section G.2.4), soit des entrées DNS sont manquantes ;

3. s'assurer que le service `WinRM` dispose des droits d'accès sur tous les journaux selectionnés dans les abonnements du collecteur (problématique traitée en section G.2.3). Lorsque ce n'est pas le cas, le journal d'évènements `Microsoft-Windows-Forwarding/Operational` devrait faire apparaître des évènements d'identifiant 101 ;

4. dans le journal `Microsoft-Windows-WinRM/Operational`, les évènements 142 ou 161 (code d'erreur 0x80338012) peuvent indiquer qu'un serveur mandataire (*proxy*) http a été configuré dans les options réseau des systèmes abonnés. Si c'est le cas, modifier leur configuration pour ne pas utiliser de serveur mandataire pour les adresses internes telles que celles des serveurs de collecte. L'utilisation d'un serveur mandataire avec `WinRM` fait l'objet de l'article [50] de Microsoft ;

5. lorsqu'un serveur de collecte s'abonne à lui-même, un filtre des IPv6 autorisées à se connecter (cf. tableau 5) peut poser problème étant donné que le collecteur utilisera l'IPv6 interne de la machine par défaut.

```
Get-WSManInstance -ResourceURI winrm/config/listener -Enumerate -Computername [FQDN du serveur de collecte]
```

Listing 54 – Commande PowerShell de vérification des interfaces d'écoute de `WinRM`

```
HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\EventForwarding\SubscriptionManager
```

Listing 55 – Valeur de clé de registre de configuration de l'URL du serveur de collecte

```
winrm identify -r:http://[FQDN DU SERVEUR DE COLLECTE]:5985
```

Listing 56 – Commande *batch* de vérification de la connectivité avec le serveur de collecte

```
klist tickets
```

Listing 57 – Commande *batch* d'énumération des tickets Kerberos

# Annexe H
# Arborescence personnalisée de journaux pour les serveurs collecteurs d'évènements

Tous les évènements transférés par les systèmes clients pour un abonnement donné sont enregistrés dans un unique journal du serveur collecteur d'évènements, configurable à la création d'un abonnement. Il peut alors s'agir d'un des journaux Windows historiques du serveur (Application, Système et Sécurité) ou d'un de ses nombreux journaux des services et applications prédéfinis. Le journal unique intitulé « Évènements transférés » est proposé par défaut et il est dédié à cet usage.

Lorsque les évènements ne font que transiter par des serveurs de collecte pour être ensuite ingérés dans des outils de détection et d'analyse des incidents de sécurité (en interne ou externalisés à un PDIS), il est pertinent qu'ils soient tous enregistrés dans un seul et même journal du serveur collecteur d'évènements. En l'absence de tels outils ou pour répondre à des besoins particuliers, il peut en revanche s'avérer utile de disposer de plusieurs journaux distincts, ce qui permet notamment :

- de configurer des tailles différentes de journaux et des politiques distinctes de rétention ou de transfert vers d'autres équipements (vers d'autres serveurs de collecte d'évènements ou vers différents SIEM par exemple) ;
- de définir au cas par cas l'emplacement de chaque fichier de journal sur des volumes de stockage distincts, ces volumes pouvant alors présenter différentes caractéristiques (volumétrie, disponibilité, performance, etc.) ;
- d'octroyer des droits de lecture journal par journal, à des utilisateurs ayant des besoins de consultation de ces derniers (par exemple, un administrateur en charge de la maintenance des règles AppLocker [10] pourrait avoir un droit de lecture uniquement sur le journal de centralisation des évènements d'Applocker) et tout en respectant les recommandations de protection des journaux du guide générique sur la journalisation [6].

Comme chaque abonnement (cf. section G.1.4) n'écrit par ailleurs ses évènements que dans un seul journal, la séparation des évènements collectés en différents journaux nécessite de configurer plusieurs abonnements complémentaires. Cette séparation des abonnements peut suivre différentes logiques, comme par exemple :

- une séparation par catégories de systèmes (postes de travail, postes d'administration, serveurs, contrôleurs de domaine, ressources très sensibles, moins sensibles, etc.) ;

10. AppLocker est un mécanisme de restriction logicielle. Se référer au recommandations de l'ANSSI pour la mise en œuvre d'une politique de restrictions logicielles sous Windows [2].

- une séparation par types d'évènements (authentifications, stratégies de restriction logicielle, fonctionnalités de *Windows Defender*, etc.).

Pour définir une arborescence structurée de journaux, une méthode consiste à écrire un manifeste d'instrumentation. Les spécifications d'un tel manifeste sont détaillées dans le centre de documentation de Microsoft [24]. L'écriture d'un manifeste d'instrumentation pour la création de journaux de transfert d'évènements a également fait l'objet d'un tutoriel [27] de l'éditeur, reposant sur l'utilisation d'un assistant graphique intégré au SDK (*Software Development Kit*) de Windows : `EcManGen` (*Event Channel Manifest Generator*). La procédure simplifiée proposée ci-après s'inspire de ces deux sources d'information mais n'utilise pas cet assistant graphique.

L'ajout de journaux sur les serveurs collecteurs d'évènements se réalise en plusieurs étapes détaillées dans les sections H.1 à H.3 :

1. écriture du manifeste d'instrumentation ;
2. installation du SDK de Windows et compilation du manifeste ;
3. ajout et configuration des journaux sur les serveurs collecteurs d'évènements.

# H.1 Écriture d'un manifeste d'instrumentation

L'écriture d'un manifeste simplifié pour couvrir le seul besoin de centralisation des évènements transférés ne requiert pas de s'intéresser en détail aux spécifications des manifestes d'instrumentation. Les possibilités de localisation linguistique peuvent également être ignorées la plupart du temps. Il est ainsi possible de partir du modèle de manifeste du listing 58 et de l'adapter par copier-coller des balises `<provider>` en respectant les quelques indications qui suivent :

- chaque `<provider>` doit avoir son propre GUID renseigné dans l'attribut `guid` correspondant. Par simplicité, il est possible d'utiliser un générateur de GUID aléatoire ;
- chaque `<provider>` doit indiquer un chemin de DLL dans ses attributs `resourceFileName` et `messageFileName`. Il s'agit de la DLL qui sera compilée à l'aide du manifeste : elle n'existe donc pas encore au moment de l'écriture du manifeste d'instrumentation. Il est recommandé de spécifier un chemin dans `C:\Windows\System32\` (qui n'est accessible en écriture que par des administrateurs) et de choisir un nom de DLL qui ne prête pas à confusion ;
- chaque `<provider>` du manifeste peut être vu comme un dossier de l'arborescence des journaux des services et applications, telle qu'elle apparaîtra dans la console de l' « observateur d'évènements » de Windows. Dans le nom de chaque `<provider>` (attribut `name`), le caractère « tiret » (« - ») fait office de séparateur de dossiers (tout comme le caractère « \ » dans un chemin UNC). Ainsi, un nom de `<provider>` « WEC-Workstations » se traduit par un sous-dossier « Workstations » dans le dossier parent « WEC ». L'arborescence ne peut toutefois pas excéder 3 niveaux de dossiers imbriqués, à partir du quatrième niveau les tirets cessent d'être pris en compte comme des séparateurs de dossiers et font partie intégrante du nom du dossier. Par simplicité, l'attribut `symbol` de chaque `<provider>` doit être renseigné à l'identique que l'attribut `name`, en remplaçant néanmoins chaque caractère « tiret » par un caractère « tiret bas » (« _ ») également appelé *underscore* ;

- chaque `<channel>` peut être vu comme un journal. Son nom (attribut `name`) doit reprendre le nom de son `<provider>` suivi du caractère « tiret » puis du nom de journal souhaité. Ainsi, le nom de `<channel>` « WEC-Workstations-System » se traduit par un journal nommé « System » dans le sous-dossier « Workstations » du dossier parent « WEC » ;
- il ne peut y avoir que sept `<channel>` maximum déclarés dans chaque `<provider>` (c'est-à-dire sept journaux par sous-dossier), en revanche il peut y avoir autant de `<provider>` que souhaité.

L'écriture d'un manifeste d'instrumentation pour obtenir une arborescence personnalisée de journaux consiste ainsi à copier-coller un ensemble de balises `<provider>` tel qu'illustré dans le listing 58 (l'exemple de manifeste d'instrumentation complet est proposé au téléchargement sur GitHub [11]). Chaque entité peut ainsi définir une arborescence de journaux adaptée à la fois à ses besoins de sécurité, aux abonnements configurés et à la taille de son système d'information.

## Information

L'objectif de cette annexe et du listing 58 est simplement de créer une arborescence personnalisée de journaux simples et à des fins de centralisation catégorisée. Pour rentrer plus en profondeur dans l'utilisation des manifestes d'instrumentation pour la définition d'évènements personnalisés, de filtres, tâches, opérations, etc., se reporter à la documentation de Microsoft [24].

```
<!-- Le début de manifeste a été tronqué dans cet extrait -->
<!-- Journaux Legacy -->
<provider name="WEC-T2-Legacy" symbol="WEC_T2_Legacy" guid="{CF27F07F-7013-483A-BC74-97A0F6AA3201}"
          resourceFileName="C:\Windows\system32\WECEventChannels.dll" messageFileName="c:\Windows\system32\WECEventChannels.dll">
  <!-- Toujours laisser la balise <events> tel quelle dans chacun des <provider> -->
  <events>
    <event symbol="DUMMY_EVENT" value="100" version="0" template="DUMMY_TEMPLATE"
           message="$(string.Custom Forwarded Events.event.100.message)">
    </event>
  </events>
  <!-- Ici, 3 journaux sont définis : System, Application, Security. -->
  <channels>
    <channel name="WEC-T2-Legacy-System" type="Operational" enabled="true"></channel>
    <channel name="WEC-T2-Legacy-Application" type="Operational" enabled="true"></channel>
    <channel name="WEC-T2-Legacy-Security" type="Operational" enabled="true"></channel>
  </channels>
  <!-- Toujours laisser la balise <templates> tel quelle dans chacun des <provider> -->
  <templates>
    <template tid="DUMMY_TEMPLATE">
      <data name="Prop_UnicodeString" inType="win:UnicodeString" outType="xs:string">
      </data>
      <data name="PropUInt32" inType="win:UInt32" outType="xs:unsignedInt">
      </data>
    </template>
  </templates>
</provider>
<!-- Journaux des fonctionnalités liées à la restriction de code (applocker, SRP, CI...) -->
<provider name="WEC-T2-CodeRestriction" symbol="WEC_T2_CodeRestriction" guid="{CF27F07F-7013-483A-BC74-97A0F6AA3202}"
          resourceFileName="C:\Windows\system32\WECEventChannels.dll" messageFileName="c:\Windows\system32\WECEventChannels.dll">
  <events>
    <event symbol="DUMMY_EVENT" value="100" version="0" template="DUMMY_TEMPLATE"
           message="$(string.Custom Forwarded Events.event.100.message)">
    </event>
  </events>
  <channels>
    <channel name="WEC-T2-CodeRestriction-AppLocker Exe and DLL" type="Operational" enabled="true"></channel>
    <channel name="WEC-T2-CodeRestriction-AppLocker MSI and Script" type="Operational" enabled="true"></channel>
    <channel name="WEC-T2-CodeRestriction-CodeIntegrity" type="Operational" enabled="true"></channel>
  </channels>
  <templates>
    <template tid="DUMMY_TEMPLATE">
      <data name="Prop_UnicodeString" inType="win:UnicodeString" outType="xs:string">
      </data>
      <data name="PropUInt32" inType="win:UInt32" outType="xs:unsignedInt">
      </data>
    </template>
  </templates>
</provider>
<!-- Et ainsi de suite avec autant de <provider> que nécessaire -->
<!-- La fin de manifeste a été tronquée dans cet extrait -->
```

Listing 58 – Extrait des `<provider>` définis dans un exemple de manifeste d'instrumentation

Une fois ce manifeste d'instrumentation 58 compilé et installé (voir section H.2), l'arborescence qui en résulte se traduira visuellement dans l'« observateur d'évènements » de Windows tel qu'illustré par la figure 21.

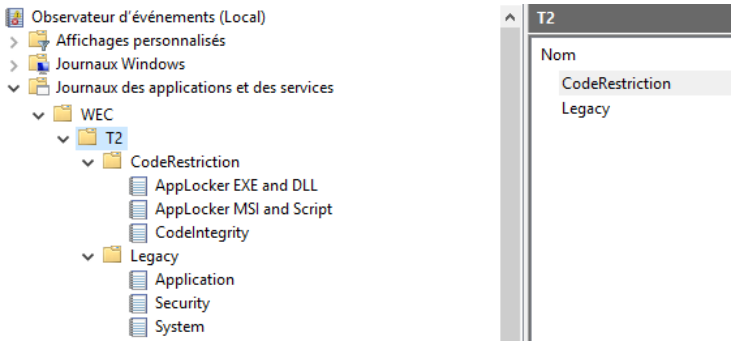


FIGURE 21 – Exemple d'arborescence personnalisée de journaux, telle qu'affichée dans l'« observateur d'évènements » de Windows

## H.2 Compilation d'un manifeste d'instrumentation

La compilation du manifeste d'instrumentation nécessite l'installation du SDK [11] de Windows. Il est recommandé de le faire sur un système jetable plutôt que directement sur un système en production. L'utilisation d'une machine virtuelle sous Windows 10 avec le dernier SDK répond ainsi tout-à-fait au besoin.

Une fois le SDK installé, la suite d'instructions *batch* du listing 59 permet de compiler le manifeste d'instrumentation. À l'issue de cette compilation, le manifeste d'instrumentation est accompagné d'une DLL du même nom. Ces deux fichiers doivent ensuite être installés sur les serveurs collecteurs d'évènements pour ajouter les journaux définis dans le manifeste.

```
REM Pour toutes les lignes de commandes ci-dessous :
REM 1) remplacer les chemins des binaires du SDK par ceux réellement présents sur le
REM système utilisé pour la compilation.
REM 2) déposer le manifeste d'instrumentation dans le dossier "c:\temp\" ou changer les chemins
REM dans chacune des lignes de commande.
REM 3) remplacer le terme "WECEventChannels" par celui donné au manifeste d'instrumentation, s'il
REM est différent.

"C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64\mc.exe" c:\temp\WECEventChannels.man

"C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64\mc.exe" -css
WECEventChannels.DummyEvent c:\temp\WECEventChannels.man

"C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64\rc.exe" c:\temp\WECEventChannels.rc

"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /win32res:C:\temp\WECEventChannels.res
/unsafe /target:library /out:C:\temp\WECEventChannels.dll C:\temp\WECEventChannels.cs
```

Listing 59 – Lignes de commande *batch* pour la compilation d'un manifeste d'instrumentation

11. Les SDK de Windows 10 sont téléchargeables depuis le site Web de Microsoft [42].

### Information

Il est à noter que cette compilation est à réaliser une fois pour toutes. Si par la suite des balises `<channel>` ou `<provider>` sont ajoutées, modifiées ou supprimées du manifeste d'instrumentation (pour ajouter, modifier ou supprimer des journaux), la DLL compilée reste quant à elle inchangée. Cet environnement de compilation peut donc être détruit à l'issue de la compilation initiale.

## H.3 Installation d'un manifeste d'instrumentation

Le fichier `.man` (le manifeste d'instrumentation) et sa `.DLL` (compilée à partir du manifeste d'instrumentation en section H.2) doivent être déposés sur les serveurs collecteurs d'évènements, à l'emplacement défini dans le manifeste par les attributs `resourceFileName` et `messageFileName`. Une fois les fichiers déposés à leur emplacement prévu, la commande *batch* du listing 60 permet – avec des privilèges d'administration locaux – d'installer le manifeste d'instrumentation à l'aide de l'outil `WEVTUtil` [49], ce qui a pour conséquence d'ajouter les journaux qu'il définit. Ils deviennent alors utilisables par les abonnements du service collecteur d'évènements.

```
wevtutil im c:\Windows\System32\WECEventChannels.man
```

Listing 60 – Commande *batch* d'installation d'un manifeste d'instrumentation

À la suite de l'installation du manifeste, il convient de configurer la taille de chacun des journaux ajoutés afin qu'ils soient en mesure de recevoir le volume attendu d'évènements transférés. Leur taille par défaut est de 1 Mo, ce qui est insuffisant pour de la centralisation d'évènements. Le script PowerShell du listing 61 illustre une méthode de redimensionnement en masse des journaux.

```
# Le redimensionnement s'effectue pour chaque journal dont le chemin complet commence par "WEC-".
# Si l'arborescence définie par le manifeste est différente, il convient de changer le pattern :
$array = wevtutil el | select-string -pattern "WEC-"
foreach ($s in $array) {
    # Taille de 1 Go :
    wevtutil sl $s /ms:1086373952
}
```

Listing 61 – Redimensionnement en masse de journaux en PowerShell

### Attention

Le manifeste d'instrumentation peut être modifié par la suite pour ajouter, modifier ou supprimer des journaux. Il est dans ce cas à noter que le remplacement du fichier `.man` ne suffit pas : l'ancien manifeste doit tout d'abord être désinstallé et le nouveau manifeste doit être installé par la suite, comme indiqué en commandes *batch* par le listing 62 (l'observateur d'évènements doit par ailleurs être fermé pendant l'opération de remplacement). Les journaux qui restent définis à l'identique par le manifeste de remplacement restent inchangés (ils gardent leurs paramètres et leur contenu), en revanche ceux qui ont changé de nom complet (arborescence + nom de journal) perdent leurs contenus et leurs paramètres.

```
REM 1) arrêt du service collecteur d'évènements
net stop wecsvc
REM 2) désinstallation de l'ancien manifeste [renseigner le bon nom de fichier]
wevtutil um c:\Windows\System32\WECEventChannels.man
REM 3) remplacement du manifeste [renseigner la source et la destination adéquates]
copy /Y c:\temp\WECEventChannels.man c:\Windows\System32\
REM 4) installation du nouveau manifeste  [renseigner le bon nom de fichier]
wevtutil im c:\Windows\System32\WECEventChannels.man
REM 5) démarrage du service collecteur d'évènements
net start wecsvc
```

Listing 62 – Remplacement d'un manifeste d'instrumentation

# Liste des recommandations

# Bibliographie


[1] *ACSC's Windows Event Logging - GitHub repository*.
Dépôt github, ACSC, juillet 2017.
https://github.com/AustralianCyberSecurityCentre/windows_event_logging.

[2] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*.
Note technique DAT-NT-013/ANSSI/SDE/NP v2.0, ANSSI, janvier 2017.
https://www.ssi.gouv.fr/windows-restrictions-logicielles.

[3] *Attaques par rançongiciels, tous concernés*.
Guide ANSSI-GP-077 v1.0, ANSSI, septembre 2020.
https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident.

[4] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide.

[5] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://www.ssi.gouv.fr/securisation-admin-si.

[6] *Recommandations de sécurité pour l'architecture d'un système de journalisation*.
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
https://www.ssi.gouv.fr/journalisation.

[7] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf.

[8] *Prestataires de réponse aux incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, août 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pris_referentiel_v2.0.pdf.

[9] *Les serveurs de temps NTP français*.
Page web, GIP RENATER.
https://services.renater.fr/ntp/serveurs_francais.

[10] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[11] *Exemple de manifeste d'instrumentation*.
Dépôt github, ANSSI, Jun 2021.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Example_of_ManifestProvider.xml.

[12] *Exemple de script PowerShell pour le déploiement automatisé de sysmon*.
Dépôt github, ANSSI, Jun 2021.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Example_of_sysmon_deployment_script.ps1.

[13] *Exemple de tâche à exécution immédiate pour l'exécution de scripts PowerShell sur les systèmes*.
Dépôt github, ANSSI, Jun 2021.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Example_of_immediate_scheduled_task.xml.

[14] *Requête WEC de sélection standard d'évènements à centraliser*.
Dépôt github, ANSSI, Jun 2021.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Standard_WEC_query.xml.

[15] *Script PowerShell de désactivation des plugins WinRM à l'exception de celui nécessaire à la collecte d'évènements*.
Dépôt github, ANSSI, Jun 2021.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Restrict_PowerShell_plugins_to_WEF_only.ps1.

[16] *Script PowerShell de modification du descripteur de sécurité du journal Microsoft-Windows-PowerShell/Operational*.
Dépôt github, ANSSI, Jun 2021.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Change_SDDL_of_PowerShell_operational_log.ps1.

[17] *Script PowerShell de configuration des journaux (activation, taille et permissions de lecture)*.
Dépôt github, ANSSI, Jan 2022.
https://github.com/ANSSI-FR/guide-journalisation-microsoft/blob/main/Configure-Channel.ps1.

[18] *Group Policy for Beginners*.
Technet, MICROSOFT, avril 2011.
https://technet.microsoft.com/en-US/library/hh147307(v=ws.10).aspx.

[19] *Access Control Lists*.
Windows it center, MICROSOFT, mai 2018.
https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-lists.

[20] *Advanced security auditing FAQ*.
Windows it center, MICROSOFT, avril 2017.
https://docs.microsoft.com/en-US/windows/security/threat-protection/auditing/advanced-security-auditing-faq.

[21] *Events are not forwarded if the collector is running Windows Server*.
Support microsoft, MICROSOFT, mai 2020.
https://support.microsoft.com/en-US/help/4494462/events-not-forwarded-if-the-collector-runs-windows-server.

[22] *FSMO placement and optimization on Active Directory domain controllers*.
Support microsoft, MICROSOFT, avril 2018.

https://support.microsoft.com/en-US/help/223346/fsmo-placement-and-optimization-on-active-directory-domain-controllers.

[23] *Group Policy Preferences*.
Windows it center, MICROSOFT, août 2016.
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn581922(v=ws.11).

[24] *Writing an Instrumentation Manifest*.
Windows it center, MICROSOFT, mai 2018.
https://docs.microsoft.com/en-us/windows/win32/wes/writing-an-instrumentation-manifest.

[25] *Network security : Configure encryption types allowed for Kerberos*.
Windows it center, MICROSOFT, avril 2017.
https://docs.microsoft.com/en-US/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos.

[26] *Problems with Kerberos authentication when a user belongs to many groups*.
Windows it center, MICROSOFT, août 2020.
https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-authentication-problems-if-user-belongs-to-groups.

[27] *Creating Custom Windows Event Forwarding Logs*.
Windows it center, MICROSOFT, mai 2016.
https://docs.microsoft.com/en-US/archive/blogs/russellt/creating-custom-windows-event-forwarding-logs.

[28] *What is Microsoft Management Console ?*
Windows it center, MICROSOFT, septembre 2020.
https://docs.microsoft.com/en-US/troubleshoot/windows-server/system-management-components/what-is-microsoft-management-console.

[29] *Network security : LAN Manager authentication level*.
Windows it center, MICROSOFT, avril 2017.
https://docs.microsoft.com/en-US/windows/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level.

[30] *Network security : Minimum session security for NTLM SSP based (including secure RPC) servers*.
Windows it center, MICROSOFT, avril 2017.
https://docs.microsoft.com/en-US/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-servers.

[31] *How the Windows Time Service Works*.
Windows it center, MICROSOFT, mai 2018.
https://docs.microsoft.com/en-US/windows-server/networking/windows-time-service/how-the-windows-time-service-works.

[32] *Configure the Windows Time Service (on the PDC emulator)*.
Windows it center, MICROSOFT, juillet 2020.

https://docs.microsoft.com/en-US/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731191(v=ws.10).

[33] *Enterprise access model*.
Windows it center, MICROSOFT, décembre 2020.
https://docs.microsoft.com/en-US/security/compass/privileged-access-access-model.

[34] *À propos de la signature de scripts PowerShell*.
Windows it center, MICROSOFT, juillet 2020.
https://docs.microsoft.com/en-US/powershell/module/microsoft.powershell.core/about/about_signing?view=powershell-7.1.

[35] *Description of User Account Control and remote restrictions in Windows Vista*.
Windows it center, MICROSOFT, août 2020.
https://docs.microsoft.com/en-US/troubleshoot/windows-server/windows-security/user-account-control-and-remote-restriction.

[36] *4663(S) : An attempt was made to access an object.*
Windows it center, MICROSOFT, avril 2017.
https://docs.microsoft.com/en-US/windows/security/threat-protection/auditing/event-4663.

[37] *Security Descriptor Definition Language for Conditional ACEs*.
Windows it center, MICROSOFT, mai 2018.
https://docs.microsoft.com/en-us/windows/win32/secauthz/security-descriptor-definition-language-for-conditional-aces-.

[38] *Get Started with Software Inventory Logging*.
Windows it center, MICROSOFT, octobre 2017.
https://docs.microsoft.com/en-us/windows-server/administration/software-inventory-logging/get-started-with-software-inventory-logging.

[39] *Sysmon*.
Windows it center, MICROSOFT, novembre 2019.
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

[40] *March 2016 anti-malware platform update for Endpoint Protection clients*.
Support microsoft, MICROSOFT, janvier 2016.
https://support.microsoft.com/en-us/topic/march-2016-anti-malware-platform-update-for-endpoint-protection-clients-d99f5dc9-b7a0-bdb2-5161-3efc43d889fa.

[41] *Service Accounts, Virtual Accounts*.
Windows it center, MICROSOFT, mars 2021.
https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts#virtual-accounts.

[42] *Windows SDK and emulator archive*.
Windows dev center, MICROSOFT, juin 2020.
https://developer.microsoft.com/en-us/windows/downloads/sdk-archive/.

[43] *Setting up a Source Initiated Subscription*.
Windows it center, MICROSOFT, décembre 2018.
https://docs.microsoft.com/en-US/windows/win32/wec/setting-up-a-source-initiated-subscription.

[44] *WECUtil*.
Windows it center, MICROSOFT, juillet 2020.
https://docs.microsoft.com/en-US/windows-server/administration/windows-commands/wecutil.

[45] *Monitoring Active Directory for Signs of Compromise*.
Windows it center, MICROSOFT, mai 2017.
https://docs.microsoft.com/en-US/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise.

[46] *Appendix L : Events to Monitor*.
Windows it center, MICROSOFT, juillet 2018.
https://docs.microsoft.com/en-US/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor.

[47] *Use Windows Event Forwarding to help with intrusion detection*.
Windows it center, MICROSOFT, février 2019.
https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection.

[48] *Best practice for configuring EventLog forwarding in Windows Server 2012 R2*.
Support microsoft, MICROSOFT, mai 2020.
https://support.microsoft.com/en-us/help/4494356/best-practice-eventlog-forwarding-performance.

[49] *WEVTUtil*.
Windows it center, MICROSOFT, octobre 2017.
https://docs.microsoft.com/en-US/windows-server/administration/windows-commands/wevtutil.

[50] *Proxy Servers and WinRM*.
Windows it center, MICROSOFT, mai 2018.
https://docs.microsoft.com/en-US/windows/win32/winrm/proxy-servers-and-winrm.

[51] *Palantir's Windows Event Forwarding Guidance - GitHub repository*.
Dépôt github, Palantir, février 2019.
https://github.com/palantir/windows-event-forwarding.

[52] *Modèle modulaire de fichiers de configuration pour Microsoft Sysinternals Sysmon*.
Dépôt github, Olaf Hartong.
https://github.com/olafhartong/sysmon-modular.

[53] *Modèle de fichier de configuration pour Microsoft Sysinternals Sysmon*.
Dépôt github, SwiftOnSecurity.
https://github.com/SwiftOnSecurity/sysmon-config.

Version 1.1 - 18/07/2022 - ANSSI-PB-090

ISBN : 978-2-11-167112-6 (papier)
ISBN : 978-2-11-167113-3 (numérique)
Dépôt légal : janvier 2022

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN