GUIDE

STORMSHIELD ENDPOINT SECURITY EVOLUTION

DESCRIPTION DES LOGS

Version 2.7.1

Dernière mise à jour du document : 30 juin 2025

Référence : ses-fr-guide_des_logs-v2.7.1

Avant de commencer

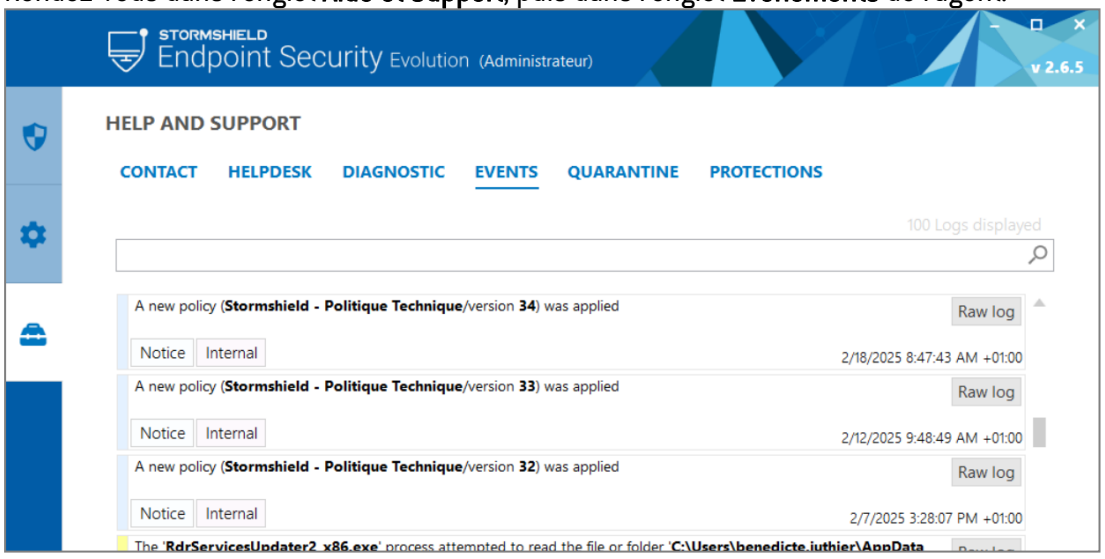
Stormshield Endpoint Security Evolution (SES Evolution) journalise l'activité des agents lors de leur fonctionnement. Pour ce faire, la solution s'appuie sur une mécanique de logs dont le format et la signification sont décrits dans ce document.

Les logs générés sont stockés au format JSON sur l'agent, le serveur et la base de données de logs et peuvent être consultés sur la console d'administration et sur l'interface de l'agent. Ils sont aussi visibles sur le serveur Syslog si vous l'avez configuré.

Ce document énumère tous les identifiants de log et détaille la signification des différents champs. Pour connaître la signification d'un log, nous vous recommandons de rechercher l'identifiant dans ce document.

Connaître les identifiants de log sur l'agent

1. Rendez-vous dans l'onglet **Aide et Support**, puis dans l'onglet **Événements** de l'agent.



2. Cliquez sur le bouton Log brut du log qui vous intéresse.
3. Copiez la valeur du champ *Type* puis puis recherchez-la dans ce document (ici *20003*).

Connaître les identifiants de log sur la console d'administration

1. Rendez-vous dans le menu **Logs agents** de la console d'administration.
2. Dans le panneau de droite, cliquez sur une ligne de log et dépliez-la.
3. Cliquez sur l'onglet **Raw Log**.
4. Copiez la valeur du champ *Type* puis recherchez-la dans ce document.

Pour plus d'informations sur les logs, reportez-vous au *Guide d'administration* de la console SES Evolution.

Champs communs à tous les événements

Champs présents dans tous les logs produits par l'agent.

Champ	Signification
Type	Type d'événement. En fonction du type d'événement, les descriptifs figurant dans les détails des logs varient. Ce champ peut prendre une des valeurs détaillées à la page LogType.
_Category	Catégorie d'événements (protection registre, fichier, ...). Ce champ peut prendre une des valeurs détaillées à la page LogCategory.
Severity	Niveau de gravité du log.
ServerReserved	Information générée par la console, permettant au serveur de traiter l'événement à réception (par exemple, le stocker en base de données ou l'envoyer à un serveur Syslog).
Attributes	Attributs du log. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section LogAttributes.
EventGuid	Identifiant unique du log généré par l'agent.
GenerateIncident	Information indiquant si le log produit doit déclencher la génération d'un incident.

Champs communs additionnels pour tous les événements envoyés via Syslog

Champs additionnels présents dans les logs envoyés via Syslog.

Champ	Signification
AgentName	Nom de l'agent émetteur du log.
AgentGuid	Guid de l'agent émetteur du log.
CategoryName	Nom de la catégorie du log.
IncidentGuid	Guid de l'incident.
AgentGroupName	Nom du groupe d'agents auquel appartient l'agent au moment de l'émission du log.
AgentGroupGuid	Guid du groupe d'agents auquel appartient l'agent au moment de l'émission du log.
SeverityName	Nom de la gravité du log.
PolicyName	Nom de la politique appliquée sur l'agent à la génération du log.
Message	Message du log.
AgentAddresses	Liste des adresses IP de l'agent.
AttackTriggerCondition	Champ "Attack intent" de la règle ayant généré le log.
AttackCVEId	Liste des CVE associées au log.
AttackSESId	Liste des identifiants associés au log.
AttackMitreTacticId	Liste des identifiants ou tags de tactiques Mitre Att&ck.
AttackMitreTacticName	Liste des tactiques Mitre Att&ck.
AttackMitreTechnicId	Liste des identifiants ou tags de techniques et sous techniques Mitre Att&ck.
AttackMitreTechnicName	Liste des techniques et sous techniques Mitre Att&ck.
OperatingSystemType	Type du système d'exploitation.

Événement n°7 : Accès aux processus

AgentOperationProcessAccess : L'agent a détecté qu'un processus demande l'accès à un autre processus ou à un de ses threads, ou bien tente de dupliquer un handle appartenant à un autre processus.

Champ	Signification
SourceProcess	Détails sur le processus qui reçoit un handle : il s'agit du processus effectuant l'action lorsqu'il s'agit d'un accès direct à l'objet, ou d'un processus tiers dans le cas d'une duplication de handle. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
TargetProcess	Détails sur le processus visé par l'accès illégitime. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Details	Détails sur l'objet visé par l'accès illégitime. Plus de détails sur ce bloc à la section AgentOperationProcessAccessDetailsProcessTemplate, AgentOperationProcessAccessDetailsThreadTemplate.
ObjectType	Type d'objet visé par l'accès illégitime (processus ou thread). Ce champ peut prendre une des valeurs détaillées à la page ProcessAccessObjectType.
Operation	Type d'opération effectuée (accès à l'objet ou duplication de handle lui appartenant). Ce champ peut prendre une des valeurs détaillées à la page ProcessAccessOperation.
DuplicatingProcess	Détails sur le processus qui effectue une duplication de handle. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.

Événement n°11 : Exécution de processus

AgentOperationProcessExecution : L'agent a détecté une création de processus.

Champ	Signification
SourceProcess	Informations sur le processus ayant demandé l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
CreatedProcess	Informations sur le processus créé. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
ParentProcess	Informations sur le processus servant de père au processus créé. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.

Événement n°39 : Accès en mode raw volume

AgentOperationRawVolumeAccess : L'agent a détecté un accès à un volume de stockage sans passer par le système de fichiers.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin du volume.
VolumeZone	Caractéristiques du volume. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
AccessType	Type d'accès (lecture ou écriture). Ce champ peut prendre une des valeurs détaillées à la page VolumeAccessType.
DataOffset	Position des données lues ou écrites.
DataLength	Longueur des données lues ou écrites.

Événement n°40 : Liaisons d'accès réseaux

AgentOperationNetworkAccessBind : L'agent a détecté qu'un processus tente d'ouvrir un port réseau afin de devenir serveur.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Protocol	Protocole IP utilisé. Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessProtocol.
AddressFamily	Famille d'adresses IP (IPv4 ou IPv6). Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessAddressFamily.
LocalAddress	Adresse IP de l'interface utilisée pour l'ouverture du port réseau.
LocalPort	Port d'écoute.

Événement n°41 : Accès réseaux entrants

AgentOperationNetworkAccessAccept : L'agent a détecté qu'un processus tente de recevoir une connexion réseau.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération réseau. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Protocol	Protocole IP utilisé. Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessProtocol.
AddressFamily	Famille d'adresses IP (IPv4 ou IPv6). Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessAddressFamily.
LocalAddress	Adresse IP de l'interface utilisée par la machine protégée par l'agent.
RemoteAddress	Adresse IP de la machine tierce.
LocalPort	Port de communication utilisé par la machine protégée par l'agent.
RemotePort	Port de communication utilisé par la machine tierce.

Événement n°42 : Accès réseaux sortants

AgentOperationNetworkAccessConnect : L'agent a détecté qu'un processus tente d'établir une connexion réseau.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération réseau. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Protocol	Protocole IP utilisé. Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessProtocol.
AddressFamily	Famille d'adresses IP (IPv4 ou IPv6). Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessAddressFamily.
LocalAddress	Adresse IP de l'interface utilisée par la machine protégée par l'agent.
RemoteAddress	Adresse IP de la machine tierce.
LocalPort	Port de communication utilisé par la machine protégée par l'agent.
RemotePort	Port de communication utilisé par la machine tierce.

Événement n°43 : Dissimulation de processus

AgentOperationProcessHollowing : L'agent a détecté une dissimulation d'identité d'un processus (Process hollowing).

Champ	Signification
SourceProcess	Informations sur le processus qui a effectué l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
CreatedProcess	Informations sur le processus créé. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Operation	Méthode utilisée pour la dissimulation de processus. Ce champ peut prendre une des valeurs détaillées à la page ProcessHollowingOperation.

Événement n°44 : Stack Pivot

AgentOperationStackPivot : Une protection mémoire de l'agent s'est déclenchée.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.

Événement n°45 : Chargement du pilote

AgentOperationDriverLoading : L'agent a détecté qu'un processus tente de charger un pilote.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin du fichier exécutable correspondant au pilote chargé.
FileOwner	Propriétaire du fichier exécutable correspondant au pilote. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
HashMd5	Hash MD5 du fichier exécutable correspondant au pilote chargé.
HashSha1	Hash SHA-1 du fichier exécutable correspondant au pilote chargé.
HashSha256	Hash SHA-256 du fichier exécutable correspondant au pilote chargé.

Événement n°46 : Protection des pilotes

AgentOperationDriverGuard : La structure DRIVER_OBJECT d'un pilote de l'agent est corrompue.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
CorruptedDriverName	Nom du pilote dont la structure DRIVER_OBJECT a été altérée.
CorruptingDriverPath	Chemin vers le pilote ayant causé la corruption.
FileOwner	Propriétaire du pilote ayant causé la corruption. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
HashMd5	Hash MD5 du pilote ayant causé la corruption.
HashSha1	Hash SHA-1 du pilote ayant causé la corruption.
HashSha256	Hash SHA-256 du pilote ayant causé la corruption.

Événement n°47 : Détournement de flux d'exécution

AgentOperationHoneyPot : Un processus tente d'appeler de manière illégitime des fonctions de kernel32.dll (Execution flow hijacking).

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
FunctionName	Nom de la fonction appelée.
CallerModuleFilename	Module ayant effectué l'appel illégitime.
ExtraParametersInfo	Paramètres donnés à la fonction appelée.

Événement n°50 : Manipulation de jetons d'accès

AgentOperationTokenGuard : L'agent a détecté qu'un processus tente de modifier son jeton de sécurité.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Details	Information complémentaire sur la modification du jeton de sécurité. Plus de détails sur ce bloc à la section AgentOperationTokenGuardDetailsTokenDuplicateTemplate, AgentOperationTokenGuardDetailsTokenModifyTemplate.
DetailsType	Type de modification du jeton de sécurité. Ce champ peut prendre une des valeurs détaillées à la page TokenGuardDetailsType.

Événement n°51 : Enregistreur de frappes

AgentOperationKeylogging : L'agent a détecté qu'un processus tente d'enregistrer les frappes clavier destinées à un autre processus.

Champ	Signification
SourceProcess	Processus à l'origine de l'enregistrement des frappes clavier. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
TargetProcess	Processus ciblé par la tentative d'enregistrement des frappes clavier. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
KeyloggingMethod	Méthode employée lors de la tentative d'enregistrement des frappes clavier. Ce champ peut prendre une des valeurs détaillées à la page KeyloggingMethod.

Événement n°53 : Heap Spray

AgentOperationHeapSpray : L'agent a détecté que la protection contre les attaques de type Heap Spray s'est déclenchée.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
PreallocatedPageHit	Page mémoire utilisée pour le Heap Spray.

Événement n°54 : Accès LRPC

AgentOperationLrpcAccess : L'agent a détecté qu'un processus tente de se connecter à un composant logiciel de l'agent.

Champ	Signification
SourceProcess	Processus à l'origine de l'action de communication LRPC (processus client LRPC). Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
CallerModuleName	Nom du module de l'agent qui a été contacté par le processus non autorisé.

Événement n°55 : Protection contre l'injection de code

AgentOperationCreateRemoteThread : L'agent a détecté qu'un processus tente d'injecter du code dans un autre processus.

Champ	Signification
SourceProcess	Processus à l'origine de l'injection de code. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
TargetProcess	Processus ciblé par l'injection de code. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.

Événement n°56 : Arrêt de processus

AgentOperationProcessExit : L'agent a détecté une fin de processus.

Champ	Signification
SourceProcess	Informations sur le processus qui se termine. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
ExitStatusCode	Code de sortie du processus.
CreatorProcessGuid	Identifiant unique généré par l'agent pour le processus ayant créé le processus qui se termine.

Événement n°57 : Pose de Hooks par des applications (tous)

AgentOperationSetWindowsHookExAll : L'agent a détecté qu'un processus tente d'injecter du code dans tous les processus avec la méthode SetWindowsHookEx.

Champ	Signification
SourceProcess	Processus à l'origine de l'action. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
HookId	Type du hook que le processus source a souhaité poser. Ce champ peut prendre une des valeurs détaillées à la page SetWindowsHookExHookId.
ModuleName	Chemin vers l'exécutable injecté.

Événement n°58 : Pose de Hooks par des applications (Windows Hooks)

AgentOperationSetWindowsHookEx : L'agent a détecté qu'un processus tente d'injecter du code dans un processus avec la méthode SetWindowsHookEx.

Champ	Signification
SourceProcess	Processus à l'origine de l'action. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
TargetProcess	Détails concernant le processus cible de l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
HookId	Type du hook que le processus source a souhaité poser. Ce champ peut prendre une des valeurs détaillées à la page SetWindowsHookExHookId.
ModuleName	Chemin vers l'exécutable injecté.

Événement n°59 : Accès aux processus avec une élévation de privilège

AgentOperationProcessAccessWithPrivilegeEscalation : L'agent a détecté qu'un processus demande l'accès à un autre processus ou à un de ses threads en utilisant une élévation de privilèges.

Champ	Signification
SourceProcess	Détails concernant le processus recevant un handle : il s'agit du processus effectuant l'action dans le cas d'un accès direct à l'objet, ou d'un processus tiers dans le cas d'une duplication de handle. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
TargetProcess	Détails sur le processus visé par l'accès illégitime. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Details	Détails sur l'objet visé par l'accès illégitime. Plus de détails sur ce bloc à la section AgentOperationProcessAccessDetailsProcessTemplate, AgentOperationProcessAccessDetailsThreadTemplate.
ObjectType	Type d'objet visé par l'accès illégitime (processus ou thread). Ce champ peut prendre une des valeurs détaillées à la page ProcessAccessObjectType.

Événement n°60 : Contournement des détections EDR

AgentOperationEDRBypass : L'agent a détecté un acteur malveillant tentant de désactiver un moyen de détection d'un EDR sur le poste.

Champ	Signification
SourceProcess	Processus détecté comme étant malveillant. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Method	Méthode de contournement détectée. Ce champ peut prendre une des valeurs détaillées à la page EDRBypassMethod.
HardwareBreakpointInformation	Informations associées au point d'arrêt matériel. Bloc vide si la méthode détectée n'est pas compatible. Plus de détails sur ce bloc à la section AgentOperationEDRBypassDetailsBreakpointInformationTemplate, AgentOperationEDRBypassDetailsNoInformationTemplate.
FunctionPatchInformation	Informations associées à l'altération de code détectée. Bloc vide si la méthode détectée n'est pas compatible. Plus de détails sur ce bloc à la section AgentOperationEDRBypassDetailsFunctionPatchInformationTemplate, AgentOperationEDRBypassDetailsNoInformationTemplate.
IdentifiedTarget	Valeur technique spécifiée par Stormshield permettant de caractériser le type d'attaque.

Événement n°64 : Fileless

AgentOperationFileless : L'agent a détecté un acteur malveillant tentant d'exécuter du code de manière suspecte.

Champ	Signification
SourceProcess	Processus détecté comme étant malveillant. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
TargetProcess	Processus cible de l'attaque. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Method	Méthode d'exécution détectée. Ce champ peut prendre une des valeurs détaillées à la page FilelessAttackMethod.
TrampolineStartInformation	Informations associées à l'utilisation de trampoline. Bloc vide si la méthode détectée n'est pas compatible. Plus de détails sur ce bloc à la section AgentOperationFilelessDetailsTrampolineStartInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.
ModuleStompingInformation	Informations associées à l'écrasement de module. Bloc vide si la méthode détectée n'est pas compatible. Plus de détails sur ce bloc à la section AgentOperationFilelessDetailsModuleStompingInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.
DynamicMemoryInformation	Informations associées à l'utilisation de mémoire dynamiquement allouée. Bloc vide si la méthode détectée n'est pas compatible. Plus de détails sur ce bloc à la section AgentOperationFilelessDetailsDynamicMemoryInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.
ThreadStartAddressSpoofingInformation	Informations associées à l'échange de l'addresse de démarrage d'un thread. Bloc vide si la méthode détectée n'est pas compatible. Plus de détails sur ce bloc à la section AgentOperationFilelessDetailsThreadStartAddressSpoofingInformationTemplate, AgentOperationFilelessDetailsNoInformationTemplate.

Événement n°103 : Création d'une clé de registre

AgentOperationRegistryKeyCreate : L'agent a détecté une création ou un renommage de clé de registre.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Details	Détails de l'opération. Plus de détails sur ce bloc à la section AgentOperationRegistryKeyCreateDetailsCreateTemplate, AgentOperationRegistryKeyCreateDetailsRenameTemplate, AgentOperationRegistryKeyCreateDetailsCreateLinkTemplate.
DetailsType	Type d'opération (création ou renommage). Ce champ peut prendre une des valeurs détaillées à la page RegistryKeyCreateDetailsType.
Path	Chemin de la clé de registre après création ou renommage.

Événement n°104 : Lecture d'une clé de registre

AgentOperationRegistryKeyRead : L'agent a détecté une lecture de clé de registre.

Champ	Signification
SourceProcess	Détails sur les processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin de la clé lue.
InformationClass	Type d'information demandée à propos de la clé de registre. Ce champ peut prendre une des valeurs détaillées à la page RegistryQueryInformationClass.

Événement n°109 : Écriture d'une clé de registre

AgentOperationRegistryKeyWrite : L'agent a détecté une écriture de clé de registre.

Champ	Signification
SourceProcess	Détails sur les processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Details	Détails de l'opération. Plus de détails sur ce bloc à la section AgentOperationRegistryKeyWriteDetailsSubkeyCreateTemplate, AgentOperationRegistryKeyWriteDetailsSubkeyRenameTemplate, AgentOperationRegistryKeyWriteDetailsSetInformationTemplate, AgentOperationRegistryKeyWriteDetailsSetSecurityTemplate.
DetailsType	Type d'opération (écriture d'information de clé ou de descripteur de sécurité). Ce champ peut prendre une des valeurs détaillées à la page RegistryKeyWriteDetailsType.
Path	Chemin de la clé écrite.

Événement n°112 : Suppression d'une clé de registre

AgentOperationRegistryKeyDelete : L'agent a détecté une suppression ou un renommage de clé de registre.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Details	Détails de l'opération. Plus de détails sur ce bloc à la section AgentOperationRegistryKeyDeleteDetailsDeleteTemplate, AgentOperationRegistryKeyDeleteDetailsRenameTemplate.
DetailsType	Type d'opération (suppression ou renommage). Ce champ peut prendre une des valeurs détaillées à la page RegistryKeyDeleteDetailsType.
Path	Chemin de la clé de registre supprimée.

Événement n°113 : Création d'une valeur de registre

AgentOperationRegistryValueCreate : L'agent a détecté une création de valeur de registre.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin de la clé de registre contenant la valeur.
ValueName	Nom de la valeur de registre.
ValueDataType	Type de valeur de registre. Ce champ peut prendre une des valeurs détaillées à la page RegistryValueType.
ValueData	Données écrites dans la valeur de registre.

Événement n°114 : Lecture d'une valeur de registre

AgentOperationRegistryValueRead : L'agent a détecté une lecture de valeur de registre.

Champ	Signification
SourceProcess	Détails sur les processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin de la clé de registre contenant la valeur.
ValueName	Nom de la valeur de registre.

Événement n°115 : Écriture d'une valeur de registre

AgentOperationRegistryValueWrite : L'agent a détecté une écriture de valeur de registre.

Champ	Signification
SourceProcess	Détails sur les processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin de la clé de registre contenant la valeur.
ValueName	Nom de la valeur de registre.
ValueDataType	Type de valeur de registre. Ce champ peut prendre une des valeurs détaillées à la page RegistryValueType.
ValueData	Données écrites dans la valeur de registre.

Événement n°116 : Suppression d'une valeur de registre

AgentOperationRegistryValueDelete : L'agent a détecté une suppression d'une valeur de registre.

Champ	Signification
SourceProcess	Détails sur le processus qui effectue l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Path	Chemin de la clé de registre contenant la valeur.
ValueName	Nom de la valeur de registre.

Événement n°173 : Création de fichier

AgentOperationFileCreate : L'agent a détecté qu'un processus tente de créer un élément sur un système de fichiers.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Descriptif si la création de l'élément est faite depuis le réseau ; descriptif vide sinon. Plus de détails sur ce bloc à la section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Détails concernant l'opération de création. Plus de détails sur ce bloc à la section AgentOperationFileDetailsCreateTemplate, AgentOperationFileDetailsCreateHardLinkDestinationTemplate, AgentOperationFileDetailsRenameDestinationTemplate, AgentOperationFileDetailsMoveFileExDestinationTemplate, AgentOperationFileDetailsSetOwnerDestinationTemplate.
DetailsType	Type de bloc de détail. Ce champ peut prendre une des valeurs détaillées à la page FileCreateDetailsType.
Path	Chemin de l'élément créé.
MatchingPath	Partie du chemin concernée par une règle de l'agent. Si le champ est vide, alors c'est le chemin complet qui est concerné par la règle.
VolumeZone	Type du volume sur lequel se trouve l'élément. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
FileObjectType	Type d'élément créé (fichier ou dossier). Ce champ peut prendre une des valeurs détaillées à la page FileObjectType.
FileOwner	Identifiant de sécurité du propriétaire de l'élément créé. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°174 : Exécution de fichier

AgentOperationFileExecute : L'agent a détecté qu'un processus tente d'exécuter un fichier.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
Path	Chemin de l'élément.
MatchingPath	Partie du chemin concernée par une règle de l'agent. Si le champ est vide, alors c'est le chemin complet qui est concerné par la règle.
VolumeZone	Type du volume où se trouve l'élément. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
FileObjectType	Type d'élément du système de fichiers (fichier ou dossier). Ce champ peut prendre une des valeurs détaillées à la page FileObjectType.
FileOwner	Propriétaire de l'élément. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
PageProtection	Droits demandés lors du chargement de l'élément en mémoire. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section MemoryProtection.

Événement n°175 : Lecture de fichier

AgentOperationFileRead : L'agent a détecté qu'un processus tente de lire le contenu d'un élément sur un système de fichiers.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Descriptif si la création de l'élément est faite depuis le réseau ; bloc vide sinon. Plus de détails sur ce bloc à la section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Détails concernant l'opération de création. Plus de détails sur ce bloc à la section AgentOperationFileDetailsSectionMappingTemplate, AgentOperationFileDetailsReadDataTemplate.
DetailsType	Type de bloc de détails. Ce champ peut prendre une des valeurs détaillées à la page FileReadDetailsType.
Path	Chemin de l'élément visé.
MatchingPath	Portion du chemin concerné par une règle de l'agent. Si le champ est vide, alors c'est le chemin complet qui a déclenché l'application de la règle.
VolumeZone	Caractérisation du volume sur lequel l'élément est placé. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
FileObjectType	Type d'élément visé (fichier ou dossier). Ce champ peut prendre une des valeurs détaillées à la page FileObjectType.
FileOwner	Identifiant de sécurité du propriétaire de l'élément visé. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°176 : Écriture de fichier

AgentOperationFileWrite : L'agent a détecté qu'un processus tente d'écrire le contenu d'un élément sur un système de fichiers.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Bloc de détails si la création de l'élément est faite depuis le réseau ; bloc vide sinon. Plus de détails sur ce bloc à la section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Détails concernant l'opération de création. Plus de détails sur ce bloc à la section AgentOperationFileDetailsCreateTemplate, AgentOperationFileDetailsCreateChildTemplate, AgentOperationFileDetailsCreateHardLinkSourceTemplate, AgentOperationFileDetailsCreateChildHardLinkDestinationTemplate, AgentOperationFileDetailsRenameChildSourceTemplate, AgentOperationFileDetailsRenameChildDestinationTemplate, AgentOperationFileDetailsMoveFileExChildSourceTemplate, AgentOperationFileDetailsMoveFileExChildDestinationTemplate, AgentOperationFileDetailsSectionMappingTemplate, AgentOperationFileDetailsWriteDataTemplate, AgentOperationFileDetailsSetInformationTemplate, AgentOperationFileDetailsSetSecurityTemplate, AgentOperationFileDetailsDeleteChildTemplate.
DetailsType	Type de bloc de détails. Ce champ peut prendre une des valeurs détaillées à la page FileWriteDetailsType.
Path	Chemin de l'élément visé.
MatchingPath	Portion du chemin concerné par une règle de l'agent. Si le champ est vide, alors c'est le chemin complet qui a déclenché l'application de la règle.
VolumeZone	Caractérisation du volume sur lequel l'élément est placé. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
FileObjectType	Type d'élément visé (fichier ou dossier). Ce champ peut prendre une des valeurs détaillées à la page FileObjectType.

Champ	Signification
FileOwner	Identifiant de sécurité du propriétaire de l'élément visé. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°177 : Suppression de fichier

AgentOperationFileDelete : L'agent a détecté qu'un processus tente de supprimer un élément sur un système de fichiers.

Champ	Signification
SourceProcess	Détails concernant le processus effectuant l'opération. Plus de détails sur ce bloc à la section ProcessStaticInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
UsbVolumeTrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate, NotUsbVolumeTrackingDataTemplate.
AccessFromNetwork	Descriptif si la suppression de l'élément est faite depuis le réseau ; descriptif vide sinon. Plus de détails sur ce bloc à la section AgentOperationFileDetailsAccessFromNetworkTemplate, AgentOperationFileDetailsAccessNotFromNetworkTemplate.
Details	Détails concernant l'opération de suppression. Plus de détails sur ce bloc à la section AgentOperationFileDetailsCreateTemplate, AgentOperationFileDetailsCreateHardLinkDestinationTemplate, AgentOperationFileDetailsRenameSourceTemplate, AgentOperationFileDetailsRenameDestinationTemplate, AgentOperationFileDetailsMoveFileExSourceTemplate, AgentOperationFileDetailsMoveFileExDestinationTemplate, AgentOperationFileDetailsSetOwnerSourceTemplate, AgentOperationFileDetailsDeleteTemplate.
DetailsType	Type d'opération. Ce champ peut prendre une des valeurs détaillées à la page FileDeleteDetailsType.
Path	Chemin de l'élément supprimé.
MatchingPath	Partie du chemin concernée par une règle de l'agent. Si le champ est vide, alors c'est le chemin complet qui est concerné par la règle.
VolumeZone	Type du volume où se trouve l'élément. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
FileObjectType	Type d'élément supprimé (fichier ou dossier). Ce champ peut prendre une des valeurs détaillées à la page FileObjectType.
FileOwner	Identifiant de sécurité du propriétaire de l'élément supprimé. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°301 : Disquette

AgentOperationFloppy : L'agent a détecté une tentative d'utilisation d'un lecteur de disquettes Plug and Play.

Champ	Signification
PnPDeviceInfo	Informations relatives au lecteur de disquettes. Plus de détails sur ce bloc à la section PnPDeviceInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.

Événement n°302 : CD/DVD

AgentOperationCDRom : L'agent a détecté une tentative d'utilisation d'un lecteur de disque optique (CD, DVD, Blu-Ray notamment).

Champ	Signification
Operation	Opération effectuée sur le lecteur de disque optique. Ce champ peut prendre une des valeurs détaillées à la page CDRomOperation.
PnPDeviceInfo	Informations relatives au lecteur de disque optique. Plus de détails sur ce bloc à la section PnPDeviceInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.

Événement n°303 : Port COM

AgentOperationComPort : L'agent a détecté une tentative d'utilisation d'un port COM.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.

Événement n°305 : Périphérique USB

AgentOperationUsbDevice : L'agent a détecté l'utilisation d'un périphérique USB.

Champ	Signification
UsbDeviceInfo	Informations relatives au périphérique USB. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate, NotUsbDeviceInfoTemplate.
PhysicalConsoleSession	Informations relatives à la session utilisateur physique (console). Plus de détails sur ce bloc à la section PhysicalConsoleSessionTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
DeviceEventType	Événement pour le périphérique USB. Ce champ peut prendre une des valeurs détaillées à la page UsbDeviceEventType.

Événement n°321 : Données de suivi d'un volume USB

AgentOperationUsbVolumeTrackingDataUpdate : Bloc indiquant un changement dans les données de suivi d'un volume.

Champ	Signification
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate.
OldTrackingData	Données de suivi du volume avant les modifications. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate.
NewTrackingData	Données de suivi du volume après les modifications. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate.
PhysicalConsoleSession	Informations relatives à la session de l'utilisateur physique (console). Plus de détails sur ce bloc à la section PhysicalConsoleSessionTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
FilesystemType	Type du système de fichiers du volume. Ce champ peut prendre une des valeurs détaillées à la page FilesystemType.
VolumePath	Chemin du volume.
TotalAllocationUnits	Nombre total d'unités d'allocations pour le volume.
SectorsPerAllocationUnit	Nombre d'unités d'allocations par secteur pour le volume.
BytesPerSector	Nombre d'octets par secteur pour le volume.
VolumeLabel	Nom du volume

Événement n°322 : Montage / démontage d'un volume USB

AgentOperationUsbVolumeMount : Bloc indiquant un changement dans les données de suivi d'un volume.

Champ	Signification
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate.
TrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate.
PhysicalConsoleSession	Informations relatives à la session de l'utilisateur physique (console). Plus de détails sur ce bloc à la section PhysicalConsoleSessionTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
FilesystemType	Type du système de fichiers du volume. Ce champ peut prendre une des valeurs détaillées à la page FilesystemType.
VolumePath	Chemin du volume.
TotalAllocationUnits	Nombre total d'unités d'allocations pour le volume.
SectorsPerAllocationUnit	Nombre d'unités d'allocations par secteur pour le volume.
BytesPerSector	Nombre d'octets par secteur pour le volume.
VolumeLabel	Nom du volume
VolumeMountEvent	Événement lié au volume (montage ou démontage). Ce champ peut prendre une des valeurs détaillées à la page UsbVolumeMountEventType.

Événement n°325 : Fin d'analyse d'un volume USB

AgentInternalUsbVolumeScanSuccess : L'agent a analysé avec succès un volume USB dans le but de restaurer le niveau de confiance.

Champ	Signification
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate.
TrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate.
ScannedFileCount	Nombre de fichiers analysés sur le volume USB.
QuarantinedFileCount	Nombre de fichiers ayant été détectés comme mis en quarantaine lors de l'analyse du volume USB.
VolumePath	Chemin du volume

Événement n°326 : Erreur d'analyse d'un volume USB

AgentInternalUsbVolumeScanError : L'agent a rencontré une erreur lors de l'analyse d'un volume USB, le niveau de confiance ne sera pas restauré.

Champ	Signification
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate.
TrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate.
ErrorCode	Code d'erreur de l'erreur rencontrée lors de l'analyse du volume USB.
VolumePath	Chemin du volume
Filepath	Chemin du fichier ayant causé l'erreur de l'analyse USB.

Événement n°327 : Erreur de calcul de l'empreinte d'un volume USB

AgentInternalUsbVolumeFootprintComputationError : Une erreur s'est produite lors du calcul de l'empreinte d'un volume USB.

Champ	Signification
UsbDeviceInfo	Informations relatives au périphérique USB sur lequel se trouve le volume. Plus de détails sur ce bloc à la section UsbDeviceInfoTemplate.
TrackingData	Données de suivi du volume. Plus de détails sur ce bloc à la section UsbVolumeTrackingDataTemplate.
ErrorCode	Code d'erreur de l'erreur produite lors du calcul de l'empreinte du volume USB.
VolumePath	Chemin du volume

Événement n°361 : Bluetooth

AgentOperationBluetoothAccess : Une radio Bluetooth (périphérique Bluetooth en écoute de connexions) sur l'agent a reçu une demande de connexion provenant d'un équipement Bluetooth tiers.

Champ	Signification
ConnectedDeviceInfo	Informations sur le périphérique qui se connecte. Plus de détails sur ce bloc à la section BluetoothDeviceInfoTemplate.
LocalRadioDeviceInfo	Informations sur la radio locale à laquelle le périphérique se connecte. Plus de détails sur ce bloc à la section BluetoothDeviceInfoTemplate.
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.

Événement n°400 : Réseau Wi-Fi

AgentOperationWifiAccessConnectedNetwork : L'agent a détecté un accès à un réseau Wi-Fi.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
ConnectionMode	Mode de connexion Wi-Fi. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section WifiConnectionMode.
AuthAlgo	Type d'authentification Wi-Fi. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section WifiAuthAlgo.
Ssid	Nom du réseau Wi-Fi.
RemoteMacAddress	Adresse MAC distante (adresse du point d'accès dans le cas du mode Infrastructure, ou adresse générée par la machine dans le cas du mode de connexion ad hoc).

Événement n°401 : Fonctionnalité Wi-Fi

AgentOperationWifiAccessFunctionnality : L'agent a détecté un accès à la fonctionnalité Wi-Fi.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.

Événement n°1000 : Logs système perdus

AgentInternalLostBuffers : L'agent a perdu des logs.

Champ	Signification
LostBuffersCount	Nombre de logs perdus.

Événement n°1006 : Démarrage d'un accès temporaire au web

AgentInternalTemporaryWebAccessStart : Un accès temporaire au web a été démarré.

Champ	Signification
User	Identifiant de l'utilisateur ayant demandé le démarrage d'un accès temporaire au web. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
Duration	Durée de l'accès temporaire au web.

Événement n°1007 : Échec du démarrage de l'accès temporaire au web

AgentInternalTemporaryWebAccessStartFailed : Le démarrage de l'accès temporaire au web a échoué.

Champ	Signification
User	Identifiant de l'utilisateur ayant demandé le démarrage d'un accès temporaire au web. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
ErrorCode	Code d'erreur correspondant à l'erreur qui a été rencontrée lors du démarrage de l'accès temporaire au web.

Événement n°1008 : Arrêt d'un accès temporaire au web

AgentInternalTemporaryWebAccessStop : Un accès temporaire au web s'est terminé.

Champ	Signification
User	Identifiant de l'utilisateur ayant demandé l'arrêt de l'accès temporaire au web. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°1009 : Échec de l'arrêt de l'accès temporaire au web

AgentInternalTemporaryWebAccessStopFailed : L'arrêt de l'accès temporaire au web a échoué.

Champ	Signification
User	Identifiant de l'utilisateur qui a demandé l'arrêt de l'accès temporaire au web. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
ErrorCode	Code d'erreur correspondant à l'erreur qui a été rencontrée lors de l'arrêt de l'accès temporaire au web.

Événement n°1010 : Échec de génération de log système

AgentInternalLogExceedMaxSize : Descriptif généré lorsqu'un log n'a pu être généré en raison d'une taille trop volumineuse.

Champ	Signification
FaultyLogType	Type du log qui n'a pas pu être généré Ce champ peut prendre une des valeurs détaillées à la page LogType.

Événement n°1011 : Nombre maximum d'accès temporaire au web atteint

AgentInternalTemporaryWebAccessMaxCountReached : Le nombre de démarrages maximum d'accès temporaires au web a été atteint.

Champ	Signification
User	Identifiant de l'utilisateur qui a demandé le démarrage de l'accès temporaire au web. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°1013 : Début de la génération massive de logs

AgentFloodStart : Log de début de génération massive de logs.

Champ	Signification
FloodID	Identifiant de la génération massive de logs.
FloodStartTime	Date de début de la génération massive de logs.
FloodInformation	Informations sur le log responsable de la génération massive de logs. Plus de détails sur ce bloc à la section AgentFloodInformationTemplate.

Événement n°1014 : Fin de la génération massive de logs

AgentFloodStop : Log de fin de la génération massive de logs.

Champ	Signification
FloodID	Identifiant de la génération massive de logs.
FloodStartTime	Date de début de la génération massive de logs.
FloodStopTime	Date de fin de la génération massive de logs.
FloodTotalGeneratedLogs	Nombre de logs générés par cette génération massive de logs.
FloodInformation	Informations sur le log responsable de la génération massive de logs. Plus de détails sur ce bloc à la section AgentFloodInformationTemplate.

Événement n°20003 : Nouvelle politique

AgentInternalNewPolicyNotification : L'agent a appliqué une nouvelle politique.

Champ	Signification
PolicyName	Nom de la politique appliquée.
PolicyVersion	Version de la politique appliquée.
PolicyGuid	Identifiant, sous forme de GUID, de la politique appliquée.
PolicyVersionInternal	Version interne à des fins de diagnostic.

Événement n°20004 : Le service ne s'est pas arrêté correctement

AgentInternalServiceDidNotEndCorrectly : Un service de l'agent a détecté que sa précédente exécution s'est terminée de manière anormale.

Champ	Signification
ServiceName	Nom du service s'étant arrêté inopinément.

Événement n°20006 : Mise à jour de l'agent

AgentInternalEndUpgradeAgentSucceeded : Une opération de mise à jour logicielle de l'agent a réussi.

Champ	Signification
VersionFrom	Version de l'agent avant mise à jour.
VersionTo	Version de l'agent présente sur la machine après la mise à jour.

Événement n°20007 : Échec de mise à jour de l'agent

AgentInternalEndUpgradeAgentFailed : Une opération de mise à jour logicielle de l'agent a échoué.

Champ	Signification
VersionFrom	Version de l'agent avant mise à jour.
VersionTo	Version de l'agent présente sur la machine après la mise à jour.
ErrorCode	Code d'erreur associé à l'échec de mise à jour logicielle de l'agent.

Événement n°20008 : Erreur d'application de la politique

AgentInternalNewPolicyErrorNotification : L'agent n'a pas pu appliquer une nouvelle politique.

Champ	Signification
PolicyName	Nom de la politique qui n'a pas pu être appliquée.

Événement n°20009 : Package de ruche

AgentInternalInvalidHivePackage : L'agent a reçu des données de politique invalides.

Champ	Signification
HivePackageFullPath	Chemin complet du fichier contenant les données de politique, au format ruche de registre.
LoadingOperationStatus	Code d'erreur associé à la tentative de chargement des données de politique.

Événement n°20010 : Démarrage de la désinstallation de l'agent

AgentInternalStartUninstallAgent : L'agent commence une désinstallation.

Événement n°20011 : Désinstallation de l'agent

AgentInternalEndUninstallAgentSucceeded : Une opération de désinstallation de l'agent a réussi.

Événement n°20012 : Échec de désinstallation de l'agent

AgentInternalEndUninstallAgentFailed : Une opération de désinstallation de l'agent a échoué.

Événement n°20013 : Fichier CAB du package de politiques invalide

AgentInternalInvalidPolicyPackageCab : L'agent n'a pas pu valider un fichier CAB contenant des politiques.

Champ	Signification
PolicyPackageCabFullPath	Chemin complet du fichier CAB contenant les politiques.
LoadingOperationStatus	Code d'erreur associé à la tentative de chargement du fichier CAB contenant les politiques.

Événement n°20015 : Détection d'une corruption noyau

AgentInternalKernelCorruptionBugcheck : L'agent a redémarré à la suite d'un écran bleu dû à une corruption des structures noyau.

Champ	Signification
Bugcheck	Informations détaillées sur l'événement d'écran bleu.

Événement n°20016 : Signature du package de politiques invalide

AgentInternalInvalidPolicyPackageSignature : L'agent n'a pas pu valider la signature d'un fichier CAB contenant des politiques.

Champ	Signification
StatusCode	Statut de la vérification de la signature.
PolicyPackageFile	Chemin du ficher CAB contenant des politiques.

Événement n°20017 : Démarrage de la mise à jour de l'agent

AgentInternalStartAgentUpgrade : L'agent commence à appliquer une mise à jour.

Champ	Signification
AgentUpgradeType	Origine de la demande de mise à jour (autonome ou depuis le serveur) Ce champ peut prendre une des valeurs détaillées à la page AgentUpgradeType.
UpgradeForced	La mise à jour a été forcée

Événement n°20018 : La signature du package de politiques a expiré

AgentInternalPolicyPackageSignerExpired : Des éléments ont expiré dans la chaîne de validation du certificat de signature du fichier CAB contenant des politiques.

Champ	Signification
PolicyPackageFile	Chemin vers le fichier CAB contenant des politiques.

Événement n°20019 : L'autoprotection LRPC a échoué

AgentInternalSelfProtectionLrpcFailure : Le module d'autoprotection permettant de valider les communications inter-modules de l'agent a rencontré une défaillance.

Champ	Signification
ServerServiceName	Nom du module ayant détecté la défaillance. Ce module joue le rôle de serveur de communication et n'a pas pu vérifier l'identité d'un autre module ayant tenté de le contacter.
SelfProtectionModuleName	Nom du module d'autoprotection défaillant.
StatusCode	Code d'erreur retourné par le module ayant détecté la défaillance.

Événement n°20020 : Erreur d'application de la politique issue de la mise à jour

AgentInternalNewPolicyFromUpdateErrorNotification : L'agent n'a pas pu appliquer une nouvelle politique reçue conjointement avec une mise à jour logicielle.

Champ	Signification
PolicyName	Nom de la politique appliquée.

Événement n°20021 : Nouvelle politique appliquée après la mise à jour

AgentInternalNewPolicyFromUpdateNotification : L'agent a appliqué une nouvelle politique reçue conjointement avec une mise à jour logicielle.

Champ	Signification
PolicyName	Nom de la politique appliquée.
PolicyVersion	Version de la politique appliquée.
PolicyGuid	GUID de la politique appliquée.
PolicyVersionInternal	Version interne à des fins de diagnostic.

Événement n°20022 : Application de la configuration

AgentInternalNewConfigurationNotification : La configuration a été appliquée avec succès.

Événement n°20023 : Erreur d'application de la configuration

AgentInternalNewConfigurationErrorNotification : L'agent n'a pas pu appliquer une nouvelle configuration.

Champ	Signification
StatusCode	Code de l'erreur.

Événement n°20024 : Erreur d'application de la configuration pour la nouvelle version

AgentInternalNewConfigurationFromUpdateErrorNotification : L'agent n'a pas pu appliquer une nouvelle configuration reçue en même temps qu'une mise à jour logicielle.

Événement n°20025 : Nouvelle configuration appliquée pour nouvelle version

AgentInternalNewConfigurationFromUpdateNotification : L'agent a planifié l'application d'une nouvelle configuration en même temps qu'une mise à jour logicielle.

Événement n°20026 : Fichier CAB du package de configuration invalide

AgentInternalInvalidConfigurationPackageCab : L'application d'une nouvelle configuration agent a échoué.

Champ	Signification
PackageCabFullPath	Chemin du fichier CAB contenant la configuration qui n'a pas pu être chargée.
LoadingOperationStatus	Résultat de l'opération de chargement.

Événement n°20027 : Retour à une version antérieure de l'agent non autorisé

AgentInternalDowngradeIsNotAuthorized : L'agent a reçu une mise à jour logicielle d'une version inférieure à sa version actuelle. Il ne l'a pas appliquée car la configuration l'interdit.

Événement n°20028 : Ouverture de session en mode sans échec

AgentInternalSafeModeSessionNotification : Une session a été ouverte en mode sans échec.

Champ	Signification
Timestamp	Date et heure de l'ouverture de session.
LoginName	Nom de domaine et d'utilisateur de la session ouverte.

Événement n°20030 : Activation du mode Maintenance

AgentInternalMaintenanceModeStart : Le mode Maintenance est activé.

Champ	Signification
User	Identifiant de l'utilisateur ayant demandé le mode Maintenance. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20031 : Désactivation du mode Maintenance

AgentInternalMaintenanceModeStop : Le mode Maintenance est désactivé.

Événement n°20032 : Mise à jour de l'agent non appliquée

AgentInternalMaintenanceModeAgentUpgradePostponed : L'agent a détecté qu'une mise à jour logicielle est disponible sur le serveur, mais elle n'est pas appliquée immédiatement car l'agent est en mode Maintenance.

Événement n°20033 : Arrêt du service Moteur de filtrage de base (BFE)

AgentInternalBfeIsStoppedNotification : L'agent a détecté que le service Moteur de filtrage de base (BFE) est arrêté.

Événement n°20034 : Échec de réparation

AgentInternalRepairFailureNotification : Descriptif de l'échec d'une réparation.

Champ	Signification
User	Identifiant de l'utilisateur ayant demandé la réparation. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
Result	Résultat d'une réparation ayant échoué.

Événement n°20035 : Fin de la réparation

AgentInternalRepairSuccessNotification : Descriptif de la réussite d'une réparation.

Champ	Signification
User	Identifiant de l'utilisateur ayant demandé la réparation. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20036 : Échec de modification des fonctionnalités actives

AgentInternalEndAgentModularityFailed : Informations relatives à l'échec d'activation ou désactivation d'un ou plusieurs modules de l'agent.

Champ	Signification
ErrorCode	Code d'erreur relatif à l'échec d'activation ou désactivation d'un ou plusieurs modules de l'agent

Événement n°20037 : Modification des fonctionnalités actives

AgentInternalEndAgentModularitySucceeded : Log indiquant l'activation ou la désactivation d'un ou plusieurs modules de l'agent

Événement n°20038 : Échec de communication avec le serveur

AgentInternalCommFinishFailedState : La machine d'états gérant la communication agent-serveur a atteint un état d'erreur irrécupérable

Champ	Signification
ErrorCode	Code d'erreur retourné par la dernière fonction d'état exécutée.
StateName	Nom du dernier état valide de la machine d'états
State	Index du dernier état valide de la machine d'états

Événement n°20039 : Application d'une mise à jour forcée

AgentInternalForcedPatchApplication : Une mise à jour forcée a été installée sur l'agent.

Événement n°20040 : Démarrage du challenge

AgentInternalChallengeStart : Un challenge a démarré sur l'agent.

Champ	Signification
Duration	Durée du challenge qui démarre. Ce champ peut prendre une des valeurs détaillées à la page ChallengeDuration.
Options	Options de challenge, comme la prise de traces. La valeur de ce champ dépend du type de challenge.
ChallengeAction	Action correspondant au challenge démarré. Ce champ peut prendre une des valeurs détaillées à la page ChallengeActionMap.

Événement n°20041 : Fin de challenge

AgentInternalChallengeStop : Un challenge a été arrêté sur l'agent.

Champ	Signification
ChallengeAction	Action correspondant au challenge arrêté. Ce champ peut prendre une des valeurs détaillées à la page ChallengeActionMap.
Manual	Détermine si l'arrêt du challenge était manuel ou automatique.
User	SID de l'utilisateur ayant demandé l'arrêt du challenge. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20042 : Échec de la fin du challenge

AgentInternalChallengeStopFailure : L'arrêt d'un challenge a échoué.

Champ	Signification
ErrorCode	L'arrêt d'un challenge a échoué.

Événement n°20043 : Mauvaise version du paquet d'installation

AgentInternalWrongCabinetVersion : La version du fichier .cab est différente de la version actuelle de l'agent.

Événement n°20044 : Plusieurs interfaces correspondant à un test réseau

AgentInternalMultipleNetworkInterfacesMatchingTest : Plusieurs interfaces réseau peuvent correspondre à un test de politique conditionnelle.

Champ	Signification
InterfaceName	Nom de l'interface tel que spécifié dans le test réseau.
InterfaceDescription	Description de l'interface telle que spécifiée dans le test réseau.

Événement n°20045 : Échec de démarrage du challenge

AgentInternalChallengeStartFailure : Le démarrage d'un challenge a échoué.

Champ	Signification
ErrorCode	Code d'erreur retourné par l'échec du démarrage de challenge.

Événement n°20048 : Événement externe

AgentOperationExternal : Descriptif de l'événement extérieur reçu par l'agent.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Description	Message de l'événement extérieur reçu par l'agent.
OriginType	Origine de l'événement extérieur reçu par l'agent.
ExtraData	Données extraites de l'événement extérieur reçu par l'agent.
Fields	Descriptif des champs de règles ayant obtenu le log. Plus de détails sur ce bloc à la section AgentFieldsTemplate.

Événement n°20049 : Nombre maximum d'essais de challenges atteint

AgentInternalChallengeTooManyFailedAttempts : Un challenge a été annulé en raison d'un trop grand nombre de tentatives.

Champ	Signification
User	SID de l'utilisateur ayant soumis la dernière réponse de challenge incorrecte. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20050 : Report de modification des fonctionnalités actives

AgentInternalMaintenanceModeAgentModularityPostponed : L'agent a détecté de nouvelles fonctionnalités actives sur le serveur, mais elles ne sont pas appliquées immédiatement car l'agent est en mode Maintenance.

Événement n°20051 : Mise à jour de l'agent non nécessaire

AgentInternalEndUpgradeAgentNothingToDo : L'opération de mise à jour logicielle à été arrêtée. L'agent est déjà à jour.

Événement n°20052 : Mise à jour du Guid de l'agent

AgentInternalEndUpgradeAgentGuidUpdated : Le GUID de l'agent à été mis à jour.

Événement n°20053 : Erreur de sortie du mode Maintenance

AgentInternalMaintenanceModeStopFailed : Le retour en mode normal de la protection à échoué.

Champ	Signification
ErrorCode	Code d'erreur ayant empêché l'arrêt du mode Maintenance.

Événement n°20054 : Ticket Kerberos

AgentOperationKerberosPassTheTicket : Bloc de détails généré lorsque l'agent détecte un vol de ticket Kerberos par Mimikatz.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
SourceProcess	Détails concernant le processus effectuant l'opération.
KirbiFileFullPath	Chemin complet du fichier Kirbi généré par Mimikatz.

Événement n°20055 : ARP spoofing

AgentOperationArpSpoofing : Descriptif généré lorsque l'agent détecte une attaque d'usurpation d'ARP.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
IPInterface	Interface contenant l'adresse IP usurpée.
SpoofedIP	Adresse IP usurpée.
OldMacAddress	Adresse MAC présente avant que l'adresse IP ne soit usurpée.
SpoofedMacAddress	Adresse MAC avec laquelle l'adresse IP a été usurpée.

Événement n°20056 : Utilisation malveillante du paramètre de décodage de Certutil

AgentOperationCertutilDecodeMaliciousUsage : Descriptif généré lorsque l'agent détecte une utilisation malveillante de l'outil certutil de Microsoft pour décoder un fichier.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
SourceProcess	Informations sur le processus certutil.
ParentProcess	Processus à l'origine de l'action de l'utilisation de certutil.
SourceFilePath	Chemin vers le fichier à décoder.
DestinationFilePath	Chemin vers le fichier décodé.
FileContentType	Type de fichier détecté. Ce champ peut prendre une des valeurs détaillées à la page CertutilDecodedFileType.
FileContent	Contenu du fichier (limité aux 80 premiers octets maximum).

Événement n°20057 : Utilisation malveillante du téléchargement de Certutil

AgentOperationCertutilDownloadMaliciousUsage : Descriptif généré lorsque l'agent détecte une utilisation malveillante de l'outil certutil de Microsoft pour télécharger un fichier.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
SourceProcess	Informations sur le processus certutil.
ParentProcess	Processus à l'origine de l'action de l'utilisation de certutil.
DownloadUrl	URL utilisée pour télécharger le fichier cible.
DestinationFilePath	Chemin vers le fichier téléchargé.

Événement n°20059 : Erreur d'exécution du script

AgentInternalScriptRuntimeError : Descriptif généré lorsqu'une erreur d'exécution se produit dans un script.

Champ	Signification
ExecutionStatus	Code d'erreur lié à l'exécution du script.
ScriptGuid	GUID du script qui a échoué.

Événement n°20060 : Persistance via WMI

AgentOperationWmiPersistence : Descriptif généré lorsque l'agent détecte une attaque de persistance via WMI.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
ConsumerType	Type de consommateur lié à un événement WMI. Ce champ peut prendre une des valeurs détaillées à la page WmiPersistenceConsumerTypeMap.
ExecutedAction	Ligne de commande ou contenu du script utilisé par WMI.
ActionName	Nom du consommateur ou de l'action utilisé par WMI.
Trigger	Conditions d'exécution WMI.
Namespace	Nom d'espace lié à WMI.
ESS	ESS lié à WMI.
Consumer	Consommateur de l'enregistrement WMI.
PossibleCause	Cause possible du déclenchement de l'événement WMI.
TimeCreated	Date et heure de création du log d'événement lié au déclenchement de WMI.

Événement n°20061 : Découverte

AgentOperationDiscovery : Log Découverte de l'environnement

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
SourceProcess	Processus source de découverte
DiscoveryProcess	Processus de découverte
BeginningTime	Date de début
TriggerTime	Date et heure de déclenchement

Événement n°20062 : Désinstallation de l'agent interdite

AgentInternalUninstallForbidden : Descriptif généré lorsqu'une désinstallation de l'agent a été bloquée par la politique.

Champ	Signification
User	SID de l'utilisateur ayant essayé de désinstaller. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
UninstallAttemptDateTime	Date et heure de la tentative de désinstallation

Événement n°20064 : Application des fonctionnalités sur l'agent

AgentInternalStartModularityAgent : L'agent applique les fonctionnalités

Événement n°20065 : Démarrage de la réparation de l'agent

AgentInternalStartRepairAgent : L'agent démarre une réparation

Champ	Signification
User	Utilisateur ayant démarré la réparation Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20066 : Espace de stockage des clichés instantanés manquant

AgentInternalVolumeWithoutShadowStorage : Les clichés instantanés ne peuvent être créés sur le volume car vous n'avez pas prévu d'espace de stockage.

Champ	Signification
VolumePath	Chemin du volume
DriveLetter	Lettre de lecteur pour le volume si elle existe
VolumeLabel	Description du volume

Événement n°20067 : Échec de création de cliché instantané

AgentInternalShadowCopyCreationFailure : Impossible de créer le cliché instantané

Champ	Signification
VolumePath	Chemin du volume
DriveLetter	Lettre de lecteur pour le volume si elle existe
VolumeLabel	Description du volume
ErrorCode	Code de l'erreur rencontrée

Événement n°20068 : Ransomware

AgentOperationRansomware : Un comportement de type ransomware a été détecté.

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
SourceProcess	Processus source du ransomware
AlteredFileListFilePath	Chemin du fichier contenant la liste des fichiers chiffrés par le ransomware
OverallAlteredFilesCount	Nombre de fichiers chiffrés par le ransomware
AlteredFiles	Chemins des 10 premiers fichiers chiffrés par le ransomware Plus de détails sur ce bloc à la section RenamedFilesRendering.

Événement n°20069 : Erreur lors du téléchargement d'une ressource

AgentInternalResourcePackageDownloadFailed : Bloc de détails généré en cas d'échec du téléchargement d'un fichier de ressource depuis le gestionnaire d'agents

Champ	Signification
StatusCode	Code d'erreur rencontré lors du téléchargement du fichier
ResourceGuid	Identifiant unique de la ressource dont le téléchargement a échoué

Événement n°20070 : Erreur de vérification de signature d'une ressource

AgentInternalInvalidResourcePackageSignature : Bloc de détails généré lorsque l'agent n'a pas pu valider la signature numérique d'un fichier cabinet contenant une ressource de politique

Champ	Signification
StatusCode	Code d'erreur rencontré lors de la vérification de signature
ResourceGuid	Identifiant unique de la ressource pour laquelle la vérification de signature a échoué
ResourcePackageFile	Chemin complet du fichier de ressource pour lequel la vérification de signature a échoué

Événement n°20071 : Échec de vérification de la signature de la SecOps

AgentInternalSecOpsInvalidPackageSignature : Bloc de détails généré lorsque l'agent n'a pas pu valider la signature numérique d'un fichier cabinet contenant une tâche d'analyse

Champ	Signification
StatusCode	Code d'erreur retourné lors de la vérification de signature
SecOpsGuid	Identifiant unique de la tâche pour laquelle la vérification de signature a échoué
SecOpsPackageFile	Chemin complet du fichier de tâche pour lequel la vérification de signature a échoué

Événement n°20072 : Échec de validation de la requête SecOps

AgentInternalSecOpsInvalidJsonSize : Bloc de détails généré lorsque la taille du fichier Json décrivant une tâche d'analyse est invalide

Champ	Signification
StatusCode	Code d'erreur retourné lors de la vérification du fichier Json de tâche d'analyse
SecOpsGuid	Identifiant unique de la tâche pour laquelle le fichier Json est invalide
SecOpsPackageFile	Chemin complet du fichier de tâche d'analyse pour lequel la taille du fichier Json est invalide
JsonSize	Taille du fichier Json de tâche d'analyse dont la taille est invalide

Événement n°20073 : Retour à une version antérieure intermédiaire nécessaire

AgentInternalDowngradeWithPivotVersion223IsRequired : L'agent a reçu une mise à jour logicielle inférieure à la version 2.2.3. L'agent doit être mis à jour vers la versions 2.2.3 avant de pouvoir être mise à jour vers une version inférieure.

Événement n°20079 : Analyse Yara de processus

AgentOperationYaraProcessAnalysisMatch : Bloc de détails généré pour chaque règle de détection de schéma Yara (processus)

Champ	Signification
SourceProcess	Processus impliqué dans l'opération de détection
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
SourceProcessImageFileDetails	Détails sur le fichier image du processus qui a été analysé Plus de détails sur ce bloc à la section AgentOperationYaraAnalysisFilesDetailsTemplate.
MatchedYaraRules	Bloc de détails lié aux règles Yara ayant permis la détection Plus de détails sur ce bloc à la section AgentOperationYaraRuleInformationTemplate.

Événement n°20080 : Analyse Yara de fichiers

AgentOperationYaraFileAnalysisMatch : Bloc de détails généré pour chaque règle de détection de schéma Yara sur un fichier

Champ	Signification
SourceProcess	Processus impliqué dans l'opération de détection
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
FileDetails	Détails sur le fichier impliqué lors de la détection Plus de détails sur ce bloc à la section AgentOperationYaraAnalysisFilesDetailsTemplate.
SourceProcessImageFileDetails	Détails sur le fichier image du processus qui a interagi avec le fichier Plus de détails sur ce bloc à la section AgentOperationYaraAnalysisFilesDetailsTemplate.
MatchedYaraRules	Bloc de détails lié aux règles Yara ayant permis la détection Plus de détails sur ce bloc à la section AgentOperationYaraRuleInformationTemplate.

Événement n°20081 : Analyse Yara de fichiers (aucun processus source)

AgentOperationYaraFileAnalysisMatchNoSourceProcess : Bloc de détails généré pour chaque règle de détection de schéma Yara sur un fichier

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
FileDetails	Détails sur le fichier impliqué lors de la détection Plus de détails sur ce bloc à la section AgentOperationYaraAnalysisFilesDetailsTemplate.
MatchedYaraRules	Bloc de détails lié aux règles Yara ayant permis la détection Plus de détails sur ce bloc à la section AgentOperationYaraRuleInformationTemplate.

Événement n°20082 : Usurpation de processus parent

AgentOperationPpidSpoofing : Protection contre l'usurpation de processus parent (PPID Spoofing)

Champ	Signification
Action	Action effectuée par l'agent. Plus de détails sur ce bloc à la section AgentActionTemplate.
Correlation	Données liées à la protection avancée Plus de détails sur ce bloc à la section AgentCorrelationTemplate.
SourceProcess	Processus à l'origine de l'attaque par usurpation de processus parent (Parent PID Spoofing)
ParentProcess	Processus derrière lequel le processus source a tenté de se cacher lors de l'usurpation de processus parent (Parent PID Spoofing)
CreatedProcess	Processus créé par le processus source lors de l'attaque de type Usurpation de processus parent (Parent PID Spoofing)
Description	Description de l'attaque de type usurpation de processus parent (Parent PID Spoofing)

Événement n°20083 : Démarrage du contrôle de l'intégrité de l'agent

AgentInternalIntegrityStart : Bloc de détails relatif au lancement d'une vérification des composants de la solution.

Champ	Signification
User	Identification de l'utilisateur ayant lancé le contrôle d'intégrité. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20084 : Fin du contrôle de l'intégrité de l'agent

AgentInternalIntegritySuccessNotification : Bloc de détails relatif au succès du contrôle d'intégrité des composants de la solution.

Champ	Signification
User	Identification de l'utilisateur ayant lancé le contrôle d'intégrité. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Événement n°20085 : Fin de la réparation nécessitant un redémarrage

AgentInternalRepairSuccessWithRebootNotification : Bloc de détails relatif au succès d'une réparation nécessitant un redémarrage du poste de travail

Champ	Signification
User	Identification de l'utilisateur ayant demandé la réparation. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
FileErrors	Nombre de différences dans les fichiers détectées lors de la vérification d'intégrité
DirectoryErrors	Nombre de différences dans les dossiers détectées lors de la vérification d'intégrité
RegistryValueErrors	Nombre de différences dans les valeurs registre détectées lors de la vérification d'intégrité
RegistryKeyErrors	Nombre de différences dans les clés de registre détectées lors de la vérification d'intégrité
ServiceErrors	Nombre de différences dans les services détectées lors de la vérification d'intégrité
DriverErrors	Nombre de différences dans les pilotes détectées lors de la vérification d'intégrité
EventLogErrors	Nombre de différences dans les journaux d'événements détectées lors de la vérification d'intégrité
PerfCounterErrors	Nombre de différences dans les compteurs de performance détectées lors de la vérification d'intégrité
WfpCalloutErrors	Nombre de différences dans les callouts WFP détectées lors de la vérification d'intégrité
WfpFilterErrors	Nombre de différences dans les filtres WFP détectées lors de la vérification d'intégrité
WfpProviderErrors	Nombre de différences dans les providers WFP détectées lors de la vérification d'intégrité
WfpSublayerErrors	Nombre de différences dans les sublayers WFP détectées lors de la vérification d'intégrité
DefenderExceptionErrors	Nombre de différences dans les valeurs registre détectées lors de la vérification d'intégrité.
WmiNamespaceErrors	Nombre d'erreurs sur les éléments espace de nom WMI
WmiProviderErrors	Nombre d'erreurs sur les éléments fournisseur WMI
WmiClassErrors	Nombre d'erreurs sur les éléments classe WMI

Événement n°20086 : La réparation a réussi et nécessite pas de redémarrage

AgentInternalRepairSuccessWithoutRebootNotification : Bloc de détails relatif au succès d'une réparation nécessitant un redémarrage du poste de travail

Champ	Signification
User	Identification de l'utilisateur ayant demandé la réparation. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
FileErrors	Nombre de différences dans les fichiers détectées lors de la vérification d'intégrité
DirectoryErrors	Nombre de différences dans les dossiers détectées lors de la vérification d'intégrité
RegistryValueErrors	Nombre de différences dans les valeurs registre détectées lors de la vérification d'intégrité
RegistryKeyErrors	Nombre de différences dans les clés de registre détectées lors de la vérification d'intégrité
ServiceErrors	Nombre de différences dans les services détectées lors de la vérification d'intégrité
DriverErrors	Nombre de différences dans les pilotes détectées lors de la vérification d'intégrité
EventLogErrors	Nombre de différences dans les journaux d'événements détectées lors de la vérification d'intégrité
PerfCounterErrors	Nombre de différences dans les compteurs de performance détectées lors de la vérification d'intégrité
WfpCalloutErrors	Nombre de différences dans les callouts WFP détectées lors de la vérification d'intégrité
WfpFilterErrors	Nombre de différences dans les filtres WFP détectées lors de la vérification d'intégrité
WfpProviderErrors	Nombre de différences dans les providers WFP détectées lors de la vérification d'intégrité
WfpSublayerErrors	Nombre de différences dans les sublayers WFP détectées lors de la vérification d'intégrité
DefenderExceptionErrors	Nombre de différences dans les exceptions Windows Defender détectées lors de la vérification d'intégrité.
WmiNamespaceErrors	Nombre d'erreurs sur les éléments espace de nom WMI
WmiProviderErrors	Nombre d'erreurs sur les éléments fournisseur WMI
WmiClassErrors	Nombre d'erreurs sur les éléments classe WMI

Événement n°20087 : Échec du contrôle de l'intégrité de l'agent

AgentInternalIntegrityErrorNotification : Bloc de détails relatif à l'échec du contrôle d'intégrité des composants de la solution.

Champ	Signification
User	Identification de l'utilisateur ayant lancé le contrôle d'intégrité. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
Result	Résultat d'un contrôle d'intégrité ayant échoué.

Événement n°20089 : Suppression de fichier par remédiation

AgentRemediationRemoveFile : Résultat de l'action de remédiation Suppression de fichier

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Fichier à supprimer

Événement n°20090 : Arrêt de processus

AgentRemediationKillProcess : Résultat de l'action de remédiation Arrêt de processus.

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Image des processus à arrêter
ProcessPID	PID du processus à arrêter
KillChildren	Paramètre de l'opération

Événement n°20091 : Suppression de clé de registre par remédiation

AgentRemediationRemoveRegistryKey : Résultat de l'action de remédiation Suppression de clé de registre

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Clé de registre à supprimer

Événement n°20092 : Suppression de valeur de registre par remédiation

AgentRemediationRemoveRegistryValue : Résultat de l'action de remédiation Suppression de valeur registre

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Chemin de la valeur registre à supprimer
TargetResourceName	Nom de la valeur registre à supprimer

Événement n°20093 : Écriture de valeur de registre par remédiation

AgentRemediationSetRegistryValue : Résultat de l'action de remédiation Définition de valeur registre

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Valeur registre à modifier
TargetResourceName	Nom de la valeur à définir

Événement n°20094 : Exécution de script

AgentRemediationExecutePowershellScript : Résultat de l'action de remédiation Exécution de script Powershell

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
ScriptName	Nom du script
ScriptGuid	Guid du script
ScriptExitCode	Code de retour du script
ScriptOutputFilePath	Nom du fichier des logs du script
ScriptOutput	Extrait des logs du script

Événement n°20095 : Récupération de fichiers depuis un cliché instantané

AgentRemediationExtractFilesFromShadowCopy : Résultat de l'action de remédiation Extraction de fichiers sauvegardés depuis un cliché instantané

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Chemin du log de restauration
RestoredFilesCount	Nombre de fichiers restaurés
OverallAlteredFilesCount	Nombre total de fichiers altérés lors de l'attaque ransomware
RestoredFiles	Liste des 10 premiers fichiers restaurés

Événement n°20097 : IoC sur un objet nommé

AgentOperationIocAnalysisNamedObjectMatch : Bloc de détails généré pour chaque règle de détection d'IoC dans le namespace des objets nommés du système

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
ObjectType	Type de l'objet ayant provoqué la détection Ce champ peut prendre une des valeurs détaillées à la page IocNamedObjectType.
ObjectFullPath	Chemin complet vers l'objet
MatchedStrings	Indicateurs ayant permis la correspondance avec l'objet Plus de détails sur ce bloc à la section AgentOperationIocMatchedStringTemplate.

Événement n°20098 : Correspondance de journal d'événements

AgentOperationIocAnalysisEventLogMatch : Bloc de détails généré pour chaque règle de détection d'IoC dans les journaux d'événements

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
Channel	Nom du canal des journaux associés à la détection
ProviderName	Nom du fournisseur ayant généré le journal
EventTypeId	Identifiant unique du journal d'événements
EventTimestamp	Date et heure de génération du journal d'événements
EventXml	Données brutes au format XML représentant l'événement
EventDetails	Détails associés à l'événement
MatchedStrings	Indicateurs ayant permis la correspondance avec l'événement Plus de détails sur ce bloc à la section AgentOperationIocMatchedStringTemplate.

Événement n°20099 : IoC sur un nom de fichier

AgentOperationIocAnalysisFilenameMatch : Bloc de détails généré pour chaque règle de détection d'IoC dans le namespace des noms de fichiers du système

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
SourceProcess	Processus impliqué dans l'opération de détection
FullPath	Chemin complet vers le fichier
MatchedStrings	Indicateurs ayant permis la correspondance avec le nom de fichier Plus de détails sur ce bloc à la section AgentOperationIocMatchedStringTemplate.

Événement n°20100 : IoC sur un nom de fichier (pas de processus source)

AgentOperationIocAnalysisFilenameMatchNoSourceProcess : Bloc de détails généré pour chaque règle de détection d'IoC dans le namespace des noms de fichiers du système

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
FullPath	Chemin complet vers le fichier
MatchedStrings	Indicateurs ayant permis la correspondance avec le nom de fichier Plus de détails sur ce bloc à la section AgentOperationIocMatchedStringTemplate.

Événement n°20101 : IoC sur une requête DNS

AgentOperationIocAnalysisDnsRequestMatch : Bloc de détails généré pour chaque règle de détection d'IoC dans le journal de requêtes DNS

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
DnsRequestTimestamp	Date et heure de génération de l'entrée dans le journal des requêtes DNS
DnsRequest	Requête DNS complète
MatchedStrings	Indicateurs ayant permis la correspondance avec la requête DNS Plus de détails sur ce bloc à la section AgentOperationIocMatchedStringTemplate.

Événement n°20105 : IoC sur un hash de fichier

AgentOperationIocFileSearchByHashFile : Bloc de détails généré pour chaque détection de fichier correspondant à un IoC de type Hash

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection. Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse. Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
FileDetails	Détails sur le fichier correspondant au hash Plus de détails sur ce bloc à la section AgentOperationIocFileSearchDetailsTemplate.
SearchMatchInformation	Informations liées à une correspondance Plus de détails sur ce bloc à la section AgentOperationIocFileSearchMatchInformationTemplate.

Événement n°20106 : IoC sur un hash de fichier image des processus

AgentOperationIocFileSearchByHashProcess : Bloc de détails généré pour chaque détection de fichier image d'un processus correspondant a un IoC de type Hash

Champ	Signification
Action	Informations liées à l'action menée par l'agent suite à la détection. Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse. Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
SourceProcessImageFileDetails	Détails sur le fichier image correspondant au hash. Plus de détails sur ce bloc à la section AgentOperationIocFileSearchDetailsTemplate.
SearchMatchInformation	Informations liées à une correspondance Plus de détails sur ce bloc à la section AgentOperationIocFileSearchMatchInformationTemplate.
SourceProcess	Informations liées au processus source.

Événement n°20107 : IoC dans la mémoire d'un processus

AgentOperationIocAnalysisTextualSearchProcessMatch : Bloc de détails généré pour chaque règle de détection d'IoC de type texte dans la mémoire d'un processus

Champ	Signification
Action	Informations liées à l'action menée par l'agent après la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
SourceProcess	Processus impliqué dans l'opération de détection
SourceProcessImageFileDetails	Détails sur le fichier image du processus qui a été analysé
MatchedStrings	Indicateur ayant permis la correspondance en mémoire

Événement n°20108 : IoC dans le fichier d'un processus

AgentOperationIocAnalysisTextualSearchFileMatch : Bloc de détails généré pour chaque règle de détection d'IoC de type texte dans un fichier donné

Champ	Signification
Action	Informations liées à l'action menée par l'agent après la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
SourceProcess	Processus impliqué dans l'opération de détection
SourceProcessImageFileDetails	Détails sur le fichier image du processus qui a été analysé
FileDetails	Détails sur le fichier qui a été analysé
MatchedStrings	Indicateur ayant permis la correspondance dans le fichier

Événement n°20109 : IoC dans le fichier d'un processus (pas de processus source)

AgentOperationIocAnalysisTextualSearchFileMatchNoSourceProcess : Bloc de détails généré pour chaque règle de détection d'IoC de type texte dans un fichier donné

Champ	Signification
Action	Informations liées à l'action menée par l'agent après la détection Plus de détails sur ce bloc à la section AgentActionTemplate.
AnalysisProperties	Informations liées aux propriétés de l'analyse Plus de détails sur ce bloc à la section AgentAnalysisPropertiesTemplate.
FileDetails	Détails sur le fichier qui a été analysé
MatchedStrings	Indicateur ayant permis la correspondance dans le fichier

Événement n°20111 : Échec d'ouverture du fichier à surveiller

AgentInternalFileMonitorOpenCursorFailure : Informations concernant l'échec d'ouverture d'un fichier censé être surveillé.

Champ	Signification
DirectoryPath	Chemin vers le répertoire contenant le fichier.
FileName	Nom du fichier.

Événement n°20112 : Erreur de téléchargement de la mise à jour

AgentInternalUpdateDownloadFailed : L'agent n'a pas pu télécharger la mise à jour.

Champ	Signification
ErrorCode	Code d'erreur associé à l'échec du téléchargement de la mise à jour logicielle de l'agent.

Événement n°20113 : Isolation des ordinateurs

AgentRemediationIsolateComputer : Une demande d'isolation a été reçue.

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation. Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
ActionDateTime	Horodatage de l'action d'isolation.

Événement n°20114 : Arrêt de l'isolation de l'ordinateur

AgentRemediationComputerIsolationLeave : Une demande d'arrêt d'isolation a été reçue.

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation. Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
ActionDateTime	Horodatage de l'arrêt de l'isolation.

Événement n°20116 : Fichier mis en quarantaine par la politique de sécurité

AgentFileQuarantinedFromProtectionRule : Un fichier a fait l'objet d'une tentative de mise en quarantaine automatique.

Champ	Signification
Result	Résultat de la tentative de mise en quarantaine (échec ou succès).
ProtectionRuleDetails	Détails sur l'analyse planifiée à l'origine de la mise en quarantaine. Plus de détails sur ce bloc à la section AgentFileQuarantineRuleDetailsTemplate.
FilePath	Chemin du fichier mis en quarantaine.
FileCreationTime	Date de création du fichier mis en quarantaine.
FileModificationTime	Date de dernière modification du fichier mis en quarantaine.
FileSize	Taille du fichier mis en quarantaine.
FileOwner	Identifiant du propriétaire du fichier mis en quarantaine. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
QuarantineObjectId	Identifiant du fichier une fois mis en quarantaine.

Événement n°20117 : Fichier restauré de quarantaine

AgentFileRestoredFromQuarantine : Un fichier a fait l'objet d'une tentative de restauration après mise en quarantaine.

Champ	Signification
RemediationSpecificData	Détails sur la tâche à l'origine de l'arrêt de quarantaine. Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
QuarantineObjectId	Identifiant du fichier mis en quarantaine.
FilePath	Chemin du fichier restauré.

Événement n°20118 : Suppression de fichier en quarantaine

AgentFileRemovedFromQuarantine : Un fichier en quarantaine a fait l'objet d'une tentative de suppression définitive.

Champ	Signification
Result	Résultat de la tentative de suppression (échec ou succès).
QuarantineObjectId	Identifiant du fichier mis en quarantaine.
FilePath	Chemin du fichier original au moment de sa mise en quarantaine.

Événement n°20119 : Fichier mis en quarantaine sur demande

AgentFileQuarantinedFromSecOpsTask : Un fichier a fait l'objet d'une tentative de mise en quarantaine, demandée par l'administrateur de la sécurité.

Champ	Signification
RemediationSpecificData	Détails sur la tâche de remédiation à l'origine de la mise en quarantaine. Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
FilePath	Chemin du fichier mis en quarantaine.
FileCreationTime	Date de création du fichier mis en quarantaine.
FileModificationTime	Date de dernière modification du fichier mis en quarantaine.
FileSize	Taille du fichier mis en quarantaine.
FileOwner	Identifiant du propriétaire du fichier mis en quarantaine. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
QuarantineObjectId	Identifiant du fichier une fois mis en quarantaine.

Événement n°20120 : Fichier restauré de quarantaine par mise à jour de l'exclusion

AgentFileRestoredFromQuarantineByExclusionUpdate : Détails sur l'arrêt de quarantaine déclenchée par la mise à jour des règles d'exclusion.

Champ	Signification
Result	Code retour de la tentative de restauration de fichier en quarantaine.
QuarantineObjectId	Identifiant du fichier restauré de quarantaine.
FilePath	Chemin initial du fichier restauré de quarantaine.

Événement n°20121 : Fichier de référence d'installation de l'agent manquant

AgentInternalAgentPatchMissing : Le référentiel d'installation de l'agent ou sa preuve d'authenticité ne sont pas présents sur le disque. L'agent va tenter de les restaurer en demandant au besoin un paquet de mise à jour auprès du gestionnaire d'agents.

Champ	Signification
SoftwareVersion	Version du logiciel.
CabMissing	Indique si le référentiel d'installation est manquant.
Pkcs7Missing	Indique si la preuve d'authenticité du référentiel d'installation est manquante.

Événement n°20122 : Restauration du fichier de référence d'installation de l'agent

AgentInternalAgentPatchRecovered : Le référentiel d'installation de l'agent a été restauré et validé.

Champ	Signification
SoftwareVersion	Version du logiciel.

Événement n°20123 : Échec de restauration du fichier de référence d'installation de l'agent

AgentInternalAgentPatchNotRecovered : Le référentiel d'installation de l'agent n'a pas pu être restauré. Il peut être nécessaire, afin de restaurer l'état de santé de l'agent, de le placer dans un groupe d'agents correspondant a sa version logicielle courante.

Champ	Signification
SoftwareVersion	Version du logiciel.

Événement n°20125 : Fichier mis en quarantaine par une analyse planifiée

AgentFileQuarantinedFromScheduledTask : Un fichier a fait l'objet d'une tentative de mise en quarantaine, déclenchée par une analyse planifiée.

Champ	Signification
RemediationSpecificData	Détails sur l'analyse planifiée à l'origine de la mise en quarantaine. Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
FilePath	Chemin du fichier mis en quarantaine.
FileCreationTime	Date de création du fichier mis en quarantaine.
FileModificationTime	Date de dernière modification du fichier mis en quarantaine.
FileSize	Taille du fichier mis en quarantaine.
FileOwner	Identifiant du propriétaire du fichier mis en quarantaine. Note : Ce champ est un SID. Les champs automatiques **FileOwnerNameLookup** et **FileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
QuarantineObjectId	Identifiant du fichier une fois mis en quarantaine.

Événement n°20126 : Suppression de répertoire

AgentRemediationRemoveDirectory : Résultat de l'action de remédiation « Retirer le dossier ».

Champ	Signification
RemediationSpecificData	Informations liées à l'action de remédiation. Plus de détails sur ce bloc à la section AgentRemediationSpecificDataTemplate.
TargetResourcePath	Dossier cible de la suppression.

Énumération : AgentUpgradeType

Liste de provenances possibles d'une mise à jour logicielle de l'agent.

Valeur numérique	Symbole associé
0	Autonomous
1	ServerDistribution

Énumération : BluetoothMajorDeviceClass

Liste des classes majeures de périphérique pour les équipements Bluetooth.

Valeur numérique	Symbole associé
0	MADC_MISCELLANEOUS
1	MADC_COMPUTER
2	MADC_PHONE
3	MADC_LAN_ACCESS_POINT
4	MADC_AUDIO_VIDEO
5	MADC_PERIPHERAL
6	MADC_IMAGING
7	MADC_WEARABLE
8	MADC_TOY
9	MADC_HEALTH
31	MADC_UNCATEGORIZED

Champ binaire : BluetoothMajorServiceClass

Liste des classes majeures de service pour les équipements Bluetooth.

Valeur binaire	Symbole associé
0x00000001	MSC_LIMITED_DISCOVERABLE_MODE
0x00000008	MSC_POSITIONING
0x00000010	MSC_NETWORKING
0x00000020	MSC_RENDERING
0x00000040	MSC_CAPTURING
0x00000080	MSC_OBJECT_TRANSFERT
0x00000100	MSC_AUDIO
0x00000200	MSC_TELEPHONY
0x00000400	MSC_INFORMATION

Énumération : BluetoothMinorDeviceClassAudioVideo

Liste des classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'dispositifs audio/vidéo'.

Valeur numérique	Symbole associé
0	MIDC_UNCATEGORIZED
1	MIDC_WEARABLE_HEADSET
2	MIDC_HANDS_FREE_DEVICE
4	MIDC_MICROPHONE
5	MIDC_LOUDSPEAKER
6	MIDC_HEADPHONES
7	MIDC_PORTABLE_AUDIO
8	MIDC_CAR_AUDIO
9	MIDC_SET_TOP_BOX
10	MIDC_HIFI_AUDIO_DEVICE
11	MIDC_VCR
12	MIDC_VIDEO_CAMERA
13	MIDC_CAMCORDER
14	MIDC_VIDEO_MONITOR
15	MIDC_VIDEO_DISPLAY_LOUDSPEAKER
16	MIDC_VIDEO_CONFERENCING
18	MIDC_GAMING_TOY

Énumération : BluetoothMinorDeviceClassComputer

Liste des classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'ordinateurs'.

Valeur numérique	Symbole associé
0	MIDC_UNCATEGORIZED
1	MIDC_DESKTOP_WORKSTATION
2	MIDC_SERVER_CLASS_COMPUTER
3	MIDC_LAPTOP
4	MIDC_HANDLED_PC_PDA
5	MIDC_PALM_SIZED_PC_PDA
6	MIDC_WEARABLE_COMPUTER

Champ binaire : BluetoothMinorDeviceClassImaging

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'dispositifs d'acquisition d'images'.

Valeur binaire	Symbole associé
0x00000001	MIDC_DISPLAY
0x00000002	MIDC_CAMERA
0x00000004	MIDC_SCANNER
0x00000008	MIDC_PRINTER

Énumération : BluetoothMinorDeviceClassNetworkApLoadFactor

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'réseaux ou points d'accès'.

Valeur numérique	Symbole associé
0	MIDC_FULLY_AVAILABLE
1	MIDC_RANGE_1
2	MIDC_RANGE_2
3	MIDC_RANGE_3
4	MIDC_RANGE_4
5	MIDC_RANGE_5
6	MIDC_RANGE_6
7	MIDC_NO_SERVICE_AVAILABLE

Énumération : BluetoothMinorDeviceClassPeripheralMajor

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'claviers ou souris'.

Valeur numérique	Symbole associé
0	MIDC_NOT_KEYBOARD_POINTING_DEVICE
1	MIDC_KEYBOARD
2	MIDC_POINTING_DEVICE
3	MIDC_COMBO_KEYBOARD_POINTING_DEVICE

Énumération : BluetoothMinorDeviceClassPeripheralMinor

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'claviers ou souris'.

Valeur numérique	Symbole associé
0	MIDC_UNCATEGORIZED
1	MIDC_JOYSTICK
2	MIDC_GAMEPAD
3	MIDC_REMOTE_CONTROL
4	MIDC_SENSING_DEVICE
5	MIDC_DIGITIZER_TABLET
6	MIDC_CARD_READER

Énumération : BluetoothMinorDeviceClassPhone

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'téléphones'.

Valeur numérique	Symbole associé
0	MIDC_UNCATEGORIZED
1	MIDC_CELLULAR
2	MIDC_CORDLESS
3	MIDC_SMARTPHONE
4	MIDC_WIRED_MODEM_VOICE_GATEWAY
5	MIDC_COMMON_ISDN_ACCESS

Énumération : BluetoothMinorDeviceHealth

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'équipements médicaux'.

Valeur numérique	Symbole associé
0	MIDC_UNDEFINED
1	MIDC_BLOOD_PRESSURE
2	MIDC_THERMOMETER
3	MIDC_WEIGHING
4	MIDC_GLUCOSE_METER
5	MIDC_PULSE_OXYMETER
6	MIDC_HEART_PULSE_RATE_MONITOR
7	MIDC_HEALTH_DATA_DISPLAY

Énumération : BluetoothMinorDeviceToy

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'gadgets'.

Valeur numérique	Symbole associé
1	MIDC_ROBOT
2	MIDC_VEHICLE
3	MIDC_DOLL_ACTION_FIGURE
4	MIDC_CONTROLLER
5	MIDC_GAME

Énumération : BluetoothMinorDeviceWearable

Liste de classes mineures de périphérique pour les équipements Bluetooth de classe majeure 'dispositifs portables'.

Valeur numérique	Symbole associé
1	MIDC_WRIST_WATCH
2	MIDC_PAGER
3	MIDC_JACKET
4	MIDC_HELMET
5	MIDC_GLASSES

Énumération : CDRomOperation

Liste des opérations sur un disque optique (CD, DVD, Blu-Ray notamment).

Valeur numérique	Symbole associé
0	READ
1	WRITE

Énumération : CertificateSignatureState

Liste des états possibles liés à la vérification d'une signature Authenticode par l'agent.

Valeur numérique	Symbole associé
0	Unavailable
1	Trusted
2	NoSignature
3	Expired
4	Revoked
5	Untrusted
6	SecuritySettings
7	BadContent
8	BadSignature

Énumération : CertutilDecodedFileType

Liste des types de fichiers détectés pour l'utilisation de la commande decode de certutil.

Valeur numérique	Symbole associé
0	Unknown
1	Certificate
2	PortableExecutable
3	ZipArchive

Énumération : ChallengeActionMap

Liste des types d'action possibles pour un challenge.

Valeur numérique	Symbole associé
0	MaintenanceMode
1	StopAgent
2	UninstallAgent
3	DiagnosticSession
4	MaxValue

Énumération : ChallengeDuration

Liste des types de durée possibles pour un challenge.

Valeur numérique	Symbole associé
0	NoDuration
1	FiveMinutes
2	ThirtyMinutes
3	TwoHours
4	OneDay
5	ThreeDays
6	OneWeek
7	TwoWeeks
8	UntilReboot
9	MaxValue

Énumération : EDRBypassMethod

Liste des méthodes de contournement prises en charge par l'agent.

Valeur numérique	Symbole associé
0	NotSpecified
1	HardwareBreakpoint
2	FunctionPatch

Champ binaire : FileAttributes

Liste des attributs d'un fichier.

Valeur binaire	Symbole associé
0x00000001	FILE_ATTRIBUTE_READONLY
0x00000002	FILE_ATTRIBUTE_HIDDEN
0x00000004	FILE_ATTRIBUTE_SYSTEM
0x00000010	FILE_ATTRIBUTE_DIRECTORY
0x00000020	FILE_ATTRIBUTE_ARCHIVE
0x00000040	FILE_ATTRIBUTE_DEVICE
0x00000080	FILE_ATTRIBUTE_NORMAL
0x00000100	FILE_ATTRIBUTE_TEMPORARY
0x00000200	FILE_ATTRIBUTE_SPARSE_FILE
0x00000400	FILE_ATTRIBUTE_REPARSE_POINT
0x00000800	FILE_ATTRIBUTE_COMPRESSED
0x00001000	FILE_ATTRIBUTE_OFFLINE
0x00002000	FILE_ATTRIBUTE_NOT_CONTENT_INDEXED
0x00004000	FILE_ATTRIBUTE_ENCRYPTED
0x00008000	FILE_ATTRIBUTE_INTEGRITY_STREAM
0x00010000	FILE_ATTRIBUTE_VIRTUAL
0x00020000	FILE_ATTRIBUTE_NO_SCRUB_DATA
0x00040000	FILE_ATTRIBUTE_RECALL_ON_OPEN
0x00400000	FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS

Énumération : FileCreateDetailsType

Liste des types de blocs de détails relatifs aux opérations de création de fichiers.

Valeur numérique	Symbole associé
0	FILE_CREATE
1	FILE_CREATE_HARDLINK_DESTINATION
2	FILE_RENAME_DESTINATION
3	FILE_MOVEFILEEX_DESTINATION
4	FILE_SET_OWNER_DESTINATION

Énumération : FileCreateDisposition

Liste des méthodes permettant de créer un fichier.

Valeur numérique	Symbole associé
0	FILE_SUPERSEDE
1	FILE_OPEN
2	FILE_CREATE
3	FILE_OPEN_IF
4	FILE_OVERWRITE
5	FILE_OVERWRITE_IF

Champ binaire : FileCreateOptions

Options diverses concernant l'ouverture ou la création de fichiers.

Valeur binaire	Symbole associé
0x00000001	FILE_DIRECTORY_FILE
0x00000002	FILE_WRITE_THROUGH
0x00000004	FILE_SEQUENTIAL_ONLY
0x00000008	FILE_NO_INTERMEDIATE_BUFFERING
0x00000010	FILE_SYNCHRONOUS_IO_ALERT
0x00000020	FILE_SYNCHRONOUS_IO_NONALERT
0x00000040	FILE_NON_DIRECTORY_FILE
0x00000080	FILE_CREATE_TREE_CONNECTION
0x00000100	FILE_COMPLETE_IF_OPLOCKED
0x00000200	FILE_NO_EA_KNOWLEDGE
0x00000400	FILE_OPEN_REMOTE_INSTANCE
0x00000800	FILE_RANDOM_ACCESS
0x00001000	FILE_DELETE_ON_CLOSE
0x00002000	FILE_OPEN_BY_FILE_ID
0x00004000	FILE_OPEN_FOR_BACKUP_INTENT
0x00008000	FILE_NO_COMPRESSION
0x00010000	FILE_OPEN_REQUIRING_OPLOCK
0x00020000	FILE_DISALLOW_EXCLUSIVE
0x00100000	FILE_RESERVE_OPFILTER
0x00200000	FILE_OPEN_REPARSE_POINT
0x00400000	FILE_OPEN_NO_RECALL
0x00800000	FILE_OPEN_FOR_FREE_SPACE_QUERY

Énumération : FileDeleteDetailsType

Liste des types de blocs de détails relatifs aux opérations de suppression de fichiers.

Valeur numérique	Symbole associé
0	FILE_CREATE
1	FILE_CREATE_HARDLINK_DESTINATION
2	FILE_RENAME_SOURCE
3	FILE_RENAME_DESTINATION
4	FILE_MOVEFILEEX_SOURCE
5	FILE_MOVEFILEEX_DESTINATION
6	FILE_SET_OWNER_SOURCE
7	FILE_DELETE

Champ binaire : FileDeleteFlags

Liste des options de suppression de fichiers.

Valeur binaire	Symbole associé
0x00000001	FILE_DISPOSITION_DELETE
0x00000002	FILE_DISPOSITION_POSIX_SEMANTICS
0x00000004	FILE_DISPOSITION_FORCE_IMAGE_SECTION_CHECK
0x00000008	FILE_DISPOSITION_ON_CLOSE
0x00000010	FILE_DISPOSITION_IGNORE_READONLY_ATTRIBUTE

Champ binaire : FileDesiredAccess

Champ binaire correspondant aux droits d'accès à un élément d'un système de fichiers.

Valeur binaire	Symbole associé
0x00000001	FILE_READ_DATA
0x00000002	FILE_WRITE_DATA
0x00000004	FILE_APPEND_DATA
0x00000008	FILE_READ_EA
0x00000010	FILE_WRITE_EA
0x00000020	FILE_EXECUTE
0x00000040	FILE_DELETE_CHILD
0x00000080	FILE_READ_ATTRIBUTES
0x00000100	FILE_WRITE_ATTRIBUTES
0x00010000	DELETE
0x00020000	READ_CONTROL
0x00040000	WRITE_DAC
0x00080000	WRITE_OWNER
0x00100000	SYNCHRONIZE
0x01000000	ACCESS_SYSTEM_SECURITY
0x02000000	MAXIMUM_ALLOWED
0x10000000	GENERIC_ALL
0x20000000	GENERIC_EXECUTE
0x40000000	GENERIC_WRITE
0x80000000	GENERIC_READ

Énumération : FileInformationClass

Liste des types d'informations pouvant être lues ou écrites sur un fichier.

Valeur numérique	Symbole associé
4	FileBasicInformation
15	FileFullEaInformation
19	FileAllocationInformation
20	FileEndOfFileInformation
31	FileMoveClusterInformation
36	FileTrackingInformation
39	FileValidDataLengthInformation
44	FileSfioReserveInformation
71	FileCaseSensitiveInformation
74	FileStorageReserveIdInformation
75	FileCaseSensitiveInformationForceAccessCheck

Énumération : FilelessAttackMethod

Méthode d'exécution de code fileless.

Valeur numérique	Symbole associé
0	ThreadStartAddressSpoofing
1	DynamicMemory
2	ModuleStomping
3	Trampoline

Énumération : FileMoveFileExOperation

Liste des opérations de système de fichiers pouvant être planifiées au redémarrage.

Valeur numérique	Symbole associé
1	FILE_MOVEFILEEX_DELETE
2	FILE_MOVEFILEEX_RENAME
3	FILE_MOVEFILEEX_REPLACE

Énumération : FileObjectType

Liste des types d'éléments sur un système de fichiers.

Valeur numérique	Symbole associé
0	FILE_OBJECT_TYPE_FILE
1	FILE_OBJECT_TYPE_DIRECTORY
2	FILE_OBJECT_TYPE_UNKNOWN

Énumération : FileReadDetailsType

Liste des types de blocs de détails relatifs aux opérations de lecture de fichiers.

Valeur numérique	Symbole associé
0	FILE_SECTION_MAPPING
1	FILE_READ_DATA

Champ binaire : FileRenameFlags

Liste des options de renommage de fichiers.

Valeur binaire	Symbole associé
0x00000001	FILE_RENAME_REPLACE_IF_EXISTS
0x00000002	FILE_RENAME_POSIX_SEMANTICS
0x00000004	FILE_RENAME_SUPPRESS_PIN_STATE_INHERITANCE
0x00000008	FILE_RENAME_SUPPRESS_STORAGE_RESERVE_INHERITANCE
0x00000010	FILE_RENAME_NO_INCREASE_AVAILABLE_SPACE
0x00000020	FILE_RENAME_NO_DECREASE_AVAILABLE_SPACE
0x00000040	FILE_RENAME_IGNORE_READONLY_ATTRIBUTE
0x00000080	FILE_RENAME_FORCE_RESIZE_TARGET_SR
0x00000100	FILE_RENAME_FORCE_RESIZE_SOURCE_SR

Énumération : FilesystemType

Liste de types de système de fichiers pour un volume.

Valeur numérique	Symbole associé
0	UNKNOWN
1	RAW
2	NTFS
3	FAT
4	CDFS
5	UDFS
6	LANMAN
7	WEBDAV
8	RDPDR
9	NFS
10	MS_NETWARE
11	NETWARE
12	BSUDF
13	MUP
14	RSFX
15	ROXIO_UDF1
16	ROXIO_UDF2
17	ROXIO_UDF3
18	TACIT
19	FS_REC
20	INCD
21	INCD_FAT
22	EXFAT
23	PSFS
24	GPFS
25	NPFS
26	MSFS
27	CSVFS
28	REFS

Valeur numérique	Symbole associé
29	OPENAFS

Énumération : FileWriteDetailsType

Liste des types de blocs de détails relatifs aux opérations d'écriture de fichiers.

Valeur numérique	Symbole associé
0	FILE_CREATE
1	FILE_CREATE_CHILD
2	FILE_CREATE_CHILD_HARDLINK_DESTINATION
3	FILE_RENAME_CHILD_SOURCE
4	FILE_RENAME_CHILD_DESTINATION
5	FILE_MOVEFILEEX_CHILD_SOURCE
6	FILE_MOVEFILEEX_CHILD_DESTINATION
7	FILE_SECTION_MAPPING
8	FILE_WRITE_DATA
9	FILE_SET_INFORMATION
10	FILE_SET_SECURITY
11	FILE_DELETE_CHILD
12	FILE_CREATE_HARDLINK_SOURCE

Énumération : IOCAlgorithmDigest

Champ binaire correspondant à différents algorithmes de hash pouvant être utilisés dans une recherche d'IoC.

Valeur numérique	Symbole associé
0	MD5
1	SHA1
2	SHA256
3	Fuzzy

Énumération : IocNamedObjectType

Liste des types d'objet système supportés

Valeur numérique	Symbole associé
0	Undefined
1	AlpcPort
2	Callback
3	Device
4	Directory
5	Driver
6	Event
7	FilterConnectionPort
8	Job
9	Key
10	KeyedEvent
11	Mailslot
12	Mutant
13	Pipe
14	Partition
15	Section
16	Semaphore
17	Session
18	SymbolicLink
19	Timer
20	Type
21	WindowStation

Énumération : KeyloggingMethod

Champ binaire correspondant aux méthodes d'enregistrement des frappes clavier.

Valeur numérique	Symbole associé
1	GetAsyncKeyState
2	GetKeyState
4	GetKeyboardState
8	GetRawInputBuffer
16	GetRawInputData
32	SetWindowsHookEx

Champ binaire : LogAttributes

Champ binaire correspondant à la catégorie des événements agent.

Valeur binaire	Symbole associé
0x00000000	None
0x00000001	SelfProtection
0x00000002	Protection
0x00000004	Internal
0x00000008	Audit
0x00000010	Context
0x00000020	External
0x00000100	Flood

Énumération : LogCategory

Liste des catégories d'événements possibles.

Valeur numérique	Symbole associé
0	ProcessAccess
1	Registry
2	File
3	Keylogging
4	Other

Énumération : LogType

Liste des événements possibles.

Valeur numérique	Symbole associé
7	AgentOperationProcessAccess
8	AgentOperationProcessAccessDetailsProcess
9	AgentOperationProcessAccessDetailsThread
10	AgentOperationProcessAccessEmptyBlock
11	AgentOperationProcessExecution
39	AgentOperationRawVolumeAccess
40	AgentOperationNetworkAccessBind
41	AgentOperationNetworkAccessAccept
42	AgentOperationNetworkAccessConnect
43	AgentOperationProcessHollowing
44	AgentOperationStackPivot
45	AgentOperationDriverLoading
46	AgentOperationDriverGuard
47	AgentOperationHoneyPot
48	AgentOperationTokenGuardDetailsTokenDuplicate
49	AgentOperationTokenGuardDetailsTokenModify
50	AgentOperationTokenGuard
51	AgentOperationKeylogging
53	AgentOperationHeapSpray
54	AgentOperationLrpcAccess
55	AgentOperationCreateRemoteThread
56	AgentOperationProcessExit
57	AgentOperationSetWindowsHookExAll
58	AgentOperationSetWindowsHookEx
59	AgentOperationProcessAccessWithPrivilegeEscalation
60	AgentOperationEDRBypass
61	AgentOperationEDRBypassDetailsNoInformation
62	AgentOperationEDRBypassDetailsBreakpointInformation
63	AgentOperationEDRBypassDetailsFunctionPatchInformation

Valeur numérique	Symbole associé
64	AgentOperationFileless
65	AgentOperationFilelessDetailsDynamicMemoryInformation
66	AgentOperationFilelessDetailsModuleStompingInformation
67	AgentOperationFilelessDetailsTrampolineStartInformation
68	AgentOperationFilelessDetailsThreadStartAddressSpoofingInformation
69	AgentOperationFilelessDetailsNoInformation
100	AgentOperationRegistryKeyCreateDetailsCreate
101	AgentOperationRegistryKeyCreateDetailsRename
102	AgentOperationRegistryKeyCreateDetailsCreateLink
103	AgentOperationRegistryKeyCreate
104	AgentOperationRegistryKeyRead
105	AgentOperationRegistryKeyWriteDetailsSubkeyCreate
106	AgentOperationRegistryKeyWriteDetailsSubkeyRename
107	AgentOperationRegistryKeyWriteDetailsSetInformation
108	AgentOperationRegistryKeyWriteDetailsSetSecurity
109	AgentOperationRegistryKeyWrite
110	AgentOperationRegistryKeyDeleteDetailsDelete
111	AgentOperationRegistryKeyDeleteDetailsRename
112	AgentOperationRegistryKeyDelete
113	AgentOperationRegistryValueCreate
114	AgentOperationRegistryValueRead
115	AgentOperationRegistryValueWrite
116	AgentOperationRegistryValueDelete
150	AgentOperationFileDetailsAccessFromNetwork
151	AgentOperationFileDetailsAccessNotFromNetwork
152	AgentOperationFileDetailsCreate
153	AgentOperationFileDetailsCreateChild
154	AgentOperationFileDetailsCreateHardLinkDestination
155	AgentOperationFileDetailsCreateChildHardLinkDestination
156	AgentOperationFileDetailsRenameSource
157	AgentOperationFileDetailsRenameChildSource

Valeur numérique	Symbole associé
158	AgentOperationFileDetailsRenameDestination
159	AgentOperationFileDetailsRenameChildDestination
160	AgentOperationFileDetailsMoveFileExSource
161	AgentOperationFileDetailsMoveFileExChildSource
162	AgentOperationFileDetailsMoveFileExDestination
163	AgentOperationFileDetailsMoveFileExChildDestination
164	AgentOperationFileDetailsSetOwnerSource
165	AgentOperationFileDetailsSetOwnerDestination
166	AgentOperationFileDetailsSectionMapping
167	AgentOperationFileDetailsReadData
168	AgentOperationFileDetailsWriteData
169	AgentOperationFileDetailsSetInformation
170	AgentOperationFileDetailsSetSecurity
171	AgentOperationFileDetailsDelete
172	AgentOperationFileDetailsDeleteChild
173	AgentOperationFileCreate
174	AgentOperationFileExecute
175	AgentOperationFileRead
176	AgentOperationFileWrite
177	AgentOperationFileDelete
178	AgentOperationFileDetailsCreateHardLinkSource
300	PnPDeviceInfo
301	AgentOperationFloppy
302	AgentOperationCDRom
303	AgentOperationComPort
304	UsbDeviceInfo
305	AgentOperationUsbDevice
306	NotUsbDeviceInfo
320	UsbVolumeTrackingData
321	AgentOperationUsbVolumeTrackingDataUpdate
322	AgentOperationUsbVolumeMount

Valeur numérique	Symbole associé
323	NotUsbVolumeTrackingData
324	PhysicalConsoleSession
325	AgentInternalUsbVolumeScanSuccess
326	AgentInternalUsbVolumeScanError
327	AgentInternalUsbVolumeFootprintComputationError
350	BluetoothDeviceInfoDefault
351	BluetoothDeviceInfoComputer
352	BluetoothDeviceInfoPhone
353	BluetoothDeviceInfoNetworkApLoadFactor
354	BluetoothDeviceInfoAudioVideo
355	BluetoothDeviceInfoPeripheral
356	BluetoothDeviceInfoImaging
357	BluetoothDeviceInfoWearable
358	BluetoothDeviceInfoToy
359	BluetoothDeviceInfoHealth
360	BluetoothDeviceInfo
361	AgentOperationBluetoothAccess
400	AgentOperationWifiAccessConnectedNetwork
401	AgentOperationWifiAccessFunctionnality
1000	AgentInternalLostBuffers
1006	AgentInternalTemporaryWebAccessStart
1007	AgentInternalTemporaryWebAccessStartFailed
1008	AgentInternalTemporaryWebAccessStop
1009	AgentInternalTemporaryWebAccessStopFailed
1010	AgentInternalLogExceedMaxSize
1011	AgentInternalTemporaryWebAccessMaxCountReached
1012	AgentFloodInformation
1013	AgentFloodStart
1014	AgentFloodStop
20002	AgentInternalLostBuffers
20003	AgentInternalNewPolicyNotification

Valeur numérique	Symbole associé
20004	AgentInternalServiceDidNotEndCorrectly
20006	AgentInternalEndUpgradeAgentSucceeded
20007	AgentInternalEndUpgradeAgentFailed
20008	AgentInternalNewPolicyErrorNotification
20009	AgentInternalInvalidHivePackage
20010	AgentInternalStartUninstallAgent
20011	AgentInternalEndUninstallAgentSucceeded
20012	AgentInternalEndUninstallAgentFailed
20013	AgentInternalInvalidPolicyPackageCab
20015	AgentInternalKernelCorruptionBugcheck
20016	AgentInternalInvalidPolicyPackageSignature
20017	AgentInternalStartAgentUpgrade
20018	AgentInternalPolicyPackageSignerExpired
20019	AgentInternalSelfProtectionLrpcFailure
20020	AgentInternalNewPolicyFromUpdateErrorNotification
20021	AgentInternalNewPolicyFromUpdateNotification
20022	AgentInternalNewConfigurationNotification
20023	AgentInternalNewConfigurationErrorNotification
20024	AgentInternalNewConfigurationFromUpdateErrorNotification
20025	AgentInternalNewConfigurationFromUpdateNotification
20026	AgentInternalInvalidConfigurationPackageCab
20027	AgentInternalDowngradeIsNotAuthorized
20028	AgentInternalSafeModeSessionNotification
20030	AgentInternalMaintenanceModeStart
20031	AgentInternalMaintenanceModeStop
20032	AgentInternalMaintenanceModeAgentUpgradePostponed
20033	AgentInternalBfeIsStoppedNotification
20034	AgentInternalRepairFailureNotification
20035	AgentInternalRepairSuccessNotification
20036	AgentInternalEndAgentModularityFailed
20037	AgentInternalEndAgentModularitySucceeded

Valeur numérique	Symbole associé
20038	AgentInternalCommFinishFailedState
20039	AgentInternalForcedPatchApplication
20040	AgentInternalChallengeStart
20041	AgentInternalChallengeStop
20042	AgentInternalChallengeStopFailure
20043	AgentInternalWrongCabinetVersion
20044	AgentInternalMultipleNetworkInterfacesMatchingTest
20045	AgentInternalChallengeStartFailure
20046	AgentAction
20047	AgentFields
20048	AgentOperationExternal
20049	AgentInternalChallengeTooManyFailedAttempts
20050	AgentInternalMaintenanceModeAgentModularityPostponed
20051	AgentInternalEndUpgradeAgentNothingToDo
20052	AgentInternalEndUpgradeAgentGuidUpdated
20053	AgentInternalMaintenanceModeStopFailed
20054	AgentOperationKerberosPassTheTicket
20055	AgentOperationArpSpoofing
20056	AgentOperationCertutilDecodeMaliciousUsage
20057	AgentOperationCertutilDownloadMaliciousUsage
20058	AgentCorrelation
20059	AgentInternalScriptRuntimeError
20060	AgentOperationWmiPersistence
20061	AgentOperationDiscovery
20062	AgentInternalUninstallForbidden
20063	AgentInternalLogExceedMaxSize
20064	AgentInternalStartModularityAgent
20065	AgentInternalStartRepairAgent
20066	AgentInternalVolumeWithoutShadowStorage
20067	AgentInternalShadowCopyCreationFailure
20068	AgentOperationRansomware

Valeur numérique	Symbole associé
20069	AgentInternalResourcePackageDownloadFailed
20070	AgentInternalInvalidResourcePackageSignature
20071	AgentInternalSecOpsInvalidPackageSignature
20072	AgentInternalSecOpsInvalidJsonSize
20073	AgentInternalDowngradeWithPivotVersion223IsRequired
20074	AgentAnalysisProperties
20075	AgentOperationYaraRuleInformationTag
20076	AgentOperationYaraRuleInformationMetadata
20077	AgentOperationYaraRuleInformation
20078	AgentOperationYaraAnalysisFilesDetails
20079	AgentOperationYaraProcessAnalysisMatch
20080	AgentOperationYaraFileAnalysisMatch
20081	AgentOperationYaraFileAnalysisMatchNoSourceProcess
20082	AgentOperationPpidSpoofing
20083	AgentInternalIntegrityStart
20084	AgentInternalIntegritySuccessNotification
20085	AgentInternalRepairSuccessWithRebootNotification
20086	AgentInternalRepairSuccessWithoutRebootNotification
20087	AgentInternalIntegrityErrorNotification
20088	AgentOperationYaraRuleInformationMatchedString
20089	AgentRemediationRemoveFile
20090	AgentRemediationKillProcess
20091	AgentRemediationRemoveRegistryKey
20092	AgentRemediationRemoveRegistryValue
20093	AgentRemediationSetRegistryValue
20094	AgentRemediationExecutePowershellScript
20095	AgentRemediationExtractFilesFromShadowCopy
20096	AgentRemediationSpecificData
20097	AgentOperationIocAnalysisNamedObjectMatch
20098	AgentOperationIocAnalysisEventLogMatch
20099	AgentOperationIocAnalysisFilenameMatch

Valeur numérique	Symbole associé
20100	AgentOperationIocAnalysisFilenameMatchNoSourceProcess
20101	AgentOperationIocAnalysisDnsRequestMatch
20102	AgentRemediationRestoredFileFromShadowCopy
20103	AgentOperationIocFileSearchDetails
20104	AgentOperationIocFileSearchMatchInformation
20105	AgentOperationIocFileSearchByHashFile
20106	AgentOperationIocFileSearchByHashProcess
20107	AgentOperationIocAnalysisTextualSearchProcessMatch
20108	AgentOperationIocAnalysisTextualSearchFileMatch
20109	AgentOperationIocAnalysisTextualSearchFileMatchNoSourceProcess
20110	AgentOperationIocMatchedString
20111	AgentInternalFileMonitorOpenCursorFailure
20112	AgentInternalUpdateDownloadFailed
20113	AgentRemediationIsolateComputer
20114	AgentRemediationComputerIsolationLeave
20115	AgentFileQuarantineRuleDetails
20116	AgentFileQuarantinedFromProtectionRule
20117	AgentFileRestoredFromQuarantine
20118	AgentFileRemovedFromQuarantine
20119	AgentFileQuarantinedFromSecOpsTask
20120	AgentFileRestoredFromQuarantineByExclusionUpdate
20121	AgentInternalAgentPatchMissing
20122	AgentInternalAgentPatchRecovered
20123	AgentInternalAgentPatchNotRecovered
20124	AgentActionTag
20125	AgentFileQuarantinedFromScheduledTask
20126	AgentRemediationRemoveDirectory
20127	AgentInternalPolymorphicLog
11	AgentOperationProcessExecution
1012	AgentFloodInformation
1013	AgentFloodStart
1014	AgentFloodStop

Énumération : MemoryMappingType

Type de mapping mémoire.

Valeur numérique	Symbole associé
0x00020000	MEM_PRIVATE
0x00040000	MEM_MAPPED
0x01000000	MEM_IMAGE

Champ binaire : MemoryProtection

Liste des protections mémoire

Valeur binaire	Symbole associé
0x00000001	PAGE_NOACCESS
0x00000002	PAGE_READONLY
0x00000004	PAGE_READWRITE
0x00000008	PAGE_WRITECOPY
0x00000010	PAGE_EXECUTE
0x00000020	PAGE_EXECUTE_READ
0x00000040	PAGE_EXECUTE_READWRITE
0x00000080	PAGE_EXECUTE_WRITECOPY
0x00000100	PAGE_GUARD
0x00000200	PAGE_NOCACHE
0x00000400	PAGE_WRITECOMBINE
0x00000800	PAGE_GRAPHICS_NOACCESS
0x00001000	PAGE_GRAPHICS_READONLY
0x00002000	PAGE_GRAPHICS_READWRITE
0x00004000	PAGE_GRAPHICS_EXECUTE
0x00008000	PAGE_GRAPHICS_EXECUTE_READ
0x00010000	PAGE_GRAPHICS_EXECUTE_READWRITE
0x00020000	PAGE_GRAPHICS_COHERENT

Énumération : NetworkAccessAddressFamily

Liste des modes d'adressages IP.

Valeur numérique	Symbole associé
2	IPV4
23	IPV6

Énumération : NetworkAccessOperation

Liste des types d'opérations de communication réseau.

Valeur numérique	Symbole associé
0	Connect
1	Bind
2	Accept

Énumération : NetworkAccessProtocol

Liste des protocoles IP de communication réseau.

Valeur numérique	Symbole associé
6	TCP
17	UDP

Champ binaire : PrivilegeHigh

Champ binaire correspondant à la seconde partie des privilèges que le jeton de sécurité d'un processus peut inclure.

Valeur binaire	Symbole associé
0x00000001	SE_RELABEL_PRIVILEGE
0x00000002	SE_INC_WORKING_SET_PRIVILEGE
0x00000004	SE_TIME_ZONE_PRIVILEGE
0x00000008	SE_CREATE_SYMBOLIC_LINK_PRIVILEGE
0x00000010	SE_DELEGATE_SESSION_USER_IMPERSONATE_PRIVILEGE

Champ binaire : PrivilegeLow

Champ binaire correspondant à la première partie des privilèges que le jeton de sécurité d'un processus peut inclure.

Valeur binaire	Symbole associé
0x00000004	SE_CREATE_TOKEN_PRIVILEGE
0x00000008	SE_ASSIGNPRIMARYTOKEN_PRIVILEGE
0x00000010	SE_LOCK_MEMORY_PRIVILEGE
0x00000020	SE_INCREASE_QUOTA_PRIVILEGE
0x00000040	SE_MACHINE_ACCOUNT_PRIVILEGE
0x00000080	SE_TCB_PRIVILEGE
0x00000100	SE_SECURITY_PRIVILEGE
0x00000200	SE_TAKE_OWNERSHIP_PRIVILEGE
0x00000400	SE_LOAD_DRIVER_PRIVILEGE
0x00000800	SE_SYSTEM_PROFILE_PRIVILEGE
0x00001000	SE_SYSTEMTIME_PRIVILEGE
0x00002000	SE_PROF_SINGLE_PROCESS_PRIVILEGE
0x00004000	SE_INC_BASE_PRIORITY_PRIVILEGE
0x00008000	SE_CREATE_PAGEFILE_PRIVILEGE
0x00010000	SE_CREATE_PERMANENT_PRIVILEGE
0x00020000	SE_BACKUP_PRIVILEGE
0x00040000	SE_RESTORE_PRIVILEGE
0x00080000	SE_SHUTDOWN_PRIVILEGE
0x00100000	SE_DEBUG_PRIVILEGE
0x00200000	SE_AUDIT_PRIVILEGE
0x00400000	SE_SYSTEM_ENVIRONMENT_PRIVILEGE
0x00800000	SE_CHANGE_NOTIFY_PRIVILEGE
0x01000000	SE_REMOTE_SHUTDOWN_PRIVILEGE
0x02000000	SE_UNDOCK_PRIVILEGE
0x04000000	SE_SYNC_AGENT_PRIVILEGE
0x08000000	SE_ENABLE_DELEGATION_PRIVILEGE
0x10000000	SE_MANAGE_VOLUME_PRIVILEGE
0x20000000	SE_IMPERSONATE_PRIVILEGE

Valeur binaire	Symbole associé
0x40000000	SE_CREATE_GLOBAL_PRIVILEGE
0x80000000	SE_TRUSTED_CREDMAN_ACCESS_PRIVILEGE

Champ binaire : ProcessAccessMask

Champ binaire correspondant aux droits d'accès à un processus.

Valeur binaire	Symbole associé
0x0001	PROCESS_TERMINATE
0x0002	PROCESS_CREATE_THREAD
0x0004	PROCESS_SET_SESSIONID
0x0008	PROCESS_VM_OPERATION
0x0010	PROCESS_VM_READ
0x0020	PROCESS_VM_WRITE
0x0040	PROCESS_DUP_HANDLE
0x0080	PROCESS_CREATE_PROCESS
0x0100	PROCESS_SET_QUOTA
0x0200	PROCESS_SET_INFORMATION
0x0400	PROCESS_QUERY_INFORMATION
0x0800	PROCESS_SUSPEND_RESUME
0x1000	PROCESS_QUERY_LIMITED_INFORMATION
0x2000	PROCESS_SET_LIMITED_INFORMATION
0x10000	DELETE
0x20000	READ_CONTROL
0x40000	WRITE_DAC
0x80000	WRITE_OWNER
0x100000	SYNCHRONIZE

Énumération : ProcessAccessObjectType

Liste des types d'objets concernés par la protection contre l'accès aux processus.

Valeur numérique	Symbole associé
1	Process
2	Thread

Énumération : ProcessAccessOperation

Liste des opérations pouvant déclencher la protection contre l'accès aux processus.

Valeur numérique	Symbole associé
1	Open
2	Duplicate

Énumération : ProcessHollowingOperation

Liste des méthodes utilisées pour la dissimulation de processus.

Valeur numérique	Symbole associé
1	EntryPointDataModification
2	EntryPointRelocation
3	PebImageBaseAddressModification
4	ProcessDoppelganging
5	ProcessHerpaderping
6	ProcessGhosting

Champ binaire : RegistryAccessMask

Champ binaire correspondant aux droits d'accès à une clé de registre.

Valeur binaire	Symbole associé
0x0001	KEY_QUERY_VALUE
0x0002	KEY_SET_VALUE
0x0004	KEY_CREATE_SUB_KEY
0x0008	KEY_ENUMERATE_SUB_KEYS
0x0010	KEY_NOTIFY
0x0020	KEY_CREATE_LINK
0x0200	KEY_WOW64_32KEY
0x0100	KEY_WOW64_64KEY
0x00010000	DELETE
0x00020000	READ_CONTROL
0x00040000	WRITE_DAC
0x00080000	WRITE_OWNER
0x02000000	MAXIMUM_ALLOWED

Champ binaire : RegistryCreateOptions

Champ binaire correspondant à diverses options lors de la création d'une clé de registre.

Valeur binaire	Symbole associé
0x0001	REG_OPTION_VOLATILE
0x0002	REG_OPTION_CREATE_LINK
0x0004	REG_OPTION_BACKUP_RESTORE
0x0008	REG_OPTION_OPEN_LINK
0x0010	REG_OPTION_DONT_VIRTUALIZE

Énumération : RegistryKeyCreateDetailsType

Liste des types de descriptif des opérations de création de clés de registre.

Valeur numérique	Symbole associé
0	REGISTRY_KEY_CREATE
1	REGISTRY_KEY_RENAME
2	REGISTRY_KEY_CREATE_LINK

Énumération : RegistryKeyDeleteDetailsType

Liste des types de descriptif des opérations de suppression de clés de registre.

Valeur numérique	Symbole associé
0	REGISTRY_KEY_DELETE
1	REGISTRY_KEY_RENAME

Énumération : RegistryKeyWriteDetailsType

Liste des types de descriptif des opérations d'écriture de clés de registre.

Valeur numérique	Symbole associé
0	REGISTRY_KEY_CREATE_SUBKEY
1	REGISTRY_KEY_RENAME_SUBKEY
2	REGISTRY_KEY_SET_INFORMATION
3	REGISTRY_KEY_SET_SECURITY

Énumération : RegistryQueryInformationClass

Liste des types d'informations pouvant être lues sur une clé de registre.

Valeur numérique	Symbole associé
0	KeyBasicInformation
1	KeyNodeInformation
2	KeyFullInformation
3	KeyNameInformation
4	KeyCachedInformation
5	KeyFlagsInformation
6	KeyVirtualizationInformation
7	KeyHandleTagsInformation
8	KeyTrustInformation
9	KeyLayerInformation

Énumération : RegistrySetInformationClass

Liste des types d'informations pouvant être écrites sur une clé de registre.

Valeur numérique	Symbole associé
0	KeyWriteTimeInformation
1	KeyWow64FlagsInformation
2	KeyControlFlagsInformation
3	KeySetVirtualizationInformation
4	KeySetDebugInformation
5	KeySetHandleTagsInformation
6	KeySetLayerInformation

Énumération : RegistryValueType

Liste des types de valeur de registre possibles.

Valeur numérique	Symbole associé
0	REG_NONE
1	REG_SZ
2	REG_EXPAND_SZ
3	REG_BINARY
4	REG_DWORD
5	REG_DWORD_BIG_ENDIAN
6	REG_LINK
7	REG_MULTI_SZ
8	REG_RESOURCE_LIST
9	REG_FULL_RESOURCE_DESCRIPTOR
10	REG_RESOURCE_REQUIREMENTS_LIST
11	REG_QWORD

Énumération : RemediationActionResultMap

Résultat d'une action de remédiation

Valeur numérique	Symbole associé
0	Success
1	Ignore
2	Error
3	Partial

Champ binaire : ScriptTriggers

Champ binaire correspondant aux différents déclencheurs utilisables pour le lancement d'exécutions par le service de script.

Valeur binaire	Symbole associé
0x00000000	None
0x00000001	PolicyPackageChange
0x00000002	Periodic
0x00000004	NetworkEvent
0x00000008	RuleEvent
0x00000010	StopAgent
0x00000020	PolicyApplied
0x00000040	Scheduled
0x00000080	SecOps

Champ binaire : SecurityClass

Liste des types d'informations pouvant être lues ou écrites sur un descripteur de sécurité d'une clé de registre.

Valeur binaire	Symbole associé
0x00000001	OWNER_SECURITY_INFORMATION
0x00000002	GROUP_SECURITY_INFORMATION
0x00000004	DACL_SECURITY_INFORMATION
0x00000008	SACL_SECURITY_INFORMATION
0x00000010	LABEL_SECURITY_INFORMATION
0x00000020	ATTRIBUTE_SECURITY_INFORMATION
0x00000040	SCOPE_SECURITY_INFORMATION
0x00000080	PROCESS_TRUST_LABEL_SECURITY_INFORMATION
0x00000100	ACCESS_FILTER_SECURITY_INFORMATION
0x00010000	BACKUP_SECURITY_INFORMATION
0x10000000	UNPROTECTED_SACL_SECURITY_INFORMATION
0x20000000	UNPROTECTED_DACL_SECURITY_INFORMATION
0x40000000	PROTECTED_SACL_SECURITY_INFORMATION
0x80000000	PROTECTED_DACL_SECURITY_INFORMATION

Énumération : SetWindowsHookExHookId

Champ correspondant aux types de hooks possibles avec SetWindowsHookEx.

Valeur numérique	Symbole associé
0xffffffff	WH_MSGFILTER
0	WH_JOURNALRECORD
1	WH_JOURNALPLAYBACK
2	WH_KEYBOARD
3	WH_GETMESSAGE
4	WH_CALLWNDPROC
5	WH_CBT
6	WH_SYSMSGFILTER
7	WH_MOUSE
8	WH_HARDWARE
9	WH_DEBUG
10	WH_SHELL
11	WH_FOREGROUNDIDLE
12	WH_CALLWNDPROCRET
13	WH_KEYBOARD_LL
14	WH_MOUSE_LL

Énumération : Severity

Liste des niveaux de gravité des événements consignés dans les logs.

Valeur numérique	Symbole associé
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

Champ binaire : ThreadAccessMask

Champ binaire correspondant aux droits d'accès à un thread d'un processus.

Valeur binaire	Symbole associé
0x0001	THREAD_TERMINATE
0x0002	THREAD_SUSPEND_RESUME
0x0004	THREAD_ALERT
0x0008	THREAD_GET_CONTEXT
0x0010	THREAD_SET_CONTEXT
0x0020	THREAD_SET_INFORMATION
0x0040	THREAD_QUERY_INFORMATION
0x0080	THREAD_SET_THREAD_TOKEN
0x0100	THREAD_IMPERSONATE
0x0200	THREAD_DIRECT_IMPERSONATION
0x0400	THREAD_SET_LIMITED_INFORMATION
0x0800	THREAD_QUERY_LIMITED_INFORMATION
0x1000	THREAD_RESUME
0x10000	DELETE
0x20000	READ_CONTROL
0x40000	WRITE_DAC
0x80000	WRITE_OWNER
0x100000	SYNCHRONIZE

Énumération : TokenGuardDetailsType

Liste des types de modifications des jetons de sécurité.

Valeur numérique	Symbole associé
0	TokenDuplicate
1	TokenReplace
2	TokenModify

Énumération : TrampolineType

Type de trampoline détecté.

Valeur numérique	Symbole associé
0	None
1	X64Pattern
2	X86Pattern

Énumération : UsbDeviceClass

Liste des classes de périphériques USB.

Valeur numérique	Symbole associé
0x00	IN_INTERFACE_DESCRIPTORS
0x01	AUDIO
0x02	COMMUNICATIONS_CDC_CONTROL
0x03	HID
0x05	PHYSICAL
0x06	IMAGE
0x07	PRINTER
0x08	MASS_STORAGE
0x09	HUB
0x0A	CDC_DATA
0x0B	SMART_CARD
0x0D	CONTENT_SECURITY
0x0E	VIDEO
0x0F	PERSONAL_HEALTHCARE
0x10	AUDIO_VIDEO_DEVICES
0x11	BILLBOARD_DEVICE_CLASS
0x12	USB_TYPE_C_BRIDGE_CLASS
0xDC	DIAGNOSTIC_DEVICE
0xE0	WIRELESS_CONTROLLER
0xEF	MISCELLANEOUS
0xFE	APPLICATION_SPECIFIC
0xFF	VENDOR_SPECIFIC

Énumération : UsbDeviceEventType

Liste des événements relatifs aux périphériques USB.

Valeur numérique	Symbole associé
0x00	CONNECT
0x01	DISCONNECT

Énumération : UsbVolumeEnrollFileState

Liste des états du fichier d'enrôlement pour un périphérique USB.

Valeur numérique	Symbole associé
0x00	NOT_FOUND
0x01	MALFORMED
0x02	BAD_VERSION
0x03	BAD_ENCRYPTION
0x04	CONTENT_MISMATCH
0x05	VALID

Énumération : UsbVolumeMountEventType

Liste d'événements relatifs au montage ou démontage d'un volume.

Valeur numérique	Symbole associé
0x00	MOUNT
0x01	UNMOUNT

Énumération : UsbVolumeTrustFootprintFileState

Liste des états du fichier d'empreinte pour un périphérique USB.

Valeur numérique	Symbole associé
0x00	NOT_FOUND
0x01	MALFORMED
0x02	BAD_VERSION
0x03	BAD_ENCRYPTION
0x04	CONTENT_MISMATCH
0x05	VALID

Énumération : VolumeAccessType

Liste des modes d'accès à un volume sans passer par le système de fichiers.

Valeur numérique	Symbole associé
1	Read
2	Write

Champ binaire : VolumeZone

Champ binaire correspondant aux caractéristiques d'un volume de stockage.

Valeur binaire	Symbole associé
0x00000001	OPERATING_SYSTEM
0x00000002	COMPUTER_BOOT
0x00000004	SYSTEM_SNAPSHOT
0x00000008	CD_ROM
0x00000010	ISO
0x00000020	VIRTUAL_DISK
0x00000040	FLOPPY
0x00000080	REMOTE_LANMAN
0x00000100	REMOTE_CSC
0x00000200	REMOTE_RDP_DR
0x00000400	REMOTE_WEBDAV
0x00000800	REMOTE_MAILSLOT
0x00001000	REMOTE_VMWARE
0x00002000	REMOTE_VBOX
0x00004000	REMOTE_UNKNOWN
0x00008000	REMOVABLE_UNKNOWN
0x00010000	NOT_REMOVABLE_UNKNOWN

Champ binaire : WifiAuthAlgo

Liste des types d'authentification sur les réseaux Wi-Fi.

Valeur binaire	Symbole associé
0x00000001	Wpa2Enterprise
0x00000002	Wpa2Personal
0x00000004	WpaEnterprise
0x00000008	WpaPersonal
0x00000010	Open
0x00000020	Shared

Champ binaire : WifiConnectionMode

Liste des modes de connexion Wi-Fi.

Valeur binaire	Symbole associé
0x00000001	Infrastructure
0x00000002	AdHoc

Énumération : WmiPersistenceConsumerTypeMap

Liste des types de consommateurs détectés lors d'une persistance via WMI.

Valeur numérique	Symbole associé
0	CommandLineEventConsumer
1	ActiveScriptEventConsumer

Bloc : AgentActionTagTemplate

Détails relatifs à un tag MITRE associé à une règle.

Champ	Signification
RuleTag	Nom du tag associé à la règle qui a déclenché la génération du log.

Bloc : AgentActionTemplate

Descriptif d'une action prise par l'agent.

Champ	Signification
PolicyGuid	Identifiant de la politique associée à la règle à l'origine de l'événement.
PolicyVersion	Version de la politique associée à la règle à l'origine de l'événement.
RuleGuid	Identifiant d'une sous-règle précise à l'intérieur d'une règle (paramètre interne au produit).
BaseRuleGuid	Identifiant de la règle associée au log.
IdentifierGuid	Identifiant unique de l'identifiant d'application ayant occasionné l'événement.
Blocked	Indication d'un blocage par l'agent.
RequestMoveToQuarantine	Requête pour mettre le processus source en quarantaine. Il s'agit d'une requête qui n'a pas encore été effectuée.
UserDecision	Indication de la décision de l'utilisateur.
SourceProcessKilled	Indication de l'arrêt par SES du processus effectuant l'opération.
RuleTags	Tags associés à la règle qui a déclenché la génération du log. Plus de détails sur ce bloc à la section AgentActionTagTemplate.

Bloc : AgentAnalysisPropertiesTemplate

Bloc de détails généré pour tous les logs liés à des analyses (exemple : analyses YARA)

Champ	Signification
AnalysisUnitGuid	Identifiant unique de l'unité d'analyse
Triggers	Déclencheurs associés à l'analyse Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section ScriptTriggers.
AssociatedEventGuid	Identifiant du log ayant provoqué le démarrage de l'analyse
AssociatedScheduledTaskGuid	Identifiant de la tâche planifiée associée à l'analyse
AssociatedSecOpsGuid	Identifiant de la tâche d'analyse associée à l'analyse
AssociatedSecOpsRequestGuid	Identifiant de la requête de la tâche associée à l'analyse
AssociatedBaseRuleGuid	Identifiant de la règle de base ayant permis le lancement de l'analyse.
AssociatedRuleGuid	Identifiant de la règle ayant permis le lancement de l'analyse.

Bloc : AgentCorrelationTemplate

Descriptif des informations d'une protection avancée

Champ	Signification
PackageGuid	Identifiant unique de la protection
PackageVersion	Version de la protection avancée.
AttackIntent	Intention de l'attaque identifiée par la protection par corrélation.

Bloc : AgentFieldsTemplate

Descriptif des champs de règle associés au transfert d'événements.

Champ	Signification
_RuleGuid	Identifiant d'une sous-règle précise à l'intérieur de la règle (la signification est interne au produit).
_BaseRuleGuid	Identifiant de la règle associée à l'événement.

Bloc : AgentFileQuarantineRuleDetailsTemplate

Informations relatives à la règle à l'origine de la mise en quarantaine.

Champ	Signification
RuleGuid	Identifiant d'une règle précise à l'intérieur du groupe de règles (la signification est interne au produit).
BaseRuleGuid	Identifiant pour la règle à l'origine de la mise en quarantaine
PolicyGuid	Identifiant de la politique à laquelle la règle se rapporte.
PolicyVersion	Numéro de version de la politique à laquelle la règle se rapporte.

Bloc : AgentFloodInformationTemplate

Informations sur la source de la génération massive de logs.

Champ	Signification
TriggeringEventGUID	GUID de l'événement responsable de la génération massive de logs.
TriggeringEventBaseRuleGUID	GUID de la règle responsable de la génération massive de logs.
TriggeringEventPolicyGUID	GUID de la politique responsable de la génération massive de logs.
TriggeringEventPolicyVersion	Version de la politique responsable de la génération massive de logs.
TriggeringEventTimestamp	Heure du log ayant déclenché la génération massive de logs.

Bloc : AgentInternalPolymorphicLogTemplate

Log polymorphique

Bloc : AgentOperationEDRBypassDetailsBreakpointInformationTemplate

Informations complémentaires liées à un contournement des moyens de détection d'un EDR. Ce bloc contient les informations spécifiques aux points d'arrêts matériels.

Champ	Signification
ModuleName	Nom du module impacté tel qu'il est défini dans la table d'export du module PE.
NearestSymbol	Nom de la routine dans laquelle a été détecté le point d'arrêt.

Bloc : AgentOperationEDRBypassDetailsFunctionPatchInformationTemplate

Informations complémentaires liées à un contournement des moyens de détection d'un EDR. Ce bloc contient les informations spécifiques à l'altération du contenu d'une fonction.

Champ	Signification
ModuleName	Nom du module impacté tel qu'il est défini dans la table d'export du module PE.
NearestSymbol	Nom de la routine qui a été altérée.
ExpectedOpCodes	Code de la routine servant de base pour la comparaison.
ReadOpCodes	Code de la routine qui était effectivement exécutée.

Bloc : AgentOperationEDRBypassDetailsNoInformationTemplate

Informations complémentaires liées à un contournement des moyens de détection d'un EDR.
Ce bloc est vide.

Bloc : AgentOperationFileDetailsAccessFromNetworkTemplate

Descriptif de l'accès à un système de fichiers par un client depuis le réseau.

Champ	Signification
ShareName	Chemin du partage auquel accède le client réseau.
AddressFamily	Famille d'adressse IP (IPv4 ou IPv6). Ce champ peut prendre une des valeurs détaillées à la page NetworkAccessAddressFamily.
Address	Adresse IPv4 ou IPv6 du client réseau.
Port	Port de communication sur lequel le client réseau s'est connecté.

Bloc : AgentOperationFileDetailsAccessNotFromNetworkTemplate

Bloc vide qui apparaît lorsque l'accès à un fichier est fait en local.

Bloc : AgentOperationFileDetailsCreateChildHardLinkDestinationTemplate

Bloc de détails relatifs à la création d'un nouveau hard link fils d'un répertoire sur un système de fichiers, lorsque le chemin de destination correspond à une règle de l'agent.

Champ	Signification
FileName	Nom de l'élément créé.
SourcePath	Indique le chemin source du hard link.
Flags	Options de création de hard link. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsCreateChildTemplate

Bloc de détails relatifs à la création d'un nouveau sous-élément d'un répertoire sur un système de fichiers.

Champ	Signification
FileName	Nom de l'élément créé.
Disposition	Paramètres de création. Ce champ peut prendre une des valeurs détaillées à la page FileCreateDisposition. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page CreateFileW, section dwCreationDisposition.
Options	Options de création diverses. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileCreateOptions. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page FLT_PARAMETERS, section Options.
Attributes	Attributs indiqués. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileAttributes. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page CreateFileW, section dwFlagsAndAttributes.
DesiredAccess	Droits d'accès demandés. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileDesiredAccess. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page CreateFileW, section dwDesiredAccess.

Bloc : AgentOperationFileDetailsCreateHardLinkDestinationTemplate

Bloc de détails relatifs à la création d'un nouveau hard link sur un système de fichiers, lorsque le chemin de destination correspond à une règle de l'agent.

Champ	Signification
SourcePath	Indique le chemin source du hard link.
Flags	Options de création de hard link. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsCreateHardLinkSourceTemplate

Bloc de détails relatifs à la création d'un nouveau hard link sur un système de fichiers, lorsque le chemin source correspond à une règle de l'agent.

Champ	Signification
DestinationPath	Indique le chemin de destination du hard link.
Flags	Options de création de hard link. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsCreateTemplate

Descriptif de la création d'un nouvel élément sur un système de fichiers.

Champ	Signification
Disposition	Paramètres de création. Ce champ peut prendre une des valeurs détaillées à la page FileCreateDisposition. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page CreateFileW, section dwCreationDisposition.
Options	Options diverses de création. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileCreateOptions. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page FLT_PARAMETERS, section Options.
Attributes	Attributs indiqués. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileAttributes. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page CreateFileW, section dwFlagsAndAttributes.
DesiredAccess	Droits d'accès demandés. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileDesiredAccess. Pour plus d'informations sur ce champ, consultez la documentation Microsoft à la page CreateFileW, section dwDesiredAccess.

Bloc : AgentOperationFileDetailsDeleteChildTemplate

Bloc de détails relatifs à la suppression d'un sous-élément d'un répertoire d'un système de fichiers.

Champ	Signification
FileName	Nom de l'élément supprimé.
Flags	Options de suppression. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileDeleteFlags.

Bloc : AgentOperationFileDetailsDeleteTemplate

Bloc de détails relatifs à la suppression d'un élément d'un système de fichiers.

Champ	Signification
Flags	Options de suppression. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileDeleteFlags.

Bloc : AgentOperationFileDetailsMoveFileExChildDestinationTemplate

Bloc de détails relatifs à la suppression ou au déplacement d'un sous-élément d'un répertoire d'un système de fichiers, planifiés au démarrage, lorsque le chemin de destination correspond à une règle de l'agent.

Champ	Signification
FileName	Nom de l'élément déplacé ou supprimé.
SourcePath	Chemin de l'élément source.
Operation	Nature de l'opération (déplacement, suppression, remplacement). Ce champ peut prendre une des valeurs détaillées à la page FileMoveFileExOperation.
IsNewOperation	Indique s'il s'agit d'une nouvelle opération ayant été planifiée au redémarrage, ou s'il s'agit, par exemple, d'une modification manuelle du registre ayant pu réordonnancer les opérations déjà planifiées.

Bloc : AgentOperationFileDetailsMoveFileExChildSourceTemplate

Bloc de détails relatifs à la suppression ou déplacement d'un sous-élément d'un répertoire d'un système de fichiers, planifiés au démarrage, lorsque le chemin source correspond à une règle de l'agent.

Champ	Signification
FileName	Nom de l'élément déplacé ou supprimé.
DestinationPath	Chemin de l'élément destination.
Operation	Nature de l'opération MoveFileEx (déplacement, suppression, remplacement). Ce champ peut prendre une des valeurs détaillées à la page FileMoveFileExOperation.
IsNewOperation	Indique s'il s'agit d'une nouvelle opération ayant été planifiée au redémarrage, ou s'il s'agit, par exemple, d'une modification manuelle du registre ayant pu réordonnancer les opérations déjà planifiées.

Bloc : AgentOperationFileDetailsMoveFileExDestinationTemplate

Descriptif sur la suppression ou le déplacement d'un élément d'un système de fichiers planifié au démarrage, lorsque le chemin de destination est concerné par une règle de l'agent.

Champ	Signification
SourcePath	Chemin de l'élément source.
Operation	Nature de l'opération (déplacement, suppression, remplacement). Ce champ peut prendre une des valeurs détaillées à la page FileMoveFileExOperation.
IsNewOperation	Indique s'il s'agit d'une nouvelle opération planifiée au redémarrage, ou plutôt d'une modification manuelle du registre ayant réordonnancé les opérations déjà planifiées.

Bloc : AgentOperationFileDetailsMoveFileExSourceTemplate

Descriptif sur la suppression ou le déplacement d'un élément d'un système de fichiers planifié au démarrage, lorsque le chemin source est concerné par une règle de l'agent.

Champ	Signification
DestinationPath	Chemin de l'élément de destination.
Operation	Nature de l'opération MoveFileEx (déplacement, suppression, remplacement). Ce champ peut prendre une des valeurs détaillées à la page FileMoveFileExOperation.
IsNewOperation	Indique s'il s'agit d'une nouvelle opération ayant été planifiée au redémarrage, ou s'il s'agit, par exemple, d'une modification manuelle du registre ayant pu réordonnancer les opérations déjà planifiées.

Bloc : AgentOperationFileDetailsReadDataTemplate

Bloc de détails relatifs à la lecture des données d'un élément d'un système de fichiers.

Bloc : AgentOperationFileDetailsRenameChildDestinationTemplate

Bloc de détails relatifs au renommage d'un sous-élément d'un répertoire d'un système de fichiers, lorsque le chemin de destination correspond à une règle de l'agent.

Champ	Signification
FileName	Nom de l'élément renommé.
SourcePath	Chemin de l'élément avant renommage.
Flags	Options de renommage. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsRenameChildSourceTemplate

Bloc de détails relatifs au renommage d'un sous-élément d'un répertoire d'un système de fichiers, lorsque le chemin source correspond à une règle de l'agent.

Champ	Signification
FileName	Nom de l'élément renommé.
DestinationPath	Chemin de l'élément après renommage.
Flags	Options de renommage. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsRenameDestinationTemplate

Descriptif du renommage d'un élément d'un système de fichiers, lorsque le chemin de destination est concerné par une règle de l'agent.

Champ	Signification
SourcePath	Chemin de l'élément avant renommage.
Flags	Options de renommage. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsRenameSourceTemplate

Descriptif du renommage d'un élément d'un système de fichiers, lorsque le chemin source est concerné par une règle de l'agent.

Champ	Signification
DestinationPath	Chemin de l'élément après renommage.
Flags	Options de renommage. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section FileRenameFlags.

Bloc : AgentOperationFileDetailsSectionMappingTemplate

Bloc de détails relatifs au chargement en mémoire d'un élément d'un système de fichiers.

Champ	Signification
PageProtection	Droits demandés lors du chargement de l'élément en mémoire. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section MemoryProtection.

Bloc : AgentOperationFileDetailsSetInformationTemplate

Bloc de détails relatifs à l'écriture des informations d'un élément d'un système de fichiers.

Champ	Signification
InformationClass	Type d'information écrites. Ce champ peut prendre une des valeurs détaillées à la page FileInformationClass.

Bloc : AgentOperationFileDetailsSetOwnerDestinationTemplate

Descriptif du changement de propriétaire d'un élément d'un système de fichiers, lorsque l'élément est concerné par une règle de l'agent.

Champ	Signification
OldFileOwner	Propriétaire initial de l'élément. Note : Ce champ est un SID. Les champs automatiques **OldFileOwnerNameLookup** et **OldFileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Bloc : AgentOperationFileDetailsSetOwnerSourceTemplate

Descriptif du changement de propriétaire d'un élément d'un système de fichiers, lorsque l'élément est concerné par une règle de l'agent.

Champ	Signification
NewFileOwner	Nouveau propriétaire demandé pour l'élément. Note : Ce champ est un SID. Les champs automatiques **NewFileOwnerNameLookup** et **NewFileOwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Bloc : AgentOperationFileDetailsSetSecurityTemplate

Bloc de détails relatifs à l'écriture du descripteur de sécurité d'un élément d'un système de fichiers.

Champ	Signification
SecurityInformation	Type d'informations écrites à propos du descripteur de sécurité. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section SecurityClass.

Bloc : AgentOperationFileDetailsWriteDataTemplate

Bloc de détails relatifs à l'écriture des données d'un élément d'un système de fichiers.

Bloc : AgentOperationFilelessDetailsDynamicMemoryInformationTemplate

Informations complémentaires liées à l'utilisation de mémoire dynamiquement allouée.

Champ	Signification
ModuleName	Nom du module utilisé.
MemoryMapping	Type de mapping mémoire utilisé. Ce champ peut prendre une des valeurs détaillées à la page MemoryMappingType.
InitialPageProtection	Droits initiaux de la page. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section MemoryProtection.
FinalPageProtection	Droits finaux de la page. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section MemoryProtection.

Bloc : AgentOperationFilelessDetailsModuleStompingInformationTemplate

Informations complémentaires liées à l'écrasement de module.

Champ	Signification
ModuleName	Nom du module altéré.
FinalPageProtection	Droits finaux de la page. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section MemoryProtection.

Bloc : AgentOperationFilelessDetailsNoInformationTemplate

Bloc vide.

Bloc : AgentOperationFilelessDetailsThreadStartAddressSpoofingInformationTemplate

Informations complémentaires liées à l'échange de l'adresse de démarrage d'un thread.

Champ	Signification
ModuleName	Nom du module cible de l'exécution. Vide si indisponible.

Bloc : AgentOperationFilelessDetailsTrampolineStartInformationTemplate

Informations complémentaires liées à l'utilisation de trampoline.

Champ	Signification
ModuleName	Nom du module cible de l'exécution. Vide si indisponible.
TrampolinePattern	Motif de trampoline détecté. Ce champ peut prendre une des valeurs détaillées à la page TrampolineType.

Bloc : AgentOperationIocFileSearchDetailsTemplate

Détails sur le fichier correspondant au hash.

Champ	Signification
FileFullPath	Chemin vers le fichier
FileCreateTime	Date de création
LastModified	Date de dernière modification
Owner	Identifiant du propriétaire Note : Ce champ est un SID. Les champs automatiques **OwnerNameLookup** et **OwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
HashMd5	Hash MD5
HashSha1	Hash SHA1
HashSha256	Hash SH256
HashSSDeep	Hash SSDEEP

Bloc : AgentOperationIocFileSearchMatchInformationTemplate

Informations liées à une correspondance.

Champ	Signification
HashAlgorithm	Algorithme de hash utilisé Ce champ peut prendre une des valeurs détaillées à la page IOCAlgorithmDigest.
SimilarityRate	Taux de similarité
MatchedHash	Hash correspondant au déclenchement

Bloc : AgentOperationIocMatchedStringTemplate

Template technique servant à serialiser les tableaux de chaines

Champ	Signification
MatchedString	Indicateur ayant permis la correspondance dans le fichier

Bloc : AgentOperationProcessAccessDetailsProcessTemplate

Descriptif de l'accès à un processus.

Champ	Signification
DesiredAccess	Droits d'accès demandés pour l'accès au processus. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section ProcessAccessMask.
MatchingAccess	Droits d'accès accordés par l'agent pour l'accès au processus. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section ProcessAccessMask.

Bloc : AgentOperationProcessAccessDetailsThreadTemplate

Descriptif de l'accès à un thread dans un processus.

Champ	Signification
DesiredAccess	Droits d'accès demandés pour l'accès au thread. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section ThreadAccessMask.
MatchingAccess	Droits d'accès accordés par l'agent pour l'accès au thread. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section ThreadAccessMask.

Bloc : AgentOperationProcessAccessEmptyBlockTemplate

Bloc vide qui apparaît lorsque l'accès à un processus ou à un thread se manifeste par l'acquisition d'un handle sur l'objet, et non par la duplication d'un handle appartenant au processus cible.

Bloc : AgentOperationRegistryKeyCreateDetailsCreateLinkTemplate

Descriptif de la création d'une clé de registre obtenue en tant que lien symbolique.

Champ	Signification
TargetPath	Chemin de la clé de registre vers laquelle pointe le lien symbolique créé.

Bloc : AgentOperationRegistryKeyCreateDetailsCreateTemplate

Descriptif de la création d'une clé de registre.

Champ	Signification
Options	Options diverses de création de clé de registre. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section RegistryCreateOptions.
DesiredAccess	Droits demandés sur la clé de registre. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section RegistryAccessMask.

Bloc : AgentOperationRegistryKeyCreateDetailsRenameTemplate

Descriptif de la création d'une clé de registre obtenue via le renommage d'une clé existante.

Champ	Signification
SourcePath	Chemin de la clé de registre avant renommage.

Bloc : AgentOperationRegistryKeyDeleteDetailsDeleteTemplate

Descriptif de la suppression d'une clé de registre.

Bloc : AgentOperationRegistryKeyDeleteDetailsRenameTemplate

Descriptif de la suppression d'une clé de registre obtenue via le renommage d'une clé existante.

Champ	Signification
DestinationPath	Nouveau chemin demandé pour la clé de registre.

Bloc : AgentOperationRegistryKeyWriteDetailsSetInformationTemplate

Descriptif de l'écriture d'informations d'une clé de registre.

Champ	Signification
InformationClass	Type d'informations écrites à propos de la clé de registre. Ce champ peut prendre une des valeurs détaillées à la page RegistrySetInformationClass.

Bloc : AgentOperationRegistryKeyWriteDetailsSetSecurityTemplate

Descriptif de l'écriture du descripteur de sécurité d'une clé de registre.

Champ	Signification
SecurityInformation	Type d'informations écrites à propos du descripteur de sécurité. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section SecurityClass.

Bloc : AgentOperationRegistryKeyWriteDetailsSubkeyCreateTemplate

Descriptif de la création d'une sous-clé dans une clé de registre.

Champ	Signification
Options	Options diverses de création de clé de registre. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section RegistryCreateOptions.
DesiredAccess	Droits demandés sur la clé de registre. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section RegistryAccessMask.
SubkeyName	Nom de la sous-clé créée.

Bloc : AgentOperationRegistryKeyWriteDetailsSubkeyRenameTemplate

Descriptif du renommage d'une sous-clé dans une clé de registre.

Champ	Signification
SourcePath	Chemin de la clé de registre avant renommage.
DestinationPath	Nouveau chemin demandé pour la clé de registre.

Bloc : AgentOperationTokenGuardDetailsTokenDuplicateTemplate

Descriptif de la modification d'un jeton de sécurité par duplication d'un jeton tiers.

Champ	Signification
User	Identifiant de sécurité de l'utilisateur dont le jeton est dupliqué. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.

Bloc : AgentOperationTokenGuardDetailsTokenModifyTemplate

Descriptif de la modification directe d'un jeton de sécurité.

Champ	Signification
PrivilegesLow	Seconde partie des privilèges demandés. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section PrivilegeLow.
PrivilegesHigh	Première partie des privilèges demandés. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section PrivilegeHigh.

Bloc : AgentOperationYaraAnalysisFilesDetailsTemplate

Bloc de détails généré pour lister les détails d'un fichier d'analyse YARA

Champ	Signification
FileFullPath	Chemin absolu vers le fichier
FileCreateTime	Date et heure de création du fichier
LastModified	Date et heure de dernière modification du fichier
Owner	Informations sur l'identité du propriétaire du fichier Note : Ce champ est un SID. Les champs automatiques **OwnerNameLookup** et **OwnerDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
HashMd5	Hash MD5 du fichier
HashSha1	Hash SHA1 du fichier
HashSha256	Hash SHA256 du fichier
HashSSDeep	Hash SSDeep du fichier

Bloc : AgentOperationYaraRuleInformationMatchedStringTemplate

Bloc de détails généré pour lister les correspondances d'une règle Yara

Champ	Signification
MatchedStringValue	Valeur de la correspondance textuelle

Bloc : AgentOperationYaraRuleInformationMetadataTemplate

Bloc de détails généré pour lister les détails d'une méta-donnée associée à une règle Yara

Champ	Signification
MetadataKey	Clé associée à la méta-donnée
MetadataValue	Valeur associée à la méta-donnée

Bloc : AgentOperationYaraRuleInformationTagTemplate

Bloc de détails généré pour lister les détails d'un tag associé à une règle Yara

Champ	Signification
TagName	Nom du tag

Bloc : AgentOperationYaraRuleInformationTemplate

Bloc de détails généré pour lister les détails d'une règle Yara

Champ	Signification
MatchedRule	Nom de la règle Yara ayant trouvé une correspondance
Tags	Liste des tags associés à la règle Yara Plus de détails sur ce bloc à la section AgentOperationYaraRuleInformationTagTemplate.
Metadatas	Liste des meta-données associées à la règle Yara Plus de détails sur ce bloc à la section AgentOperationYaraRuleInformationMetadataTemplate.
MatchedStrings	Correspondance textuelle pour la règle Yara Plus de détails sur ce bloc à la section AgentOperationYaraRuleInformationMatchedStringTemplate.

Bloc : AgentPEInfoTemplate

Informations contenues dans les ressources du fichier PE.

Champ	Signification
OriginalFilename	Nom donné au fichier lors de sa création.
Description	Description du rôle du fichier
ProductName	Nom du produit qui embarque le fichier
CompanyName	Nom de l'entreprise ayant généré le fichier
FileVersion	Version du fichier

Bloc : AgentRemediationRestoredFileFromShadowCopyTemplate

Informations liées à la restauration d'un fichier

Champ	Signification
Filename	Chemin d'un fichier restauré à partir d'un cliché instantané

Bloc : AgentRemediationSpecificDataTemplate

Eléments spécifiques communs aux logs de remédiation

Champ	Signification
Result	Code de résultat de l'action de remédiation Ce champ peut prendre une des valeurs détaillées à la page RemediationActionResultMap.
StatusCode	Code de statut de l'action de remédiation
SecOpsTaskGuid	Identifiant de la tâche issue de la SecOps
SecOpsTaskRequestGuid	Identifiant de la requête issue de la SecOps
ScheduledTaskRequestGuid	GUID de la tâche planifiée.

Bloc : BluetoothDeviceInfoAudioVideoTemplate

Descriptif d'un périphérique Bluetooth de type dispositif audio ou vidéo.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type dispositif audio ou vidéo. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceClassAudioVideo.

Bloc : BluetoothDeviceInfoComputerTemplate

Descriptif d'un périphérique Bluetooth de type ordinateur.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type ordinateur. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceClassComputer.

Bloc : BluetoothDeviceInfoDefaultTemplate

Descriptif d'un périphérique Bluetooth.

Champ	Signification
Info	Complément d'information relatif à la nature d'un périphérique Bluetooth.

Bloc : BluetoothDeviceInfoHealthTemplate

Descriptif d'un périphérique Bluetooth de type équipement médical.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type équipement médical. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceHealth.

Bloc : BluetoothDeviceInfoImagingTemplate

Descriptif d'un périphérique Bluetooth de type dispositif d'acquisition d'images.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type dispositif d'acquisition d'images. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section BluetoothMinorDeviceClassImaging.

Bloc : BluetoothDeviceInfoNetworkApLoadFactorTemplate

Descriptif d'un périphérique Bluetooth de type réseau ou d'un point d'accès.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type réseau ou un point d'accès. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceClassNetworkApLoadFactor.

Bloc : BluetoothDeviceInfoPeripheralTemplate

Descriptif d'un périphérique Bluetooth de type clavier ou souris.

Champ	Signification
Major	Complément d'information relatif à un périphérique Bluetooth permettant de définir si le périphérique est un clavier ou une souris. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceClassPeripheralMajor.
Minor	Complément d'information relatif à la nature d'un périphérique Bluetooth. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceClassPeripheralMinor.

Bloc : BluetoothDeviceInfoPhoneTemplate

Descriptif d'un périphérique Bluetooth de type téléphone.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type téléphone. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceClassPhone.

Bloc : BluetoothDeviceInfoTemplate

Descriptif d'un périphérique Bluetooth.

Champ	Signification
ClassOfDevice	Valeur de la classe de périphérique.
DeviceName	Nom du périphérique.
MajorServiceClass	Valeur de la classe majeure de service. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section BluetoothMajorServiceClass.
MajorDeviceClass	Valeur de la classe majeure de périphérique. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMajorDeviceClass.
MinorDeviceClass	Valeur de la classe mineure de périphérique. Plus de détails sur ce bloc à la section BluetoothDeviceInfoComputerTemplate, BluetoothDeviceInfoPhoneTemplate, BluetoothDeviceInfoNetworkApLoadFactorTemplate, BluetoothDeviceInfoAudioVideoTemplate, BluetoothDeviceInfoPeripheralTemplate, BluetoothDeviceInfoWearableTemplate, BluetoothDeviceInfoToyTemplate, BluetoothDeviceInfoHealthTemplate, BluetoothDeviceInfoDefaultTemplate.

Bloc : BluetoothDeviceInfoToyTemplate

Descriptif d'un périphérique Bluetooth de type gadget.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type gadget. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceToy.

Bloc : BluetoothDeviceInfoWearableTemplate

Descriptif d'un périphérique Bluetooth de type dispositif portable.

Champ	Signification
Info	Complément d'information relatif à un périphérique Bluetooth de type dispositif portable. Ce champ peut prendre une des valeurs détaillées à la page BluetoothMinorDeviceWearable.

Bloc : CertificateInformationRendering

Informations sur un certificat

Champ	Signification
Algorithm	Algorithme de signature pour le certificat.
IssuerCN	Nom commun (CN) de l'émetteur.
SubjectCN	Nom commun (CN) de l'objet.
SigningTime	Date et heure de la signature.
ValidityStart	Date de début de validité.
ValidityEnd	Date de fin de validité.

Bloc : NotUsbDeviceInfoTemplate

Bloc vide apparaissant lorsqu'un accès fichier n'est pas effectué sur un périphérique de stockage de masse USB.

Bloc : NotUsbVolumeTrackingDataTemplate

Bloc vide apparaissant lorsqu'un accès fichier n'est pas effectué sur un périphérique de stockage de masse USB.

Bloc : PhysicalConsoleSessionTemplate

Bloc indiquant les données de la session de la console.

Champ	Signification
PhysicalConsoleSessionId	Identifiant de la session de la console.
LoginUserName	Nom de l'utilisateur connecté sur la session de la console (format "nom de domaine/nom d'utilisateur").

Bloc : PnPDeviceInfoTemplate

Descriptif d'un périphérique Plug and Play.

Champ	Signification
ClassGuid	GUID de la classe du périphérique Plug and Play.
ClassName	Nom de la classe du périphérique Plug and Play.
DeviceDescription	Description du périphérique Plug and Play.
FriendlyName	Nom commun du périphérique Plug and Play.
Manufacturer	Fabriquant du périphérique Plug and Play.

Bloc : ProcessStaticInfoTemplate

Descriptif d'un processus.

Champ	Signification
PID	Identifiant du processus (Process Identifier).
ProcessGuid	Identifiant unique généré par l'agent pour ce processus.
ProcessImageName	Chemin de l'exécutable du processus.
VolumeZone	Type du volume sur lequel se trouve l'élément. Ce champ peut prendre des valeurs binaires qui se combinent et sont détaillées à la section VolumeZone.
ProcessCommandLine	Ligne de commande du processus.
User	Identifiant de sécurité de l'utilisateur dont le jeton est utilisé comme principal du processus. Note : Ce champ est un SID. Les champs automatiques **UserNameLookup** et **UserDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
IntegrityLevel	Identifiant de sécurité du niveau d'intégrité du processus. Note : Ce champ est un SID. Les champs automatiques **IntegrityLevelNameLookup** et **IntegrityLevelDomainLookup** résolvent ce SID respectivement en un nom et un domaine.
SessionID	Identifiant de la session sous laquelle le processus s'exécute.
HashMd5	Hash MD5 de l'exécutable principal du processus.
HashSha1	Hash SHA-1 de l'exécutable principal du processus.
HashSha256	Hash SHA-256 de l'exécutable principal du processus.
IsProtectedOrCritical	Indique si le processus est protégé ou critique.
CertificateSignatureState	Valeur indiquant l'état de la signature numérique d'un processus. Ce champ peut prendre une des valeurs détaillées à la page CertificateSignatureState.
Certificates	Certificats ayant signé le processus. Plus de détails sur ce bloc à la section CertificateInformationRendering.
ProcessStartTime	Date et heure de démarrage du processus.
ProcessStartTimeRaw	Date et heure de démarrage du processus représentées par un nombre entier.
PEInformation	Informations issues du fichier PE

Bloc : RenamedFilesRendering

Liste partielle des fichiers renommés lors d'une attaque ransomware présumée.

Champ	Signification
SourceFilename	Nom du fichier initial.
DestinationFilename	Nom du fichier chiffré.

Bloc : UsbDeviceInfoTemplate

Descriptif d'un périphérique USB.

Champ	Signification
VendorId	Identifiant du constructeur du périphérique USB.
ProductId	Identifiant du modèle du périphérique USB.
Class	Classe du périphérique USB. Ce champ peut prendre une des valeurs détaillées à la page UsbDeviceClass.
SubClass	Sous-classe du périphérique USB.
Protocol	Protocole du périphérique USB.
SerialNumber	Numéro de série du périphérique USB.
VendorName	Nom du constructeur du périphérique USB.
ProductName	Nom du modèle du périphérique USB.
Interfaces	Interfaces du périphérique USB. Plus de détails sur ce bloc à la section UsbDeviceInterfacesRendering.

Bloc : UsbDeviceInterfacesRendering

Informations sur le périphérique USB.

Champ	Signification
Class	Classe du périphérique. Ce champ peut prendre une des valeurs détaillées à la page UsbDeviceClass.
Subclass	Sous-classe du périphérique.
Protocol	Protocole

Bloc : UsbVolumeTrackingDataTemplate

Données de suivi d'un volume USB.

Champ	Signification
EnrollFileState	État du fichier d'enrôlement (non présent, présent mais invalide, présent mais contient des données incohérentes, présent et valide). Ce champ peut prendre une des valeurs détaillées à la page UsbVolumeEnrollFileState.
FootprintFileState	Etat du fichier d'empreinte (non présent, présent mais invalide, présent mais contient des données incohérentes, présent et valide) Ce champ peut prendre une des valeurs détaillées à la page UsbVolumeTrustFootprintFileState.
VendorId	Identifiant du constructeur du périphérique USB, tel qu'indiqué dans le fichier d'enrôlement.
ProductId	Identifiant du modèle du périphérique USB, tel qu'indiqué dans le fichier d'enrôlement.
SerialNumberHashSha256	Hash 256 du numéro de série du périphérique USB, tel qu'indiqué dans le fichier d'enrôlement.
EnrollGuid	Identifiant unique du volume enrôlé.

documentation@stormshield.eu