Configurer des exclusions de processus de terminal sécurisé sur MacOS et Linux

Table des matières

Introduction

Ce document décrit l'évolution, la configuration et les différences des exclusions de processus sur macOS et Linux.

Aperçu

À partir de la version 1.11.0 du connecteur, Secure Endpoint ajoute la prise en charge des exclusions de processus sur macOS et Linux. Par le passé, la configuration de Secure Endpoint pour ignorer les activités d'une application macOS ou Linux nécessitait une combinaison de règles d'exclusion de chemin, d'extension de fichier et/ou de caractère générique. Comme ces règles ciblent les fichiers et les répertoires et ne peuvent pas être associées à un programme ou un processus, plusieurs règles étaient souvent nécessaires pour chaque programme et chaque règle peut inutilement exclure des activités de plusieurs programmes. Les exclusions de processus offrent un moyen plus direct et plus précis d'exclure les activités logicielles bénignes. Lorsqu'elles sont utilisées correctement, les exclusions de processus peuvent améliorer considérablement les performances de Secure Endpoint avec un minimum d'effets négatifs sur la sécurité du système.

Les règles d'exclusion de processus sont gérées dans la console Web Secure Endpoint. Chaque règle se compose des éléments suivants :

- Le chemin complet (absolu) vers l'exécutable du programme,
- Le nom d'utilisateur du processus (facultatif) et
- Indique si les processus enfants doivent également être exclus (par défaut : non)

Lorsqu'une règle d'exclusion de processus correspond à un processus en cours d'exécution, toutes les activités effectuées par ce processus, et éventuellement ses processus enfants, sont exclues de l'analyse.

À partir de la version 1.15.2 du connecteur, le chemin d'exclusion de processus accepte les caractères génériques (« * »). Un caractère générique correspond à n'importe quel jeu de caractères dans un niveau de fichier ou de répertoire.

À partir de la version 1.2.0 du connecteur et de l'introduction du moteur de protection comportementale, les exclusions de processus sont appliquées à tous les moteurs et pas seulement aux analyses de fichiers.

> IMPORTANT !
>
> Avec l'ajout de l'exclusion de processus dans les connecteurs Mac et Linux 1.11.0, l'interprétation des règles existantes de chemin d'accès, d'extension de fichier et de caractères génériques est également en train de changer. Il n'y a aucun changement de comportement pour les connecteurs 1.10.x et plus anciens. Toutefois, les mêmes règles que celles de la section 1.11.0 ne s'appliquent pas aussi largement. Référez-vous à la section Modifications du chemin d'accès, extension de fichier et règles d'exclusion générique pour plus de détails.

Préparation des exclusions de processus

Avant de mettre à niveau vos terminaux macOS et Linux, trois points importants doivent être pris en compte :

1. Les connecteurs 1.10.x et antérieurs ignorent les règles d'exclusion de processus.
2. Les connecteurs 1.11.0 et plus récents respectent les règles d'exclusion de processus, mais interprètent les règles de chemin, d'extension de fichier et de caractères génériques différemment des connecteurs plus anciens. Cela peut nuire aux performances du système.
3. Les connecteurs Mac 1.10.0 et Linux 1.11.0 ont introduit des optimisations génériques d'analyse à l'exécution qui limitent la perte de performances de la nouvelle interprétation décrite dans (2).
4. 1.2.0 applique les exclusions de façon universelle à tous les moteurs

Modifications du chemin, de l'extension de fichier et des règles d'exclusion générique

Dans la version 1.10.x et les versions antérieures des connecteurs : les règles Fichier, Chemin et Caractère générique excluent le fichier ou le répertoire cible de l'analyse pour les opérations suivantes :

- Créer
- Modifier
- Renommer
- Exécuter

Dans la version 1.11.0 et les versions plus récentes des connecteurs : l'interprétation des règles de chemin d'accès, d'extension de fichier et de caractères génériques a changé de telle sorte qu'en cas de correspondance, l'exécution de fichier déclenche une analyse au lieu d'être exclue.

La création, la modification et le changement de nom des fichiers continuent d'être exclus. Les motivations de ce changement sont les suivantes :

1. Il évite l'exclusion indésirable de l'activité d'exécution lors de l'exclusion des répertoires de fichiers de données.
2. Il complète mieux les règles d'exclusion de processus en permettant d'exclure indépendamment les opérations d'exécution et de non-exécution sur le même chemin.
3. Il aligne l'interprétation macOS et Linux de ces règles avec Secure Endpoint sous Windows.

Dans la plupart des cas, l'augmentation de l'utilisation du processeur Secure Endpoint est estimée à moins de 20 %. Dans certains cas, l'utilisation du processeur Secure Endpoint peut diminuer. Cela est possible si les optimisations génériques d'analyse à l'exécution de la nouvelle version du connecteur sont plus efficaces que les règles d'exclusion utilisées.

Guide de mise à niveau du connecteur

Pour les systèmes précédemment réglés à l'aide d'exclusions, une attention particulière doit être portée après la mise à niveau vers la version 1.11.0 (ou ultérieure) pour s'assurer que les performances du système sont toujours satisfaisantes. Les étapes de mise à niveau recommandées sont les suivantes :

1. Sans effectuer de modifications d'exclusion, mettez à niveau le connecteur.
2. Évaluer les performances du système après la mise à niveau.
3. Si les performances du système après la mise à niveau sont satisfaisantes, supprimez les règles Path, File Extension et Wildcard Exclusion qui ciblent les exécutables de programme au lieu des fichiers de données. Ces règles ne sont plus nécessaires. De nouvelles règles d'exclusion de processus peuvent ensuite être ajoutées pour améliorer encore les performances à la convenance.
4. Si les performances du système après la mise à niveau ne sont pas satisfaisantes, remplacez les règles Path, File Extension et Wildcard Exclusion qui ciblent les programmes exécutables par les règles Process Exclusion correspondantes.

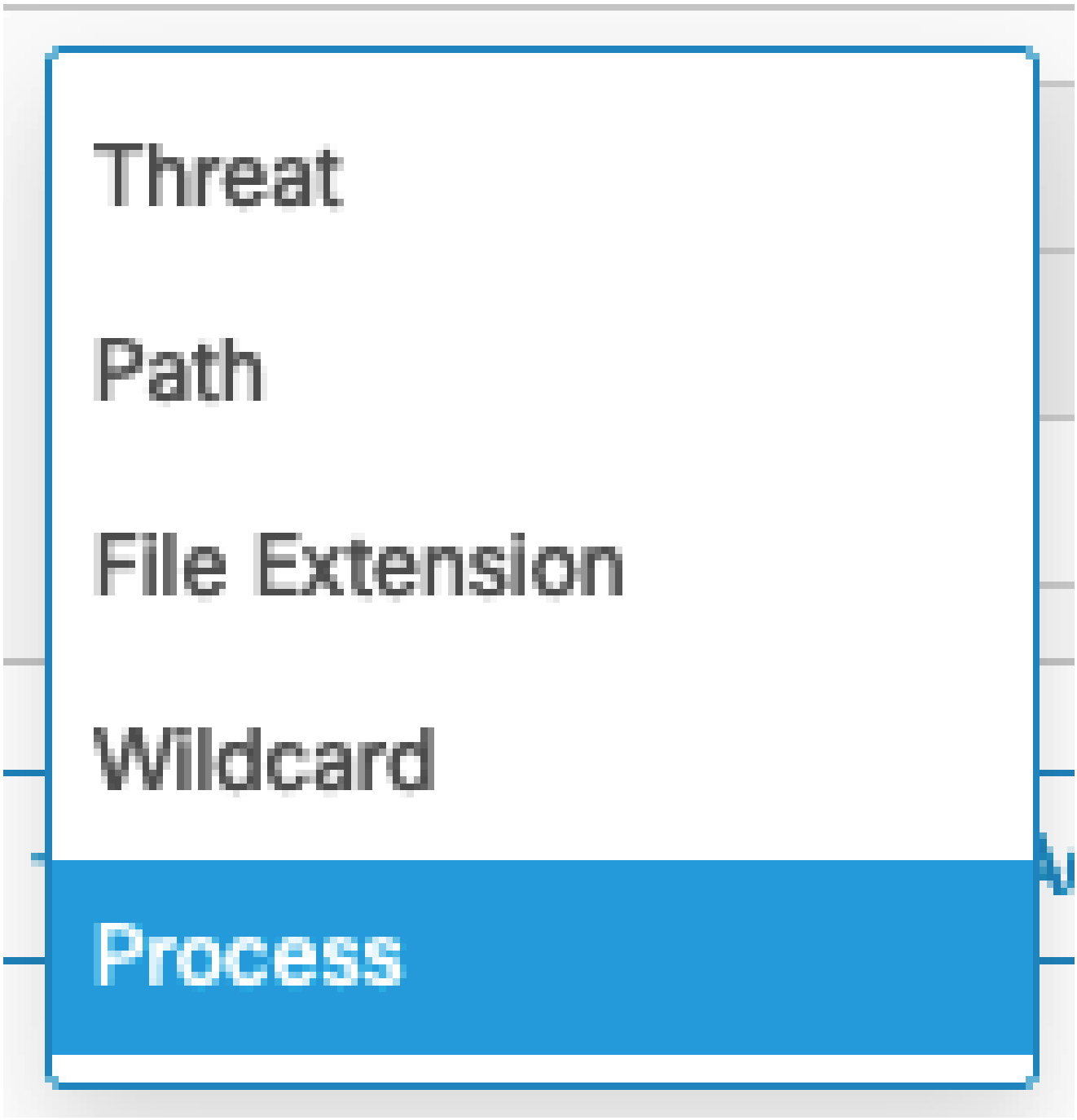
Dans les déploiements plus importants où les connecteurs sont mis à niveau par phases, il est recommandé de reporter la modification ou la suppression des règles de chemin d'accès, d'extension de fichier et d'exclusion générique jusqu'à ce que tous les connecteurs aient été mis à niveau vers la version 1.11.0 ou ultérieure. Ainsi, les connecteurs plus anciens qui reposent sur des règles d'exclusion existantes ne sont pas affectés avant la mise à niveau du terminal.

5. Si la mise à niveau vers le connecteur version 1.2.0 ou ultérieure et les performances du système après la mise à niveau ne sont pas satisfaisantes, recherchez l'erreur 18 et reportez-vous à la Défaillance du connecteur Linux du terminal sécurisé 18 conseils sur les étapes de correction.

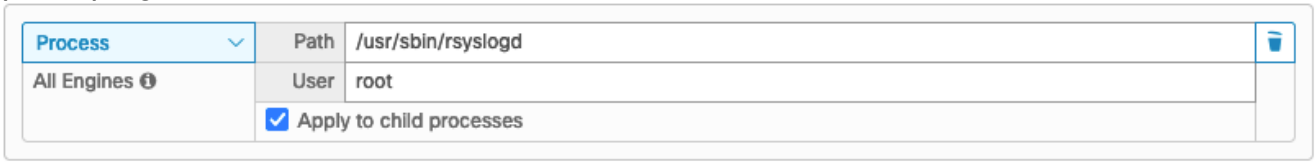
Ajout de règles d'exclusion de processus

Les règles d'exclusion de processus peuvent être créées à l'aide du portail Web Secure Endpoint. La procédure est la suivante :

1. Recherchez le jeu d'exclusions à modifier. Cliquez sur Ajouter une exclusion et sélectionnez Processus.

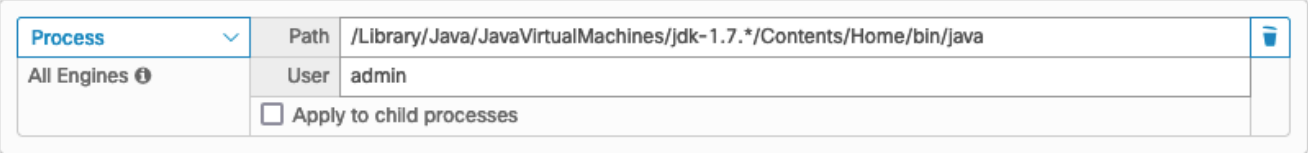


2. Entrez le chemin absolu du programme à exclure, le compte d'utilisateur qui exécute le programme (facultatif) et si l'exclusion doit s'appliquer à tous les processus enfants créés par le programme.



À partir de la version 1.15.2 du connecteur, des caractères génériques (*) peuvent être

utilisés dans le chemin d'accès pour représenter n'importe quel nombre de caractères dans un répertoire unique. Il est recommandé d'utiliser le caractère générique pour couvrir le nombre minimum de caractères requis pour fournir l'exclusion requise. Le caractère générique peut également être utilisé avec des caractères dans un répertoire pour réduire encore plus l'exclusion.



3. Cliquez sur Ajouter une exclusion pour ajouter d'autres règles (répétition des étapes 1 et 2) ou cliquez sur Enregistrer pour enregistrer le jeu d'exclusions.

Meilleures pratiques d'exclusion des processus

- N'excluez jamais le processus de démarrage : le processus de démarrage (`launchd` sur macOS, `init` ou `systemd` sur Linux) est responsable de la création de tous les autres processus sur le système et se trouve au sommet de la hiérarchie des processus. L'exclusion du processus de démarrage et de tous ses processus enfants désactiverait efficacement la surveillance Secure Endpoint.
- Spécifier l'utilisateur lorsque cela est possible : si le champ Utilisateur est laissé vide, l'exclusion s'applique à tout processus exécutant le programme spécifié. Bien qu'une règle qui s'applique à n'importe quel utilisateur soit plus flexible, cette large portée pourrait involontairement exclure une activité qui doit être surveillée. La spécification de l'utilisateur est particulièrement importante pour les règles qui s'appliquent aux programmes partagés tels que les moteurs d'exécution (par exemple, `java`) et les interpréteurs de script (par exemple, `bash`, `python`). La spécification de l'utilisateur limite l'étendue et indique à Secure Endpoint d'ignorer des instances spécifiques tout en surveillant d'autres instances.
- Éviter le chevauchement entre les règles d'exclusion de processus et les règles de chemin/extension de fichier/caractère générique : Lors de l'exclusion de l'analyse de l'exécution d'un programme, une bonne protection consiste à détecter les modifications de ce programme approuvé et à déclencher l'analyse des fichiers. S'assurer que le chemin d'accès spécifié dans une règle d'exclusion de processus n'est pas couvert par une règle Chemin d'accès/Extension de fichier/Caractère générique garantit que la modification de fichier ne sera pas exclue involontairement de l'analyse.
- Minimiser le nombre de règles : Bien que les connecteurs Mac et Linux n'imposent pas de limite de nombre maximal de règles d'exclusion de processus, davantage de règles peuvent entraîner une surcharge d'évaluation supplémentaire. Choisissez le processus parent de plus haut niveau qui identifie de manière unique l'application à exclure et utilisez l'option Appliquer au processus enfant pour réduire le nombre de règles.

Différences par rapport à Windows Implementation

L'ajout de la prise en charge des exclusions de processus et la réduction de l'étendue des règles de chemin, d'extension de fichier et de caractères génériques permettent d'aligner plus étroitement les exclusions macOS et Linux sur Windows. Toutefois, il subsiste d'importantes différences de mise en oeuvre :

1. Les règles d'exclusion de processus macOS et Linux acceptent un nom d'utilisateur facultatif pour accompagner le chemin d'accès complet de l'exécutable du processus, tandis que Windows accepte une valeur de hachage SHA-256 facultative. L'exclusion d'un processus par sa valeur de hachage SHA-256 n'est actuellement pas prise en charge sur macOS et Linux.
2. Les moteurs Activité malveillante et Processus système sont réservés à Windows et ces types d'exclusion ne sont donc pas disponibles sur macOS et Linux.
3. Les règles d'exclusion de processus macOS et Linux s'appliquent à tous les moteurs et ne sont pas séparées par moteur comme c'est le cas sous Windows.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.