Guide de FireAMP des exclusions sur Windows

Contenu

Introduction

Ce document fournit une instruction sur la façon dont trouver les fichiers détectés et décrit un processus pour les exclure. Quand vous exécutez l'AMP de Cisco pour des points finaux (également connus sous le nom de FireAMP) sur un ordinateur, vous pourriez éprouver le problème de performance sur une application ou sur l'ordinateur lui-même. Ceci pourrait se produire en raison des exécutions lecture/écriture excessives, de la pagination, ou du tourillonnement. Ceci peut entraîner des questions avec les applications qui exigent les traitements de fichier exclusifs, tels que l'application de base de données ou le logiciel d'enregistrement.

> **Attention** : L'exclusion réduit votre zone de couverture. Quand vous excluez un répertoire ou un fichier, FireAMP ne balaye pas dans ce répertoire. Afin d'éviter l'exclusion des fichiers excessifs, vous devriez être spécifique autant que possible.

Comment trouver les fichiers détectés

Quand vous voulez exclure des fichiers, vous pouvez adopter une large approche ou écrire une exclusion très spécifique avec un masque afin de couvrir juste un fichier affecté. Débuts de ce document avec une identification de base des répertoires de Microsoft Windows.

Fichiers de C:\Program

La plupart des applications sont installées dans ce répertoire. Ce répertoire est souvent la source pour le taux de mouvements du fichier sur le système et est le foyer primaire. Cisco sera sur la surveillance pour des applications de base de données et toute autre logiciels antivirus aussi bien que classe des propriétaires ou logiciel maison.

Données de C:\Program

Ce répertoire est parfois utilisé pour cacher ou enregistrer les fichiers temporaires. Dans ce répertoire, vous pourriez noter beaucoup d'activités qui dépendent des applications.

C:\Users

Ce répertoire facilite de divers répertoires utilisateurs, tels que l'appareil de bureau, les documents, les téléchargements, et l'appdata. Le répertoire d'appdata est universellement utilisé pour les fichiers temporaires, des fichiers de navigation Internet, historique, et ainsi de suite.

> **Attention** : En raison du nombre de fichiers et de données qui sont téléchargés dans ce répertoire, vous devriez faire attention quand vous spécifiez une exclusion, et essayez de devoir aussi précis que possible sélectionner les fichiers « sûrs ».

C:\Windows

Ce répertoire a les fichiers système. Vous généralement n'avez pas besoin d'exclure beaucoup à partir de ce répertoire pendant qu'il est manipulé par le positionnement par défaut d'exclusion. Vous pourriez vouloir exclure ce répertoire pour cacher, telle que la mise en cache pour des fichiers journal de la Configuration Manager (SCCM) et du Windows de System Center.

Types pris en charge d'exclusion

Menace : C'est le nom d'une menace qui n'est pas mise en quarantaine. Aucun fichier qui déclenche un nom particulier de menace ne serait mis en quarantaine. Un exemple est `Win.Malware.PDF`

Chemin : C'est un emplacement de système de fichier unique. Voici que vous pouvez utiliser un chemin spécifique tel que `C:\Program Files\Cisco`, ou vous pouvez utiliser la liste spéciale constante d'ID d'élément (CSIDL).

> **Note**: Un CSIDL est une variable intégrée qui est identifiée par Windows et peut être utile dans les scénarios où un chemin pourrait résider sur différents identificateurs de lecteur. Un exemple est `CSIDL_PROGRAM_FILES \ Cisco`. Cet exemple couvre `C:\Program Files\Cisco` et `D:\Program Files\Cisco`. Travail de CSIDLs seulement dans des exclusions de chemin. Référez-vous à la documentation Windows pour une liste complète de CSIDLs disponible.

Masque : Ce type doit être utilisé toutes les fois qu'un masque (*) est désiré dans l'exclusion. Exemple : `C:\Program Files\Cisco\ *.tmp`

Extension de fichier : C'est une exclusion simple pour une extension de fichier de type de fichier. Un exemple est `.txt`.

Quand exclure

Symptôme

Si vous exécutez FireAMP et problèmes de performance d'expérience avec le système ou avec une application spécifique, ceci pourrait être une indication de manque de réponse à l'entrée d'utilisateur, de représentation lente d'un traitement automatisé, de crash, ou d'erreurs. Parfois l'application affiche une erreur spécifique.

Vérification

Afin de déterminer les fichiers ou les répertoires qui sont balayés et comment fréquemment, suivez ces étapes :

Étape 1 : La première étape est de générer le module diagnostique et de l'extraire. C'est des archives 7zip et exige d'une application de l'extraire.

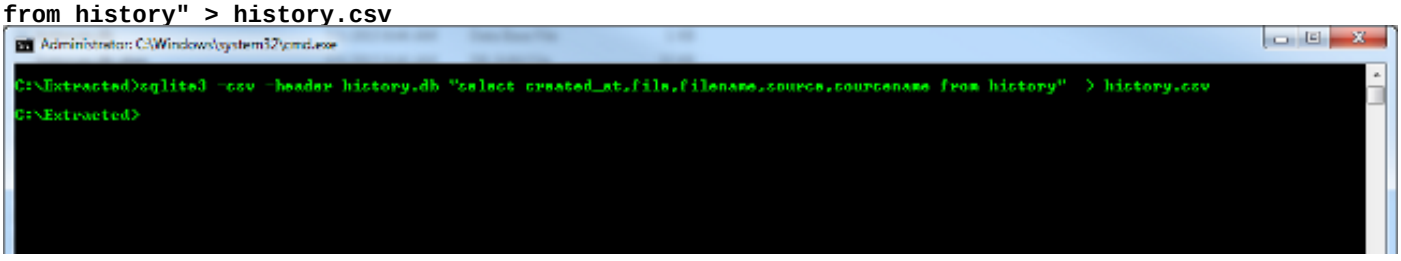
Étape 2 : La deuxième étape est d'accéder au `fichier history.db` à partir du fichier diagnostique.

`Le fichier history.db` est un fichier de base de données de SQLite qui maintient tout le FireAMP a détecté des fichiers. Chaque ligne inclut la disposition, le nom du fichier, le SHA de fichier, le fichier source, et le SHA de source. La source est le fichier qui a créé/a accédé au fichier lui-même. Ceci nous permet de voir comment l'application s'est comportée et ce qu'il a fait.

Dans cet exemple, la commande SQLite3 est utilisée afin de convertir la base de données d'historique en fichier de la valeur séparé par virgule (CSV).

- Téléchargez la binaire SQLite3 précompilée pour votre système d'exploitation.
- Extrayez le module diagnostique de FireAMP avec une application telle que 7zip.
- Naviguez vers le répertoire diagnostique extrait et trouvez le `fichier history.db` dans les `fichiers de` C_ `\ programme \ Sourcefire \ fireAMP \ répertoire`.
- Dans un terminal ou une invite de commande, appelez la binaire SQLite3 que vous avez téléchargée et fournissez au `fichier history.db` cette commande. (Cette commande le suppose que SQLite3 est dans un emplacement spécifié dans vos variables d'environnement pour votre système d'exploitation, ou doit être placée dans le répertoire diagnostique.)

```
sqlite3 -csv -header history.db "select created_at,file,filename,source,sourcename
from history" > history.csv
```



Vous ne verrez pas la confirmation ou la sortirez si la commande est réussie.

Si la commande manquait, soyez sûr que vous avez spécifié l'emplacement de la binaire SQLite3. Si vous voyez n'importe quels autres messages en vue de le `history.db classer`, vous pourriez devoir effacer les quatre fichiers historiques de l'ordinateur hôte affecté tandis que le service est arrêté, qui lui permet pour générer un ensemble frais de fichiers la prochaine fois que le service est commencé.

Étape 3 : Une fois que le fichier CSV a été généré vous pouvez l'ouvrir avec votre application préférée de tableur. Les applications telles que Microsoft Excel pourraient te permettre pour convertir le fichier CSV en table, qui te permet pour filtrer/tri. Examinez la documentation Microsoft pour que la façon utilise Exceler.

Les colonnes primaires aux utiliser sont :

- **nom du fichier** : Ce champ affiche que le fichier est analysé par FireAMP.
- **sourcename** : Cet champ affiche le processus ou exécutable que saisi le traitement (lecture/écriture et ainsi de suite). Ces données sont utilisées afin de déterminer si les fichiers sont traités par une application de confiance ou autrement.
- **created_at** : C'est l'horodateur sur l'événement pour la détection du fichier.

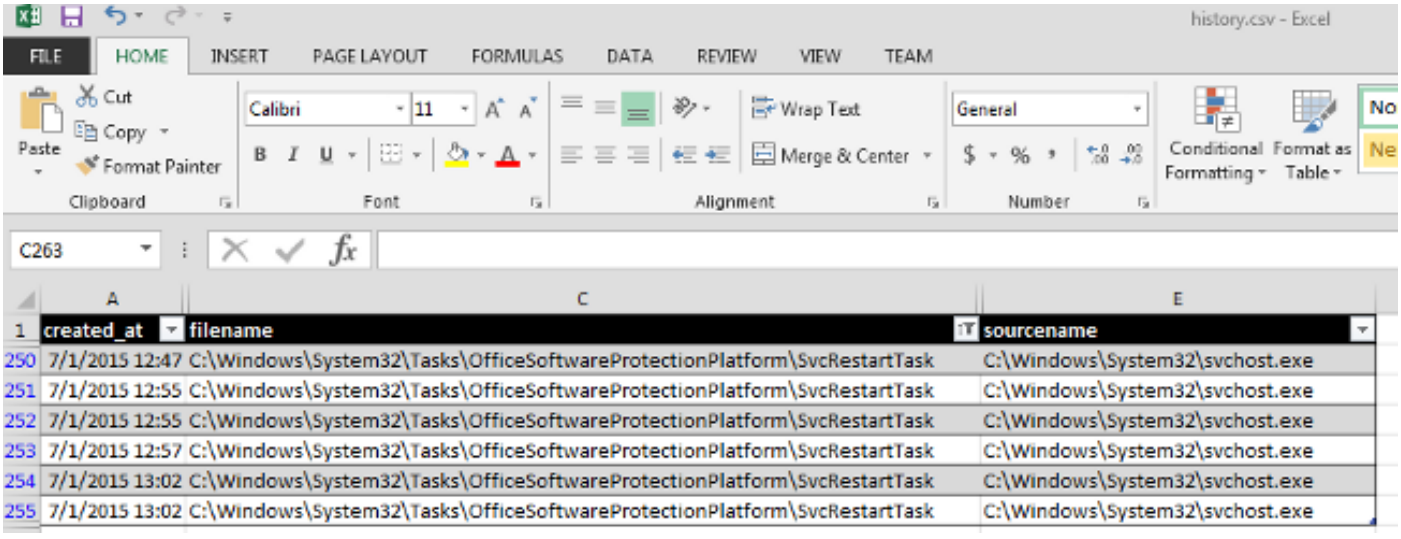
Dépannez

En ce moment il y a quelques options :

- Si vous éprouviez juste le problème de performance, vous pouvez trier la table par le **created_at** qui est l'horodateur balayé et voir les événements les plus récents. Vous pouvez parcourir les détections et le travail vers l'arrière afin de voir ce qui s'est produit.
- Vous pouvez également rechercher ou rechercher les applications qui pourraient avoir été récemment affectées par FireAMP.

Ce que vous voulez rechercher est quelque chose comme le même fichier qui est analysé à plusieurs reprises qui pourrait avoir différentes valeurs de SHA. Vous voulez également regarder le type de fichier afin de voir si c'est comportement prévu.

Dans cet exemple, le fichier a été « bureau » recherché. Les résultats prouvent aux fichiers que FireAMP a balayé qu'eu le mot « bureau » dans le nom du fichier ou le chemin. Vous pouvez également voir le processus de source qui a traité le fichier correspondant.



Dans cet exemple, FireAMP balaye un relié aux données à un service de Microsoft Office. Si

vous voulez exclure ceci, vous pourriez créer une exclusion simple de chemin telle que celle affichée ici :

```
C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask
```

Parfois, les exclusions ne sont pas aussi simples. De temps en temps vous voyez l'activité comme ceci dans d'autres zones comme,

```
C:\Users\Username\Appdata\
```

Par exemple, dites qu'il y a une application de test cette des caches au répertoire d'appdata avec un nom du fichier spécifique. Vous pouvez exclure quelque chose avec le nom donné.

```
C:\Users\Test\Appdata\Temp\cookies
C:\Users\Test\Appdata\Temp\cache
C:\Users\Test\Appdata\Temp\Test\testcachefile20150116.tmp
```

Cet exemple exclut des fichiers de cache pour l'application de temp. Cependant, vous ne voulez pas exclure le répertoire de temp pendant que le cache d'Internet classe comme les téléchargements/images pourraient résider dans ce répertoire. Vous pouvez également rétrécir vers le bas le répertoire au répertoire de test, toutefois l'application pourrait se connecter à l'Internet aussi bien, ou avez d'autres fichiers de cache qui ne nuisent pas à la représentation ou pourraient potentiellement être ouverts pour risquer. Un caractère générique est utilisé pour exclure ceci.

```
C:\Users\Test\Appdata\Temp\Test\testcachefile*.tmp
```

Comme vous voyez, un masque (*) a été utilisé pour expliquer n'importe quoi entre les lettres et le point dans le nom du fichier. Ce masque exclut n'importe quel fichier qui apparie cette expression. C'est un exemple de la façon dont vous pouvez rétrécir vers le bas des exclusions afin d'empêcher trop de risque.

Vous pouvez également utiliser des caractères génériques pour des noms de chemin d'accès complet. Voici un exemple semblable ;

```
C:\Users\Test\Appdata\Temp\Test\20150116\cache\testfilecache083022.tmp
C:\Users\Test\Appdata\Temp\Test\20150117\cache\testfilecache092533.tmp
C:\Users\Test\Appdata\Temp\Test\20150118\cache\testfilecache104431.tmp
```

Exclusions de masque - Les exclusions peuvent être faites sur une expression de masque où le chemin et le nom du fichier peuvent être exprimés. C'est-à-dire, si le nom du fichier est constant, puis lui est le meilleur « contraignent » le masque à un chemin spécifique. Ainsi si AIM.exe existe toujours dans C:\Program classe (x86)*\AIM.EXE regarderait dans n'importe quel sous-répertoire.

Après que vous trouviez vos exclusions désirées de FireAMP, vous pouvez suivre les étapes répertoriées en cet article afin de les implémenter dans votre tableau de bord et réaliser l'essai.

Version 5.0+

Dans la version 5.0+, les taux de mouvements du fichier ne sont plus connectés dans `history.db`. Une nouvelle structure pour les fichiers analysés et les chemins se trouvent dans historyex.db. Un script de `python`, non pris en charge par le centre d'assistance technique Cisco (TAC), est disponible dans la Communauté de CiscoSupport. Sur un environnement Linux, le

script peut convertir le historyex.dbto une `virgule` fichier séparé de la valeur (CSV). Il te permet pour passer en revue les activités pour des exclusions.

Documents connexes

- Configurez et gérez les exclusions dans FireAMP
- Révision des balayages de fichier sur v5.0+
- Support et documentation techniques - Cisco Systems