

Comment collecter les journaux ProcMon pour résoudre les problèmes AMP au démarrage

Contenu

[Introduction](#)

[Procédure:](#)

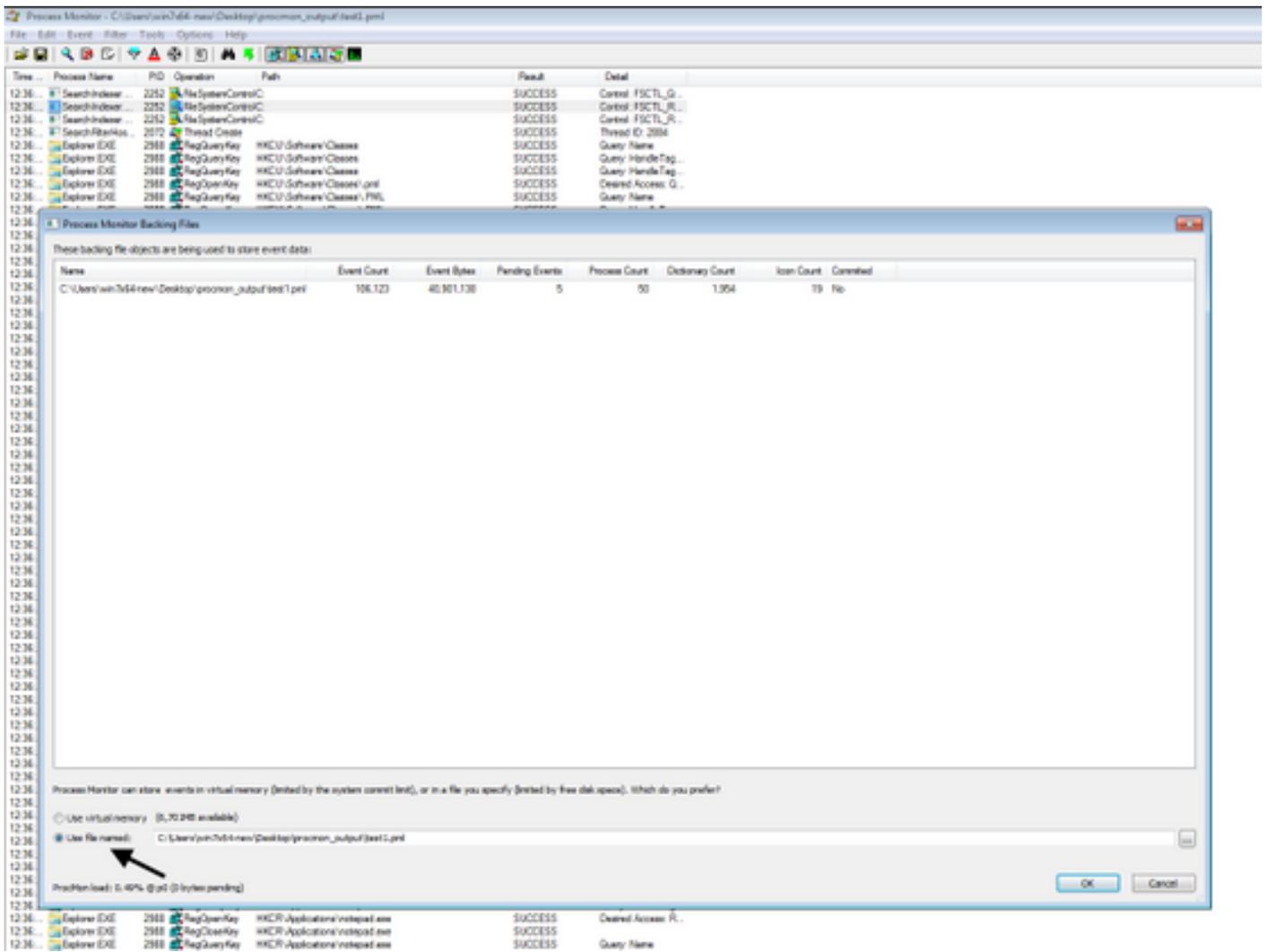
Introduction

En tant qu'administrateur système, vous pouvez obtenir des journaux détaillés à l'aide du Moniteur de processus (procmon.exe) pour déterminer si le connecteur FireAMP est suspendu au cours du processus de démarrage de l'ordinateur. Ces journaux seront également demandés par le TAC de Cisco afin de résoudre de tels problèmes. Process Monitor est un utilitaire gratuit qui peut nous aider ici. Vous pouvez le télécharger gratuitement à l'adresse <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

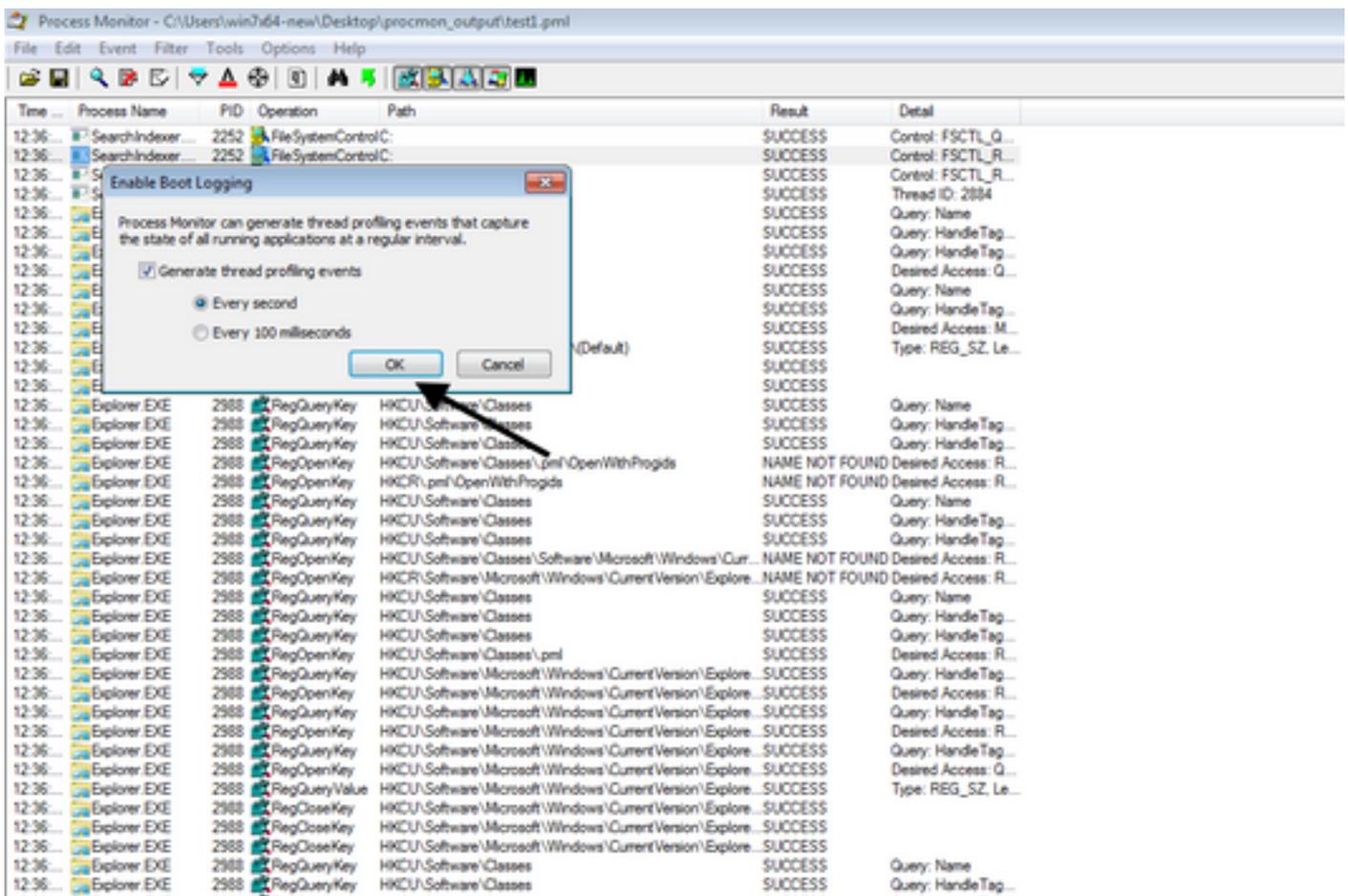
Ce document décrit les étapes de collecte des journaux ProcMon et du vidage de la mémoire si le problème survient lors d'un processus de démarrage du système (ce qui signifie qu'il génère des BSOD au démarrage). Ces journaux sont nécessaires pour capturer les événements système qui se produisent pendant le démarrage.

Procédure:

1. Installer les machines d'essai de manière à ce que le problème puisse être reproduit facilement.
2. Téléchargez et exécutez l'outil ProcMon en tant qu'administrateur. Accédez à **Fichier -> Fichiers de sauvegarde du Moniteur de processus** et sélectionnez un **chemin d'accès**.



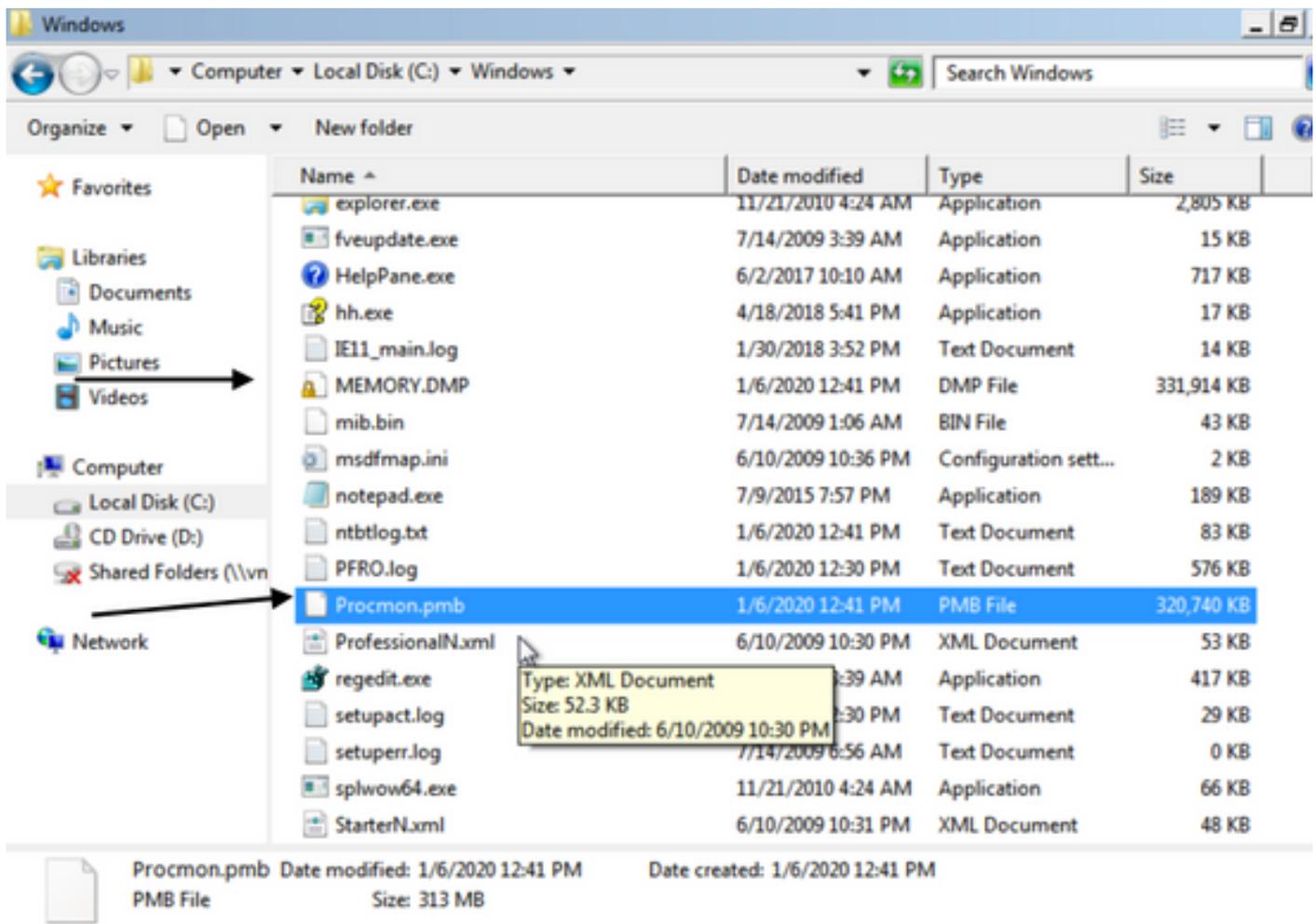
3. Dans l'outil Procmon, accédez à Options -> Activer la journalisation de démarrage.



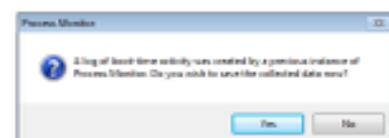
5. Assurez-vous que tous les filtres pertinents sont sélectionnés dans Procmon et que les données sont collectées.

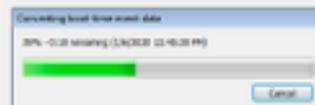
6. Si vous ne parvenez pas à répliquer le plantage, vous pouvez forcer le plantage de Windows à l'aide de l'utilitaire NotMyFault64.exe que vous pouvez obtenir de <https://live.sysinternals.com/files/>

Les instructions relatives à l'exécution de sont disponibles ici : <https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump>



7. Si vous pouvez éventuellement le démarrer en « mode normal » si les fichiers PMB sont générés dans le fichier C:\Windows folder, alors si vous lancez à nouveau ProcMon, vous verrez les journaux suivants. À partir de là, vous pouvez réenregistrer les événements en cliquant sur le bouton Enregistrer.





Time	Process Name	PID	Operation	Path	Result	Detail
12:41...	smss.exe	292	Process Start		SUCCESS	Parent PID: 4, Com...
12:41...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 296
12:41...	smss.exe	292	Load Image	C:\Windows\System32\smss.exe	SUCCESS	Image Base: 0x779...
12:41...	smss.exe	292	Load Image	C:\Windows\System32\ntldr.dll	SUCCESS	Image Base: 0x779...
12:41...	smss.exe	292	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ima...	NAME NOT FOUND	Desired Access: Q...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	REPARSE	Desired Access: R...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	SUCCESS	Desired Access: R...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 74,752, Len...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 1,024, Leng...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 107,008, Le...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448, Le...
12:41...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 300
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset Length: 2,560
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MinNT	REPARSE	Desired I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MinNT	NAME NOT FOUND	Desired I/O Flags: Normal
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	REPARSE	Desired Access: Al...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	SUCCESS	Desired Access: Al...
12:41...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	
12:41...	smss.exe	292	RegSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_SZ, Le...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 0, Name: A...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 1, Name: M...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 2, Name: N...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 3, Name: Pl...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 4, Name: P...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 5, Name: U...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NO MORE ENTRI...	Index: 6, Length: 4...
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...