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 <u>https://docs.microsoft.com/en-us/sysinternals/downloads/procmon</u>

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.

ons Monitor - C/Uh	ser/win7464 new/Deskte	piprocessor_putpttitutLperi						
Popea Name	PD Operation 2012 Million States	he		Anat C	Netal			
Search-Indexer Search-Indexer Search-Indexer Explorer DAL Explorer DAL Explorer DAL Explorer DAL Explorer DAL	2252 Alle System Core 2252 Alle System Core 2252 Alle System Core 2353 Alle System Core 2353 Alle System Ser 2353	HC HC HC HCU/dotware/Dasses HCU/dotware/Dasses HCU/dotware/Dasses/ond HCU/dotware/Dasses/ond HCU/dotware/Dasses/INI		UCCESS Co UCCESS Co UCCESS Co UCCESS Co UCCESS Co UCCESS Co UCCESS Co	vend (FSCTL_R.) vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R. vend FSCTL_R.			
Process Manito	e Becking Film							
These backing file of	bleck are being used to sk	en evert data						
Name		Event Court	Event Bates Panel	ra Evente - Prov	en Court Determer Court	Inst Court Committeel		
C-User/wn/M4	Free ^r (Deektop) process _i ou	tpur (rest 1 peri	40.01.38	5	50 1.954	13 No		
Process Haritar can	n store woards in vitual rea	very (imited by the system constitute	t), or in a file you specify (inited by free data spe	en). Which do you profect			
Cite intalient	cy (0,7026 analola)	Parity in the first of						
	-	- Provide da rescar Orcifica (m. 1994)						
ProcPaniload: 5.49	Pia () () (v (a paraling)						(ox	Canot
Equipme D.E. Equipme D.E. Equipme D.E.	2000 RegCoerKey 2000 RegCoerKey 2000 RegCoerKey	HICR Applications' vehicual and HICR Applications' vehicual and HICR Applications' vehicual and	5	UCCESS De UCCESS DE	network Accesses R			

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

🗳 Po	poess Mori	tor - C:\	Users\wir	7x64-rew\Deskt	opiprocmon_output/test1.pml			
File	Edit Ever	t Rite	r Tools	Options Hel	,			
l ek f		E1	🗢 A	4 Aluman	Ten			
		e os i	× 🖷	- Analysia	- Top			
Tree.	 Process 	Name	PID	Fort		Rend	Detail	
12:36:	. #*Seard	hindeser.	2252	Herbfield	Colum	SUCCESS	Cantrol: FSCTL_Q.	
12:36:	. CE Seard	hindeser.	2252	rigings	Courses and a second se	SUCCESS	Cantrol: FSCTL_R	
12:36:	 #?Seard 	hindeser.	2252	Configure	Symbols	SUCCESS	Cantrol: FSCTL_R	
12.36:	Search	FilterHoo	s 2072			SUCCESS	Thread ID: 2884	
12:36:	- Explor	w EXE	2988	Select Co	umne	SUCCESS	Query: Name	
12.36:		BY EXE	2968	Marco D		SUCCESS	Query: HandleTag	
12:36:	- Capito	1212	2366	rinory u	epon.	SUCCESS	Query: Handle I ag	
1236.		ELD-R	- 211	Profiling	Events	SUCCESS	Desred Access: U.	
12.36	- Depart	W DAD	1			SUCCESS	Duesy Mande Tex	
12.36	- Entre	- DE	2568	Enable Bo	et Legging	0000000	Centred Access M	
12.36	Dete	N EXE	2568			SUCCESS	Ture BEG S7 In	
12.36	Entre	DE	2568	Show Re	ofved Network Addresses Cb5+N	SUCCESS	When constrained and the	
12.36	Ecio	ev EXE	2568	Hex File 0	Wisets and Lengths	SUCCESS		
12:36:	Epilor	WENE	2988	Hen Dance	on and Thread IDs	SUCCESS	Query: Name	
12.36:	- Epilor	er EXE	2968	THEFTER		SUCCESS	Query: HandleTag	
12:36:	Epiar	# DE	2988	RegQueryKey	HRCU/Software/Classes	SUCCESS	Query: Handle Tag	
12.36:	. Epior	er EXE	2968	RegOpenitey	HKCU\Software\Classes\.pnf\Open\IIIthProgids	NAME NOT FOUND	Desired Access: R.,	
12:36:	- 🕞 Esplor	# DE	2988	RegOpenKey	HKCR\pm\OpenWithProgide	NAME NOT FOUND	Desired Access: R.	
12.36:	- Epilor	ex EXE	2968	RegQueryKey	HKCU/.Software/Classes	SUCCESS	Query: Name	
12.36	- Epsior	# DE	2968	RegGueryKey	HKCU/Software/Classes	SUCCESS	Query: Handle Tag	
12.36.	- Defor	ALEXE	2965	RegQueyKey	HKCU/Software/Classes	SUCCESS	Query: HandleTag	
12.36.	- Deter	WEXE SVE	2965	RegUpentay	HRLD Software Casses Software Metsoft We	dewerbure. NAME NOT FOUND	Dealed Access R.	
12.36.	- Delo	EXENC.	2966	Registeritey	HKLH Software Gloosoft Unnobed Current Vers	an apploite. Make Not House	Cesred Access: PL.	
12.36	- Entry	W EVE	2300	Baglussynay	HIT IS SHARE CARE	SILCESS	Duesy Hande Tes	
12.96	- Enlo	IN EVE	2300	Bendumiter	Hill 10 Software Classes	SUCCESS	Query Hande Tag	
12.35	Facility	N FXF	2988	BegOpenKey	HKCID Software/Classes/conf	SUCCESS	Desired Access: B	
12:36	Eelo	# DE	2988	ReqQuertier	HXCU/Software/Microsoft/Windows/Current/Anti	an\Explore, SUCCESS	Query: Handle Tag.	
12:35:	Explor	er EXE	2988	RegOpenKey	HKCU/Software/Microsoft/Windows/Current/Versid	on/Explore_SUCCESS	Desired Access: R	
12:36	Epplor	# DE	2988	RegQueryKey	HKCU/Software/Microsoft/Windows/Qurrent/Versit	on Explore . SUCCESS	Query: Handle Tag	
12:35:	- Epplor	R EXE	2968	RegOpenKey	HKCU/Software/Microsoft/Windows/Current/Jersi	on Eplore SUCCESS	Desired Access: R	
12:36	- Explor	w DE	2968	RegGueryKey	HKCU/Software/Microsoft/Windows/Qurrent/Verst	an/Explore . SUCCESS	Query: Handle Tag	
12.36:	. Califictor	R DE	2968	RegOpenKey	HKCU-Software/Microsoft/Windows/Current/Jersi	on Explore SUCCESS	Desired Access: Q	
12.36:	- 🕞 Deke	w DE	2968	RegQueyValu	 HRCU/Software/Microsoft/Windows/Current/Versit 	on/Explone. SUCCESS	Type: REQ_SZ, Le	
12.36:	. Defor	REAL BALL	2968	RegCloseKey	HKCU-Software Microsoft Windows Current Versi	on Explore _SUCCESS		
12.36:	- Depicy	W EXE	2565	fleg.costay	HKE, U-Software (Microsoft ()Weddwar (Durent Veral	an Upplem . SUCCESS		
12.36.	D(0)	BUEXE	2966	Heg Josefley	HKLU-Software-Molosoft-Immobiles-Current version	on Explore . SUCCESS	O No.	
12:30:	- Copo	WEAE	2300	Progradery way	HALLU-SOTVARE CARDING	SUCCESS	Query: name	
12.36	- Endo	I EVE	2900	Barlauriter	HRC1D Schoore/Classes	SUCCESS	Query Hande Tag	
12.35	Entity	IN FAF	2968	Rectoroter	HRC1D.Software/Classes/Applications/applicational ex	NAME NOT FOUND	Desired Access: R	
12.36	Ender	# DE	2988	RegOmentar	HKCR\Amicators\notenad are	SUCCESS	Destred Access: R.	
12.35	Delo	NEXE	2968	RegCloseKey	HKCR' Applications' notepad eve	SUCCESS		
12.36	- Epsion	W DE	2968	RegQueryKey	HKCU/Software/Cleaner	SUCCESS	Query: Name	
12.36:	- Dekor	N DE	2968	RegQueryKey	HIKCU/.Software/Classes	SUCCESS	Query: HandleTag	
12:36:	- Calipion	w DE	2988	RegionryKey	HKCU/Software/Classes	SUCCESS	Query HandleTag	
12.36:	- Califiction	R DE	2968	RegOpenKey	HKCU/Software/Classes/Applications/instepad.ex	NAME NOT FOUND	Desired Access: R	
12:36:	- 🙀 Espior	w DE	2568	RegOpenKey	HKCR' Applications \notepad ass	SUCCESS	Dealed Access: R.	
12.36:	- Bplor	ex EXE	2968	RegQueryKey	HKCR'/Applications'/notepad.exe	SUCCESS	Query: Name	
12:36:	- topio	W EXE	2368	fiegGuery/fay	MALM Applications Indeped and	SUCCESS	Query: Handle Tag	
		10.00	0000	AND DOUGHT PORT AND	and the second state of the second second second second as	ALL CALLS AND AL	in second seconds. It	

4. Sélectionnez Générer des événements de profilage des menaces et Toutes les secondes.

🎒 Proc	ess Monitor - C/	Users\win7164-new\Desktop	p.procmon_output\test1.pmi	1			
File Ed	fit Event Filte	r Tools Options Help					
- e2 III		👄 A 🚓 🖻 🗛 🗖					
		A 🖶 Ø. 🗇 🖬 🧃					
Time	Process Name	PID Operation	Path		Result	Detail	
12:36:	Searchindexer		AC:		SUCCESS	Control: FSCTL_Q_	
12:36	Searchindexer		XC:		SUCCESS	Control: FSCTL_R	
12:36	S Easthin Day	d Longing)	SUCCESS	Control: FSCTL_R	
12:36	ES Chable bot	n cogging			SUCCESS	Thread ID: 2884	
12:36	Barran M	where can paper she through our	Allow as works that can be as		SUCCESS	Query: Name	
12:36	E the state	of all running applications at a r	equiar interval.		SUCCESS	Query: HandleTag	
12:36	20		cyrre mer ren		SUCCESS	Query: HandleTag	
12:36	🔚 🛛 🖓 Ger	erate thread profiling events			SUCCESS	Desired Access: Q	
12:36	in E	a former and			SUCCESS	Query: Name	
12:36:	1	Every second			SUCCESS	Query: HandleTag	
12:36	1	Every 100 milliseconds			SUCCESS	Desired Access: M	
12:36	E			(Default)	SUCCESS	Type: REG_SZ, Le	
12:36:	a 6		OK Cancel		SUCCESS		
12:36	H			1	SUCCESS		
12:36	Explorer.EXE	2988 RegQueryKey	HKCU/Salinase/Casses		SUCCESS	Query: Name	
12:36	Diplorer EXE	2988 KegGueryKey	HKCU Software leases		SUCCESS	Query: Handle Tag	
12:36	Explorer EXE	2966 RegQueryKey	HICU Software Classe		SUCCESS	Query: Handle Tag	
12.36	Explorer.EXE	2966 RegOpenkey	HRLU/Software/Classes/pm/	OpenWithPlogids	NAME NOT FOUND	Desired Access: R	
12.36	Diblover, EXE	2505 Pregupenkey	HNUN pri Openvien Progida		NAME NOT FOUND	Desred Access: H	
12.35	Explorer EXE	2500 ReguleryNey	HALU Software Classes		SUCCESS	Query: Name	
12.05	Explorer EXE	2500 Pegaleytey	HNLU GOTWARE Classes		0000633	Query, Hande Tag	
12.30	Explorer EXE	2900 Performance	UNCLE Calculate Casses	and the second of the second for second	NUME NOT FOUND	Query: Hande Lag	
12-36	Evolowy EVE	2500 PagOpenkey	HNCO (Software Classes (Software) Microsoft Mi	Hare (Hecrosoft (Windows (Curr	NAME NOT FOUND	Desired Access: R	
12-36	Evolver EXE	2988 BanCrepuperney	HKC10 Software Origination of the	considerer verson copore.	SUCCESS	Ouer Name	
12.36	Funitower EXE	2988 RenDuevier	HKC11/Software/Classes		SUCCESS	Query HandeTan	
12:36	Funitowr EXE	2958 BecQueryKey	HKC10 Software/Classes		SUCCESS	Query Hande Tag	
12-36	Epolow EXE	2988 RecOpenKey	HKCU/Software/Classes/ onl		SUCCESS	Desired Access: R	
12:36	Evolover EXE	2988 RenOvervilley	HKC10.Software\Microsoft\We	down\CurrentVersion\Explore	SUCCESS	Query HardeTan	
12:36	Explorer EXE	2988 RecOpenKey	HKCU/Software/Mcrosoft/W/	ndows\CurrentVersion\Explore	SUCCESS	Desired Access: R	
12:36	Explorer EXE	2988 ReqQueryKey	HKCU/Software/Microsoft/Wir	ndows\CurrentVersion\Explore	SUCCESS	Query: Hande Tag	
12:36	Explorer EXE	2988 RegOpenKey	HKCU/Software/Microsoft/Wir	ndows\CurrentVersion\Explore	SUCCESS	Desired Access: R	
12:36	Explorer EXE	2988 ReqQueryKey	HKCU\Software\Microsoft\Win	ndows\CurrentVersion\Explore	SUCCESS	Query: Hande Tag	
12:36	Explorer EXE	2988 RegOpenKey	HKCU/Software/Microsoft/Win	ndows\CurrentVersion\Explore	SUCCESS	Desired Access: Q	
12:36	Explorer EXE	2988 RegQueryValue	HKCU\Software\Mcrosoft\Win	dows/Current/Version/Explore	SUCCESS	Type: REG_SZ, Le	
12:36	Eplorer EXE	2988 RegCloseKey	HKCU/Software/Mcrosoft/Wir	ndows\CurrentVersion\Explore.	SUCCESS		
12:36	Biplover EXE	2988 RegCoseKey	HKCU/Software/Mcrosoft/Wir	ndows\CurrentVersion\Explore.	SUCCESS		
12:36	Biplover EXE	2988 RegCloseKey	HKCU\Software\Mcrosoft\We	ndows/Current/Version/Explore.	SUCCESS		
12:36:	Biplover.EXE	2988 KRegQueryKey	HKCU/.Software/Classes		SUCCESS	Query: Name	
12:36	Biplover EXE	2988 KegQueryKey	HKCU\Software\Classes		SUCCESS	Query: Handle Tag	

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 <u>https://live.sysinternals.com/files/</u>

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

Provan Westur - Cittle	and the set of the set	Paraceter, Julipul Acid, prel			
the dat dura the	North College Pade				
2 B 4 9 5 1	4 0 X A				
Ins., Anna tara	ND General	Fat	Sea.4	Ganal	
Cit. Eldines	THE BARNES	Company Residence (APV 111) All services	9.00200	Other Distances	
23. 8 4.00	100 Cashings	C Proper RenCennut P (1) 1 41 and 10	9.00200	Ware/eater Te.	
23 EM.m	1707 Automation	C Prepar RenCennal P 121 All and by	8,0000-040001	Department 161	
23. Exter	170 Charles Tes	18,34 Selecter Human's Western M*Contentioners for	NUMBER	COMMENTATION R.	
23. 14.00	The second section	18,34 Selver Hunsell Westers M Carentenory Se	And other stores	COMMENCED NO.	
23. 19.00	The Course of the	NUM Selver Hunself Westers If Cyterchenory Se	New York Policy	COMPACTAGE N.	
2.2	20 Printer Springs	Company Renders and Company and Street Street	100.00	Accession (Acc-	
Sales and and	The second second	Company New York and the Party of the	100.000	And in case of	
100	in the second	A charged from the country of the state of the	10000	When when he	
Con Contract	The last windows	Constant Rest and shift 11 th 40 eres but	B. PTER LINETYL	Castler Tree 14	
12 M History	110 Charlester	18. M School House House 17 Catentineers In	NAME AND POST	COMPACT Access 19	
23. 10.00	The Constrainty	TRUM Schware Human? Ministree 167 Current Inson Tru	NAME AND POST OF	COMPACT ACCESS 19.	
23. Exten	The second second	18, M Schwarz Human? Ministree 10" Current among Six	NAME OF TAXABLE	COMMENCED N.	
23. 84.00	170 Bellandarded	Propert Rendered AP 11 / AL events	10.00	Accession (S.	
2 H B	The second second	Wegen Nercess AMP 11 Tracine 1g	10.00	Accession (F)	
22.20.00	N. BURNER	Pages Nervec at 15 have be	141.50	the post of	
20.00	and the second second	Company New York and the Party of the	A PROPERTY OF A PROPERTY OF	Contraction 14	
Con Contract	I'm Branketter	the lot between the party billing to be a party party for	sand out they	Constant Array 6	
COLUMN TWO IS NOT	1 IN CONTRACTOR	TR.M. Schwarz (Retract: Westwork) Constrainers To	NAME OF TAXABLE	Column Array 6	
Cit. Extras	100 Paginetter	15.14 Selvers Hunsell Westwork? Currentinger: To	NAME OF TAXABLE	COMPACT Access 10	
Cit. Extrac	100 Minandramed	Chapter Ren Carol and Child All and the	9.00 895	Accessive in	
23. DAte:	100 Minandrated	Companition (acculate (1)) that are by	140.005	Acception 18	
33. EX.46	THE BANKING	Proper NerCent ART 11141 av 19	10.00	The 2110120	
22. 20.00	and the second	Proper Nercecrule* Settle	1.41 Pt-1	DOM: NA.P.	
20-00-00	and a second	Copper Nervacy and Dates in	100.000	Column Panel 1.	Independent Conference (Upper Construction)
20- 10- Mar	in another	Company Services of States & Long	and sold the	Contract Second Second	Statement (Statement
20.000	and the second sec	Company Real and All Street B	1.00 000	the Allow	Conference of Information Informatio Information Information Information Information Infor
1 M 1 M 1	The second se	Company Real And All Street & and	sand only store	Country brown it.	
Co. Common	110 Bulanchestert	Company Revolution and Instance do	9.40 (99)	Accelering H.	Exception of the Control of Co
Cold. B Marcan	IN BURNING THE	Company Revolution and Instance do	0.00000	Office 1-075-741-8	The same is a proper of the same size of the same
COL. Kitchen	110 Bulanintenate	E Proper RevCentuil#1018 strawing	0.0088	internal matter free.	
U.M. Kirken	110 Advantitions	E Proper RenGest AMP (1) 5 House by	Burner, Support,	Center Ine 14	Enverteine of Conditional weather that mean decising
Vill. Exten	100 Performance	HUM Schwarz (Actual) Ministree M. Current Association	NAME AND POST	COunt Arous P.	REARCHER LEASE AT 1110 Proceeding lines
VOL. EXC.	The Page Section	HEAL Officer (Read) Medice (Contribution) In	NUME HOT POINT	COMPACTOR P.	81-86-282# 13-55 P# (318) generation and gen.
COL. EXC.	The second	HEAL OFFICER REPORT NUMBER OF CAREFURNEY IN	NAME OF TAXABLE	COMPARIANCE P.	21 (20-22) 10 (17 12 (20 12)))))))))))))))))))))))))))))))))))
20.00	IN BOAD APORT	Constant New Card and Constant and the	TALL POL	Accession from 18	ALCONE 1215 IN THE REPORT OF A DECEMBER OF A
10.00	The second second	A respect that they are the set of a set of	1000	Other Designation	[[][h/h]][h/h].[h] h/m]
20.000	The second second	Colorest Resident and Table 1 and the	0.000	internation in	1 Diprist 19,870,046,761 April 1980
10.000	100 Million Million	Concern Rev Carry 489-11 Publishes Inc.	A PHONE DURING	Castor Ing. 14	Excellence of a state of the
10. Com	100 Charlester	viel of Antonio Oceanit's Strategy of Complement In-	want out their	Classed Array R.	
U.M. Without	110 Paul service	HEAV School (Research Ventres 10 Carentinger) In	water right rights	Classed Arrest R.	and any approximately and an approximately and a standard and
U.S. Kirken	110 Paginetter	HKM (Mean Hennel Western W Constitution) In	And HOT YOUR	Classed Arrest R.	
U.M. Kirken	100 Blanchardert	2 Propert RenCentral #1018 at sea by	0.00000	Acute In 2.	 Protocorrespondences and an analytic process of the p
10. Dr. 10. au	IN Alasharian	C Prepar NerCash 48* 715 at yearing	P.40.001	Acateria 3.	
10. Distant	IN ADDA	1 Proper NerCent diff (115 at use by	P.41.891	the Britch	
10.0	The Date of the local date of	 Property Net Carry MP 111 Bit and base base 	ALC: NOT THE OWNER.	standard in	1
20.00	The Standard	AND ADDRESS OF ADDRESS OF ADDRESS	and other	Count I want it	1
10.00	190 Charlester	out to be an interest interest in the second second interest inter	hand out of the	Contract Income 18	1
12.00	110 Paulantin	HEAD Information and Manhouse In Company on the	and out they	Control Array II	1
U.M. Watan	100 Allen Arriet	C Propert Res Carol al #1010 all and ba	P.ACTER	Accession (in case)	1
1218 . Whites	100 Manharitett	C Proper RenCennatif* (218 at use by	BACCENT	Accelerity 20	1
1230. El-Mann	100 Balancia	C Proper Ner/CechildP (218 at see by	PLOCENT	Obs 2008.01	1
10. Exten	W Dathant	C Proper RenCennut#1018 at use by	PLOCET	Ward agen In.	1
12. 14.00	IN Caryliniums	C Physic NerCash (MP-11) 41 (m) ha	BUMER DISTANT	CoderTra 14	1
10.00	The Pay Service	NUM Orleany Royal Western IT Commission To	And April Poly	Contract Access 10	1
10.0	The second second	in the second dense of Constants in	And April Pope	Contract Access 10	1
2 C	THE REPORTS	Probaness Rest Rest and Rest Rest Rest Rest Rest	B.CO.T.	Second Sec. 7	1
12.00	100 Allendering	C Wagon Res Card 400121 Bull on In-	0.00000	Sector In 12	
1218 B Marrie	100 Andres	C Proper Rev Central #1011 All year ba	9.0000	Office (20.000 Not	
U.M. Bottobler	153 Country	C /August Calor / Maget 10Roate Tools Included	Net ALT YORK	Control Access 10.	
C.M. Evergence and	200 Challenter	HR_M	PLOCETT	Core Andrina	
CH. Evennese	200 Challenter	NUMBER AND ADDRESS OF ADDRES	PU00811	Change Access 10.	
CH. Compressee	200 Challenge	HEM SOFTWARE ASSAULT ASSAULT	PLOCET	Care NA Same	
C.S. Compression	CRI Challendert	HEALD COTTACHE ASSAULT ASSAULT	BOWER SOO DK		
C.S. Compression	CT Children and	NUMBER OF ADDRESS AND ADDRESS	PUOLEYN	Tax PELIC In.	
C.S. Compression	City of the Company	NUMBER OF STREET ASSOCIATES	P.0.01		
A DECEMBER OF THE OWNER OWNER OF THE OWNER OWNE	THE PARTY AND INCOME.	THE MAN PROPERTY AND ADDRESS OF ADDRESS	100.00	Control Agender Test	
Contraction of the local division of the loc	THE PROPERTY AND	IN MACHINE AND ADDRESS AND	B. C. THE	Date of Lots	
12 M Company on	THE PROPERTY.	THE MODEL WATCH ADDRESS AND ADDRES	BUTTER TOURS		
CH. Compression	CHI Charles	THE M STATE WATCH ADDRESS ADDRE	9.0720	New FIEL SP 14	
CH. Durgroups	(10 Challes	HEALING THAT AND ADDIVING ME	9.00201		
		A DE REPORTE A DE RECEIRE DE RECE	41. M. 14		
COLUMN TO A REAL PROPERTY.	1440 F	Contraction of the second second second second	a water the		

7. Crash de la machine.

8. Démarrez l'ordinateur en mode sans échec et collectez manuellement **Procmon.pmb** et **MEMORY.DMP**, les deux fichiers se trouvent dans C:\Windows folder. Ces fichiers doivent être partagés avec le TAC Cisco.

New folder		Date modified 11/21/2010 4:24 AM 7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM	Type Application Application Application Application Text Document DMP File	Size 2,805 KB 2,805 KB 15 KB 717 KB 17 KB 17 KB 14 KB 331,914 KB	
me ^ explorer.exe fveupdate.exe HelpPane.exe hh.exe IE11_main.log MEMORY.DMP mib.bin		Date modified 11/21/2010 4:24 AM 7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM	Type Application Application Application Application Text Document DMP File	Size 2,805 KB 15 KB 717 KB 17 KB 14 KB 331,914 KB	
explorer.exe fveupdate.exe HelpPane.exe hh.exe IE11_main.log MEMORY.DMP mib.bin		11/21/2010 4:24 AM 7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM	Application Application Application Application Text Document DMP File	2,805 KB 15 KB 717 KB 17 KB 14 KB 331,914 KB	
fveupdate.exe HelpPane.exe hh.exe IE11_main.log MEMORY.DMP mib.bin		7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM	Application Application Application Text Document DMP File	15 KB 717 KB 17 KB 14 KB 331,914 KB	
HelpPane.exe hh.exe IE11_main.log MEMORY.DMP mib.bin		6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM	Application Application Text Document DMP File	717 KB 17 KB 14 KB 331,914 KB	
hh.exe] IE11_main.log] MEMORY.DMP] mib.bin		4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/6/2020 12:41 PM	Application Text Document DMP File	17 KB 14 KB 331,914 KB	
] IE11_main.log] MEMORY.DMP] mib.bin		1/30/2018 3:52 PM 1/6/2020 12:41 PM	Text Document DMP File	14 KB 331,914 KB	
] MEMORY.DMP] mib.bin		1/6/2020 12:41 PM	DMP File	331,914 KB	
mib.bin					
		7/14/2009 1:06 AM	BIN File	43 KB	
msdfmap.ini		6/10/2009 10:36 PM	Configuration sett	2 KB	
notepad.exe		7/9/2015 7:57 PM	Application	189 KB	
ntbtlog.txt		1/6/2020 12:41 PM	Text Document	83 KB	
PFRO.log		1/6/2020 12:30 PM	Text Document	576 KB	
Procmon.pmb		1/6/2020 12:41 PM	PMB File	320,740 KB	
ProfessionalN.xml		6/10/2009 10:30 PM	XML Document	53 KB	
regedit.exe	Type: XML Document	:39 AM	Application	417 KB	
setupact.log	Size: 52.3 KB	30 PM	Text Document	29 KB	
setuperr.log	Date modified: 0/10/20	7/14/2009 6:56 AM	Text Document	0 KB	
splwow64.exe		11/21/2010 4:24 AM	Application	66 KB	
📑 StarterN.xml		6/10/2009 10:31 PM	XML Document	48 KB	
	notepad.exe ntbtlog.bt PFRO.log ProfessionalN.xml regedit.exe setupact.log setuperr.log splwow64.exe StarterN.xml modified: 1/6/2020 1 Size: 313 MB	notepad.exe ntbtlog.txt PFRO.log Procemon.pmb ProfessionalN.xml regedit.exe setupact.log setupact.log setuperr.log splwow64.exe StarterN.xml modified: 1/6/2020 12:41 PM Date creation Size: 313 MB	notepad.exe 7/9/2015 7:57 PM ntbtlog.txt 1/6/2020 12:41 PM PFRO.log 1/6/2020 12:30 PM Procmon.pmb 1/6/2020 12:30 PM ProfessionalN.xml 6/10/2009 10:30 PM regedit.exe 1/9/2015 7:57 PM setupact.log 1/6/2020 12:41 PM setupact.log 1/6/2020 10:30 PM setuperr.log 7/14/2009 10:30 PM splwow64.exe 11/21/2010 4:24 AM StarterN.xml 6/10/2009 10:31 PM modified: 1/6/2020 12:41 PM Date created: 1/6/2020 12:41 PI Size: 313 MB 5/10/2009 10:21 2:41 PI	notepad.exe 7/9/2015 7:57 PM Application ntbtlog.bt 1/6/2020 12:41 PM Text Document PFRO.log 1/6/2020 12:30 PM Text Document Procmon.pmb 1/6/2020 12:30 PM Text Document ProfessionalN.xml 6/10/2009 10:30 PM XML Document regedit.exe 1/9/2015 7:57 PM Application setupact.log 1/6/2020 12:41 PM PMB File Setupact.log 7/14/2009 10:30 PM XML Document setuperr.log 7/14/2009 0:56 AM Text Document splwow64.exe 11/21/2010 4:24 AM Application StarterN.xml 6/10/2009 10:31 PM XML Document modified: 1/6/2020 12:41 PM Date created: 1/6/2020 12:41 PM XML Document size: 313 MB Size: 313 MB Date created: 1/6/2020 12:41 PM Size: 313 MB	

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.

Paces: Monitor - Syard	energy www.cycomercult.	DMA			
File Edit Event Filter	Tools Options Help				
i 📽 📓 💐 🕸 🗔 🔻	4 4 1	(d) (d) (d) (d)			
Time Process Name	FID Operation	Tab	final	Detel	

Franka Monitor	Ξ
2 Along of least-time activity same constituting a previous instance of Process Mantins. Do you with its same time collected data new?	
Tm. He	

_
Genet

🔰 Process Monitor - Sysi	internals: www.sysinternals.	com		
File Edit Event Filter	Tools Options Help			
📽 🖬 🔌 🕸 🖾 🛛	🗢 🛆 😳 🖻 🛤 🖣			
Time Process Name	PID Operation	Path	Result	Detail
12:41: Fames exe	292 🧟 Process Start		SUCCESS	Parent PID: 4, Com
2.41: Famas exe	292 ar Thread Create		SUCCESS	Thread ID: 295
2.41: Tames exe	292 E Load Image	C:\Windows\System32\amss.exe	SUCCESS	Image Base: 0x479
2.41: Pamas exe	292 ar Load Image	C:\Windows\System32vitdl.dll	SUCCESS	Image Base: 0x779
241: Pamas exe	292 RegOpenKey	HKLM\Software\Morosoft\Windows NT\CurrentVersion\Ima	NAME NOT FOUN	D Desired Access: Q
41: Fames exe	292 RepOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
2.41: Pamas exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41 smss.exe	292 KRegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1.024
41: E smss.exe	292 KRepQueryValue	HKLM'\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1,024
41 smss.exe	292 RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	
41: Pamas exe	292 Koreate File	C://Windows	SUCCESS	Desired Access: E
41 Smss.exe	292 ReadFile	C:\\Windows\System32\amas.exe	SUCCESS	Offset: 74,752, Len
41: Pamas exe	292 🛃 ReadFile	C:\Windows\System32\amss.exe	SUCCESS	Offset: 1,024, Long
41 Smss.exe	292 ReadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offset: 107,008, Le
41: Resmos.exe	292 MeadFie	C:\Windows\System32\amas.exe	SUCCESS	Offset: 104,448, Le
41 smss.exe	292 See Thread Create		SUCCESS	Thread ID: 300
41: Romas exe	292 ReadFile	C:\Windows\System32\amas.exe	SUCCESS	Offse Offset: 104,448
41 smss.exe	292 🛃 ReadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offse Length: 2,560
41: Ersmas exe	292 KegOpenKey	HKLM'\System\CurrentControlSet\Control\MinINT	REPARSE	Desi L/O Rags: Non-cached, Paging L/O, Synchronous Paging L/O
41: Famos exe	292 RegOpenKey	HKLM\System\CurrentControlSet\Control\MnINT	NAME NOT FOUN	D Desi Priority: Normal
41: Pamas exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\.	REPARSE	Desired Access: Al
41: I smss.exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\.	SUCCESS	Desired Access: Al
41: Pamas exe	292 KRegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	0
41: Pamos exe	292 RepSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_SZ, Le
41: Pamas exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
41: I amos exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41: Famas exe	292 KRepQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_DWO
41: Internet exe	292 RegQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_MULT
41: Stres exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_MULT
41: Elamos exe	292 RegQueryValue	HKLM'System'CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_MULT
41 Stres exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 4,094
41: Elamos exe	292 RegQueryValue	HKLM'System/CurrentControlSet'Control'SESSION MANA	SUCCESS	Type: REG_DWO
41: Smiss.exe	292 RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	D Length: 4,094
41: emes.exe	232 RegQueryValue	HKLM System/CurrentControlSet/Control/SESSION MANA	NAME NOT FOUN	D Length: 4,094
41 Smiss.exe	232 ReguleryValue	HKLM/System/CurrentControlSet/Control/SESSION MANA.	NAME NOT FOUN	D Length: 4,094
41: erismes.exe	232 ReguleryValue	HKLM System CurrentControlSet Control SESSION MANA.	SUCCESS	Type: NEG_MULT
41. Smiss.exe	252 RegOpenkey	HKLM System CurrentControlSet Control SESSION MANA.	SUCCESS	Desred Access: M
41:	202 Preguleyvaue	HKLM System Current Control SESSION MANA.	SUCCESS	Type: NEG_MULT
41 amos exe	252 Reguleyvaue	HKLM (System CurrentControlSet Control (SESSION MANA	NAME NOT FOUN	U Length: 4,094
41 Promosieve	202 Preguleyvaue	HKLM System Current on the Control SESSION MANA.	50006555	Type: HEG_HOLT
41 Smos.exe	252 Repuese value	HKLM (System CurrentControlSet Control (SESSION MANA	SUCCESS	
41	202 Preguoseney	HALM System Current on book Control SESSION MANA.	2000622	Desired Assess M
41	202 Reguperkey	INCM Gystem Current Control Set Control SESSION MANA.	CUCCESS	Index O Name A
A1 Brance and	202 PasEn militar	LVI M Custon Custon Custon Caston Control COCCOM MANA	CINCESS	Index 5 Name M
41	292 RecEnceValue	HALM CYREM LUTERLOTED SELLOTED SELLOTED SESSION MANA	SUCCESS	Index 3 Name M
A1 Brends and	292 PasEn militar	LVI M Crater Crater Control Set Control (CCCCCA) MANA	CLUCEDO	Index 3 Name Of
di amos exe	202 Regenunivaue	HALM Gyster Lutter Lore Dist Lore Disc 53504 MANA.	CUCCESS	Index 4 Name 8
A1 Press eve	292 ResEnceValue	LIVE ME System Control Set Control SESSION MANA	0000633	Index 5 Name 11
41	202 Progenum value	HALM Gyster LUTERLOTED SR. LOTED SESSION MANA.	NO MODE ENTER	Index: 6 Lanoth: 4
A1 Brance and	292 Regenuit value	HALM System Control Set Control SESSION MANA.	SUCCESS	
A1: Dames and	292 ResOurceMay	HIGH Grand Control Control Control CERCICAL MARKA	CUCCESS	Daried Access M
supercise	eve meguperney	INTER OVER COLORDON FORD SE22YON WARK.	3000633	VEHEV /VVEH. P