Cómo recopilar registros de ProcMon para resolver problemas de AMP al inicio

Contenido

Introducción Procedimiento:

Introducción

Como administrador del sistema, es posible que desee obtener registros detallados mediante el Monitor de procesos (procmon.exe) para determinar si el conector de FireAMP se bloquea durante el proceso de inicio del equipo. El TAC de Cisco también solicitará estos registros para resolver tales problemas. Process Monitor es una utilidad gratuita que puede ayudarnos aquí. Esto se puede descargar libremente desde <u>https://docs.microsoft.com/en-us/sysinternals/downloads/procmon</u>

Este documento describe los pasos sobre cómo recopilar registros ProcMon y vaciado de memoria si el problema ocurre durante un proceso de arranque del sistema (lo que significa que está generando BSODs en el arranque). Estos registros son necesarios para capturar los eventos del sistema que tienen lugar durante el arranque.

Procedimiento:

1. Configure las máquinas de ensayo de tal manera que el problema pueda reproducirse fácilmente.

2. Descargue y ejecute la herramienta ProcMon como administrador. Vaya a File -> Process Monitor Backing Files y seleccione una Path.

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/wei/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 constit in	t), or in a file you specify (inited by free data spe	en). Which do you profect			
Cite intalient	cy (0,7026 analola)	Peritorian a to front of						
	-	- Propertie de restrace (Tradiera Jung 2 dans						
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. En Procmon Tool, vaya a **Options -> Enable Boot Logging**.

💐 Pn	cons Monite	or - C:\L	laan),win	7x64-rww\Deskto	piprocmon_output/test1.pml			
File	Edit Event	Filter	Tools	Options Help				
all all a		P.L.						
	9	DA	Y 🗛 🤉	Aways on	Tep			
Tree .	Process N	lare .	PID	Fort		Rend	Detail	
12:36:	# Search	hdeer	2252	Mahfaha	Calum .	SUCCESS	Cantrol: FSCTL_Q.	
12:36:	. (It Search)	ndeser .	. 2252	riginga	CONTR	SUCCESS	Cantrol: FSCTL_R	
12:36:	#7Search1	hdeer	2252	Configure	Symbols	SUCCESS	Cantrol: FSCTL_R.	
12.36:	Searchi	FilterHos.	. 2072	conget		SUCCESS	Thread ID: 2884	
12:36:	. 🐊 Explore	DE	2988	Select Colu	anna	SUCCESS	Query: Name	
12:36:	2000	EVE	2988	11.0		SUCCESS	Query: HandleTag	
12:36:	- Depose	EDE:	2988	Platory De	pth	SUCCESS	Query: Handle Tag	
12.36:	- Eplore	(Date)	2968	Profiling E	unta	SUCCESS	Desired Access: Q.	
12.36.	- Lickow	EXE	1	-		SULLESS	Query: Name	
12.06.	- DOOD	EVE.	2998	Enable Box	t Logging	30,0633	Guery: Handle rag	
12.36	- Departer	243	2300			SUCCESS	Date DEC 57 14	
12.36	Enime	EVE.	2900	V Show Reso	Ived Network Addresses Ctrl+N	SUCCESS	1999. H00_34. UL.	
12.36	Ection	EXE	2548	Hex File Of	feets and Lengths	SUCCESS		
12.96	Enlow	EVE	2488		171 110	SUCCESS	Ocean: Name	
12.35	Entitor	EXE	2988	Plax Proces	s and Thread IDs	SUCCESS	Query HandeTan	
12:36	Epilow	DE	2988	BegQuerter	HKEU/Software/Classes	SUCCESS	Query Hande Tag	
12:35	Explore	EXE	2968	RegOpenKey	HKEU/Software/Classes\.onf/Open/WithProoids	NAME NOT FOUND	Desired Access: B	
12:36	Eplow	DE	2988	RegOpenKey	HKCR\.om\.OpenWithProgide	NAME NOT FOUND	Desired Access: R.	
12:36:	Epipe	EXE:	2968	RegQuesKer	HKEU/Software/Classes	SUCCESS	Query: Name	
12:36	Eplow	DE:	2568	RegilizeryKey	HKEU/Software/Cleaner	SUCCESS	Query: Handle Tag	
12.36:	Delore	(DE	2968	RegQueryKey	HKCUNSoftware/Classes	SUCCESS.	Query: HandleTag	
12:36:	Delow	DE:	2988	RegOpenKey	HRCU/Software/Classes/Software/Microsoft/Windows/Curr	NAME NOT FOUND	Overved Access: R.	
12.36:	Delore	(DE	2968	RegOpenKey	HRCR\Software\Microsoft\Windows\Current\Version\Explore	. NAME NOT FOUND	Desired Access: R.,	
12:36:	. 🎇 Epiow	DE	2568	RegiliueryKey	HKCU/Software/Classes	SUCCESS	Query: Name	
12:36:	Epice	(DE	2968	RegQueryKey	HKEU/Software/Classes	SUCCESS	Query: HandleTag	
12:36:	- Espiorer	EXE	2968	RegQueyKey	HKCU/Software/Classes	SUCCESS	Query: HandleTag	
12:36:	Epiore	EDE	2968	RegOpenitey	HKEU\Software\Classes\pnl	SUCCESS	Desired Access: R	
12:36:	Con Links of	EXE	2568	rieguueytay	HALU/Software/Microsoft/Windows/Lurrent/Version/Explore	SUCCESS	Query: Handle I ag	
12.36:	- Epore	SE	2968	Hegupenkey	HALU-Software Microsoft Windows Current Version (Explore	SUCCESS	Desired Access: R.	
12.36:	- Diplore	EAR	2300	rieg Juey fuy	HALU Software Wicrosoft Windows Summit Version Soplar	SUCCESS	Guery: Handle Lag	
12.06	- Colore	EVE.	2500	Barlymer	History Control of Control of Control of Control Contr	0000000	Orana Manda Tan	
12:36	Deive	ENE	2588	BaglosoKer	1971D Software Microsoft White and Some Version Sciper	SUPPESS	Desired Access D	
12.36	- Delaw	DE	2588	BanduaryValue	HIC U.Software/Microark/Wedges/Current/Janion/Ecology	SUCCESS	Tree BEQ 57 Le	
12:36	Ector	EXE	2568	BagCaseKey	HKC1D-Software/Microsoft/Windows/CurrentVenion/Ecology	SUCCESS	the contraction of the	
12:36	Epipe	DE	2588	RegCinesKey	HKCU/Software/Microsoft/Windows/Current/Jensor/Explore	SUCCESS		
12:36:	Eclore	EVE:	2968	RegCloseKey	HKCU/Software/Microsoft/Windows/Current/Jersion/Explore	SUCCESS		
12:36:	Epilore	DE	2588	RegQueryKey	HKEU/Software/Classes	SUCCESS	Query: Name	
12:36:	Epipe	EVE:	2968	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag	
12:36:	Eplow	DE	2988	RegQueryKey	HKEU/Software/Classes	SUCCESS	Query: Handle Tag	
12:36:	Epipe	(E)(E)	2968	RegOpenKey	HKEU/\Software/Classes\Applications/instepad.exe	NAME NOT FOUND	Desired Access: R.,	
12.36	Eplow	DE	2988	RegOpenKey	HKCR\Applications\notepad asse	SUCCESS	Desired Access: R.	
12.36:	Delore	(E)(E)	2968	RegDoseKey	HRCR'Applications' notepad eve	SUCCESS		
12.36	Epiow	EDE	2968	RegiouryKey	HRCU/Software/Cleane	SUCCESS	Guery: Name	
12.36:	Delore	EXE:	2968	Regaunykey	HKC UNSOftware/Classes	SUCCESS	Query: HandleTag	
12.36	Delow	EXE:	2968	Regioury fay	HRLU/Software/Classes	SUCCESS	Guery Handle Tag	
12.36.	Dente	5/2	2968	negopenkey	HKC 0-Software Classes Applications incleped eve	NAME NOT FOUND	Cesired Access: R	
12.36	Deparent	EXE	2368	regupentay	HALIN upplications violepad asie	SUCCESS	Ceared Access: N.	
12.36	abpore	5/2	2968	negaveyney	HML H VPDHOADONS VIOLEDAD ENE	0000255	Quely: Name	
12:36:	Cebber	EVE	2300	A DesCourse	HALF Oppositions (Compact and USE 10 Colleges) (Compact Section (Instance) Coll (co	NAME NOT DOWN	Caulary: manche rag	

4. Seleccione Generar eventos de perfiles de amenazas y Cada segundo.

🎒 Proc	ess Monitor - C:\	Users\win7x64-new\Desktop	p\procmon_output\test1.pmi	1			
File Ed	lit Event Filte	r Tools Options Help					
- 2 III		🖶 A 🚓 🖻 🗛 🗖					
	1 2 8 21	A 🖶 AL 🖂 🖬 🖌					
Time	Process Name	PID Operation	Path		Result	Detail	
12:36:	Searchindexer	2252 RieSystemContro	xC:		SUCCESS	Control: FSCTL_Q_	
12:36	Searchindexer		NC:		SUCCESS	Control: FSCTL_R	
12:36	S Fashia Bas	a Longing)	SUCCESS	Control: FSCTL_R	
12:36:	ES Chable bot	st cogging			SUCCESS	Thread ID: 2884	
12:36	Call Description	where one passaraha through one	fine a sector that each on		SUCCESS	Query: Name	
12:36	E the state	onitor can generate thread pro	ning events that capture		SUCCESS	Query: HandleTag	
12:36:	20		egoda anto rat.		SUCCESS	Query: Handle Tag	
12:36	Ger 🖉 Ger	erate thread profiling events			SUCCESS	Desired Access: Q	
12:36	E				SUCCESS	Query: Name	
12:36	1	Every second			SUCCESS	Query: Handle Tag	
12:36	E	Every 100 milliseconds			SUCCESS	Desired Access: M	
12:36	E			(Default)	SUCCESS	Type: REG_SZ, Le	
12:36	1		OK Cancel		SUCCESS		
12:36	E				SUCCESS		
12:36	Explorer.EXE	2988 KRegQueryKey	HKCU/Salivase/Classes		SUCCESS	Query: Name	
12:36	Eplow EXE	2988 KRegQueryKey	HKCU Software Wasses		SUCCESS	Query: Handle Tag	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU/Software/Classe		SUCCESS	Query: Handle Tag	
12:36	Explorer.EXE	2988 KRegOpenKey	HKCU/Software/Classes/pmi/	OpenWithProgids	NAME NOT FOUND	Desired Access: R	
12:36	Eplorer.EXE	2988 KRegOpenKey	HKCR\.pml\OpenWithProgids		NAME NOT FOUND	Desired Access: R	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name	
12:36	Explorer.EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36	Eplorer.EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: HandleTag	
12:36	Explorer.EXE	2988 KegOpenKey	HKCU/Software/Classes/Softw	rare\Mcrosoft\Windows\Curr	NAME NOT FOUND	Desired Access: R	
12:36	Explorer.EXE	2988 KRegOpenKey	HKCR\Software\Mcrosoft\We	ndows/Current/Version/Explore.	NAME NOT FOUND	Desired Access: R	
12:36	Eplover.EXE	2988 KRepQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36	Explorer.EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Handle Tag	
12:36	Explorer.EXE	2988 KRegOpenKey	HKCU\Software\Classes\.pml		SUCCESS	Desired Access: R	
12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Microsoft\Wir	<pre>>dows\CurrentVersion\Explore.</pre>	SUCCESS	Query: Handle Tag	
12:36:	Explorer.EXE	2988 KRegOpenKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore.	SUCCESS	Desired Access: R	
12:36	Eplorer.EXE	2988 KRegQueryKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore.	SUCCESS	Query: HandleTag	
12:36	Explorer EXE	2988 RegOpenKey	HKCU\Software\Mcrosoft\Wv	dows/Current/Version/Explore.	SUCCESS	Desired Access: R	
12:36:	Explorer.EXE	2988 KRegQueryKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore.	SUCCESS	Query: HandleTag	
12:36	Diplorer.EXE	2368 RegOpenKey	HRCU/Software/Microsoft/Wir	ndows \Current Version \Explore.	SUCCESS	Desired Access: Q	
12.36	Explorer EXE	2388 RegQueryValue	HNLU\Software\Microsoft\W/	ndows (Current Version \Explore.	SUCCESS	Type: REG_SZ, Le	
12:36	Biplover.EXE	2368 RegCoseKey	HNLU/Software/Microsoft/Wir	ndows (Current Version \Explore.	SUCCESS		
12:36	Diplorer EXE	2965 KegCloseKey	HKLU/Software/Microsoft/Wir	dows 'Current Version 'Explore.	SUCCESS		
12:36	Explorer EXE	2388 RegCoseKey	HRCU/Software/Microsoft/Wir	ndows \Current Version \Explore.	SUCCESS		
12.36	Diblover EXE	2368 RegQueryKey	HNLU/Software/Classes		SUCCESS	Query: Name	
12:36	Explorer.EXE	2966 RegQueryKey	HKCU Software Classes		SUCCESS	Query: Handle Tag	

5. Asegúrese de que todos los filtros relevantes estén seleccionados en Procmon y que se estén recopilando datos.

6. Si no puede replicar el desperfecto, puede forzar el desperfecto de Windows utilizando la utilidad NotMyFault64.exe que puede obtener de <u>https://live.sysinternals.com/files/</u>

Las instrucciones sobre cómo ejecutarlas aquí: <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

	Display American 201 American American 201	Int Bask C Auguer Marc Claus (MPT111) Bask BCC200 Marc Marc Claus (MPT111) Bask BCC200 Marc Marc Claus (MPT111) Bask BCC200 Marc Marc Claus (MPT111) Bask BCC200 C Auguer Marc Claus (MPT111) Bask BCC200 </th <th>Out Out Out 2500 (2014) Ott 2500 (2014) Ott 2500 (2014) Ott 2500 (2014) Mate 2014) 700 (201</th>	Out Out Out 2500 (2014) Ott 2500 (2014) Ott 2500 (2014) Ott 2500 (2014) Mate 2014) 700 (201
未冊 [2] 未冊 [2] 点 点冊 [2]] 点 点 冊 [2]] 点 点 冊 [2]] 点 点 冊 [2]]]]]]]]]]]]]]]]]]]	10 Autorship 11 Autorship 12 Autorship 13 Autorship 14 Autorship 15 Autorship 16 Autorship 17 Autorship 18 Autorship 19 Autorship 10 Autorship 11 Autorship 12 Autorship 13 Autorship 14 Autorship 15 Autorship 16 Autorship 17 Autorship 18 Autorship 19 Autorship 10 Autorship 10 Autorship 10 Autorship <th>Compare Non-Const 444-11 Series No. Const 444-11 Series No. Const 444-11 Series No. Const 444-14 Series No. Const 444-14</th> <th>Oracle 2015/07: Vitand Analy Ten. 197 Vitand Analy Ten. 197</th>	Compare Non-Const 444-11 Series No. Const 444-11 Series No. Const 444-11 Series No. Const 444-14	Oracle 2015/07: Vitand Analy Ten. 197 Vitand Analy Ten. 197
其此	1 Schedulard 1 Schedulard 2 Schedulard <td></td> <td>The second of the second se</td>		The second of the second se
	10 Control of the second	In the second seco	The Control Annual PA The Control Annual PA Sector State Annual PA Sector S
	10 Conjunction 10 Conjunction 10 Conjunction 10 Landon Andree 10 Landon Andree <td< td=""><td>III. (A Description of House Ho</td><td>CIPC/Deard Ansame A. Recard Ansame A. Recard Ansame A. Recard Ansame A. Recard Ansame A. Recard Ansame A. Profile Ansame A. Recard Ansame A. Recard</td></td<>	III. (A Description of House Ho	CIPC/Deard Ansame A. Recard Ansame A. Recard Ansame A. Recard Ansame A. Recard Ansame A. Recard Ansame A. Profile Ansame A. Recard
未冊 (四) 其未冊 (四) [1] [1] [1] [1] [1] [1] [1] [1] [1] [1]	10 Construction 10 Co	III.// Adaptive Hand Version 11 Constraints In 2017 (2017) Interface Name Interface Name III. Adaptive Hand Version 2017 (2017) Interface Name Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface III. Adaptive Hand Version 2017 (2017) Interface Interface Interface	0190 See Avan A. Ancar S. M. Maran S. M. Maran S. M. Maran J. M. Maran Maran Maran Maran Maran Maran Maran Mara
未初一 (円) 素子(一) 素子(一) 素子(一) 素子(一) 素子(一) (一) 素子(一) (一) (一) (一) (一) (一) (一) (一)	1	() Augus Marc (and Ma	Recard to 2. Recard to 2. Recard South No. 1997 (Net Your South
素品》 [四]美点品》 [四]	1		Aligned Science 1, 2011 Control (1994)
2.mm 2.mm	Image Control Image Second Image Second <td>Compare Net (2000 and 2011 Balance Na 0.00000 Compare Net (2000 and 2010 and 201</td> <td>(244, 2010) 0.00- (244, 2010) 0</td>	Compare Net (2000 and 2011 Balance Na 0.00000 Compare Net (2000 and 2010 and 201	(244, 2010) 0.00- (244, 2010) 0
	1 Schedungen 1 Schedungen <td></td> <td>τ) το ματά τόμα τη δετά τ) το ματά τόμα π. το ματά τόμα π. το ματά τόμα π.</td>		τ) το ματά τόμα τη δετά τ) το ματά τόμα π. το ματά τόμα π. το ματά τόμα π.
	10 Conjunction 11 Conjunction 12 Conjunction	Image: Mode of Stream of Stream of Construence Stream of	1100 (Januari Annua, R. 1997) Annual Annua, R. 1997) Annual Annua, R. 1997 (Januari Annua, R. 1997) Annual Annua, R. 19
	Image: Section of the sectio	Initial Construction of the construction of	1999) Search Aroune A. Recard Tool R., Recard Tool R., Recard Tool R., 1999, Search S., 1999, Sea
二十十一 「四 二十十一 「四 二十十一 」 「四 二十十 」 「四 二十十 」 「四 二十 二十 二十 二 二十 二十 二 二十 二 二十 二十 二 二十 二十 二 二十 二 二 二 二	 Bergersen, S. S.	High Schwart Michael Workswich Programmerschild Nader 2017 Images Michael	Child Canadi Aroma A. Macarrolo R., Macarrolo R., Mara 2001 Nu. (Mara 2001 Nu. (Mara 2001 Nu. (Mara 2001 Nu. (Mara 2001 Nu. (Mara 2001 Nu. Macarrolo R. Macarrolo R. Macarrolo R. Mara 2001 Nu. (Mara 2001 Nu. (
未初 二、一、一、一、一、一、一、一、一、一、一、一、一、一、一、一、一、一、一、一	101 20	() Augus Marcian AM-11 (1 Aruse 19 () Augus Marc	Biologie frag Biologie frag Biogan Frag Biogan Frag Biogan Frag Biogan Frag Diel Collegie Biogan Frag Diel Collegie Biogan Frag Biogan Frag Biogan Frag Distant Assam Frag Distant Assam </td
未必一 19 大山山 19 大山 19 丁 19 丁 19 丁 19 丁 19 丁 19 丁 19 丁 19 丁	10 0 0.0000 (model) 10 0 0.00	() Pages Normal Article (1999) () Pages No	Mutanti-Series R., Hara (2001) N., Caralla (2001) N., Particle Control (2001) N., Particle Control (2001) N., Particle Control (2001) N., Hara (2001) N.,
末44 (平) 末44 (-)) 末44	Image: Section of the sectio	Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2013) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2014) Program Net (2	The (2011-1- marked base)
2. 世紀	Comparison of the second	Trapper Net (2012) Trapper Net (2012	τ) (Australian Co.) (Australian Co.) (Australian Co.) (Aus
	construction c	Compare Number of the second sec	The second secon
	Control of the second sec	Image: Review of Proceedings of the Control	Control Lance Access P. A. Control Lance Access P. A. Responsible and Access P. A. Responsible and P. A. Control Lance Access P. A. Control Lance Access P. Control Lance A
二十一、四、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、		High Strategie Hander Mitsbase HV Constrainers III. Saldh Strategie I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and all 1) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and 11) 1.6 const top 6.00000 I Angele Marc (and	CHILD Land Arount P., Roquerriso JE, Roquerriso JE, Doner Van D., Doner Van D., Dira (1975) A. J. Oral Ling C.
未一部 素上部 (第 素上部)(10)(10)(10)(10)(10)(10)(10)(10)(10)(10	10 2-3-3-2 10 2-3-3-2 </td <td>(Augus Marchan JM-11 & Augus 19 (Augus Marchan JM-11 & Au</td> <td>Alicentrical R. Microarchine R. Microarchine R. Microarchine R. Destaine Vaca B. Destaine Vaca B. Destaine Vaca B. Destaine Vaca B. Microarchine R. Microarchine R. Microarc</td>	(Augus Marchan JM-11 & Augus 19 (Augus Marchan JM-11 & Au	Alicentrical R. Microarchine R. Microarchine R. Microarchine R. Destaine Vaca B. Destaine Vaca B. Destaine Vaca B. Destaine Vaca B. Microarchine R. Microarchine R. Microarc
其44 1年 大44 1 大44 1	 Alexandrawa 	(Augus Marchard Marchards Bargenseg (Augus Marchard Marchards Bargenseg (Augus Marchards Marchards Bargenseg	Accession 8. Intel 1991, 201, 201, 201, 201, 201, 201, 201, 20
未必一 1年 大山(1) 市 市 市 市 市 市 市 市 市 市 市 市 市 市 市 市 市 市 市	IV Artes/A IV Artes/Artes/A IV Artes/Artes/A IV Artes/Artes/Artes/A IV Artes/A	Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Nuclear Mar 12 de par leg Augus Aug	I Har 2010-20, Souther A and D. Souther A and D. Souther A and D. Souther A and D. March
末冊 二部 大冊 二部 市内 二 市内 二 目 日 日 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	 Ausch 	Pages Nuclear Markes & 64/000 Pages Nuclear Markes &	proteine Nat (R. Portaine Nat (R. 1962) Sance Access A. 1962 Sance Access A. 1962 Sance Access A. 1962 Sance Access A. 1964 Life Access A. 1964 Sance Access A. 1964 San
末44 19 天44 19 大き44 19 大54 19 19 19 大54 19 19 19 19 19 19 19 19 19 19 19 19 19 1	 A José No. A José No.	maps Maps <td< td=""><td>Produce Asso 0 (Har 1075 N A Har 2015 N A Har 2015 N A Har 2016 N A Ha</td></td<>	Produce Asso 0 (Har 1075 N A Har 2015 N A Har 2015 N A Har 2016 N A Ha
* == + = + = + = + = + = + = + = + = + =	 Alexandra Alexandra		101 (2018) Series Course A. 100 (Series Course A. 100 (Series Course A. 100 (Series A. 10
	 Alashin 	2 Program Nucleury (MP hasses do	Her X Strept Her X Strept 100 Januar Annue X United 101 N L A United 101 N L A United Strept Annue R Oriol Januar Annue R Annuer Annue R Her 2010 Januar Annue R United Strept Annue R United Strept Annue R United Strept Annue R Direct Januar Annue R Direct Januar Annue R Direct Januar Annue R Josef Janu
た。 中一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	 Antonia Antonia	Program Nucl Cognit All Houses do sur Section 4. Vargane Nucl Cognit All Houses do SUCCED Vargane Nucl Cognit All Houses do	(e) Carace A constraints (Nat 107 Ma) (Nat 107 Ma) (Na
た。 市 市 市 市 市 市 市 市 市 市 市 市 市	 Alexandrator Alexa	(Appen Nachon (AP) Lease 6 6,0799 (Appen Nachon (AP) Lea	Angerete K. (Har 1,01,01), Usual and Salarith. PT, Death The 150, 0040 Annue Arsan R. (040) Annue Arsan R. (040) Annue Arsan R. Alexanetes B. Maraterias B. Usual Annue F. Usual Annue F. Usual Annue F. (Usual Annue F. (Usual Annue F.) (Usual Annue F.) (Usual Annue F.) (Usual Annue F.) (Usual Annue F.)
た。 市 市 市 市 市 市 市 市 市 市 市 市 市	 Annundrach Annundrach		Har 1 (F) (H) 5, Verandersfelder PFI, Gegenethen 142, Debid Lawest Annuel A. Bergenethen B. Bergenether B. Bergenether B. Urband Annuel A. Verandersfeld B. Verandersfeld B. Verandersfeld B. Debid Cawest Annuel A.
		2. Argun Nucleur (APV) 15 draws to 4. Argun Nucleur (APV) 15 draws to 7. Argun Nucleur (APV) 15 draws	Vicual Sector No. Yes, Cogator Non 147, Ordel Learnet Across R. Ordel Learnet Across R. Microsov Rev. Microsov Rev. Microsov Rev. Water 2019, UKL, Vicual Sector No. Vicual Across R. Ordel Canant Across R. Ordel Canant Across R.
	 Andrewick Andrewick	Chapter Nuclear (MP-1) Bit case (p) APPE(10) August Nuclear (MP-1) Bit case (p) APPE(10) August Nuclear (MP-1) Bit case (p) August Nuclear (MP-1) Bit	PT., Cogato The 140, DHD Lawet Arous R., DHD Lawet Arous R., DHD Lawet Arous R., Broater-Dar JL, Broater-Dar JL, Broater-Dar JL, UKang 2048, DB, Victorianter The PT., Cogato The 140, DHD Dawet Arous R., DHD Dawet Arous R.
中純 1% 市井田 1% 市田 1% 市田 1% 田 1% 田 1% 1% 1% 1% 1% 1% 1% 1% 1% 1% 1% 1% 1% 1%		The product shared finance of Constraints (S. 1889) 617 628 (S. 1899) 618 (S. 1899) 618 (S. 1899) 617 1. August Nacional Alfred Statistics (S. 1899) 617 2. August Nacional Alfred Statistics (S. 1899) 2. August Nacional Alfred Statistics (S. 1899) 3. August Nacional	Control Association P., Control Association R., Stream Taxonic R., Alexanization R., Alexanization R., Office 20,000,100, United Science P., Control Science R., Control Science R., Co
市井田 18 市井田 18 市 市井田 18 市 市井田 18 市 市井田 18 市 市 市 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日	No Paglanta No Paglanta No Paglanta No Paglanta No Paglanta No Paglanta No Paglanta	Model and second encourses of Contribution Line (2017) Model (2017) And Anno Anno Anno Anno Anno Anno Anno	Herd Lanes Arous R. Recator for B. Recator for B. Broater for B. Utera Data for Utera Data for Ph. Data for Tra 1010 Canes Arous R.
10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 11 10 12 10 13 10 14 10 15 10 16 10 17 10 18 10 19 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10	N Alasharia N Alasharia N Alasharia N Alasharia	Angen Render of Annuel Statements Angen	Roseria 2. Roseria 2. Oka 20010 Vinačatnih Vilozatnih 1000 sesti Anse 8.
	N shackets N shacks	1 August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial 1 August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial 1 August Nu Carco and 111 and an initial 1 August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial 1 August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial 1 August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial August Nu Carco and 111 and an initial 1 August Nu Carco and 111 and 1111 and 1111 and 111 and 111 and 111 and 111 and 111 and 111 and 11	Broate-Sa 2, Ohar 2016108, UtaraDeater Int, OHD Dawn Arcess R. OHD Dawn Arcess R.
A.m. 18 A.m.	N Alashina	Program RevConstation (1994) and representing 0.00000 Program RevConstation (1994) and representing 0.00000 Program RevConstation (1994) and representing 0.00000 REVERSIDE REVERSIDE REVCONSTATION (1994) REVERSIDE REVERSIDE REVCONSTATION (1994)	Char 2010.00 Union/optimize W1, Coater Tris 16 DHD Datest Access 9, DHD Datest Access 9,
作品 市合 市合 市合 市合 市合 市合 市合 市合 市合 市合	N Cartherat	Proper NacCest diP 118 drawing 0.0008 Proper NacCest diP 118 Proper NacEst diP 118 Proper NacCest diP 118 Proper NacCest diP 118	VicesCaster Tex. 19. Deater Tex. 15. DHD Damit Access R. DHD Damit Access R.
Am 16	The Party of the P	 Proper Ner Central P (11) at use ing 8,000 https://doi.org/10.1016/j.jc/10000/j.jc/10	Wi, Date Tra 16, DPDDate Acces R. DPDDate Acces R.
*** 18 *** 18 **** 18 **** 18 *** 18 *** 18 **** 18 *** 18 *** 18 *** 18 *** 18 *** 18 *** 18 *** 18 *** 18	The second second second	HE.M. Manage Monard Windows IT Construment Inc. Kind HET A	DIPECtanist Acres #
**************************************	The Page Section	the second second billion of a second s	CONCIDENT ACTING
1 1 Ame 1	The first section	CONTRACTOR OF A CONTRACTOR OF	
	The second section	The provide standing of Company and the standing of the	Contractor Acres 1
	The standards	Company and the company of the second s	Render for 1
**************************************	IN A MARTIN	C Angen RevOew dill 718 strate to	Other Division
	10 Databland	C Proper RevCent (RP-1) Put you're ta Bucchill	Where Courts In
Am 18 Am 18 Am 18 Am 18 Am 18 Am 18 Am 18 Am 18 Am 18 Am 18	10 Alam/Ridge	El Prepar RenCent alle 128 et anche Burrels pur	WL. Destor True 14
	10 Challentin	HEM School Result Western IT Constitution Tox. NAME HET F	DIFCOMMENTATIONS R.
Aun 190 Aun 190 Aun 190 Aun 190 Aun 190 Aun 190	N Parlow No.	HEM Scheme Honsell Window 10 Contribution Do. 2008 (2017)	DIPODetrail Access PL
Am 150 Am 150 Am 150	IN Challentine	HEAD Original Writes IT Constants In 2018 (CT P	OPD Cashel Acres R.
Am 13	in a law have	Company New Carry AMP (11) # (Healthy D.C.C.D.)	decate the 2
Am 135	THE REAL PROPERTY.	Colorest Residence (1997) 11 di series	Other Division of
fiam 100	W hallow	Colours Resident del 110 di centre Bucchini	Whether Station Ten
	10 Cardena	C Proper Res Card diff (1) if all res by B. proto cur	WL. Daster True 141
fram 130	10 Charles in	HEM Schwart Roman Windows 17 Commission Tex. Salet 1671	DEFC Created Access PL
film 120	W Challentin	HEM Select Hone & Writes & Constants In 2010 (2017)	DIPOCHEMI Arises R.
film 120	TV Challentin	HEM Selver Hunsell Western 17 Contributors Tox, 304E VET 7	DIPODetrol Arises PL
film 136	N Carlanderie	C Proper RenCenn INP/2011 all year by BLCCOTT	Acceleration 21.
n - 175	The Shancharder	C Prepar RenCard INF 111 drives ha	Merate-Dat 21
120	The second second	C Prepar Render (10 Million hg BLCCDD)	Contract in the local division of the local
10.0	THE PROPERTY.	C Property and Property State and St	Concerning of the local of the
	Table Concerning	NEW CONTRACTOR AND ADDRESS OF THE OWNER.	Contract Access 18
	THE PARTY OF	HEM STATISTIC Access ACCIVITIES IN COLOR	Contr. N.S. Sality
100	100 Challenster	HEM SOFTWARE ADDRESS ADDRESS BUTTON TOP	DM.
100000	CHI Charles	HEM SOFTWARE Association (CADING ASSOCIATION SUCCESS)	Tax PELSE in
100	THE PARTY NAME	HEM SOFTWARE ADDIES	
20	and the second second	9.0000	Corry Rends Inc.
200	(10) Challenster	THE REPORT OF A DESCRIPTION OF A DESCRIP	Charles Access 14
	CRI Challandra	States and the second s	the real party .
ACCESSION AND ADDRESS OF ADDRESS ADDRE		THE REPORT OF A PROPERTY AND A PROPERTY OF A	and the second second second
		HEM STATE Annual ACTIVATE BUTTO	THE PARTY OF THE

7. Acelere la máquina.

8. Inicie la máquina en el modo seguro y recopile manualmente **Procmon.pmb** y **MEMORY.DMP**, ambos archivos están en C:\Windows folder. Estos archivos se compartirán con Cisco TAC.

Computer	▼ Local Disk (C:) ▼ Win	dows 👻	• ()	Search Windows	_	_
Organize - Open -	New folder			,	i≡ • ⊡	
🔆 Favorites	Name +		Date modified	Type	Size	
 Libraries Documents Music Pictures 	Freupdate.exe HelpPane.exe Phh.exe		7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM	Application Application Application Text Document	15 KB 717 KB 17 KB 14 KB	
Videos	MEMORY.DMP		1/6/2020 12:41 PM 7/14/2009 1:06 AM	DMP File BIN File	331,914 KB 43 KB	
Local Disk (C:)	msdfmap.ini notepad.exe ntbtlog.bt PERO log		6/10/2009 10:36 PM 7/9/2015 7:57 PM 1/6/2020 12:41 PM 1/6/2020 12:30 PM	Configuration sett Application Text Document	2 KB 189 KB 83 KB 576 KB	
Network	ProcessionalN.xml ProfessionalN.xml Professiona	Type: XML Document Size: 52.3 KB Date modified: 6/10/20	1/6/2020 12:30 PM 6/10/2009 10:30 PM 39 AM 39 AM 30 PM 30 PM 7/14/2009 10:36 AM 11/21/2010 4:24 AM 6/10/2009 10:31 PM	PMB File XML Document Application Text Document Text Document Application XML Document	320,740 KB 53 KB 417 KB 29 KB 0 KB 66 KB 48 KB	
Procmon.pmb PMB File	StarterN.xml Date modified: 1/6/2020 1 Size: 313 MB	2:41 PM Date crea	6/10/2009 10:31 PM sted: 1/6/2020 12:41 PM	XML Document	48 KB	

7. Opcionalmente, si puede arrancarlo en "modo normal" si los archivos PMB se generan en el C:\Windows folder, entonces si inicia ProcMon de nuevo, verá los siguientes registros. En este caso, puede volver a guardar los eventos haciendo clic en el botón Guardar.

Process Monitor - Sysintemails www.spsintemails.com			
File Edit Event Filter Tools Options Help			
Text _ Passes Rane FE Danatan Fab	Read.	Detel	

Putora Monite	Ξ
2 log of local time solidly us control by a persistal inducer of Process Station Co.you with its analisis added data new?	,
Tm. No	
/	
,	

_
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: Pamas 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: Stres 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 Smiss.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 0 Name A
A1 Brance and	202 PasEn militar	LVI M Custon Custon Custon Caston Control COCCOM MANA	0000633	Index 5 Name M
41	292 RecEnceValue	HALM CYREM LUTERLOTED SELLOTED SELLOTED SESSION MANA	SUCCESS	Index 3 Name M
A1 Brends and	292 ResEnceValue	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 Landb 4
A1 Brance and	292 Regenuit value	HALM System Control Set Control SESSION MANA.	SUCCESS	
41	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