如何收集ProcMon日誌以排除AMP啟動問題

目錄

<u>簡介</u> 過程:

簡介

作為系統管理員,可能需要使用進程監控器(procmon.exe)獲取詳細日誌,以確定在電腦啟動過程中 FireAMP聯結器是否發生掛起。思科TAC也會要求這些日誌排除此類問題。Process Monitor是一個 免費的實用程式,可以在此處幫助我們。可從<u>https://docs.microsoft.com/en-</u> <u>us/sysinternals/downloads/procmon</u>免費下載

本文檔介紹在系統引導過程中(這意味著它在引導時生成BSOD)出現問題時如何收集ProcMon日 誌和記憶體轉儲的步驟。 需要這些日誌來捕獲引導期間發生的系統事件。

過程:

1. 設定測試機器,以便問題可以容易地再現。

2.以管理員身份下載並運行ProcMon工具。轉到File -> Process Monitor Backing Files並選擇路徑。

🚰 Process Maritar - Cl.Buerluri-O.dil-mail.Dealtapl.process.putput.text1.pml												
nie i												
Tes .	Poose Name	PD Operation	Path			Feed	Detail					
1236 1236 1236 1236 1236 1236 1236 1236	Searchindeau S	2212 A Na System Cr 2212 A Na System Cr 2212 A Na System Cr 2212 A Thread Creat 2018 A NagGuery Ke 2018 A NagGuery Ke 2018 A NagGuery Ke 2018 A NagGuery Ke	HELU Software HELU Software HELU Software HELU Software HELU Software HELU Software	(Cases (Coore (Cases (Cases), pril (Cases), PM,		SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Control FSC Control FSC Control FSC Thread D: 2 Coarty Name Coarty Hand Coarty Hand Coarty Hand Coarty Hand Coarty Name	L.G. L.R. L.R. M M M M G.				
12.36	Process Manito	r Backing Film										
1236	These backing file of	kjects are being used to	store event data:									
1236	Name			Event Court	Event Bytes	Panding Events	Process Court	Octoney Court	kom Count	Connelled		
12.86 12.85 12.86	Process Havitar car	n ellarer anvanda in chiluad in	senary (inded by t	te system convet linte	t), or ma file you a	querify (instant by from	e dade sepancea), stilhedr	de yau profer?				
1236	O Use vitual new	ary (0,70240 analobia))									
12.36	Con file named:	C Stervise 7x84	ten/Desktop/proce	in_pulput/pert2.prd								-
1234												
12.36	ProcPaniowit D. 49	% @pl (Dirytes pendin	e)								OK	Cancel
1234	Datow DE Datow DE Datow DE	2000 RegOverKey 2000 RegOverKey 2000 RegOverKey	HIER Applicat HIER Applicat HIER Applicat	ons'vetepad and ons'vetepad and ons'vetepad and		SUCCESS SUCCESS SUCCESS	Duared Acce Query Name	# Ř.				

3.在Procmon工具中,轉到選項—>啟用引導記錄。

🎒 Pri	ocess Monits	er - C:\l	Users/win	7x64-rww\Decktop	procmon_output/test1.pml			
File I	Edit Event	Riter	Tools	Options Help				
all all		P		41	T			
		CV	Y 🗛 🤉	Always on	Tob			
Tree .	Process N	lare .	PID	Font		Result	Detail	
12:36:	. #?Searchi	hdeer.	. 2252	Mark Ended (alars.	SUCCESS	Control: FSCTL_Q.	
12:36:	. CE Search	rdeser.	2252	riginga	antra -	SUCCESS	Cantral: FSCTL_R	
12:36:	 #?Searchi 	hdeer	2252	Configure	Symbols	SUCCESS	Cantrol: FSCTL_R	
12.36:	 Searchil 	Renhos	. 2072			SUCCESS	Thread ID: 2884	
12:36:	. Septore	DE	2988	Select Colu	mna	SUCCESS	Query: Name	
12:36:	2000	EVE	2968			SUCCESS	Query: HandleTag	
12:36:	- Lipson	EXE:	2968	Platory De	10h	SUCCESS	Query: Handle Tag	
12.36:	- Dolore	Dia.	2968	Profiling Ex	anta	SUCCESS	Desired Access: Q.	
12.36	- Diplow	EXE	1	-		SULLESS	Guery: Neme	
12.36:	- DOOTS	EAE	2968	Enable Boo	t Logging	SUCCESS	Query: Handle Tag	
12.36.	Denne	2,42	2366			20/2522	Deered Access: N	
12.36	- Decore	200	2200	V Show Reso	Ived Network Addresses Ctrl-N	SUCCESS	1999: P000_96. 08	
12:36	- Colore	EVE	2300	Hex File Of	feets and Lanoths	SUCCESS		
12.96	Enime	EVE	2300			SUCCESS	Overs News	
12.36	- Colore	EVE	2000	Hex Proces	s and Thread IDs	CINTECC	Duesy Hande Tag	
12.96	Enlos	EVE	2448	Burghurgher	HICTID-S-theory/Classes	SUCCESS	Query Hande Tag	
12:35	Enior	EXE	2968	BagCoanKey	HIT ID Software (Casses), on Disection Provide	NAME NOT FOUND	Desired Access: R	
12.36	Factors	EVE	2948	Ban Damker	HICR) and Oner-Wat-Provide	NAME NOT FOUND	Destrant Access: R.	
12:35	Fician	EXE	2968	BagQueryRev	HKE1D/Software/Classes	SUCCESS	Duey Name	
12.36	Entra	DE	2968	BagGuerrifer	HKCUP.Software/Classes	SUCCESS	Query Hande Tea.	
12:36	Delow	EXE	2968	RegQueryKey	HRELP.Software/Classes	SUCCESS	Query HandleTag.	
12.36	Deter	DE	2568	RegOpenKey	HKCU/Software/Classes/Software/Microsoft/Window	WOLLT NAME NOT FOUND	Destred Access: R.	
12:36:	Dekore	EXE:	2968	RegOpenikey	HRER\Software\Microsoft\Windows\CurrentVersion\	Explore . NAME NOT FOUND	Desired Access: R.,	
12:36:	Epiow	DE	2568	RegilizeryKey	HKCU/Software/Classes	SUCCESS	Query: Name	
12.36:	. Beiore	DE	2968	RegQueryKey	HKEU/Software/Classes	SUCCESS	Query: HandleTag	
12:36:	. 🔚 Eplow	DE	2988	RegularyKey	HKEU/Software/Classes	SUCCESS	Query: Handle Tag	
12.36:	. Epicore	EVE:	2968	RegOpenKey	HKEU/Software/Classes/.pnil	SUCCESS	Desired Access: R	
12:36:	. 🎧 Esplorer	DE	2988	RegQueryKey	HKEU/Software/Microsoft/Windows/Qurrent/Version/	Explore SUCCESS	Query: Handle Tag	
12.36:	Epiore	(DE)	2968	RegOpenKey	HRCU/Software/Microsoft/Windows/Current/Version/	ExploreSUCCESS	Desired Access: R.,	
12:36:	- Dekorer	DE	2968	RegQueryKey	HXEU/Software/Microsoft/Windows/Qurrent/Version/	Explore SUCCESS	Query: Handle Tag	
12.36:	 Bolow 	BAB	2968	RegOpenKey	HRCU/Software/Microsoft/Windows/Current/Version/	Explore. SUCCESS	Desired Access: R.,	
12.36	- Epiow	EDE	2968	RegGueryKey	HREU/Software/Microsoft/Windows/Gurrent/Ventory/	Explone. SUCCESS	Query: Handle Tag	
12.36:	- DEROTE	EXE	2966	RegOpenikey	HREU/Software/Morosoft/Windows/Current/Version/	Explore_SUCCESS	Desired Access: Q	
12.36.	Deter	EDG:	2968	Regulary Velue	HRE, U.Software (Microsoft (Windows) Current Vention)	Explore. SUCCESS	Type: PEIG_SZ, Le	
12.36:	Dekore	202	2968	Regulateray	HK2 U-Software Microsoft (Windows Current Version)	ExploreSUCCESS		
12.36	- Distant	EAE	2300	Tieg. Costay	HALD CONVERSION OF CONCEASE CONTRACT STREET	Dopper SUCCESS		
12.00.	- Devoe	EVE	2300	Par Duro Kar	HALO SOTATE ORODOLE OF DOMESSION OF SOME OF SOME	CODING	Owner Marrie	
12:30	- Copore	EVE	2300	Page and the	HALD CONVERTING	CIPPECE	Duese Hande Teo	
12.06.	Entre	EVE	2900	Barlumfer	HWC10-S-theres/Classes	SUCCESS	Query Hande Tag	
12:30	- Delve	EVE	2300	Regional Fer	UPTID Schurge/Chasse) instrational related	NAME NOT DO NO	Desired Access: D	
12.36	Entre	EVE	2988	Ban Damker	HCR Andrating voteral and	SUCCESS	Destrad Access R.	
12:35	Ecion	EXE	2965	BagCaseKey	HRE'R' Applications' optroad num	SUCCESS	A REPAIR OF A REPAIR OF A REPAIR	
12:36	Entre	EDE	2568	BagQueryKey	HICU/Software/Classes	SUCCESS	Query Name	
12:36	Delow	EXE:	2968	RegQueryKey	HKEU/Software/Classes	SUCCESS	Query HandleTag	
12:36	Epipe	DE	2568	RegiouryKey	HKCU/Software/Classes	SUCCESS	Query Hande Tag	
12:36	Delore	EXE	2968	RegOpenKey	HKEU/Software/Classes/Applications/Indexed ever	NAME NOT FOUND	Desired Access: R	
12:36	Epiow	DE	2968	RegOpenKay	HXCR Applications Viotepad asse	SUCCESS	Desired Access: R.	
12:36:	Epipe	EVE:	2968	RegQuery Key	HKCR' Applications' notepad eve	SUCCESS	Query: Name	
12:36:	Eplow	DE	2988	RegularyKey	HKCR\Applications\notepad ase	SUCCESS	Query: Handle Tag	
12:36	The Deriver	EVE	7988	Can Coan Fer	UNTIL Software/Change) indication/ordered avail	MARE NAME NOT ON AN	Desired Rosses: D	

4.選擇Generate threat profiling events,然後選擇Every second。

🎒 Proc	Process Monitor - C/Users\win7h64-new\Desktop\procmon_output\test1.pml								
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 riterien		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		The second secon	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 RegOpenKey	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	Epplorer 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.確保在Procmon中選擇了所有相關的篩選器並且正在收集資料。

6.如果無法複製崩潰,可以使用從中獲得的實用程式NotMyFault64.exe強制崩潰Windows <u>https://live.sysinternals.com/files/</u>

以下是關於如何運行的說明: <u>https://docs.microsoft.com/en-us/windows/client-</u> management/generate-kernel-or-complete-crash-dump

Provan Vientur - Ci	Charlose Cell Anno Cellin	granes, supplied, prof			
The Date Durit The	a fools (priors this				
2 B 4 9 6	* 4 0 E A				
Ins. Annua Annu	No destas	East.	land.	Gent	
on Dates	Int Banda	Column Resident diff. 11.0 down in	0.0000	Other Distances	
23. 84.00	120 Advantage	C August RenCase 447-111-41-ave by	9.40.000	Warmal August Tra-	
23. 14.00	1707 Deltary Winfords	C Proper Renders AMP 311 At see by	8,0000-040001	Department 161	
23. 8.4.40	The Contraction of the Party of	18,M Silver House Write VC renteen in	AND NOT THE	Change Access 19.	
23. 19.00	The Contraction of the	18,M Selectro Rectard Westers VC prestrance: To	New York Works	Cashel Access 7.	
State States	The second second	Provide the second state of contracts to	Automatic and a state of	Street Access 10.	
COLUMN TWO IS NOT	1707 Schenchentert	C Proper Revolution differ 11 ft all use but	B.41 (201)	Accession 18	
23. 84.00	100 Bulletin	C Proper Renders AP 11 Betrevite	9.40.2215	(Ref. (5.000.00)).	
23. Exten	170 Databaran	C Prepara Renda constant 11.11 At over high	9.00205	ichanal mater In-	
23. 19.00	The last working	C Veper Rendern ART 11 Million No.	States ordered	Coder True 141	
20.00	The second second	The Manhamman Street Street and Street and Street S	and the state	Canada Array 1	
2.0. 8.0.00	100 Charlester	18.M Schwart Human Westwork? Current lancers for	And the Party	Casesd Access 10.	
CH. Exten	170 Bellandarder	C Proper NerCennid? 1114 are to	9.00205	Accession (R.)	
23. Ext.m.	170 Belandarded	 Proper Nerroexcell[®] 111 Acres by 	140.005	Accession (5.)	
22.20	The second se	Pages Nerces and Conditioning	141.000	the post of	
20.000	The Designation	Compare Services and the first service	a press lutrage	Canadian Intel State	
CO. Even	100 Charlester	TRUE Schwarz (Actual) Weather 171 (anotheres) for	next next rises	Cases Access 74	
CH. ENDer	The Page server	18, M Schware (Actual) Meathers 1011 preschangers Tex	AND NOT YORK	Canad Access PL	
23. EX.m.	The second second	HEAD Schwarz (Resard) Medines IV Currentianers To	NAME AND POST OF	Canad Acons P.	
10 million 10	in handarder	Property for the second of the second	10000	Access for 1	
Contraction of the local division of the loc	Line Manufa	Company Revolution (1971) 11 (1971) 11	The state of the s	The later of	
Contraction of the local division of the loc	The second	Company Party and wide' to any da	9.41 222	Partients True 18	
COL EXCHANCE	THE REPORTS	Proper Net Cash AP Internal	9,40,995	Octave Ase 0.	Ministratives Citizedentilipaterelli periode
23. Exten	100 Automative Stage	 Vegen NerCentAP transit 	9.00895	One 195243	End and the subject of
2.0. 10.00	The second second	Proper Nerces and Index & pund	NAME AND POST	Cases Arrest P.	
2.0	The second se	Company Read and Life Street in our	sand only share	Canada Street B	
Contraction of the local division of the loc	110 Advantage	Company Rest Carry 418" States 45	9.40 (89)	Accelering H.	Example in 2014 State Stat State State State State State Stat State State S
Cit. Extrac	100 Automative	 Prepar NorCascille*Interval 	0.00005	Ofer 101526-3	The same of a real of the same of a real of the state
20. Exten	110 Australia	C Proper RenGest AMP (118 at seeing	9.40.995	identifiation for	
20.004	IN BANKING	C Vrepan RevCascular (1) 5 drues to	a second second	Control 16	Figure and the contract of the
20.000	The State Section	with the Induced in the second state of the providence of the	same raid where	Canada Annual II	AN ADDRESS 15,124 MIL (2012) Processing and the second
Col. Electron	110 Performentes	HUM Schwarz (Remark Western W Commission) The	NAME OF FRIDE	Castral Array P.	#3#338# 1137 # 3185 (#1596##1150pp
U.M. Kirken	110 Autochardert	C Proper RenCentral Profile Acres by	9,00895	Accelerible 28.	81 48-4818 [3] (3) (3) (3) (3) (3) (3) (3) (3) (3) (3)
12.00. E.M. ave	190 Blancharder	C Proper Rel Cent AMP (118 at see by	0.00895	Acateria 3.	Tribute Distance Statement Production
20.000	IN ANY A	C Vegeen NerCarrister (1881) and the	BACKER.	Cold Diversion.	1 Martin P. W. W. Martin Martin Press
20.000	The Advantation	Compare Residence and Control of the second	a print putter.	Castler Ing. 14	direction or said built many displicit support. Our income for the
U.S. Kittan	100 Charlester	HUM School (Reset Wester 10 Constitute) for	want not hove	Canadi Arran R.	the base of the second s
U.S. Erban	110 Paylor No.	HUM Mean Menad Western W Carenheser Ter	And showing the	Cashal Access 16.	Construction of the product of the second seco
10. Dr	110 Pagisertes	HEAL Dream Monard Western W Carentiesen In	AND HER POPPORT	Cashat Access 74.	the base of the first state in the state of the first state of the base of the state of the state of the state
20.00	The state of the state	C Proper Ner Carrier 1971 191 at un 19	The second second	Accession 18	
20.000	THE MARKING	Colours Resident and Table at an in-	0.00000	Otor Distant.	
U.M. Kirken	110 Allantifumate	C Proper RenCent diff (1) Reframing	0.00000	Ware agin In.	1
1230. Eldone	100 Billion/Writers	C Proper RenCentatiff (1) 8 at yearing	BUMPH DUPPYL	Destor Trac 16	1
No. Of the	The Paylor Has	HEM Scheme Honsell Western M Commission Se	NUME AND ADDRESS	Cases Arrest R.	1
10.0	The Part Service	and the second states of the second states in the	and out they	Canada Annas A	\
12.00	100 million families	C Property Ren Carry (1971) 11 di una ba	B.CORT	Accession from 18	1
1218. E.M. au	100 Manharded	C Proper RenCent all 7218 at sec by	BUCCERE	Accelerities 20.	1
Vill. Extens	100 Million	C Propert RenCarol (RP-218 at use by	BLOOP IT	Obs 208851	1
10.00	100 Camphonate	C Vegate RenCarol dill* 11 8 all and by	0.0000	Warman and in the	\ \
10.0	190 Charlensin	out to Advance the new Property of the second	hand out it was	Castral Action 18	1
12.00	100 Charles Tes	ARCM Schemer Human Windows W Comprisioners Stre	NAME OF TAXABLE	Cashed Arrest R.	\ \
1238. Wolf-and	100 Charlester	NUM Select Wood? Western W Contributors Tor	AND REPORT FORM	Control Actions 74.	1
123. Edited	100 Cambriel	C Prepare RenCarol (MP/2010-4) res ha	BLOODIN	Accelerities 21	
12	100 Million Charden	C Veget Re/Cental#1018 diaming	PLOCETT	Monate-Day 21.	
The Designation	The Control of	Company of the Constant of the Property of	weet out they	Contract in case of the	
U.S. Company	200 Challenner	HEN .	P.ACTIN	Conty Randa Inc.	
CH. Company	210 Charles	HEALING PROVIDE ADDRESS ADDRESS ADDRESS ADDRESS ADDRES	PLOCENT	Channel Access 19.	
CH. Compression	200 Challensee	HEALDON'S AND ADDIVING ADDIV	PLOCEIN .	Gen NA Same.	
A Real Property and	200 Philometer	ALL STRUCTURE ALL ALL ALL ALL ALL ALL ALL ALL ALL AL	BUTTER TOO DA	And and an other	
State State State	THE PRODUCTION	THE R. LEWIS CO., NAME AND ADDRESS OF TAXABLE PARTY.	B. CO. BRID	100.00.00	
VIII. Company on	THE PARTY AND	HEN COLUMN	3.00200	loss hadoles.	
23. Dumpton and	200 Challenter	HEM SOFTWARE Assess FACEWORK	9.000mm	Channel Access 10.	
CH. Elements	290 Challenger	HEALING AND ADDRESS AND ADDRESS ADDRES ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS	9.00207	Gery NA Safe.	
2.8. Compression	200 Challenger	NUMBER OF STREET, AND ADDREED,	BUTTER TOO DA	And and an other	
Con Company of	THE PARTY NAME	IN STRUCT Annual APPACIAL	240.000	100 100,00,00	
Name of Corner of Street of	1000701	and the strength of the streng	a voichea		

7.使機器崩潰。

8.將電腦引導至安全模式並手動收集**Procmon.pmb**和**MEMORY.DMP**,這兩個檔案都位於 C:\Windows資料夾中。這些檔案將與Cisco TAC共用。

Windows					_	8
🗸 🗸 🗸 🗸 🗸	 Local Disk (C:) Wind 	dows 👻	+ 🔯	Search Windows		
Organize 👻 📄 Open 👻	New folder)III • 🗐	
🚖 Favorites	Name A		Date modified 11/21/2010 4:24 AM	Type Application	Size 2,805 KB	
 Libraries Documents Music Pictures Videos 	 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 7/14/2009 1:06 AM	Application Application Application Text Document DMP File BIN File	15 KB 717 KB 17 KB 14 KB 331,914 KB 43 KB	
P Computer Local Disk (C:) CD Drive (D:) Shared Folders (\\vn	 msdfmap.ini notepad.exe ntbtlog.txt PFRO.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 Text Document	2 KB 189 KB 83 KB 576 KB	
🗣 Network	ProcessionalN.xml ProfessionalN.xml Professional	Type: XML Document Size: 52.3 KB Date modified: 6/10/200	1/6/2020 12:41 PM 6/10/2009 10:30 PM 339 AM 330 PM 30	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	

7.(可選)如果在C:\Windows資料夾中生成PMB檔案,則可以將其引導至「正常模式」,則如果再 次啟動ProcMon,您將看到以下日誌。通過此步驟,您可以通過按一下「儲存」按鈕重新儲存事件

0

Process Monitor - Sysintemais www.spsintemais.com			
File Edit Event Filter Tools Options Help			
Texe Process Name PED Operation: Path	final	Detel	

Paura M	antise .	Ξ
0	Ling of local-time activity was control by a previous instance of Process Mantine. Do you might to save the collected data wav?	'
	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: Pamas 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: 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	INCH Gyster Correct Control State 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 SESSION 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	
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