# 如何收集ProcMon日志以排除启动时的AMP问题

## 目录

<u>简介</u> 步骤:

### 简介

作为系统管理员,您可能希望使用进程监控器(procmon.exe)获取详细日志,以确定FireAMP连接器 在计算机启动过程中是否出现挂起。思科TAC也会请求这些日志来排除此类问题。进程监控器是一 个免费的实用程序,可帮助我们进行此操作。可以从https://docs.microsoft.com/enus/sysinternals/downloads/procmon免费下<u>载</u>

本文档介绍在系统引导过程中出现问题时如何收集ProcMon日志和内存转储(这意味着它在引导时 生成BSOD)的步骤。 需要这些日志来捕获引导期间发生的系统事件。

#### 步骤:

1.以这种方式设置测试机,使问题易于重现。

2.以管理员身份下载并运行ProcMon工具。转至"文件"—>"进程监控器备份文件"并选择路径。

trest Filter	Tools Options Help					
9 B C	ବ୍ଧ ବୋଷା 🖊 🤻					
Recent Name     Search Indexe     Search Index     Search In	PD Genetian PD Genetian 2212 A Markyson Cares 2212 A Markyson Cares 2212 A Markyson Cares 2212 A Markyson Care 2212 A Marky Genetican 2212 A Marky Genetican 2213 A Marky Genetican 2214 A Marky Genetican 2215 A Ma	Park Park Park Park Park Park Park Park	Freed SUCCESS	Detail Central FSCTL_G. Central FSCTL_R. Central FSCTL_R. Central FSCTL_R. Detail FSCTL_R. Detail File Cavey Hande Tag. Cavey Hande Tag. Cavey Hande Tag. Cavey Hande Tag. Cavey Hande Tag. Cavey Hande Tag. Cave Hande Tag. C	keen Court Converteed 19 No	
Process Martian or O Use vitualmen I Can file named Procifien load: 1.4	en stara evente in vituel nem nyry (1,70240 eveldele) C. Lierr/pet-Mid-nem Pri- (1,91 (Dryter pending) 2018 (Dryter pending)	nery (Jostad by Die system connect in Specificp/process_subject/jacit.pro NICR-dyplocters/subject and	t), or in a file you specify (initial by the SUCCISS	t dels speces). Which de you profer? Desired Accesse Ñ		an Cancel

3.在Procmon工具中,转到"选**项" — >"启用引导日志记录**"。

27 Pi	rocess Morri	tor - C:\	Users/win	7x64-rew\Desktop	piprocmon_output/test1.pml				
File	Edit Even	t Rite	Tools	Options Help					
		0.021	- A -	Alumnum	Ten I				
-		DX [	Y 🗛 1	Annalistic	rep				
Time	Process	Name	PID	Fort			Rend	Detail	
12.36	. IF Search	hdeer.	2252	Mahlahad	alar.	1	SUCCESS	Cantrol: FSCTL_Q	
12.36	LE Search	indexer.	2252	regespere	ann.		SUCCESS	Cantrol: FSCTL_R	
12:36	#?Search	hindeser.	2252	Configure	iumbola -	1	SUCCESS	Cantrol: FSCTL_R.	
12.36	Search	FilterHos	2072				SUCCESS	Thread ID: 2884	
12:36	. Epian	# DE	2988	Select Colu	mna	1	SUCCESS	Query: Name	
12.36		EXENE.	2968	Marco De	all.		SUCCESS	Query: HandleTag	
12.36	- Epper	- PAR	2368	Planoty Lep			SUCCESS	Query: Handle Lag	
12.08		E DAL	2010	Profiling Ex	anta		5000E35	Desired Access: U.	
12.36	Dela	W EXE					SUCCESS	Duesy Mande Tes	
12.36	Entre	# DE	2568	Enable Boo	t Logging	-	SUCCESS	Destract Access: N	
12.36	Deix	N EXE	2568			-	SUCCESS	Type: REG. SZ. Le.	
12.36	Epin	DE	2568	Y Show Keep	And Network Addresses Chil-N	-	SUCCESS	Aber cana "ber en :	
12.36	Epploy	NEXE	2968	Hex File Of	feets and Lengths		SUCCESS		
12:36	Epiav	# EXE	2988	Hen Dances	a and Thread IDa		SUCCESS	Query: Name	
12.36	. Bolon	B/E/E	2968			1	SUCCESS	Query: HandleTag	
12:36	🔛 Epilor	# DE	2988	RegQueryKey	HKEU/Software/Classes	1	SUCCESS	Query: Hande Tag	
12.35	Epion	er EXE	2968	RegOpenKey	HKEU\Software\Classes\.pnf\Oper\WithProgids	. 1	NAME NOT FOUN	D Desired Access: R	
12.36	🥁 Explor	#DE	2968	RegOpenKey	HKCR\pm\OperWithProgide	1	NAME NOT FOUN	D Desired Access: R.	
12.36	- Dekor	ek EXE	2968	RegQuery Key	HKCU\Software\Classes	1	SUCCESS	Query: Name	
12.36	- Epilon	# DE	2968	RegGueryKey	HKCU/Software/Cleaner	1	SUCCESS	Query: Handle Tag	
12.36	Dokor	A EXE	2968	RegQueyKey	HISCU'/Software/Classes		SUCCESS	Query: HandleTag	
12.36	- Delor	W EDE	2968	RegOpenKey	HICU'Software'Classes'Software'Microsoft'Wi	Indows/Curr1	NAME NOT FOUN	D Desired Access: R.	
12.36	- Dekon	IN EXE	2968	Registentiev	HKCR Software Morosoft Windows Current Ver	son (Explore . )	NAME NOT FOUN	D Desired Access: R	
12.36	- Diso	WEXE	2300	Regularytay	HILLU-Software Chastes	-	SUCCESS	Cuery: Name	
12.36		R/EXE	2968	Hegaueynzy	HKCU-Software Classes		SUCCESS	Guery: Handle Tag	
12.36	- Dpor	WEAE	2300	The guade your and	HILLU Software Change		SUCCESS	Desired Access: D	
12.06	- Color	EVE	2900	Barlyman	HACO SURVICE CLOSEDS (prill	and Franker	SILCCESS	Create Hendle Test	
12.36	- Entro	W EXE	2968	BacCoacKey	HILD CONVERTING CONTRACTOR CONTRACTOR	sion) Evolute 3	SIGNESS	Desired Access: R	
12.36	- Entre	I EVE	2948	Banduanter	HICLD Scheme/Mensel/Wedges/Correct/Ser	son Spring 1	SUCCESS	Overs Hande Ten	
12.35	Delte	IN FOR	2968	BacCoacKey	HICLD Software/Microsoft/Windows/Current/Art	sion' Explore 5	SUCCESS	Desired Access: R	
12.36	Enter	# DE	2568	BagQueryKey	HKCU/Software/Microael/Window/Current/int	nor Emires	SUCCESS	Query Handle Tex.	
12.36	Delor	N EXE	2968	RegOpenKey	HKEU/Software/Microsoft/Windows/Current/An	sion/Explore . 1	SUCCESS	Desired Access: Q	
12.36	Explore	# DE	2988	RegQueryValue	HICU Software (Microsoft (Windows) Current Vers	stor/Explore.5	SUCCESS	Type: REG_SZ, Le	
12.36	Califiction	BC3 W	2968	RegCloseKey	HKCU-Software/Microsoft/Windows/Current/Vers	sion'Explore .1	SUCCESS		
12.36	🔚 Epiav	# DE	2568	RegCloseKey	HKCU/Software/Microsoft/Windows/Current/Vers	sion\Explore.5	SUCCESS		
12.36	Calepton	B/E/E	2968	RegCloseKey	HKEU/Software/Microsoft/Windows/Current/Vers	sion\Explore5	SUCCESS		
12:36	🥁 Esplan	# EXE	2988	RegQueryKey	HKCU/Software/Classes	1	SUCCESS	Query: Name	
12.36	🔁 Epion	er D/E	2968	RegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36	🕞 Eplor	#DE	2988	RegQueryKey	HKCU/Software/Classes	1	SUCCESS	Query: Handle Tag	
12:36	- Epilon	er EXE	2968	RegOpenKey	HKCU/Software/Classes/Applications/indepad.e	exe 1	NAME NOT FOUN	D Desired Access: R	
12.36	- Eplan	W EXE	2968	HegOpenTay	HALH Applications indeped are	1	SUCCESS	Desired Access: R.	
1236	- Delor	K EXE	2968	Regulateray	HALH Applications violepad eve		SUCCESS	0	
12.36	Dekon	543 1	2368	riegularytay	HALU-Software Casses	1	SUCCESS	Guery: Neme	
1235	- Dekor	EVE -	2968	Hogasoyney	HALD CONTRACT COSSES	-	0000835	Guery Hande Tag	
12.35	- Copies	EVE I	2368	Page and the second	With Schemes (Second Sector Sector)		NAME NOT DO N	Deviced Access D	
12.96	Entre	EVE	2300	Begloonly	HILP American and and and	040	SUCCESS	Desired Access: R.	
12.16	Entre	N EVE	2949	Baglymore	Her Pi Androtions' ontered are		SIMPERS	Deer Name	
12.96	Feder	EDE	2948	Beglamiter	HICR Applications Insternal and		SUCCESS	Query Hendle Ten	
12.35	Derive	EVE:	2968	Barlowier	UNTIN Coffee and Changes's Applicational and a	ana) Dishlar 1	NAME NOT ON BUILDING	Differing Access D	

4.选择"生**成威胁分析事**件并**每秒"。** 

🎒 Proc	Process Monitor - C/\Users\win7\64-new\Desktop\procmon_output\test1.pml							
File Ed	lit Event Filte	r Tools Options Help						
- 2 E		👄 A 🚓 🖻 🗛 🗖						
		A 🖶 ØA   🖬   🖬 🤞						
Time	Process Name	PID Operation	Path		Result	Detail		
12:36:	Searchindexer	2252 ReSystemContro	AC:		SUCCESS	Control: FSCTL_Q		
12:36	Searchindexer		AC:		SUCCESS	Control: FSCTL_R		
12:36	S Eachla Rea	ot Longing			SUCCESS	Control: FSCTL_R		
12:36	ES CHARGE DO	or coyying			SUCCESS	Thread ID: 2884		
12:36	Barrens M	with can penerate thread on	Allon events that can use		SUCCESS	Query: Name		
12:36	E the state	of all running applications at a r	equiar interval.		SUCCESS	Query: HandleTag		
12:36:	20				SUCCESS	Query: HandleTag		
12:36	📜 E 📝 Ger	verate thread profiling events			SUCCESS	Desired Access: Q		
12:36	E	(B. Every second			SUCCESS	Query: Name		
12:36:	<b>1</b>	<ul> <li>Every second</li> </ul>			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			OK Cancel		SUCCESS			
12:36	H			1	SUCCESS	ô		
12.36	Explorer EXE	2355 Reguleykey	HNLU Calification Classes		SUCCESS	Query: Name		
12.36	Diblove, EVE	2300 ReguleryNey	HNLU Software leases		2000622	Guery: Handle Tag		
12.35	Explorer EXE	2565 Kineguuerykey	HNLU Software Classe	Country Design	SUCCESS	Query: Handle Lag		
12.05	Explorer EXE	2305 Regupenkey	HNLU (Software Classes (prin)	OpenwithProgram	NAME NOT FOUND	Desired Access: H		
12.39	Englow EVE	2900 Reguperivey	UNCLE Calculation (Classes)		CLICCECC	Oversi Name		
12:30	Europer EVE	2900 ReguleryNey	HMC0 Contware Classes		CI INTERE	Query, Name		
12-36	Evolowy EXE	2988 Back and an	HKC1D Software Classes		SUPPESS	Query Hande Tag		
12.36	European EVE	2988 BasCoasKey	HK/TI/ Software/Classes/ Softw	The Company Manager (man	NAME NOT FOUND	Designed Access: R		
12:36	Funitowr EXE	2988 BenOpenKey	HICE\Software\Monsoft\W/r	dows\QueentVersion\Explore	NAME NOT FOUND	Desired Access: R		
12-36	Epolow EXE	2988 RecQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name		
12:36	Evolover EXE	2988 RecQueryKey	HKCU/Software/Classes		SUCCESS	Query Hande Tao		
12:36	Explorer EXE	2988 RegQuer/Key	HKCU/Software/Classes		SUCCESS	Query Hande Tag		
12:36	Epplorer EXE	2988 RegOpenKey	HKCU\Software\Classes\.pml		SUCCESS	Desired Access: R		
12:36	Explorer EXE	2988 RegQueryKey	HKCU\Software\Mcrosoft\Wr	dows\CurrentVersion\Explore.	SUCCESS	Query: Handle Tag		
12:36:	Explorer EVE	2988 RegOpenKey	HKCU/Software/Mcrosoft/Wir	dows\CurrentVersion\Explore.	SUCCESS	Desired Access: R		
12:36	Eplorer EXE	2988 RegQueryKey	HKCU/Software/Mcrosoft/Wir	dows\CurrentVersion\Explore.	SUCCESS	Query: Handle Tag		
12:36	Explorer EXE	2988 RegOpenKey	HKCU\Software\Microsoft\Wir	dows/Current/Version/Explore.	SUCCESS	Desired Access: R		
12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Mcrosoft\Wir	ndows\CurrentVersion\Explore.	SUCCESS	Query: HandleTag		
12:36	Eplorer EXE	2988 RegOpenKey	HKCU/Software/Mcrosoft/Wir	dows/Current/Version/Explore.	SUCCESS	Desired Access: Q		
12:36	Explorer.EXE	2988 RegQueryValue	HKCU\Software\Microsoft\We	dows\CurrentVersion\Explore.	SUCCESS	Type: REG_SZ, Le		
12:36	Epplorer.EXE	2988 RegCoseKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore.	SUCCESS			
12:36	Biplover EXE	2988 KegCloseKey	HKCU/Software/Microsoft/Wir	dows/Current/Version/Explore.	SUCCESS			
12:36	Biplover EXE	2988 RepCoseKey	HKEU\Software\Mcrosoft\We	dows/Current/Version/Explore.	SUCCESS			
12:36	Biplover.EXE	2900 RegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name		
12:36	Explorer EXE	2388 RegQueryKey	HRCU Software Classes		SUCCESS	Query: Handle Tag		

5.确保在Procmon中选择所有相关过滤器并收集数据。

6.如果无法复制崩溃,则可以使用NotMyFault64.exe实用程序强制Windows崩溃,您可以从该实用 程序获取 <u>https://live.sysinternals.com/files/</u>

有关如何运行这些命令的说明如下: <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

	Process Westlan - Cit	Anti-the new Deliver	Personal and Ard and			
	the dat durit the	Scale Options Fide				
Im       No.       No.       No.       No.       No.         Im       No.       No.       No.       No.       No.       No.       No.         Im       No.	1 B C C	🕈 🛓 🕹 🖄 🛤 🖣				
11       10       No.       No.       No.         12       10       No.       No.       No.         12       10       No.       No.       No.       No.         12       10       No.       No.       No.       No.       No.       No.         12       10       No.       No.       No.       No.       No.       No.       No.         12       10       No.	Ins., Peopletane	PD Geetter	Fat	Feat	Ownel	
	238. Whitee	100 Bulletin	C Proper NorConcell* 251 Allowing	9.00201	Ofer (2004.007)	
	23. KM #	170 Datablerate	C Prepar RenCash 487-3554Leeutra	100000	WanaCeator Te.	
	23. 10.00	The last widow	C Wegen Rendem AMP 11141 des top	a reaction of the	Outer free 14V.	
	10.00	The Charleston	18. M Schwart Rouged Western 17 Constitution for	NAME AND POST	Classed Arrest R	
	1238 KM #	170 Charlester	18, M Schwart Human Western W Constitution for	NAME AND POST	Chanal Access 10	
	23. KM #	170 Pelandarded	Wegen NerCennikh 115 All de ha	100.000	Access for 2	
	20.000	THE REAL PROPERTY.	Program Rest and with 110 all see by	100000	The Avenue	
<pre>Number Number Numb</pre>	23. 810.00	170 Bellamintonam	Compan Rendering All 111 All pering	9.40.000	internel matter from	
<pre>Numerican set in the set in</pre>	23. Exten	170 Automation	Entropy Number (2014) (2014) (2014)	BUTTER DUPPE.	Department of the	
<pre>Numerican section section</pre>	23. KW.ee	The Contraction	18, M Scheger Human Weather 17 C prestrement Sta	And the state	Change Access 7	
<pre>style="target_relation_re</pre>	Contraction of the local division of the loc	The second section	18 M Schwart Human Western 17 Cutatilance In	NAME OF TAXABLE	Canada Access 10	
<pre>Numerican section section</pre>	CH. ENLINE	100 Manchestert	E Vegen NerCennikk (151-b) av 19	9.00205	Accession (R.	
<pre>Numerican section section</pre>	23. Exten	110 Moundanted	Proper Nerclass AM 1114Cae by	10.00	Access for 2	
<pre>Ret = ret = r</pre>	22. 10.44	The second	Company New York and Print Atlanting	1.41.200	the post of	
<pre>style="tabular type: type</pre>	20.000	The second second	Property Services and Think on the	a press lutters.	Castor Ing. 16	
<pre>Not in the interval inter</pre>	CH. ENLINE	The Paginetter	18,14 Selvery Hoteld' Medice 17 Carethesen Inc.	NAME AND POST	Constant Access 10	
<pre>style="tabular style="tabular s</pre>	28. Exten	The Indiana in the	TRUE Schwarz (Actual) Medice 171 ( January South	NAME OF TAXABLE	Name Arrest R.	
<pre>style="table_</pre>	22. 20.40	The second	The Monte Second Works of Calendration In	A COMPANY OF THE OWNER	Classif Arcass PL	
<pre>style="task type="task type=</pre>	20.000	1 In this part of the second	Company Report and All 11 Public day by	TAX POL	Accession in	
0         0	Cit. Extras	THE BUNNIN	( Vegan NerCental P (1) 540 and 10	940.005	The 21 YO	
Visite	28. Exten	100 Buckle	Proper NerCent AP Netro B	9.40 (995	Delane half.	
<pre>style="bit_style=</pre>	22-22-20	THE REAL PROPERTY.	Proper Nerces AP 1411.0	10000	Colored Page 11	Deterration Civiliant Civiliant Civiliant
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	20.000	In alasta	Company Residence and Property de Journal	want out that	Consult Arran P.	Enderstand signified areas
<pre>style="type://www.systems/systems</pre>	Cit. Exten	100 Britstin	Compan NerCass AMP Index &	9.00895	the Allege	Endowing a first sector of the trage of the trade of the
<pre>style="table_partial_grammation_partial_gramma</pre>	28. EX.44	110 Billeonfe	Proper Net Cech 48P trace do nat	NAME OF PERSON	Classe Array P.	the second se
<pre>start is the start is the</pre>	20.000	The second second	Comparing the Card of Print and	2.40 200	other 1475 March	The second
<pre>style="task style="task s</pre>	20.000	110 Bulgarintenan	Company Rest Card All P. 711 State and Inc.	0.40000	where a start in	WARE CITAL RADIES OF THE BODY
<pre>visit visit v</pre>	U.S. Error	110 Alban Winters	C Proper Net/Cect-MP1711141-awing	Burner Surry	Depter Ing. 16.	Resolution of Conference Solution and Advances
<pre>visit visit v</pre>	28.004	The Indiana and	HEAD SHOW INCOME VIEW AND A CONTRACT IN	NAME OF TAXABLE	Classe Arrest P.	PL/95/2020 15:029 87 02120 Press/Planting
0       0	20.000	100 Charlester	visit in the second strategy of Complement In	NAME OF TAXABLE	Castral Array 6	
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	U.M. Kirkan	100 million/hardwrite	C Propert RenCentral Print Atoms by	9.400898	Accelerities 20.	87-86-1018 (3)-10 - 10 - 10 - 10 - 10 - 10 - 10 - 10
<pre></pre>	U.S. Erten	100 Bilanchardert	C Proper NetCent 48*/718 at secile	9.40995	Rentedos 3.	TO RECEIPT TO A DECEMBER OF THE PARTY OF THE
10       10 <t< td=""><td>20.000</td><td>IN ANY A</td><td>C Proper Ner Central P (11) At sea by</td><td>0.41.000</td><td>One Nonite</td><td>1 Martin 20, 407 (1997) States from</td></t<>	20.000	IN ANY A	C Proper Ner Central P (11) At sea by	0.41.000	One Nonite	1 Martin 20, 407 (1997) States from
<pre></pre>	10.000	110 Alandining	C Proper Rev Card diff. 71 Put you be	a prist party.	Castor Ing. 14	Environmental a Patiet mana diseli tragicat. Ega Essena Judia (se
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	U.M. Kirkan	110 Charleette	HEAP School (Reset) Western 10 Caretrianter In-	NAME NOT FORM	Contrast Access 14	to have been built and believe the terms believe by the terms of a second second
<pre></pre>	128. Exten	110 Challentin	HCM Orbany (Reserved) Ventree 10 Carentiesers In-	NUM HOT FORM	Classed Arrest R.	
1       1	20.000	The Page Service	HEAP Official Menade Western In Carentineers In	And Her Pope	Castle Arrest P.	Exclusion and a both same disclosured on internet of a first factor disclosed on a surgeon and a series
10 mm       10 mm <td< td=""><td>10.000</td><td>100 Alambarian</td><td>C Proper Rev Cent (187-117 at use by</td><td>0.0000</td><td>Rentring 3.</td><td></td></td<>	10.000	100 Alambarian	C Proper Rev Cent (187-117 at use by	0.0000	Rentring 3.	
0         0	U.M. Kirkan	100 Advarte	C Proper RenCentatiff (118 alcone by	9.40895	Ofer 25,001425	
0         0	12.00. E.M. and	100 Cardelenate	C Prepar Rel Central Print House by	9.60891	Ware age in	1
1         1	20.000	The Day Street or a	2 Physics Net Class (MP 121) drives by	and out they	Comparing 14	1
10         1         0	10.00	100 Charlestin	HEAD Information and Advance of Complement In-	And NOT YORK	Castral Array R.	1
0.0         0.0         0.0         0.00         0.000<	U.M. Kirkum	100 Challenties	HEM School Honsell Western 10 Carentineers Inc.	AND REPORT	Costral Acres #	1
1         1	10.0	100 Million Review	C Wegen RenCennal#1018 at weite	B.CORT	Accelerities 21.	1
U.S. Marken         U.S. Markenske, J. Angen Ruchard M.D. Markenske, J. Markenske,	12	100 Advarta	C Proper Rev Card diff (1) if do not be	0.0000	Ofer Distant	1
U.S. (A. Marcon, U.S., Marcon, M.S. (A. Marcon, Marcon, M.S. (C. Mar	1218 . Whitem	100 Alberthmate	C Vegen RenCard (MP/2018 at use by	0.0000	Ware Ceptor Te.	\ \
1         0.0.000         10.0.000         0.0.00000         0.0.00000         0.0.00000         0.0.00000 <td< td=""><td>12.00. El Marco</td><td>100 BalanyWeisen</td><td>2 Proper RenCennet#1018 at use he</td><td>BUMPHONEWL</td><td>Outer Ine 16</td><td>1</td></td<>	12.00. El Marco	100 BalanyWeisen	2 Proper RenCennet#1018 at use he	BUMPHONEWL	Outer Ine 16	1
10         10<	10.0	The Propose Figs	HEM Scheme Human Western 17 Carentineers for	And set your	Changed Arress R.	1
No.         No.         No.         No.         No.         No.           100         100         100         100         100.000         Reservice 3.         0.000         Reservice 3.         0.0000         Reservice 3.         0.00000         Reservice 3.         0.000000         Reservice 3.         0.000000         Reservice 3.         0.0000000         Reservice 3.         0.000000000	10.00	120 Charlestin	HE M Information of Manual Victoria and Company and In-	and set they	Contract Access 10	1
U.S.         M.M.         U.S.         Maximum Control (1)	1218 Wolfsman	100 albanhavieri.	C Proper RenCennist#1018 at use ha	PLOCENT.	Access for 21	
Unit         Unit <th< td=""><td>1238. 8 141.000</td><td>100 Manchesteri</td><td>C Propert Ren Carlo (687-257 all less ha</td><td>PLOOPIN</td><td>Access Sec 2.</td><td></td></th<>	1238. 8 141.000	100 Manchesteri	C Propert Ren Carlo (687-257 all less ha	PLOOPIN	Access Sec 2.	
101         Compose 201         C	U.S. WHAT	TOUR ACCOUNTS	C Prepar RenCennatif 111 et an ha	1.0.01	Own 25 Official	
VI.0         Computation	Co. Company on	TRD Charlesone	C Property of the second s	0.0000	Game Rando Inc.	
U.S.         Unsubure         U.S. Unsubure	U.S. Concern	210 Challenne	HEM SOFTWARE Associative Decision	PLOCEIN	Change Access 10.	
U.S. Companya 200         Description 200         Descript	CH. Compression	200 Challense	NEM COTTAGE Assess ADDICING IN	PLOCETT.	Gen NA Safe.	
No.         Displayment         Displayment <thdisplayment< th=""> <thdis< td=""><td>Contraction of the local division of the loc</td><td>200 Philomited</td><td>THE MOST NAME ADDRESS OF THE OWNER</td><td>BUTTER TOO DA</td><td>And the other</td><td></td></thdis<></thdisplayment<>	Contraction of the local division of the loc	200 Philomited	THE MOST NAME ADDRESS OF THE OWNER	BUTTER TOO DA	And the other	
VI.R.         Displaymentary         Displaymentary </td <td>C.M. Company on</td> <td>200 Charles</td> <td>NEW COTTONY AND ADDRESS OF</td> <td>9.00200</td> <td></td> <td></td>	C.M. Company on	200 Charles	NEW COTTONY AND ADDRESS OF	9.00200		
VID:         Displayments         Displayments         Displayment         Displayment <thdisplayment< th=""> <thdisplayment< th=""> <thd< td=""><td>23 Comproment</td><td>290 Challenter</td><td>na_s</td><td>P-00201</td><td>Day Antrible</td><td></td></thd<></thdisplayment<></thdisplayment<>	23 Comproment	290 Challenter	na_s	P-00201	Day Antrible	
1         0	CH. Evennue	200 Charles for	NUMBER AND ADDRESS OF ADDRES	NOCEN	Chanal Access PL	
22 Foreneses     20 Programme     2	State State of State	THE PRODUCTS	THE R. LEWIS CO., Name of Address of Address of Address	B PERSON NUMBER	Care N. Lare.	
2.8 Eventures ID Eventure ID Eventure ID Eventure Although Although ID	CH. Company on	CHO Charlenson	NEM SOFTWARE ADDRESS ADDRE	9.0.00	New PEDLAT In-	
Bening 13,33 of 45,841 assess 2014 Eacher to Character And Anna Charling Internet Anna Anna Charling Internet Anna Anna Anna Anna Anna Anna Anna Ann	CH. Evenness	210 Charles	HALM SOFTWARE ADDRESS ADDRESS ON ON	9.00205		
	Showing SOUTH of MICHIN	and WU B	what he Critican win Add man the Region on which the	af Aur Currel		

#### 7.撞机。

8.将计算机引导到安全模式并手动收集**Procmon.pmb和MEMORY.DMP**,两**个文件都**在C:\Windows folder中。这些文件将与思科TAC共享。

J Windows					_	8		
🚱 🖓 🖉 🗸 Compute	r 🔻 Local Disk (C:) 👻 Win	dows 🔻	÷ 📴	Search Windows				
Organize 👻 🗋 Open 🔹	New folder				)= • 🖬			
🚖 Favorites	Name A		Date modified 11/21/2010 4:24 AM	Type Application	Size 2,805 KB			
<ul> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> </ul>	fveupdate.exe HelpPane.exe hh.exe IE11_main.log MEMORY DMP		7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM 1/30/2018 3:52 PM 1/5/2020 12:41 PM	Application Application Application Text Document	15 KB 717 KB 17 KB 14 KB			
Computer Local Disk (C:) CD Drive (D:) Shared Folders (\\vn	mib.bin msdfmap.ini notepad.exe ntbtlog.bt		7/14/2009 1:06 AM 6/10/2009 10:36 PM 7/9/2015 7:57 PM 1/6/2020 12:41 PM 1/6/2020 12:30 PM	BIN File Configuration sett Application Text Document Text Document	43 KB 2 KB 189 KB 83 KB 576 KB			
🗣 Network	<ul> <li>Procmon.pmb</li> <li>ProfessionalN.xml</li> <li>regedit.exe</li> <li>setupact.log</li> <li>setuperr.log</li> <li>splwow64.exe</li> <li>StarterN.xml</li> </ul>	Type: XML Document Size: 52.3 KB Date modified: 6/10/20	1/6/2020 12:41 PM 6/10/2009 10:30 PM :39 AM :30 PM :30 PM :30 PM 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 Date modified: 1/6/2020 12:41 PM PMB File Size: 313 MB Date created: 1/6/2020 12:41 PM								

7.或者,如果PMB文件在C:\Windows folder文件中生成,则如果能够将其引导到"正常模式",则如 果再次启动ProcMon,将看到以下日志。从而,您可以通过点击Save按钮重新保存事件。

Precess Monitor - Sysintemels: www.sprintemak.zam			
File Edit Event Filter Tools Options Help			
Image: State and State			
Tine Pourse Name PD Operation Path	final	Detel	



_
Genet

🔰 Process Monitor - Sysi	internals: www.sysinternals.	com		
File Edit Event Filter	Tools Options Help			
📽 🖬 🔌 🕸 🖾 🛛	⇒ <b>∆</b> ⊕ 🖲 🖊 🖣			
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	INCH Gyster Correct Control State Control SESSION MANA.	CUCCESS	Index 0 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 ResEnceValue	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	
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