## 起動時にAMPの問題をトラブルシューティング するためにProcMonログを収集する方法

内容

<u>概要</u> 手順:

## 概要

システム管理者は、プロセスモニタ(procmon.exe)を使用して詳細なログを取得し、コンピュータ の起動プロセス中にFireAMPコネクタがハングするかどうかを確認できます。これらのログは、 このような問題のトラブルシューティングのためにCisco TACから要求されます。Process Monitorは無料のユーティリティで、ここで役立ちます。これはhttps://docs.microsoft.com/enus/sysinternals/downloads/procmonから自由にダウンロードで<u>きます</u>

このドキュメントでは、システムブートプロセス中に問題が発生した場合(つまり、ブート時に BSODを生成している場合)に、ProcMonログとメモリダンプを収集する手順について説明しま す。 これらのログは、ブート中に発生するシステムイベントをキャプチャするために必要です。

## 手順:

1.試験機を簡単に再現できるようにセットアップする。

2.管理者としてProcMonツールをダウンロードして実行します。[File] -> [Process Monitor] [Backing Files]の順に選択し、[Path]を選択します。

g Pro	ons Monitor - C/(De	ari, ini da	new/Deakter	/processor.pd	tpot/soit1.ped								
nie D	At tweet Filter	Teols Opt	ions Help										
	Property lines	A 90		P LONGPON			En t	Dated					
1236 1236 1236 1236 1236 1236 1236 1236	Searchindear     S	200 a 44 200	EpitenCore EpitenCore EpitenCore read Create gCore Ray gCore Ray gCore Ray gCore Ray gCore Ray	IC IC IC IC IC IC IC IC IC IC IC IC IC I	v Cases v Cases v Cases v Cases v Cases), pri v Cases), pri		SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Cantol FSC Control FSC Cantol FSC Cantol FSC Deard FSC Canty Name Canty Name Desired Acce Gamy Name	L.Q. L.R. M M M M King K Q.				
236	Precess Monitor	Backing File											
2.36	These backing file of	tjects are beit	queed to sto	re event datas									
1236	Name				Event Court	Event Bytes	Pending Events	Process Court	Octoney Court	keen Count	Connected		
	Citteryaniste	rev Cestop	\$00000_04	pur reen t per	106.123	40.001.00	5	50	1.04	3	Te.		
12.36	Process Haritar cen	store events	an official rear	sary (inited by)	the system convert lan	<li>c) or in a file you is</li>	pecify (initial by the	det spece). 10hzh	de you prefer?				
236	O Use vitual new	ry (0,7224	(articles)										
236	@ Use Renamed:	Cilibera	per544-se	(Desiting (proce	en_pulpuf(bell.pri								-
12.34													
236	Pro/Honipad: 0.49	s ext bird	(pribreq ed									x	Canot
1236	Externe DE Externe DE Externe DE	2343 44 2343 44 2343 44	адаран Кар адаран Кар адарану Кар	HCR Application HCR Application HCR Application	tora' vehicad and tora' vehicad ave tora' vehicad ave		SUCCESS SUCCESS SUCCESS	Duared Acce Guery Name	# Ř.				

3. Procmonツールで、[Options] -> [Enable Boot Logging]に移動します。

🎒 Pn	ocess Monite	ter - C:\	Users\win	7x64-rww\Desktop	piprocmon_output/test1.pml				
File	Edit Event	Filter	Tools	Options Help					
l el f		P.L.	- A -	Alumnum	Too 1				
			V 🗛 🤉	Adversion	rep				
Tree .	Process N	lare .	PID	Fort			Renit	Detail	
12:36:	. #*Searchi	rdeer.	2252	Hablaht	alara -		SUCCESS	Cantrol: FSCTL_Q.	
12.36:	. El Search	ndeser	2252				SUCCESS	Canbol: FSCTL_R	
12:36:	. #!Search	rckeer.	2252	Configure	Symbols	1	SUCCESS	Cantral: FSCTL_R.	
12.36:	<ul> <li>Searchi</li> </ul>	RerHos.	. 2072	er ici			SUCCESS	Thread ID: 2884	
12:36:	- Delow	EXE	2568	Select Colu	mna		SUCCESS	Query: Name	
12.36:		EVE	2968	Mater De	-th	-	SUCCESS	Query: HandleTag	
12:36:	- Epon	EVE.	2366	reactly be	in.		SUCCESS	Guery: Handle Leg	
12.36.		EVE.	100	Profiling Ex	ants		3000535	Desred Access. U.	
12.36	- Depore	EVE					SUCCESS	Duesy Mande Tes	
12.36	- Colore	EVE .	2588	Envible Boo	t Logging		0000000	Centred Access M	
12.36	Detan	EXE:	2568				22322010	Tute BEG S7 In	
12.36	Enior	EVE .	2548	V Show Resol	Ived Network Addresses Chi+N		SUCCESS	We ned the wo	
12.36	Entition	EXE	2948	Hex File Of	feets and Lengths	-	SICCESS		
12.36	Emission	EVE	2588		175-110-		SUCCESS	Overv: Neme	
12.36	Eciore	EXE	2968	Pills Proces	a and i hread the	-	SUCCESS	Query HandeTag	
12:36	Emigra	EVE	2988	Requerter	HKEU/Software/Classes		SUCCESS	Query Hande Tag	
12:36:	Ectore	EXE	2968	RegOpenKey	HKEU/Software/Classes/.pnf/Open/WithProvids	1	NAME NOT FOUND	Desired Access: R	
12:36	Eplow	DE	2988	RegOpenKey	HKCR\pm(\OpenWithPropide		NAME NOT FOUND	Desired Access: R.	
12:36:	- Epiore	EXE:	2968	RegQuer/Key	HKCU/Software/Classes	1	SUCCESS	Query: Name	
12:36	Epkow	DE:	2968	RegQueryKey	HKCU/Software/Cleaner	1	SUCCESS	Query: Handle Tag	
12.36:	. Dolore	EXE:	2968	RegQueyKey	HKCU/Software/Classes	1	SUCCESS	Query: HandleTag	
12.36:	- Cipiow	DE	2568	RegOpentary	HICU/Software/Cleases/Software/Microsoft/We	ndews\Curr1	NAME NOT FOUND	Desired Access: R.	
12.36:	. Cabelore	EDE:	2968	RegOpenKey	HKCR\Software\Microsoft\Windows\CurrentVers	ion'Explore.1	NAME NOT FOUND	Desired Access: R	
12:36:	. 🔚 Epiaw	DE	2988	RegiouryKey	HKCU/Software/Classes	5	SUCCESS	Query: Name	
12.36:	. Cabelore	EDE:	2968	RegQueryKey	HKCU-Software/Classes	1	SUCCESS	Query: HandleTag	
12:36:	- 🕞 Epiore	DE	2568	RegCosyllay	HICU/Software/Classes	1	SUCCESS	Query: HandleTag	
12:36:	<ul> <li>Bplote</li> </ul>	EVE	2968	RegOpenKey	HKEU\Software\Classes\pnl		SUCCESS	Desired Access: R	
12:36:	. Epicer	EXE	2968	RegGueryKey	HKEU/Software/Microsoft/Windows/Gurrent/Vers	sion \Explore . 3	SUCCESS	Query: Handle Tag	
12.36:	- DEKORS	EXE	2968	RegOpenikey	HKEU/Software/Microsoft/Windows/Current/Jers	son Explore	SUCCESS	Desired Access: R.	
12:36:	- Diplore	EXE	2968	Regularyflay	HKLU/Software/Microsoft/Windows/Eurent/Vers	sion \Explore 3	SUCCESS	Query: Handle I ag	
12.36:	- DOOTS	SAG	2968	Hegupenkey	HKLU-Software Microsoft Windows Current Vers	son Explore	SUCCESS	Desired Access: R.	
12.36.	Desaw	243	4366	rieg avery fary	HALU Software Official Overdene surrent vers	son Vooplore . 3	SUCCESS	Galery: Handle Leg	
12.36		0.00	2444	Burghundhin	HALO SOTWAR ORODOL OFFICERS CONST. HAS	son Explore	SUCCESS SUCCESS	Deared Access, u.,	
12.36	- Ectore	EVE	2544	Bay Conten	1997 19 Software Greenwell Windows Proved And	inch Evolute 1	SINCESP SINCESP	type: rana_aw, we	
12.36	Enlos	EVE	2488	Ban has fee	HICLD Software Microsoft Windows Const Vers	tori Emine	RUCCERS		
12.36	Entitive	EVE	294.8	Bay Dockey	HET ID Software/Microsoft / Windows/Consoft/Jerry	ion) Funiture 1	22330012		
12:36	Enlow	EVE	2988	BegQueryKey	HICU/Scheare/Classes	1	SUCCESS	Overv: Neme	
12:35	Facing	EXE	2988	BenQuenter	HKE1D Software/Classes	-	SUCCESS	Duey HandeTan	
12:36	Emission	EVE	2988	BegQueryKey	HKEU/Software/Classes		SUCCESS	Query Hande Teo	
12:35	Epitore	EXE	2968	RegOpenKey	HKEU/Software/Classes/Applications/Instead et	1 100	NAME NOT FOUND	Desired Access: R	
12:36	Eplow	DE	2968	RegOpenKey	HKCR'/Applications'/rotepad are	1	SUCCESS	Destred Access: R.	
12:35	Delow	EXE	2968	RegCloseKey	HIKCR' Applications' instepad eve	5	SUCCESS		
12:36	Epiow	DE	2568	RegilizeryKey	HKEU/Software/Cleaner	-	SUCCESS	Query: Name	
12:36:	Delow	EXE:	2968	RegQueryKey	HIKEU//Software/Classes	1	SUCCESS	Query: HandleTag	
12:36:	- Calipiow	DE	2568	RegilizeryKay	HICU/Software/Classes	1	SUCCESS	Query HandleTag	
12.36:	- Bolore	EDE:	2968	RegOpenKey	HKCU/Software/Classes/Applications/instepad.et	1 94	NAME NOT FOUND	Desired Access: R.,	
12:36:	. 🔚 Epiaw	DE	2568	RegOpenKey	HKCR'Applications'/notepad asse	5	SUCCESS	Desired Access: R.,	
12:36:	Epipe	EXE :	2968	RegQueryKey	HKCR'Applications' notepad eve	1	SUCCESS	Query: Name	
12:36:	. 🙀 Epiow	DE	2988	RegGueryKey	HKCR'/Applications'/notepad asse	1	SUCCESS	Query: HandleTag	
12:35	Deliver	EVE	7966	Can Doan Ker	UST IN Colleges (Theses) And references and a	and Distance 1	NAME NOT ON NO	Desired Brower D	

4. [Generate threat profiling events]と[Every second]を選択します。

🎒 Proc	Process Monitor - C:\Users\win7x64-new\Desktop\procmon_output\test1.pml							
File Ed	sit Event Filte	r Tools Options Help						
- c2 🗖		💀 A 🖧 🖹 🗛 🗖						
		A 🖶 Ø. 🖬 🖬 🤞						
Time	Process Name	PID Operation	Path		Result	Detail		
12:36:	Searchindexer		AC:		SUCCESS	Control: FSCTL_Q		
12:36	Searchindexer		NC:		SUCCESS	Control: FSCTL_R		
12:36	S Eachla Day	at Longing		)	SUCCESS	Control: FSCTL_R		
12:36	P.S. Chaose Dos	n cogging			SUCCESS	Thread ID: 2884		
12:36	Bencare M	collect can canacata thread or	floor events that can use		SUCCESS	Query: Name		
12:36	E the state	of all running applications at a r	equiar interval.		SUCCESS	Query: Handle Tag		
12:36	G		and the test		SUCCESS	Query: HandleTag		
12:36	🔚 🛛 🖓 Ger	erate thread profiling events			SUCCESS	Desired Access: Q		
12:36	Care I	S frances and			SUCCESS	Query: Name		
12:36	<b>6</b>	<ul> <li>Every second</li> </ul>			SUCCESS	Query: Handle Tag		
12:36	<b>1</b>	Every 100 milliseconds			SUCCESS	Desired Access: M		
12:36	E			(Default)	SUCCESS	Type: REG_SZ, Le		
12:36	<b>a</b> 6		OK Cancel		SUCCESS			
12:36	H			1	SUCCESS			
12:36	Explorer.EXE	2988 RegQueryKey	HKCU/Saltrage/Classes		SUCCESS	Query: Name		
12:36	Diplorer EXE	2965 KegGueryKey	HNCU Software relations		SUCCESS	Query: Handle Tag		
12.36	Diplorer EXE	2966 KegGuerykey	HNLU Software Classe	A second and a second	SUCCESS	Query: Handle Tag		
12.95	Explorer EXE	2966 Aregupenkey	HKLU (Software Classes ) priv	Openwithmogids	NAME NOT FOUND	Desired Access: H		
12.30	Diplorer EXE	2900 Regupenkey	HNUH pris upen vien rogids		NAME NOT FOUND	Desred Access: H		
12.30	Evolution EVE	2500 ReguleryNey	HNCO (Software Classes		SUCCESS	Query, Name		
12.90	Evolution EVE	2988 Reguleryney	HIGHT Software Classes		SUCCESS	Query, Hande Tag		
12.30	Europer EVE	2900 Pagadeyney	LWC11, Colturant/Chasses/ Coltu	and American Million and Million	NUME NOT FOUND	Designed Access: P		
12-36	European EVE	2988 PagOpanKay	HICTO Converse Microsoft Mic	vious/Current/Jamion/Evolume	NAME NOT FOUND	Desired Access D		
12-36	Enjoyer EXE	2958 BacQuerter	HKC10 Software/Classes	Service report Seport.	SUCCESS	Query Name		
12:36	Funitiver EXE	2928 RenOverview	HKC10 Software/Classes		SUCCESS	Query HavdeTan		
12:36	Enjow EXE	2958 RecQueryKey	HKCLI/Software/Classes		SUCCESS	Query Hande Tag		
12:36	Epolorer EXE	2988 RecOpenKey	HKCU/Software/Classes/Loni		SUCCESS	Desired Access: R		
12:36	Epplorer EXE	2988 RecQueryKey	HKCU\Software\Microsoft\We	ndows\CurrentVersion\Explore	SUCCESS	Query: Handle Tao		
12:36	Epplorer EXE	2988 RegOpenKey	HKCU/Software/Microsoft/Wir	ndows\CurrentVersion\Explore	SUCCESS	Desired Access: R		
12:36	Epplorer.EXE	2988 RegQueryKey	HKCU/Software/Microsoft/Wir	ndows\CurrentVersion\Explore	SUCCESS	Query: Handle Tag		
12:36	Explorer.EXE	2988 KegOpenKey	HKCU\Software\Microsoft\We	ndows\CurrentVersion\Explore	SUCCESS	Desired Access: R		
12:36	Epplorer.EXE	2988 KRegQueryKey	HKCU/Software/Mcrosoft/W/	ndows\CurrentVersion\Explore.	SUCCESS	Query: HandleTag		
12:36	Biplorer EXE	2988 RegOpenKey	HKCU/Software/Mcrosoft/Wir	ndows\CurrentVersion\Explore.	SUCCESS	Desired Access: Q		
12:36	Explorer.EXE	2988 RepQueryValue	HKCU\Software\Microsoft\We	ndows\CurrentVersion\Explore.	SUCCESS	Type: REG_SZ, Le		
12:36	Explorer.EXE	2988 KRegCloseKey	HKCU/Software/Microsoft/We	ndows\CurrentVersion\Explore.	SUCCESS			
12:36	Explorer.EXE	2988 KegCoseKey	HKCU/Software/Mcrosoft/W/r	ndows\CurrentVersion\Explore.	SUCCESS			
12:36	Explorer EXE	2988 RepCoseKey	HKCU\Software\Mcrosoft\Wr	ndows/Current/Version/Explore.	SUCCESS			
12:36	Biplorer.EXE	2908 RegQueryKey	HKCU\Software\Classes		SUCCESS	Query: Name		
12:36	Explorer.EXE	2388 RepQueryKey	HKCU/Software/Classes		SUCCESS	Query: Handle Tag		

5.関連するすべてのフィルタがProcmonで選択され、データが収集されていることを確認します。

6.クラッシュを複製できない場合は、NotMyFault64.exeユーティリティを使用してWindowsを強制的にクラッシュさせることができます。このユーティリティは、Windowsから取得できます https://live.sysinternals.com/files/

これを実行する手順は次のとおりです。 <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

Printer Printer Cold	And the second second	Charles with a set first			
CR CAR FROM	Tools Opening Fact				
a Poos tara	PD Geester	Path	Fead	Gent	
S. Eldine	100 Bulletin	C Prepar RenCencil#10184.embp	9-00201	Ofer (\$109-107	
	The Description of the	Company New Case with 11 Million 10	5.0.00	Contraction of the	
	The last states	C Proper Ner Carrielle C 1140 en 19	a second second	Contraction 100.	
	The second second	The Manager Human Company of Company and the	and so it is a	Contract Access 1	
	The second second	18 M Schwart House & Munice M Complement for	And the Party of the	Constant Access 1	
a la	1107 Million American	1 Annual Residence and 111 All and 10	2.41700	decase for 12	
E Blatters	100 Manhandard	C Wegner RenCept ald? 111 All der bg	9.41.2215	Accessible (2)	
<ol> <li>K. M. and</li> </ol>	100 Bulletie	C Wegen RenCash AM 11140 are by	9.40.2215	(Ref. (5.000.00))	
<ol> <li>Kirken</li> </ol>	170 Datablanati	Companition and American Advances in the	9,00205	iduralization fra-	
<ul> <li>Element</li> </ul>	170 Automation	C Vegan RenCecular (1114) avia	\$,0000 (MOV).	Department 151	
<ol> <li>E. M. etc.</li> </ol>	The Contraction	18,9 Silver Road Water V Crement-St.	And the state	COMPARIANCE N.	
	The second second	18, M Silvery Road Webs 171 perhason for	And the state	COMPACT/COMP 1	
	THE R. LANSING	A charge burger wanted with the first sector by	ALC: NO.	Strengthere in the	
	THE R. LANSING	1 Annual Real and Add 121 August 1	The second	Recently P	
1.0	Line Manufa	Company Name and Address of the Address of the	The second	The Downline	
a la series	The Delawardsman	Company Name and Address of the Automation	THE PARTY.	White and in the	
<ul> <li>Element</li> </ul>	1 (N) Bellam Without	Companition and an user in the sector	B. French Langer	Department 16	
<ul> <li>E.M. and</li> </ul>	100 Charlester	150, M Schware (Actual) Medices (If Career/assers Inc.	NAME AND POST	COMPACT Access 10	
<ul> <li>Elvision</li> </ul>	100 Charlester	TRANSFORM (Actual) Medice Mr. Construment Inc.	NOT YOUR	COMPACT ACCESS 10	
<ol> <li>E.W. 40</li> </ol>	The Property	15. M Schware (Rectard Westwork? Contribution Tre	100710-00710-001	COMMENDER NO.	
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	The Bandarded	Proper NerCentral Total average	100.000	Accession in	
	The second second	Proper Nercessale 1114 de la	ALC: NO.	And and the other	
	a second	Pages Nerves and 1154 are 10	100.000	and in the lot	
	time in the second	Comment Read and Address of	ALC: NO.	Party and Party of	
1000	In Accession	Company Parciner diff frame di	241 200	the Labor	Environmentation Comparison Contraction
C. B. Marrier	The Manufe	Company Parcel and shift many de lourse	name out these	Column Array 6	the distance had a spectral diverse
E Winterson	100 Breaths	Proper Nerriary date trains th	9.0.89	inter in large	Construction and a Particle structure of the Internal Activity of th
<ul> <li>If the ans</li> </ul>	100 Blanks	Company Rev Card AMP Instead In wal	NAME AND POST	O'Cassat Arrass #	
<ul> <li>Elifeant</li> </ul>	100 Minandranteri	C Proper Net Cast JAP Instructs	9.00895	Accelerities 16	the former of a finite of the set of the o
<ol> <li>Elifeant</li> </ol>	100 Burearlebra	C Propert Net Card AMP Index 45	9,40,995	One 1012013	South Control Statistics of PER-Mark
	110 Manufacture	C Propers Net Cascillate 111 do ave ba	9.40.995	where eater in.	Management of American Statement (1997) and the statement of the statement
	in automa	C Proper Ner Carrieller (115 at see by	a second descent	Coder Ing. 16	Alternative of Conference States and
	The series	and in the second decision of the second sec	And the second	Contract in case of	21-20-2021 H-32-00 (312) Pressenting inst
	THE REPORTS	and in the second distance in the second sec	And the Party of the	Contract in case of	and the state of t
	110 Adaption	Colorest Resident and State and St.	0.00 000	Accession 10	\$1,40,400,404 [2,3],40 Sec. 40,40 Sec. 404 [2, 2, 2, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4,
a statement	110 Alambarteri	Company Resident and Child at south	0.00000	Broate-Las 28	at 46 0404 10 40 at 11 40 at 11 10 10 10 10 10 10 10 10 10 10 10 10
. Birth and	100 Advarta	C Propert Ren Carol 4087-71 Flatt and Inc.	0.00000	Office 28,049,518	1 D201 p. 20 20 20 20 20 20 20 20 20 20 20 20 20
<ol> <li>Kintune</li> </ol>	100 Alaminterrate	C Prepar RenCent all POLINATION IN	0.0088	Warmal mater Inc.	
<ol> <li>Elvisor</li> </ol>	100 Bilan/Writers	C Proper NorCasci 49P (118 at cesting	8,0101-240701	DeaterTra 16	In a down made had a set of had a set of head head head head head head head head
<ol> <li>Elvisor</li> </ol>	110 Charleette	HEM School Hensel Western W Construction In-	NAME AND POST	COunt Arrest R.	the discount of a field search of the discount from the term of the term of the term of the search o
. Elfonse	IN Paylor for	HUM School (Reset) Writes 17 Contributed In	NUM HOT FORM	Claim Arrest R.	
	The second section	HEAP School Renad Western IV Contrilation In	NUM HOT FORM	COMPACT Across 14	the feature of a first source from the structure of the feature of
	The second property	<ul> <li>Proper mercani alle con de paste</li> </ul>	BALLERS.	Accession from 18	a second s
	The state of the s	A Property of the second	B. COMMON	Other Division of the	
1000	110 Advantation	Colomorphics and the second second	B. COMM	Street asked in	*
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1100 Million Million	Colourse Resident and Article Accession	a state party	Castler Tree 141	1
i il di sec	100 Charlestin	HEM Information of Complement In	NAME OF TAXABLE	Contrast Arrays III	1
<ul> <li>Winterset</li> </ul>	100 Charlestin	will be designed to be an and the second sec	and stir rise	COnstrait Arrays III	1
<ul> <li>Windowski</li> </ul>	100 Paglasetta	HEM School (Renad) Western W Constitution In-	AND REPORT ADAM	Control Access PL	1
. Colores	100 Manhardert	C Prepare RenCennister/CEII et unu ha	0.00011	Accession (Inc. 2011)	1
	100 Manchestert	C Propert RenCarol all 7018 at reachs	PLACENT.	Acceleration 20.	1
- E.H	100 Alternative	C Prepare Ren Carol all P (217) all and has	0.00000	One 208851	\
1000	The second se	Company man card and the cost of the bas	P.40.811	Contraction in .	1
1.00	The Darry Bridging	CONTRACTOR OF CONTRACTOR OF CONTRACTOR	and sold from	Contract Inc.	\ \
	The Courts	of Manual Provide Statement Inc.	hand out of the	Contract Income 1	1
a lateral	110 Charles in	HE M Information of Manhouse Victorian Constitution in	and out they	COnstant Array 18	1
a laterate	100 million families	Compare Res Canal and Coll and any log	B-KCERT	decate-free (R	1
a laterate	100 Allendarderi	C Propert RenCario all 7/21 Reliancing	PLACENT.	Accession 20.	
W Million	100 Annula	C Vincen RenCennal P (107) di sector	0.00010	Office 20:000.004	
and the second second	153 Cheffe	C ProperCator/Weard William Tools tools conf.	NUMBER	COntrol Access PL	
<ul> <li>Intervention</li> </ul>	200 Challen Au	HR,M	P.40.0011	Core Andr No.	
<ul> <li>International</li> </ul>	200 Charles Per	HEAD SOFTWARE ASSAULT ASSAULT ASSAULT	NOCEIN	Central Access PL	
a subscription and	CRI Challensee	HEALTHONG ASSAULT ADDITION	PLOCETT.	Carly NA Same	
Contraction and	CRI Charlester	ALM OF ANY ADDRESS ADDRESS OF THE	POWER NO. DK	A	
and a set	City Manufaka	A CONTRACT ADDRESS OF CALCULARY	PUOLEN	THE PERSON IN	
and the second second	Contraction of the local data	NUMBER OF STREET ADDRESS OF STREET	P.40.001	income and the	
and the second sec	THE RECEIPTION	THE MAN PROPERTY AND ADDRESS OF THE PARTY OF	100.00	Control Age of the local sectors of the local secto	
a statement	THE PROPERTY.	THE MOST PARTY AND ADDRESS AND	1.00000	Dans No. Long.	
A Designation of the	THE PARTY NAME	THE M STATE WATCH AND ADDRESS AND A	BUTTER TOURS		
a all support and	CHI Charles and	THE M STATE WATCH ADDRESS OF ADDRES	8.0000	Tax FEL ST In	
		and he shall all all and the second statements in all all all all all all all all all al	and and an and a second se		

7.マシンをクラッシュさせます。

8.マシンをセーフモードで起動し、**Procmon.pmbとMEMORY.DMP**を手動で収集します。両方の ファイルはC:\Windows folderにあります。これらのファイルは、Cisco TACと共有する必要があ ります。

🗼 Windows					_	8
🕞 🕞 🖉 🗸 Computer	r 🕶 Local Disk (C:) 💌 Wine	dows 🔻	÷ 😝	Search Windows		
Organize 👻 📄 Open 🔹	New folder				)III • []	
🚖 Favorites	Name A		Date modified 11/21/2010 4:24 AM	Type	Size 2,805 KB	
Libraries Documents Music Pictures Videos Computer	<ul> <li>fveupdate.exe</li> <li>HelpPane.exe</li> <li>hh.exe</li> <li>IE11_main.log</li> <li>MEMORY.DMP</li> <li>mib.bin</li> <li>msdfmap.ini</li> </ul>		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 6/10/2009 10:36 PM	Application Application Application Text Document DMP File BIN File Configuration sett	15 KB 717 KB 17 KB 14 KB 331,914 KB 43 KB 2 KB	
CD Drive (D:)	notepad.exe ntbtlog.txt PFRO.log		7/9/2015 7:57 PM 1/6/2020 12:41 PM 1/6/2020 12:30 PM	Application Text Document Text Document	189 KB 83 KB 576 KB	
📭 Network	ProcessionalN.xml ProfessionalN.xml Professional	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 7/14/2009 6:56 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	Date modified: 1/6/2020 1 Size: 313 MB	2:41 PM Date crea	ated: 1/6/2020 12:41 PM	и		

7.オプションとして、C:\Windows folderディレクトリにPMBファイルが生成された場合に通常モ ードで起動できる場合、ProcMonを再起動すると、次のログが表示されます。[保存]ボタンをクリ ックすると、イベントを再保存できます。

Process Monitor - Sysintemais www.spsintemais.com		
File Edit Event Filter Tools Options Help		
Image: State and State		
Text Poster Harre FID Densities Fab	Read Detail	

Pauro Montor	Ξ
2 Log of lasticities activity was constel by a powiew index Process Manifest Do you with its secretive collected data was	7
Tm	Ne

_
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	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 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