Raccolta dei registri ProcMon per la risoluzione dei problemi AMP all'avvio

Sommario

Introduzione Procedura:

Introduzione

In qualità di amministratore di sistema, è possibile ottenere registri dettagliati utilizzando Process Monitor (procmon.exe) per determinare se il connettore FireAMP si blocca durante il processo di avvio del computer. Questi registri verranno richiesti anche da Cisco TAC per risolvere i problemi. Process Monitor è un'utilità gratuita che può aiutarci in questa fase. Il file può essere scaricato gratuitamente dal sito <u>https://docs.microsoft.com/en-us/sysinternals/downloads/procmon</u>

In questo documento viene descritto come raccogliere i log di ProcMon e i dump della memoria se il problema si verifica durante un processo di avvio del sistema (ovvero se sta generando BSOD all'avvio). Questi registri sono necessari per acquisire gli eventi di sistema che si verificano durante l'avvio.

Procedura:

1. Impostare le macchine di prova in modo che il problema possa essere facilmente riprodotto.

2. Scaricare ed eseguire lo strumento ProcMon come amministratore. Andare su File -> Process Monitor Backing Files e selezionare un Percorso.

	Tools Options Her	-									
A 10 (14)	7 🗛 😵 🔟 🛤		N								
Process Name	PID Operation	Path			Fand	Detail					
Searchindeser .	2252 Ne SystemCon 2253 Bits SystemCon	ANC .			SUCCESS	Carted FSC	1.9.				
Search-Indexer -	2212 AlefenterCor	esiC			SUCCESS	Cantral FSCT	L.R.				
Search-Rentice	2012 A Thread Create	•			SUCCESS	Thread ID: 25	104				
Epiow DE	200 🕰 fegQuey fey	MEU Soheren	Castres		SUCCESS	Guery Name					
Delow EXE	2000 Energy Joyney	WC12-Seberary	Citeres		5000055	Guery Hands	Test				
Delow DE	2968 RegOpenkey	WEU Software	Closes' onl		SUCCESS	Desired Acce	er Q .				
Epiow DE	2000 Angluey fey	INEU Software's	Cannes', PML		SUCCESS	Guery Name					
Process Manite	e Backing Film						-				
Dese bacting file	directs are being used to a	there event data:									
Name		ALC CLOCKED	Event Court	Event Bates	Pandro Evente	Process Court	Octorer Court	Inter Court	Constant		
Ciller/we/M	Anew Desktop processor of	ing [here] and	106.123	40,901,130	5	50	1954	79	No		
	The stand broken in	hages are spee	198.123	10.00			1.004		140		
	A store wants in vitual re	amory (inited by the	s system convet led	C, or in a file your	specify (insted by the	the spece). Which	do you prefer?				
roceen Mariter ce											
tocaus Haritar ca											
tocaus Haritar ca	(ry (0,70240 analobia)	in the local second	Condent Seat 2 June								
house Haritar or O'Use virtualmen II Das Riemannad	C Stervise-7454-4	en/Deilte/promer									
hoose Haritar or O'Use virtual ner B'Use für namet	ery (0,70240 erability) C-Garryten7x64 era	en/Deitspiptoren									
hoose Heriter or O'Use virtual ner E' Lise für namel	ory (0,7020 analabia) C-Gaarajoo-7x84m	en/Desklap/proces									(mod.)
toose Haritar o Otte virtuelinen E Cas für named Tooffan load: D. 0	ery (0,70340 melakia) C (Jaars/per/hidon No (6 pt (2 kytes perding)	en 'Seditaj granera									Canod
ncom Havtar or Othe virtualinem II Cha file named II Cha file named	ery (8,7026 makék) Cišanvjor/364m Pi 6 při (7 byter pendra)	en (Desktop)promor			4-4-04-4					x	Canon
tocom Haritar or Othe virtual ner Date für named TracPlan land: 1.4 Depiner 202	ry (8,729 makik) Citarype-3dan Pi 6 pi (3 interpreting) 2011 Charlow-Ary	en/Cesklap/proceor	ulvetajad am		\$000835	County Acco	. Ř.				Genost

3. In Procmon Tool, selezionare **Options -> Enable Boot Logging** (Opzioni > Abilita registrazione avvio).

🗳 Pro	cons Monite	or - C:\L	niw/med	7x64-rww\Desktop	piprocmon_output/test1.pml				
File I	Edit Event	Filter	Tools	Options Help					
l alt f		R.L.		41	T				
	9	DA	Y 🗛 🤉	Always on	Top				
Time	Process N	iane -	PID	Font			Rest	Detail	
12:36:	# Search	ideer	2252	Herb Ender (Colorer .		SUCCESS	Cantrol: FSCTL_Q	
12.36:	. CE Search	rdeier .	. 2252	riginga	Legentre a		SUCCESS	Cantrol: FSCTL_R	
12:36:	#?Search	hdeer	. 2252	Configure	Symbols		SUCCESS	Cantrol: FSCTL_R.	
12.36:	Search/	FilterHos.	. 2072				SUCCESS	Thread ID: 2884	
12:36:	Epiow	DE	2988	Select Colu	mna		SUCCESS	Query: Name	
12.36:	2000	EDE	2968	W	-		SUCCESS	Query: HandleTag	
12:36:	- Depose	EXE	2968	Plistory De	pun		SUCCESS	Query: Handle Tag	
12.36:.	- Epore	Die .	2014	Profiling Ex	ents		SUCCESS	Desired Access: Q.	
12.36.	- Desaw	5/2	1				SUCCESS	Guery: Name	
12.06.		EVE.	2900	Enable Boo	t Logging		30.0E33	Guery, Hande rag	
12.36	- Detroit	EVE	2200				SUCCESS	Date DIG S7 14	
12.36	Entre	EVE.	2444	✓ Show Reso	Ived Network Addresses Ctrl+N		SUCCESS	1396. P00_26. W.	
12.36	Errive	EVE	254.8	Hex File Of	fuets and Lengths		SUCCESS		
12:36	Enlow	EVE	2988		17. 10.		SUCCESS	Overv: Neme	
12.35	Engline	EXE	2988	PHD P7DOB	is and Thread ID's		SUCCESS	Query HandeTan	
12:36	Endors	DE	2988	RegQuervier	HREU/Software/Cleases		SUCCESS	Query Hande Tag	
12:35:	Epipe	EXE	2988	RegOpenKey	HKCU/Software/Classes\.pnf/Oper/08thProg	ids.	NAME NOT FOUND	Desired Access: R	
12:36	Epploye	DE	2988	RegOpenKey	HKCR\pm\OpenWthPropide		NAME NOT FOUND	Desired Access: R.	
12:36:	Epipe	EXE:	2968	RegQuesKey	HKCU/Software/Classes		SUCCESS	Query: Name	
12:36	Eplow	DE:	2568	RegiliveryKey	HKCU\Software\Cleaner		SUCCESS	Query: Handle Tag	
12.36:	- Dekore	(DE	2968	RegQueryKey	HIKCUNSoftware/Classes		SUCCESS	Query: HandleTag	
12:36	Delow	DE:	2988	RegOpenKey	HKCU/Software/Classes/Software/Microsoft/	Windows\Curr	NAME NOT FOUND	Desired Access R.	
12.36:	Delore	(DE	2968	RegOpenKey	HKCR\Software\Microsoft\Windows\CurrentV	Amion' Explore	NAME NOT FOUND	Desired Access: R	
12:36:	. 🎇 Epiow	DE	2568	RegiliueryKey	HRCU/Software/Classes		SUCCESS	Query: Name	
12.36:	Epice	(DE	2968	RegQueryKey	HKCU\Software\Classes		SUCCESS	Query: HandleTag	
12:36:	- Espiorer	EXE	2968	RegularyKey	HKEU/Software/Classes		SUCCESS	Query: Handle Tag	
12.36:	Epiore	EDE	2968	RegOpenKey	HKCU\Software\Classes\.pnl		SUCCESS	Desired Access: R	
12:36:	California (California)	EXE	2566	Hegulueryflay	HALU/Software/Microaot/Windows/Lurent/	Auration Vocatione	SUCCESS	Query: Handle Lag	
12.36:.	- Epore	SE	2968	Hegupenkey	HRCU/Software/Morosoft/Windows/Current/	erson Explore	SUCCESS	Desired Access: R.	
12.36.	- Desore	EAR	2300	rieguauerytary	HALU-Software Microsoft Windows Surrenty	Aereon Vocatione	SUCCESS	Guery: Handle Lag	
12.36		EVE .	2966	Barlymaker	HALL USOTWATE CHOICEDE, CHINDENS SCATERY A	eson Explore.	30,4,633	Desired Access, H.	
12.36	- Delaw	EVE	2000	BasCost	HALF CONVERT ORCOOCH OF FROM CAPER	Andrew Eventure	CULTERE	Desired Access D	
12.36	- Delaw	DE	2588	Barcharylister	HICLING the are Microard Windows Constant	familiary (Explore	SUCCESS	Tree BEQ 52 La	
12.36	Ector	EXE	2568	BegCirseKey	HKC10-Software/Microsoft/Windows/Current/V	Amion' Explore	SUCCESS	office of standing of the con-	
12:36	Epipe	DE	2588	RegCloseKey	HKCU/Software/Microaph/Windows/Current/	Amaton (Explore	SUCCESS		
12:36:	Eclore	EVE:	2968	RegCloseKey	HKCU/Software/Microsoft/Windows/Current/V	ension\Explore	SUCCESS		
12:38:	Epilore	DE	2588	RegularyKey	HKCU/Software/Classes		SUCCESS	Query: Name	
12.36:	Epipe	EVE:	2968	RegQueryKey	HKCU/Software/Classes		SUCCESS	Query: HandleTag	
12:36:	Eplow	DE	2988	RegQueryKey	HKCU/Software/Cleases		SUCCESS	Query: Handle Tag	
12.36:	Epipe	(E)(E)	2968	RegOpenKey	HKCU/Software/Classes/Applications/instepa	d.exe	NAME NOT FOUND	Desired Access: R.,	
12:36	Explore	DE	2988	RegOpenKey	HKCR\Applications\notepad are		SUCCESS	Desired Access: R.	
12.36:	Delore	(E)(E)	2968	RegDoseKey	HKCR Applications instepad eve		SUCCESS		
12.36	Epiow	EQE:	2968	RegionryKey	HKEU/Software/Classes		SUCCESS	Query: Name	
12.36.	Delore	EXE:	2968	RegQueyKey	HIKCU'/Software/Classes		SUCCESS	Query: HandleTag	
12.36	Delow	EXE:	2968	Regioury fury	HNLU/Software/Classes		SUCCESS	Query: Handle Tag	
12.36.	Dente	5/2	2968	Hegopenitzy	HKC Unsoftware Classes Applications Violepa	0.660	NAME NOT FOUND	Cesred Access: R	
12.36	Deparent	EXE	2368	negUpentay	MAL IT upplications victopiad and		SUCCESS	Ceared Access R.	
12.36.	abpore	5/2	2968	nog auny ney	HINLIN VIDDICATIONS VIDEPAD ENE		0000255	Query: Name	
12.36	Cebber	EVE	2300	A Des Const	HALT Oppications (Chevral) Instantion (Instantion	diama Di selara	NAME NOT DO AND	Desired Access D	

4. Selezionare Genera eventi profiling minaccia e Ogni secondo.

ć	🔰 Proc	ess Monitor - C:\	Users\win7x64-new\Deskto	p\procmon_output\test1.pml				
	File Ed	it Event Filte	r Tools Options Help					
ĩ	-2.53							
l	■	N 🖉 🖉	A 🐼 🖬 🖬					
Г	Time	Process Name	PID Operation	Path		Result	Detail	
Ľ	12:36	E Searchindeser	2252 ReSystemContr	elC:		SUCCESS	Control: ESCTL Q	
b	12:36	Searchindexer	2252 FileSystemContr	OC:		SUCCESS	Control: ESCTL_R	
Ľ	12:36	S				SUCCESS	Control: ESCTL_R	
	12:36	Enable Boo	xt Logging			SUCCESS	Thread ID: 2884	
	12:36					SUCCESS	Query: Name	
	12:36	Process M	onitor can generate thread pri	offing events that capture		SUCCESS	Query HandeTag	
	12:36	The scale of	or all running applications at a	reguar merval.		SUCCESS	Query: Handle Tag	
	12:36	E Gen	erate thread profiling events			SUCCESS	Desired Access: Q	
	12:36	E				SUCCESS	Query: Name	
	12:36	6	Every second			SUCCESS	Query: Handle Tag	
	12:36	E	C Every 100 milliseconds			SUCCESS	Desired Access: M	
	12:36	E C	O credy not maketories		(Default)	SUCCESS	Tipe: REG. SZ. Le	
	12:36	6		OK Cancel		SUCCESS		
	12:36	E	_			SUCCESS		
	12:36	Eplorer EVE	2988 RecQuer/Key	HKCU/Saltime/Casses	-	SUCCESS	Query: Name	
	12:36	Eplorer EXE	2988 RegQueryKey	HKCU/Software Wasses		SUCCESS	Query: Handle Tag	
	12:36	Explorer EXE	2988 RegQueryKey	HKCU\Software\Classe		SUCCESS	Query: Handle Tag	
	12:36	Eplorer EVE	2988 RepOpenKey	HKCU/Software/Classes/.pml/	OpenWithProgids	NAME NOT FOUND	Desired Access: R	
	12:36	Eplorer EXE	2988 RepOpenKey	HKCR\.pml\OpenWithProgids		NAME NOT FOUND	Desired Access: R	
	12:36	Eplorer EXE	2988 RegQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name	
	12:36	Epplorer.EXE	2988 RepQueryKey	HKCU/Software/Classes		SUCCESS	Query: Handle Tag	
	12:36	Eplorer EXE	2988 RepQueryKey	HKCU/Software/Classes		SUCCESS	Query: Handle Tag	
	12:36	Biplorer EXE	2988 RegOpenKey	HKCU\Software\Classes\Softw	rare\Mcrosoft\Windows\Curr	NAME NOT FOUND	Desired Access: R	
	12:36	Epplorer.EXE	2988 KRepOpenKey	HKCR\Software\Morosoft\Win	dows\CurrentVersion\Explore	NAME NOT FOUND	Desired Access: R	
	12:36	Biplorer.EXE	2988 KRepQueryKey	HKCU/Software/Classes		SUCCESS	Query: Name	
	12:36	Explorer.EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: Handle Tag	
	12:36	Explorer.EXE	2988 KRegQueryKey	HKCU/Software/Classes		SUCCESS	Query: HandleTag	
	12:36	Biplorer EXE	2988 KegOpenKey	HKCU\Software\Classes\.pml		SUCCESS	Desired Access: R	
	12:36	Biplorer.EXE	2988 KRegQueryKey	HKCU\Software\Mcrosoft\Wr	dows\CurrentVersion\Explore	SUCCESS	Query: HandleTag	
	12:36	Explorer.EXE	2988 RegOpenKey	HKCU/Software/Microsoft/Wir	ndows/Current/Version/Explore	SUCCESS	Desired Access: R	
Ľ	12:36	Biplorer EXE	2988 KRegQueryKey	HKCU/Software/Mcrosoft/Win	ndows/Current/Version/Explore	SUCCESS	Query: HandleTag	
	12:36	Explorer.EXE	2988 KegOpenKey	HKCU\Software\Microsoft\We	dows\CurrentVersion\Explore	SUCCESS	Desired Access: R	
	12:36	Explorer.EXE	2988 KRegQueryKey	HKCU/Software/Microsoft/Wir	ndows\CurrentVersion\Explore	SUCCESS	Query: HandleTag	
	12:36	Biplorer EXE	2988 KegOpenKey	HKCU\Software\Mcrosoft\Win	ndows\CurrentVersion\Explore	SUCCESS	Desired Access: Q	
	12:36	Explorer EXE	2988 KRegQueryValue	HKCU\Software\Microsoft\Win	dows/Current/Version/Explore	SUCCESS	Type: REG_SZ, Le	
	12:36	Explorer EXE	2988 RegCoseKey	HKCU\Software\Microsoft\Wir	dows/Current/Version/Explore	SUCCESS		
	12:36	Explorer EXE	2988 RegCloseKey	HKCU/Software/Microsoft/Win	dows/Current/Version/Explore	SUCCESS		
	12:36	Explorer EXE	2988 RegCloseKey	HKCU\Software\Microsoft\Win	dows/Current/Version/Explore	SUCCESS		
	12:36	Explorer EXE	2908 RegQueryKey	HKCU\Software\Classes		SUCCESS	Query: Name	
	12:36	Explorer EXE	2988 KRegQueryKey	HKCU\Software\Classes		SUCCESS	Query: Handle Tag	

5. Assicurarsi che tutti i filtri pertinenti siano selezionati in Procmon e che i dati siano stati raccolti.

6. Se non si è in grado di replicare l'arresto anomalo, è possibile forzare l'arresto anomalo di Windows utilizzando l'utility NotMyFault64.exe, che è possibile ottenere da <u>https://live.sysinternals.com/files/</u>

Di seguito sono riportate le istruzioni per l'esecuzione. <u>https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump</u>

Provan Westur - Cittle	and the set of the set	Paraceter, Julipul Acid, prel			
the dat dura the	North College Pade				
2 B 4 9 5 1	4 0 X A				
Ins. Anna term	ND General	Fat	Sea.0	Ganal	
Cit. Eldines	THE BARNES	Company Residence (APV 111) All services	9.00200	Other Distances	
23. 8 4.00	100 Cashings	C Proper RenCennut P (1) 1 41 and 10	9.00200	Ware/eater Te.	
23 EM.m	1707 Automation	C Prepar RenCennal P 121 All and by	8,0000-040001	Department 161	
23. Exten	170 Charles Tes	18,34 Selecter Human's Western M*Contentioners for	NUMBER	COMMENTATION R.	
23. EVEn	The second section	18,34 Selver Hunsell Westers M Carentenory Se	And the state	COMMENCED NO.	
23. 19.00	The Course of the	NUM Selver Hunself Westers If Cyterchenory Se	New York Policy	COMPACTAGE N.	
2.2	20 Printer Springs	Company Renders and Company and Street Street	100.00	Accession (Acc-	
Solution of the second se	The second second	Company New York and the Party of the	100.000	And in case of	
100	in the second	Property Revenues and Providence and	10000	When when he	
Con Contract	The last windows	Constant Revolution and Print Public and State	B. PTER LINETYL	Castler Tree 14	
12 M History	110 Charlester	18. M School House House 17 Catentineers In	NAME AND POST	COMPACT Access 19	
23. 10.00	The Constrainty	TRUM Schware Human? Ministree 167 Current Inson Tru	NAME AND POST OF	COMPACT ACCESS 19.	
23. Exten	The second second	18, M Schwarz Human? Ministree 10" Current among Six	NAME OF TAXABLE	COMMENCED N.	
23. 84.00	170 Bellandarded	Propert Rendered AP 11 / AL events	10.00	Accession (S.	
2 H B	The second second	Wegen Nercess AMP 11 Tracine 1g	10.00	Accession (F)	
22.20.00	N. BURNER	Proper Nerven all 11 hit as 10	141.50	the post of	
20.00	and the second second	Company New York and the Party of the	A PROPERTY OF	Contraction 14	
Con Contract	I'm Branketter	the lot between the party billing to be a party party for	name and store	Constant Array 6	
COLUMN TWO IS NOT	1 IN CONTRACTOR	TR.M. Schwarz (Retract: Westwork) Constrainers To	NAME OF TAXABLE	Column Array 6	
Cit. Extras	100 Paginetter	15.14 Selvers Hunsell Westwork? Current associate	NAME OF TAXABLE	COMPACT Access 10	
Cit. Extrac	100 Minandramed	Chapter Ren Carol and Child All and the	9.00 895	Accessive in	
23. DAte:	100 Minandrated	Companition (acculate (1)) that are by	140.005	Acception 18	
33. EX.46	THE BANKING	Proper NerCent ART 11141 av 19	10.00	The 2110120	
22. 20.00	and the second	Proper Nercecruit Setup 8	1.41 Pt-1	DOM: NA.P.	
20-00-00	and a second	Copper Nervacy and Dates in	100.000	Column Panel 1.	Independent Conference (Upper Construction)
20- 10- Mar	in another	Company Services of States & Long	and sold the	Contract Second Second	Statement (Statement
20.000	and the second sec	Compare Real and difference	5.00 mil	the Allow	Conference of Information Informatio Information Information Information Information Infor
1 M 1 M 1	The second se	Company Real And All Street & and	sand only store	Country brown it.	
Contraction of the local division of the loc	110 Bullanchastert	Company Revolution and Instance do	9.40 (99)	Accelering H.	Exception of the Control of Co
Cold. B Marcan	IN A REAGAN	Company Revolution and Instance do	0.00000	Office 1-075-741-8	The same is a proper of the same size of the same
COL. Kitchen	110 Bulanintenate	E Proper RevCentuil#1018 strawing	0.0088	internal matter free.	
U.M. Kirken	110 Advantitions	E Proper RenGest AMP (1) 5 House by	Burner, Support,	Center Ine 14	Enverteine of Conditional weather that mean decising
Vill. Exten	100 Performance	HUM Schwarz (Actual) Ministree M. Current Association	NAME AND POST	COunt Arous P.	REARCHER LEASE AT 1110 Proceeding lines
VOL. EXC.	The Page Section	HEAL Officer (Read) Medice (Contribution) In	NUME HOT POINT	COMPACTOR P.	81-86-282# 13-55 P# (318) generation and gen.
COL. EXC.	The second	HEAL OFFICER REPORT NUMBER OF CAREFURNEY IN	NAME OF TAXABLE	COMPARIANCE P.	21 (20-22) 10 (17 12 (20 12)))))))))))))))))))))))))))))))))))
20.00	IN BOAD APORT	Constant New Card and Constant and the	TALL POL	Accession from 18	ALCONE 1215 IN THE REPORT OF A DECEMBER OF A
10.00	The second second	A respect that they are the set of a set of	1000	Other Designation	[[][h/h]][h/h].[h] h/m]
20.000	The second second	Colorest Resident and Table 1 and the	0.000	internation in	1 Diprist 19,870,046,761 April 1980
10.000	100 Million Million	Concern Rev Carry 489-11 Publishes Inc.	A PHONE DURING	Castor Ing. 14	Excellence of a state of the
10. Com	100 Charlester	viel of Antonio Oceanit's Strategy of Complement In-	want out their	Classed Array R.	
U.M. Without	110 Paul service	HEAV School (Research Ventres 10 Carentinger) In	water right rights	Classed Arrest R.	and any approximately and an approximately and a standard and
U.S. Kirken	110 Paginetter	HKM (Mean Hennel Western W Constitution) In	And HOT YOUR	Classed Arrest R.	
U.M. Kirken	100 Manhardert	2 Propert RenCentral #1018 at sea by	0.00000	Acute In 2.	 Protocorrespondences and an analytic process of the p
10. Dr. 10. au	IN Alasharian	C Prepar NerCash 48* 715 at yearing	P.40.000	Acateria 3.	
10. Distant	IN ANY A	1 Proper NerCent diff (115 at use by	P.41.991	the Britch	
10.0	The Date of the local date of	 Property Net Carry MP 111 Bit and base base 	ALC: NOT THE OWNER.	standard in	1
20.00	The Standard	AND ADDRESS OF ADDRESS OF ADDRESS	and other	Count I want it	1
10.00	190 Charlester	out to be an interest interest in the second second interest inter	and out they	Contract Income 18	1
12.00	110 Paulantin	HEAD Information and Manhouse In Company on the	and out they	Control Array II	1
U.M. Watan	100 Allen Arriet	C Propert Res Carol al #1010 all and ba	P.ACTER	Accession (in case)	1
1218 . Whites	100 Manharitett	C Proper RenCennatif* (218 at use by	BLOCENT	Accelerity 20	1
1230. El-Mann	100 Balancia	C Proper Ner/CechildP (218 at see by	PLOCENT	Obs 2008.01	1
10. Exten	W Dathant	C Proper RenCennut#1018 at use by	PLOCET	Ware agen in	1
12. 14.00	IN Caryliniums	C Physic NerCash (MP-11) 41 (m) ha	BUMER DISTANT	CoderTra 14	1
10.00	The Pay Service	NUM Orleany Royal Western IT Commission To	And April Poly	Contract Access 10	1
10.0	The second second	in the second dense of Constants in	And April Pope	Contract Access 10	1
2 C	THE REPORTS	Probaness Rest Rest and Rest Rest Rest Rest Rest	B.CO.T.	Second Sec. 7	1
12.00	100 Allendering	C Wagon Res Card 400121 Bull on In-	0.0000	Sector In 12	
1218 B Marrie	100 Andres	C Proper Rev Central #1011 All year ba	9.0000	Office (20.000 Not	
U.M. Bottobler	153 Country	C /August Calor / Maget 10Roate Tools Included	Net ALT YORK	Control Access 10.	
C.M. Evergence and	200 Challenter	HR_M	PLOCETT	Core Andrina	
CH. Evennese	200 Challenter	NUMBER AND ADDRESS OF ADDRES	PU00811	Change Access 10.	
CH. Compressee	200 Challenge	HEM SOFTWARE ASSAULT ASSAULT	PLOCET	Care NA Same	
C.S. Compression	CRI Challendert	HEALD COTTACHE ASSAULT ASSAULT	BOWER SOO DK		
C.S. Compression	CT Children and	NUMBER OF ADDRESS AND ADDRESS	PUOLEYN	Tax PELIC In.	
C.S. Compression	City of the Company	NUMBER OF STREET ASSOCIATES	P.0.01		
A DECEMBER OF THE OWNER OWNER OF THE OWNER OWNE	THE PARTY AND INCOME.	THE MAN PROPERTY AND ADDRESS OF ADDRESS	100.00	Control Agender Test	
Contraction of the local division of the loc	THE PROPERTY AND	IN MACHINE AND ADDRESS AND	B. C. THE	Date of Lots	
12 M Company on	THE PROPERTY.	THE MODEL WATCH ADDRESS AND ADDRES	BUTTER TOURS		
CH. Compression	CHI Charles	THE M STATE WATCH ADDRESS ADDRE	9.0720	New FIEL SP 14	
CH. Durgroups	(10 Challes	HEALING THAT AND ADDIVING ME	9.00201		
		A DE REPORTE A DE RECEIRE DE RECE	41.00.00		
COLUMN TO A REAL PROPERTY.	1440 F	Contraction of the second second second second	a water the		

7. Bloccare la macchina.

8. Avviare il computer in modalità provvisoria e raccogliere manualmente **Procmon.pmb** e **MEMORY.DMP**, entrambi i file si trovano nella cartella C:\Windows. Questi file devono essere condivisi con Cisco TAC.

🕌 Windows					_	8
G - 📔 🗸 Compute	er 🔻 Local Disk (C:) 🖛 Win	dows 👻	÷ 🙀	Search Windows		
Organize 👻 🗋 Open	 New folder)= • 🗊	6
🜟 Favorites	Name A		Date modified 11/21/2010 4:24 AM	Type Application	Size 2,805 KB	
Documents	Fveupdate.exe HelpPane.exe hh.exe		7/14/2009 3:39 AM 6/2/2017 10:10 AM 4/18/2018 5:41 PM	Application Application Application	15 KB 717 KB 17 KB	
Pictures Videos	IE11_main.log MEMORY.DMP mib.bin		1/30/2018 3:52 PM 1/6/2020 12:41 PM 7/14/2009 1:06 AM	Text Document DMP File BIN File	14 KB 331,914 KB 43 KB	
Provident Computer	 msdfmap.ini notepad.exe ntbtlog.bt REPO log 		6/10/2009 10:36 PM 7/9/2015 7:57 PM 1/6/2020 12:41 PM	Configuration sett Application Text Document	2 KB 189 KB 83 KB	
Shared Folders (\\vn	 PFRO.log Procmon.pmb ProfessionalN.xml regedit.exe setupact.log setuperr.log splwow64.exe StarterN.xml 	Type: XML Document Size: 52.3 KB Date modified: 6/10/20	1/6/2020 12:30 PM 1/6/2020 12:41 PM 6/10/2009 10:30 PM :39 AM :30 PM :30 PM :30 PM 10:30 PM 11/21/2010 4:24 AM 6/10/2009 10:31 PM	Text Document PMB File XML Document Application Text Document Text Document Application XML Document	576 KB 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 PN	И		

7. Se si è in grado di eseguire l'avvio in "modalità normale" se i file PMB vengono generati nella cartella C:\Windows, se si avvia nuovamente ProcMon verranno visualizzati i seguenti log. Da questo, è possibile salvare nuovamente gli eventi facendo clic sul pulsante Salva.

2 Precess Monitor - Sysintemais www.spsintemaik.zam		
File Edit Event Filter Tools Options Help		
Time Process Name FIG Demakers Falls	Read Deal	

Preserva Mondae	Ξ
2 log of loost-line activity says control by a persistal indexes of Process Vientins. On you with its save the collected data new?	
Tm. He	

_
Genet

🔰 Process Monitor - Sysi	internals: www.sysinternals.	com		
File Edit Event Filter	Tools Options Help			
📽 🖬 🔌 🕸 🖾 🛛	🗢 🛆 😳 🖻 🛤 🖣			
Time Process Name	PID Operation	Path	Result	Detail
12:41: Fames exe	292 🧟 Process Start		SUCCESS	Parent PID: 4, Com
2.41: Famas exe	292 ar Thread Create		SUCCESS	Thread ID: 295
2.41: Tames exe	292 E Load Image	C:\Windows\System32\amss.exe	SUCCESS	Image Base: 0x479
2.41: Pamas exe	292 ar Load Image	C:\Windows\System32vitdl.dll	SUCCESS	Image Base: 0x779
241: Pamas exe	292 RegOpenKey	HKLM\Software\Morosoft\Windows NT\CurrentVersion\Ima	NAME NOT FOUN	D Desired Access: Q
41: Fames exe	292 RepOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
2.41: Pamas exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41 smss.exe	292 KRegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1.024
41: E smss.exe	292 KRepQueryValue	HKLM'\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	ID Length: 1,024
41 smss.exe	292 RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	
41: Pamas exe	292 Koreate File	C://Windows	SUCCESS	Desired Access: E
41 Smss.exe	292 ReadFile	C:\\Windows\System32\amas.exe	SUCCESS	Offset: 74,752, Len
41: Pamas exe	292 🛃 ReadFile	C:\Windows\System32\amss.exe	SUCCESS	Offset: 1,024, Long
41 Smss.exe	292 ReadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offset: 107,008, Le
41: Resmos.exe	292 MeadFie	C:\Windows\System32\amas.exe	SUCCESS	Offset: 104,448, Le
41 smss.exe	292 See Thread Create		SUCCESS	Thread ID: 300
41: Romas exe	292 ReadFile	C:\Windows\System32\amas.exe	SUCCESS	Offse Offset: 104,448
41 smss.exe	292 🛃 ReadFile	C:\Windows\System32\amsa.exe	SUCCESS	Offse Length: 2,560
41: Ersmas exe	292 KegOpenKey	HKLM'\System\CurrentControlSet\Control\MinINT	REPARSE	Desi L/O Rags: Non-cached, Paging L/O, Synchronous Paging L/O
41: Famos exe	292 RegOpenKey	HKLM\System\CurrentControlSet\Control\MnINT	NAME NOT FOUN	D Desi Priority: Normal
41: Pamas exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\.	REPARSE	Desired Access: Al
41: I smss.exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\.	SUCCESS	Desired Access: Al
41: Pamas exe	292 KRegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	NAME NOT FOUN	0
41: Pamos exe	292 RepSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA	SUCCESS	Type: REG_SZ, Le
41: Pamas exe	292 KegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R
41: I amos exe	292 KegOpenKey	HKLM'System'CurrentControlSet'Control'Session Manager	SUCCESS	Desired Access: R
41: 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 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 Lanoth: 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