How to extract Sessions from an Archiver



The Security Division of EMC Copyright © 2015 by EMC Corporation. All rights reserved.

This guide is prepared by Khaled Gamal from RSA.

There are two options to extract logs from the archiver:-

1st option: Using Broker investigation from UI:-

- Put the archiver as a data source in a Broker

🔎 Administration 👳	🚍 Hosts	🗐 Servi	ces 🔊 I	Event Sources	🛡 Hea	ilth & Wellne	ss 📚 Sj	/stem	💾 Security	Ō ²	9	RSA Se	curity Analytics	
🛔 Change Service 🛛 🛽 🖪	broker - Bro	oker C	onfig ତ											
General Files	Appliance	e Service Cor	figuration											
Aggregate Service	es							Agg	gregation Con	figuratio	on			
🕂 🗕 🌞 💩 Toggle Service 🕞 Start Aggregation 💿 Stop Aggregation									Name			Config Value		
Address		Port	Rate	Max	Behind	Collection	Status	🗆 Ag	gregation Settings					
192.168.2.122		56008	0	0	0		consuming	Aggregate Autostart 🗹						
								A	ggregate Hours		0			
								A	ggregate Interval		60000			
								A	ggregate Max Sessions		5000000			
								🗆 Se	rvice Heartbeat					
System Configura	ation							Н	leartbeat Error Restart		300			
System conligue	ation							Heartbeat Next Attempt			60			
Name			Config	Value				н	leartbeat No Response		180			
Compression			0											
Port			50003											
SSL FIPS Mode														
SSL Port			56003											
Stat Update Interval			1000											
Threads			20											
						Apply								
👤 admin 🌐 English (Unite	ed States) G	MT+00:00									Send Us	Feedback	10.5.0.0.17951-5	

- Investigate from the broker:-

Inves	tigation	•	Navigate 🛛	😂 Events	🗮 Mal	ware Analysi						Ō 🍳		RSA	Securit	y Analytics
Navigate	e															
📑 broker	- Broker	Last 3 H	lours 🗸 🤇	🕈 Query 🛞 🛽	Profile 🕑	💶 Meta 🕑	🔲 Total 🕤	🛛 📲 Descending	g 💿 🧱 Event Cou	int ⊚	Save Events	⊙ 🗲 A	ctions 🕑			Settings
0																
2015	12 20 05	5:14:00) (+00:00)				Las	st 3 Hours				2	015	12 20 08	:13:59	(+00:00)
7.5																•
											Investigat	e 🔑 R	eset Zoo	m 🗘 🗘	Options	▲ Hide
<⊖>	ource IP	Addres	s (1 value)	Q												Â
∳ ∘ Å b	Action Evo	ent (1	value) 🔎													
© ⊙ Ic	Decoder S ogdecoder	Source r (7)	(1 value) ዖ													
₩ ∘ F c	ilename Closed - Cli	ې ck to Op	en													
E≞ ∘ C	Directory Closed - Cli	ck to Op	en													
<u></u>	P Addres	s Alias	Record 🔎									_	_		_	-
👤 admin	()English	n (United	States) GMT+	00:00									Send	Us Feedba	ick 10.	5.0.0.17951-5

- Open the sessions

Investigation	🔊 🚫 Navi	gate 🥯 Evei	nts 🗮 Malwa	are Analysis				Ō	?	RSA Se	curity Analytics
📑 broker - Broker 👢	ast 3 Hours	👻 🌳 Query 😔	🛄 Profile 🛛 📒	🛿 Detail View 😔	🗲 Actions 😔	🗲 Incidents 😔	Search Event	S	Ý	Search	🔅 Settings
ip.src = '10.203.18.20'	⊙ 🖲 Cance										
Event Time	Event Type	Event Theme	Size	Details							
2015-12-20708:13:11	Log		400 bytes	 ↔ sessionid : medium : 3 device.type device.class ↔ alias.host : event.type : event.desc ✓ action : Blo user.dst : + Show Addit 	52661 32 : DLP 10.204.43.210 : 164736 : DLP Syslog scked	View Details					
2015-12-20T08:13:28	: Log		400 bytes	 ↔ sessionid : medium : 3 device.type device.class ↔ alias.host : event.type : event.type : action : Blo user.dst : + Show Addit 	52662 32 5 DLP 10.204.43.210 164736 5 DLP Syslog scked 1040 Meta	 View Details					
				 ♦ sessionid : 	52663						*
巛 🕻 Page 1	> I C	25 🗸 ever	its per page						C	isplaying 1	- 7 of 7 events
👤 admin 🌐 English (l	Jnited States)	GMT+00:00							Send U	s Feedback	10.5.0.0.17951-5

- Choose Actions->Export->Export all logs

Investigation	Navi	igate 📚 Ever	nts 🛛 🗮 Malwa	ire Analysis					Ō	P	? RSA	Security A	nalytics
📑 broker - Broker 🛛 🔒	ast 3 Hours	👻 🌹 Query 🛛	💷 Profile 💿 🔳	Detail View \odot	🗲 Actions 🕑 🗧	🗲 Incidents 😔	Se	arch Events			✓ Searce	🔹 🔅 s	ettings
ip.src = '10.203.18.20'	🙁 🖲 Canci	el			Export	> Exp	port PCAP						
Event Time	Event Type	Event Theme	Size	Details	View Event	> Exp	port All PCAP						
2015-12-20T08:13:11	Log		400 bytes	 sessionid s medium : device.type device.clas alias.host : event.type event.tesc action : Bis user.dst : Show Addi 	32 2: DLP 10.204.43.210 : 164736 : DLP Syslog bocked tional Meta 👰 V	Exp Exp Fiew Details	port All Logs						
2015-12-20108:13:28	\$ Log		400 bytes	 ↔ sessionid: medium: device.type device.clas ↔ alias.host: went.type event.type action: Bla user.dst: Show Addi 	52662 32 5: DLP 10.204.43.210 : 164736 : DLP Syslog bocked	/iew Details							
				 ♦ sessionid : 	52663								-
巛 🕻 Page 1) I C	25 ∨ even	its per page								Displayi	ng 1 - 7 of 7	events
👤 admin 🌐 English (l	United States)	GMT+00:00								Se	nd Us Feedb	ack 10.5.0.	0.17951-5

- You will find the notification showing the logs extracted and then you could download it to your PC from Profile->Jobs

💄 Profile 🛛 💿							Ō 🛡	? R	SA Security Analytics
Preferences Notifications	Jobs – I 🕞 Resume 👜 P	ause 💿 C							
Jobs	Job Name Extract Logs	Recurring No	Scheduled 2015-12-20 9:00am	Component Investigati	Owner admin	Action Download	Message Extracting logs for 7 sessio	Status Completed	Progress
	Extract Logs	No	2015-12-20 8:45am	Investigati	admin	Download	Extracting logs for 7 sessio	Completed	

2nd option: Using saget.py script from the CLI:-

- Move the script to the Archiver.
- Issue the command: chmod +x saget.py "to make it executable"
- Run the script with the query you want to extract.
- An example to run the query is :- python saget.py -L -t 192.168.2.122 -p 50108 -u admin -s "2015-Dec-01 12:00:00" -e "2015-Dec-20 12:05:00" -o archivertest2.log -q "did exists"

Where:-

-t : Archiver's IP.

- -p:REST Port.
- -u : REST username.
- -s : Start time of the query.
- -e : End time of the query.
- -o : output file to save the sessions to.
- -q : query to execute.

When you execute the query it will ask you for a password which is the password of the REST username "admin" which is "netwitness" by default.



You could now open the file archivertest2.log to check all the sessions extracted:-

Nov 6 14:47:28 CEF:0 InternetData Security 7.8 164736 DLP Sysleg 1 act=Blocked duser=
e autorité de la complete de la complete complete de la complete d
e child Ords con loginName=N/A sourceIp=1 Nov 6 14:47:28 10 10 10 CEF:0 Children Data Security 7.8 164736 DLP Syslog 1 act=Blocked duser=
Nov 6 14:47:28 10 001 10 000 CEF:0 Uthereno Data Security 7.8 164736 DLP Syslog 1 act=Blocked duser=
HTTP analyzedBy=Policy Engin
babere bage bage boardebertrochane baberaj en e
e loginName=N/A sourceIp=1
Nov 6 14:47:28 1
suser=sus
e loginName=N/A sourceIp=1
Nov 6 14:47:28 CEF:0 Data Security 7.8 164736 DLP Syslog 1 act=Blocked duser=fname=N/A msg=http://
suser= <u>catalumanhadaaaa</u> cat=sdg1 sourceServiceName=Content Gateway on
e and discussion loginName=N/A sourceIp=1000000000000000000000000000000000000
Nov 6 14:47:28 1
suser=guinester suser=guinester cat=sdg1 sourceServiceName=Content Gateway on guinester cat-HTTP analyzedBy=Policy Engin
eloginName=N/A sourceIp=10.
Nov 6 14:47:28 200 CEF:0 Data Security 7.8 164736 DLP Syslog 1 act=Blocked duser= fname=N/A msg=http://t
suser=suipierent suser=su
e loginName=N/A sourceIp=11200.10.20
Nov 6 14:47:28 1 CEF:0 Data Security 7.8 164736 DLP Syslog 1 act=Blocked duser=1 Control of the security of
suser==cat=sdg1 sourceServiceName=Content Gateway on :===================================
eloginName=N/A sourceIp=0