How to extract Sessions from an Archiver

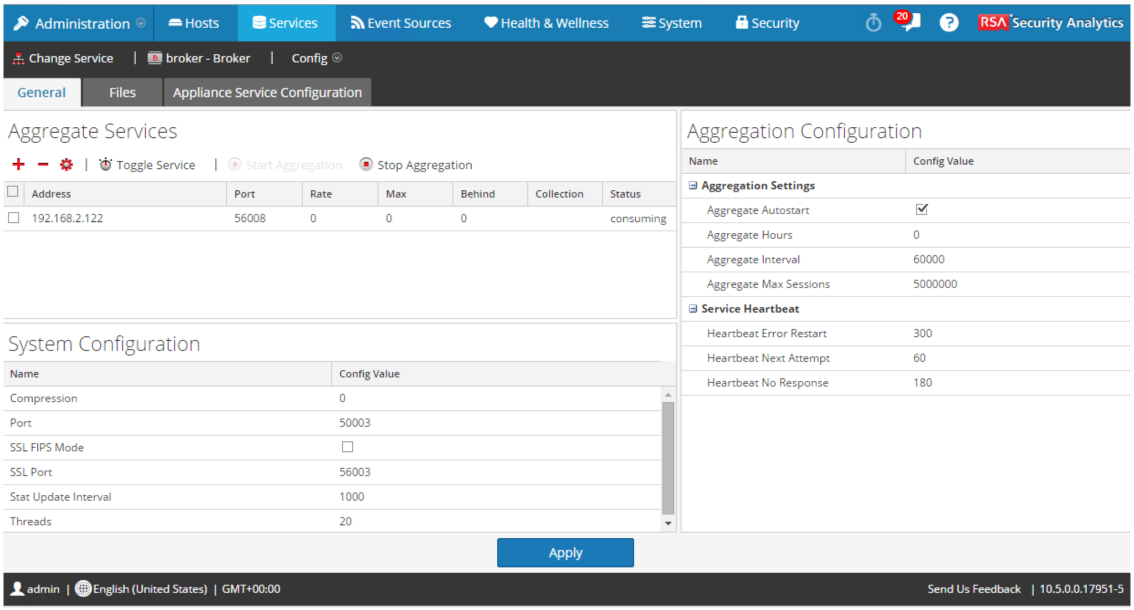
The Security Division of EMC

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



Aggregate Services

□	Address	Port	Rate	Max	Behind	Collection	Status
□	192.168.2.122	56008	0	0	0		consuming

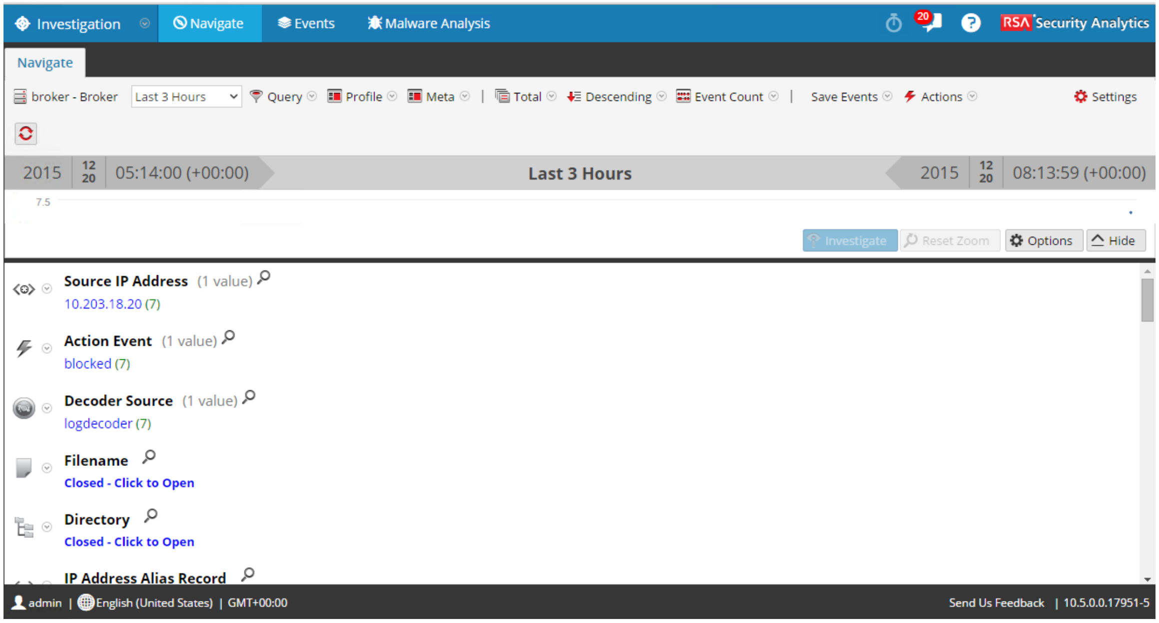
System Configuration

Name	Config Value
Compression	0
Port	50003
SSL FIPS Mode	□
SSL Port	56003
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
Aggregation Settings	
Aggregate Autostart	☑
Aggregate Hours	0
Aggregate Interval	60000
Aggregate Max Sessions	5000000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

- Investigate from the broker:-



Source IP Address (1 value)
10.203.18.20 (7)

Action Event (1 value)
blocked (7)

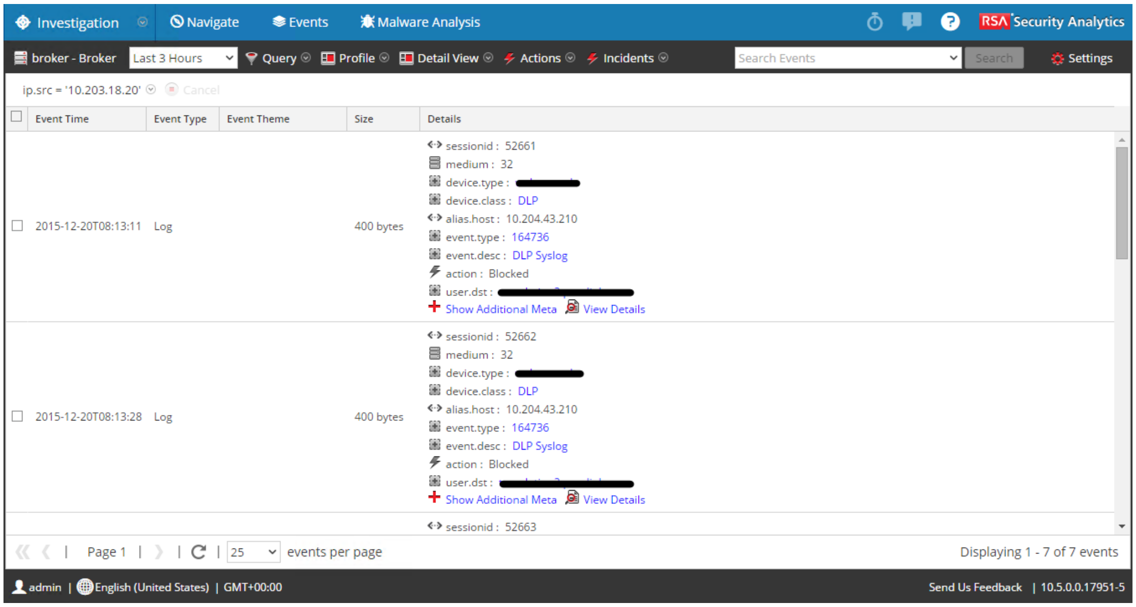
Decoder Source (1 value)
logdecoder (7)

Filename
Closed - Click to Open

Directory
Closed - Click to Open

IP Address Alias Record

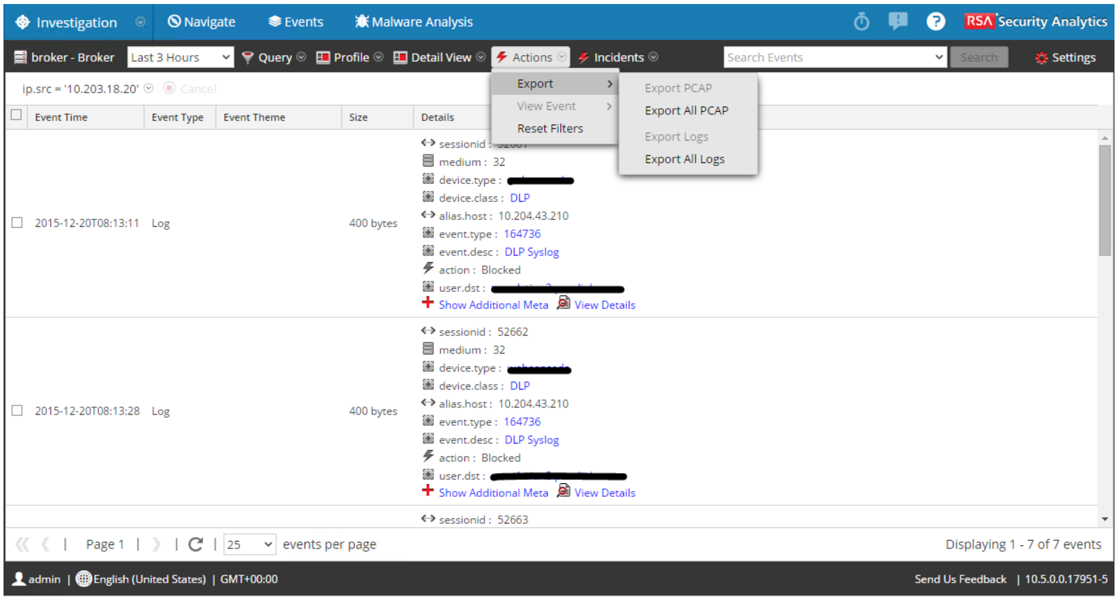
- Open the sessions



ip.src = '10.203.18.20'

	Event Time	Event Type	Event Theme	Size	Details
□	2015-12-20T08:13:11	Log		400 bytes	sessionid : 52661 medium : 32 device.type : [redacted] device.class : DLP alias.host : 10.204.43.210 event.type : 164736 event.desc : DLP Syslog action : Blocked user.dst : [redacted] Show Additional Meta View Details
□	2015-12-20T08:13:28	Log		400 bytes	sessionid : 52662 medium : 32 device.type : [redacted] device.class : DLP alias.host : 10.204.43.210 event.type : 164736 event.desc : DLP Syslog action : Blocked user.dst : [redacted] Show Additional Meta View Details
					sessionid : 52663

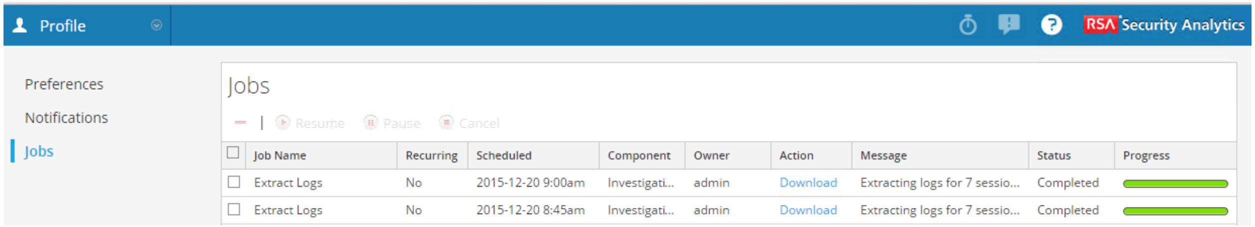
- Choose Actions->Export->Export all logs



ip.src = '10.203.18.20'

	Event Time	Event Type	Event Theme	Size	Details
□	2015-12-20T08:13:11	Log		400 bytes	sessionid : 52661 medium : 32 device.type : [redacted] device.class : DLP alias.host : 10.204.43.210 event.type : 164736 event.desc : DLP Syslog action : Blocked user.dst : [redacted] Show Additional Meta View Details
□	2015-12-20T08:13:28	Log		400 bytes	sessionid : 52662 medium : 32 device.type : [redacted] device.class : DLP alias.host : 10.204.43.210 event.type : 164736 event.desc : DLP Syslog action : Blocked user.dst : [redacted] Show Additional Meta View Details
					sessionid : 52663

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



☐	Job Name	Recurring	Scheduled	Component	Owner	Action	Message	Status	Progress
☐	Extract Logs	No	2015-12-20 9:00am	Investigati...	admin	Download	Extracting logs for 7 sessio...	Completed	🟩
☐	Extract Logs	No	2015-12-20 8:45am	Investigati...	admin	Download	Extracting logs for 7 sessio...	Completed	🟩

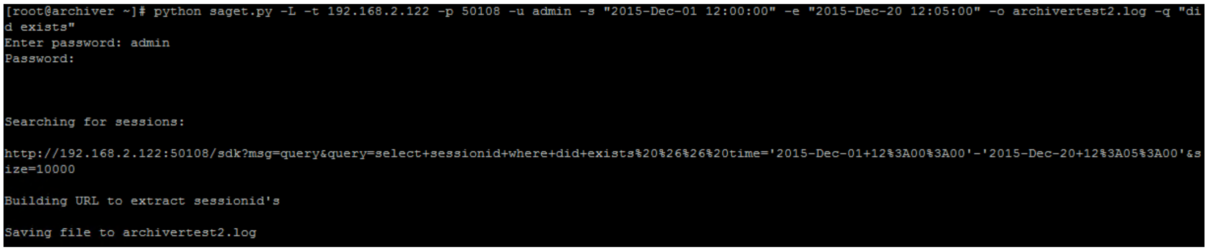
2nd option: Using saget.py script from the CLI:-

- 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:-

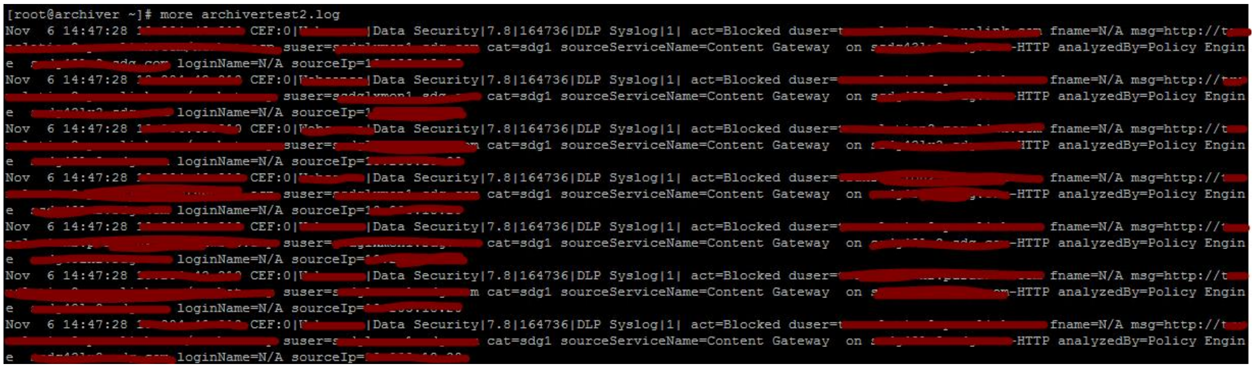
-t : Archiver’s IP.
-p : REST Port.
-u : REST username.
-s : Start time of the query.
-e : End time of the query.
-o : output file to save the sessions to.
-q : query to execute.

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.



```
[root@archiver ~]# 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 "di
d exists"
Enter password: admin
Password:



Searching for sessions:

http://192.168.2.122:50108/sdk?msg=query&query=select+sessionid+where+did+exists%20%26%26%20time='2015-Dec-01+12%3A00%3A00'-'2015-Dec-20+12%3A05%3A00'&s
ize=10000

Building URL to extract sessionid's

Saving file to archivertest2.log
```

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



```
[root@archiver ~]# more archivertest2.log
Nov  6 14:47:28 [redacted] CEF:0|[redacted]|Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted] suser=[redacted] cat=sdg1 sourceServiceName=Content Gateway  on [redacted]-HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
Nov  6 14:47:28 [redacted] CEF:0|[redacted]|Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted] suser=[redacted] cat=sdg1 sourceServiceName=Content Gateway  on [redacted]HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
Nov  6 14:47:28 [redacted] CEF:0|[redacted]Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted]suser=[redacted] cat=sdg1 sourceServiceName=Content Gateway  on [redacted]HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
Nov  6 14:47:28 [redacted] CEF:0|[redacted]|Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted] suser=[redacted] cat=sdg1 sourceServiceName=Content Gateway  on [redacted]-HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
Nov  6 14:47:28 [redacted] CEF:0|[redacted]|Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted] suser=[redacted] cat=sdg1 sourceServiceName=Content Gateway  on [redacted]-HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
Nov  6 14:47:28 [redacted] CEF:0|[redacted]|Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted] suser=[redacted]m cat=sdg1 sourceServiceName=Content Gateway  on [redacted]-HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
Nov  6 14:47:28 [redacted] CEF:0|[redacted]|Data Security|7.8|164736|DLP Syslog|1| act=Blocked duser=[redacted] fname=N/A msg=http://[redacted]
[redacted] suser=[redacted] cat=sdg1 sourceServiceName=Content Gateway  on [redacted]-HTTP analyzedBy=Policy Engin
e  [redacted] loginName=N/A sourceIp=[redacted]
```