C2150-624 Q&As

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which AQL query, when run from IBM Security QRadar SIEM V7.2.8, will show EPS broken down by domains?

A. select DOMAINNAME (domainid) as LogSource, sum(eventcount) / ((max(endTime) ? min(startTime)) / 1000) as EPS from events group by domainid order by EPS desc last 24 hours

B. select DOMAINNAME (domainqid) as LogSource, sum(eventcount) / ((max(endTime) ? min(startTime)) / 1000) as EPS from events group by domainqid order by FPM desc last 24 hours

C. select DOMAINNAME (domainid) as LogSource, sum(events) / ((max(endTime) ?min(startTime)) / 1000) as EPS from events group by domainid order by FPM desc last 24 hours

D. select DOMAINNAME (domainid) as LogSource, sum(events) / ((max(endTime) ?min(startTime)) / 1000) as EPS from events group by domainid order by EPS desc last 24 hours

Correct Answer: A

You would use single-quotes to define this search string. I believe I had an example in the presentation

yesterday I need to fix where I accidently used double-qoutes, which is incorrect.

The AQL search below uses quotes correctly:

select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) -min(startTime)) /

1000) as EPS from events WHERE logsourcename(logsourceid) = \\'Windows Auth@ 10.10.10.10\\' group

by logsourceid order by EPS desc last 5 MINUTES

Or to snag multiple log sources, for example Windows events, you could use the following:

select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) -min(startTime)) /

1000) as EPS from events WHERE logsourcename(logsourceid) is ILIKE \\'%Windows%\\' group by

logsourceid order by EPS desc last 5 MINUTES

QUESTION 2

What is the minimum required IBM Security QRadar SIEM software level to upgrade directly to V7.2.8?

A. QRadar 7.2.3

B. QRadar 7.2.4

C. QRadar 7.2.6

D. QRadar 7.2.7 Patch1

Correct Answer: B

QUESTION 3

On a flow search dashboard item in IBM Security QRadar SIEM V7.2.8, search results display real-time

last-minute data on chart.

What are the supported chart types?

A. Bar, Line, Pie, Table

B. Bar, Line, Histogram, Pie

C. Bar, Pie, Table, Time Series

D. Histogram, Pie, Table, Time Series

Correct Answer: C

QUESTION 4

What data is purged by the SIM reset process "Hard Clean" in IBM Security QRadar SIEM V7.2.8?

A. All current and historical SIM data.

B. All historical SIM data, current SIM data is retained.

C. All SIEM data, a complete reconfiguration is required.

D. All source and destination IP addresses are purged, all offenses in the database are closed.

Correct Answer: A

Hard clean Purges all current and historical SIM data, which includes offenses, source IP addresses, and destination IP addresses.

QUESTION 5

After downloading the .sfs file from Fix Central, what is the next step to upgrade IBM Security QRadar SIEM V7.2.8?

A. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Clean SIM Model.

B. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Upgrade option.

C. Use SSH to log in to the system as the root user -> Run the patch installer with the following command: /media/updates/upgrade_qradar.

D. Use SSH to log in to the system as the root user -> Copy the patch file to the /tmp directory or to another location that has sufficient disk space.

Correct Answer: D