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.pass4itsure.com/c2150-624.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An Administrator was modifying SNMP settings in an IBM Security QRadar SIEM V7.2.8 distributed

deployment.

What task should be taken to apply these changes?

A. Save Changes

B. Restart Web Server

C. Deploy Full Configuration

D. Restart PostgreSQL database

Correct Answer: C

Reference: ftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.2/QRadar/EN/QRadar_Administration_Guide_7.2.2_en.pdf

QUESTION 2

An Administrator is tasked with installing additional log sources into an IBM Security QRadar SIEM V7.2.8

deployment, bringing the total number of log source to 900. The deployment is using the default license

and the Administrator is getting an error attempting to add these additional log sources.

Why is this error happening?

A. The default license only allows 250 log sources.

B. The default license only allows 500 log sources.

C. The default license only allows 750 log sources.

D. The default license only allows 800 log sources.

Correct Answer: C

QUESTION 3

An Administrator working with IBM Security QRadar SIEM V7.2.8 has to add a new host name to a

reference set with the name "Allowed Hosts" from the command line interface.

Which command would accomplish this task?

A. ./ReferenceSetUtil.sh add Allowed\ Hosts computer.domain.com

B. ./UtilReferenceSet.sh add "Allowed Hosts" "computer.domain.com"

C. ./UtilReferenceSet.sh update Allowed\ Hosts "computer.domain.com"

D. ./ReferenceSetUtil.sh update "Allowed Hosts" "computer.domain.com"

Correct Answer: A

QUESTION 4

An IBM Security QRadar SIEM V7.2.8 Administrator needs to check if the "hostcontext" process is running. How can the Administrator do this?

A. hostcontext status

B. status hostcontext service

C. service hostcontext status

D. /etc/qradar/hostcontext status

Correct Answer: C

QUESTION 5

An IBM Security QRadar SIEM V7.2.8 Administrator assigned to a company that is looking to add QRadar into their current network. The company has requirements for 250,000 FPM, 15,000 EPS and FIPS. Which QRadar appliance solution will support this requirement?

A. QRadar 3128-C with Basic License

B. QRadar 2100-C with Basic License

C. QRadar 3128-C with Upgraded License

D. QRadar 2100-C with Upgraded License

Correct Answer: C

The upgraded license of Qradar 3128-C has 300k FPM and 15000 EPS and FIPs. Therefore the Qradar 3128-C with upgraded license is the best choice for the company.

QUESTION 6

The Administrator of an IBM Security QRadar SIEM V7.2.8 deployment needs to determine which rules

are most active in generating offenses.

How would the Administrator accomplish this from the Offenses tab of the QRadar console?

A. Rules -> Group -> "Most Active Offenses".

B. Rules -> Rules -> Offense Count to reorder the column in descending order.

C. All Offenses -> All Offenses -> Offense Count to reorder the column in descending order.

D. All Offenses -> All Offenses -> Events to reorder the column in descending order. Use the Actions menu to view the rule information for a specific offence.

Correct Answer: B

1.

Click the Offenses tab.

2.

On the navigation menu, click Rules. To determine which rules are most active in generating offenses, from the rules page, click Offense Count to reorder the column in descending order.

3.

Double-click any rule to display the Rule Wizard. You can configure a response to each rule.

QUESTION 7

What is important to understand when adding Offense Items to a Dashboard tab in IBM Security QRadar SIEM V7.2.8?

A. Minor or Hidden Offenses are not included in the values that are displayed.

B. Minor or Closed Offenses are not included in the values that are displayed.

C. Closed or Hidden Offenses are not included in the values that are displayed.

D. Closed or Assigned Offenses are not included in the values that are displayed.

Correct Answer: C

Reference: http://www-03.ibm.com/certify/jp-ja/tests/objC2150-195.shtml

QUESTION 8

When migrating the Console after restoring from an IBM Security QRadar SIEM V7.2.8 backup, what must be manually copied?

A. The Connection data and Topology data

B. The Policy Monitor questions and event or flow data

C. TheQRadar Risk Manager device configurations and Topology data

D. The certificates, any custom generated private keys and event or flow data

Correct Answer: D

QUESTION 9

A retention policy allows an IBM Security QRadar SIEM V7.2.8 Administrator to define how long the system is required to keep certain types of data and what to do when data reaches a certain age. If a 3month retention policy is defined for all events, then the system will not delete event data until it\\'s on disk timestamp is 3 months in the past. Which two choices are available in the `delete data in this bucket\\'? (Choose two.)

A. When the index is full

B. Upon reboot of the system

C. When storage space is required

D. When performance is heavily affected

E. Immediately after retention period has expired

Correct Answer: CE

From the list box, select a deletion policy. Options include: ?When storage space is required - Select this option if you want events or flows that match the Keep data placed in this bucket for parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads. When storage is required, only events or flows that match the Keep data placed in this bucket for parameter are deleted. Immediately after the retention period has expired ?Select this option if you want events to be deleted immediately on matching the Keep data placed in this bucket for parameter. The events or flows are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.

QUESTION 10

Which permission can be assigned to a user from User Roles in the IBM Security QRadar SIEM V7.2.8 Console?

A. Admin

B. DSM Updates

C. Flow Activity

D. Configuration Management

Correct Answer: A

Grants administrative access to the user interface. You can grant specific Admin permissions. Users with System Administrator permission can access all areas of the user interface. Users who have this access cannot edit other administrator accounts.

QUESTION 11

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 12

An Administrator working within IBM Security QRadar SIEM V7.2.8 has a network hierarchy that cannot support anymore network objects. To remedy this, they want to implement a supernet. Some of the customer CIDRs are:

-209.60.128.0/24

-209.60.129.0/24

-209.60.130.0/24

-

209.60.131.0/24

Which supernet should be used to shrink the amount of network objects for the supplied group of CIDRs?

A.

209.60.128.0/22

B.

209.60.129.0/23

C.

209.60.128.0/23

D.

209.60.127.0/27

Correct Answer: C

Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. Using supernetting, the network address 209.60.128.0/24 and an adjacent address 209.60.129.0/24 can be merged into 209.60.128.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses

QUESTION 13

Which is an officially supported web browser for managing IBM Security QRadar SIEM V7.2.8?

A. Safari

B. Vivaldi

C. Opera Netscape

D. Mozilla Firefox ESR

Correct Answer: D

QUESTION 14

How can an IBM Security QRadar SIEM V7.2.8 Administrator capture specific data to a reference set when QRadar receives the data from events or flow data?

A. Create or modify a report so the required data is exported to a Reference: Set.

B. On the Admin tab. create or modify the reference set to capture the required data.

C. On the Admin tab define a Custom Action to add the required data to a Reference: Set.

D. Create or modify a rule so the Rule Response will add the required data to a Reference: Set.

Correct Answer: B

You can click on the admin tab and select system configuration. The Reference: set management will be seen. Click New and configure the parameters.

QUESTION 15

An Administrator working with IBM Security QRadar SIEM V7.2.8 is constantly receiving the following

message:

"MPC: Unable to process offense. The maximum number of offenses has been reached."

What is the reason for this message?

A. The Multi Packet Capturer cannot handle more than 2500 attacks at the same time.

B. The Magistrate Processor Core has more than 2500 active Offenses or 100000 overall Offenses.

C. The Multi Packet Capturer cannot handle more than 500 offense reports at a certain point in time.

D. The Magistrate Processor Core has reached its maximum amount of network connections at a certain time.

Correct Answer: B