C2150-624 Q&As

IBM Security QRadar Risk Manager V7.2.6 Administration

Pass IBM C2150-624 Exam with 100% Guarantee

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

QUESTION 1

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 2

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 3

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to assign a report to a group

named Network Management.

What is the process for this task to be completed?

A. Reports Tab -> Select report -> Actions -> Assign Groups -> Item Groups -> select Network Management -> Assign Groups

B. Admin Tab -> Report Permissions -> select report -> Actions -> Assign Groups -> select Network Management -> Assign

C. Reports Tab -> Select report -> Actions -> Assign Users -> User Groups -> select Network Management -> Assign

Users

D. Admin Tab -> Report Permissions -> select report -> Actions -> Assign Users -> select Network Management -> Assign

Correct Answer: A

You can use the Assign Groups option to assign a report to another group

1.

Click the Reports tab.

2.

Select the report that you want to assign to a group.

3.

From the Actions list box, select Assign Groups.

4.

From the Item Groups list, select the check box of the group you want to assign to this report.

5.

Click Assign Groups

QUESTION 4

What is a precaution an Administrator should take before beginning an upgrade of IBM Security QRadar SIEM V7.2.8?

A. Close all open offenses.

B. Purge old data and events.

C. Check and close all open messages.

D. Confirm that a backup of the data is complete.

Correct Answer: D

The first precaution listed in the IBM document states that the administrator should backup data before preparing for software upgrade. Backup of the current settings is important because if anything bad happens during the upgrade, you can always revert back to the original settings.

QUESTION 5

Which appliance of the IBM Security QRadar SIEM V7.2.8 family is a specifically used to gather events from local and remote log sources?

A. QRadar Event Console

B. QRadarQFlow Collector

C. QRadar Event Collector D. QRadar Event Processor

Correct Answer: C

Gathers events from local and remote log sources.Normalizes raw log source events. During this process, the Magistrate component examines the event from the log source and maps the event to a QRadar Identifier (QID). Then, the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor.

QUESTION 6

An Administrator using IBM Security QRadar SIEM V7.2.8 is using the RegEx syntax below:

(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

What type of information is it designed to extract?

A. An IP Address

B. GPS Coordinates

C. A Telephone Number

D. A simple integer no longer than 4 digits

Correct Answer: A

Sample regular expressions:

email: (.+@[^\.].*\.[a-z]{2,}$)

URL: (http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\ S*)?$)

Domain Name: (http[s]?://(.+?)["/?:])

Floating Point Number: ([-+]?\d*\.?\d*$)

Integer: ([-+]?\d*$)

IP Address: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

For example: To match a log that resembles: SEVERITY=43 Construct the following Regular

Expression: SEVERITY=([-+]?\d*$)

QUESTION 7

The following error message is displayed when an Administrator attempts to log in to the IBM Security

QRadar SIEM V7.2.8 environment with a known valid Active Directory (AD)account:

"The username and password you supplied are not valid. Please try again."

What procedure should be followed to find the problem?

A. Run the command "adconn -q " and see if the machine can connect to the AD Servers.

B. Run the command "setaddate -q " to synchronize the system time of the QRadar environment with the Active Directory environment.

C. Run the command "ntpdate -q " and see if the offset between the QRadar machine and the Active Directory machine is larger than 300 seconds.

D. Run the command "/opt/qradar/bin/support/Check_AD.sh " and see if the output of the script displays the source of the authentication problems.

Correct Answer: B

QUESTION 8

An Administrator of an IBM Security QRadar SIEM V7.2.8 deployment needs to exclude the mail servers

from a custom rule.

How would the Administrator complete this task?

A. Create a building block that includes the IP addresses of all mail servers, use that building block in the custom rule, to exclude those hosts.

B. Create several rules excluding each mail server. Place these rules with the custom rule in a master rule, making sure the custom rule is last in the sequence.

C. Create a custom rule. In the "Rule Response" section of the Rule Wizard, select the Trigger Scan option. Add the mail server IP Addresses to the table and select exclude.

D. Create the custom rule. Create a Custom Action from the Admin Tab, to exclude the mail servers IP Addresses. In the "Rule Response" section of the Rule Wizard, select the Execute Custom Action option, selecting the appropriate Custom Action.

Correct Answer: A

Building blocks use the same tests as rules, but have no actions associated with them. Building blocks group together commonly used tests, to build complex logic, so they can be used in rules. Building blocks are often configured to test groups of IP addresses, privileged usernames, or collections of event names. For example, you might create a building block that includes the IP addresses of all mail servers in your network, then use that building block in another rule, to exclude those hosts. The building block defaults are provided as guidelines, which should be reviewed and edited based on the needs of your network.

QUESTION 9

What is the function of the dashboard tab in IBM Security QRadar SIEM V7.2.8?

A. To create reference sets.

B. To create users and roles and track their activity.

C. Dashboards allow quick access to building block and rule creation.

D. Dashboards allow organization of dashboard items into functional views.

Correct Answer: D

QUESTION 10

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 11

Where are the IBM Security QRadar SIEM V7.2.8 errors logged?

A. /var/log/qradar.error

B. /var/log/qradar/error.log

C. /opt/qradar/log/qradar.error

D. /opt/qradar/support/qradar.log

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/
c_qradar_siem_inst_logs.html

QUESTION 12

Which query, when run from IBM Security QRadar SIEM V7.2.8, will show EPS for log sources?

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

B. select logsourcename(logsourceqid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as EPS from events group by logsourceqid order by EPS desc last 24 hours

C. select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as FPS from events group by logsourceid order by EPS desc last 24 hours

D. select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min (startTime)) / 1000) as EPS from events group by logsourceid order by FPS desc last 24 hours

Correct Answer: B

QUESTION 13

An IBM Security QRadar SIEM V7.2.8 Administrator wants to create a security profile within the system but

receives an error upon saving.

What is a possible reason for this error?

A. The Administrator has used non alpha numeric value(s) in the name which is not allowed.

B. The Administrator has used less than 3 characters or more than 30 characters as name of the security profile.

C. The Administrator has mixed non alpha numeric value(s) and alpha numeric value(s) in the name which is not allowed.

D. The Administrator must bring the IBM Security QRadar SIEM V7.2.8 system first in edit mode before changes are allowed.

Correct Answer: B

In the Security Profile Name field, type a unique name for the security profile. The security profile name must meet the following requirements: minimum of 3 characters and maximum of 30 characters.

QUESTION 14

An Administrator working with an IBM Security QRadar SIEM V7.2.8 deployment needs to build an Ariel

Query to find all flow data send in the last 24 hours where the amount of bytes being sent and received are larger than 64 bytes.

What Query needs to be used?

A. SELECT * FROM flows WHERE sourceBytes> 64 anddestinationBytes> 64 LAST 1 DAY

B. SELECT * FROM flows WHERE sourceBytes> 64 AND destinationBytes> 64 LAST 1 DAYS

C. SELECT * FROM flowsdata WHERE sourceBytes> 64 AND destinationBytes> 64 LAST 1 DAY

D. SELECT * FROM flowsdata WHERE sourceBytes> 64 AND destinationBytes> 64 LAST 1 DAYS

Correct Answer: B

QUESTION 15

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