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.pass2lead.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

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to configure the deployment to

add a log source from IBM Bluemix.

What protocol is supported for this?

A. JDBC

B. LEEF

C. WinCollect

D. TLS Syslog

Correct Answer: D

QUESTION 2

An Administrator has configured a customized log source extension to provide asset updates to IBM Security QRadar SIEM V7.2.8. Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name. In this situation what will QRadar report?

A. This will cause stale asset data.

B. This will cause asset growth deviations.

C. This will cause excessive authentication failure events.

D. This will cause excessive flow data to be processed by the Magistrate.

Correct Answer: B

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the

log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses

and user names.

QUESTION 3

An Administrators will add a secondary host to an IBM Security QRadar SIEM V7.2.8 Console in a High

Availability (HA) deployment scenario.

After checking the compatibility between primary and secondary HA pairs, what other prerequisite should

the Administrator check within Managed Interfaces?

A. The shared external storage.

B. The server certificate that is issued by the local CA.

C. The existence of an additional distributed file system.

D. The communication for Distributed Replicated Block Device.

Correct Answer: D

CP port 7789 must be open and allow communication between the primary and secondary for Distributed

Replicated Block Device (DRBD) traffic.

DRBD traffic is responsible for disk replication and is bidirectional between the primary and secondary

host.

QUESTION 4

How many dashboards come by default in IBM Security QRadar SIEM V7.2.8?

A. 1

B. 5

C. 7

D. 10

Correct Answer: B

There are five default dashboards: 1 application overview 2 compliance overview 3 network overview 4 system monitoring 5 threat and security monitoring

QUESTION 5

Where are the IBM Security QRadar SIEM V7.2.8 log files located?

A. /var/qradar.log

B. /var/log/qradar.log

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

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

Correct Answer: B

You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

To help you troubleshoot errors or exceptions, review the following log files.

/var/log/qradar.log

/var/log/qradar.error

If you require more information, review the following log files:

/var/log/qradar-sql.log

/opt/tomcat6/logs/catalina.out

/var/log/qflow.debug

Review all logs by selecting Admin > System and License Mgmt> Actions > Collect Log Files.

QUESTION 6

An Administrator using IBM Security QRadar SIEM V7.2.8 needs to force an instant backup to run. Which option should be selected?

A. Backup Now

B. On Demand Backup

C. Launch On Demand Backup

D. Configure On Demand Backup

Correct Answer: D

QUESTION 7

An Administrator of an IBM Security QRadar SIEM V7.2.8 deployment has configured an asset data

source with domain information. This has created several new asset profiles.

What would explain these new asset profiles?

A. The asset data source parameter "Collateral Damage Potential" was left at the default "Not Defined"

B. The data in the asset model is domain-aware, this information is applied to all QRadar components, including server discovery.

C. The data in the asset model is used to compare flow data and identify other assets. These assets are added to a "Whitelist" database for asset reconciliation.

D. The asset data source is attempting to process an asset merge. The information from one asset is combined with the information for another asset under the premise that they are actually the same physical asset.

Correct Answer: A

QUESTION 8

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 9

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 10

When an IBM Security QRadar SIEM V7.2.8 distributed deployment requires scaling horizontally to achieve Event per Second (EPS) requirements, what QRadar Component needs to be added to meet the EPS demands?

A. Event Manager

B. Event Indexing

C. Event Collector

D. Event Processor

Correct Answer: D

QUESTION 11

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 12

An IBM Security QRadar SIEM V7.2.8 Administrator will install a High Availability (HA) pair of appliances.

The primary and secondary hosts are formatted with the same file system.

To ensure compatibility between hosts, which statement is considered a prerequisite?

A. The size of the /home partition on the secondary must be larger than the /home partition of the primary.

B. The size of the /var/opt/ha on the secondary must be larger than the /var/opt/ha partition of the primary.

C. The size of the /store partition on the secondary must be lesser than the /store partition of the primary.

D. The size of the /store partition on the secondary must be equal to or larger than the /store partition of the primary.

Correct Answer: D

Store partition requirements For example, do not pair a primary host that uses a 3 TB /store partition to a secondary host that has a 2 TB /store partition.

QUESTION 13

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 14

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 15

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.