IBM

Exam C2150-624

IBM Security QRadar SIEM V7.2.8 Fundamental Administration

Verson: Demo

[Total Questions: 10]

Question No : 1

What is needed to send the same events and flows to separate data centers or geographically separate sitesand enable data redundancy in IBM Security QRadar SIEM V7.2.8?

A. A Flashcopy or GlobalMirror License.
B. A dark fibre network and proper configuration of the backup and recovery feature.
C. A load balancer or other method to deliver the same data to mirrored appliances.
D. Use the Backup and Recovery automation feature in QRadar and a dedicated fiber channel connection.

Answer: C

Explanation:

Distribute the same event and flow data to two live sites by using a load balancer or other method to deliverthe same data to mirrored appliances. Each site has a record of the log data that is sent.
Referencehttps://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/
c_qradar_ha_data_redundancy_overview.html

Question No : 2

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

Answer: D

Explanation:

The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:
Up to 10,000 events per second
2 TB or larger dedicated event storage
Referencehttps://www.ibm.com/support/knowledgecenter/SS42VS_7.2.4/com.ibm.qradar.doc_7.2.4/
c_siem_vrt_ap_ov.html

Question No : 3

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

Answer: C
Explanation:

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.
Referencehttps://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/
c_hwg_3128_allone.html

Question No : 4

An IBM Security QRadar SIEM V7.2.8 Administrator needs to retain authentication failure data to a specificdomain, for a longer period than the rest of the event data being collected.

How is this task completed?

A. The administrator will need to create a custom rule with the appropriate filters and retention period.
B. The administrator will need to create a new Event Retention Bucket with the appropriate filters and
retention period.
C. The administrator will need to create a custom filter in the log activity tab with the appropriate parametersand retention period.
D. The administrator will need to create a custom report with the appropriate parameters and use the reportformat TAR (Tape archive).

Answer: B

Explanation:

In current versions of QRadar you can set custom retention buckets for Events and Flows. The 10 non-defaultretention buckets are processed sequentially from top to bottom. Any events that do not match the retentionbuckets are automatically placed in the default retention bucket, located at the bottom of the list. Customretention buckets allow the ability to add a time period and filters. If you enable a retention bucket with adefined criteria it will start deleting data from the time is was created. Any data that matches the customretention bucket before it was created is subject to the criteria of the default retention bucket setting. If youneed to delete data from before the Custom retention bucket was created you can shorten the defaultretention bucket so data is deleted immediately.
Referencehttp://www-01.ibm.com/support/docview.wss?uid=swg21622758

Question No : 5

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 securityprofile.
C. The Administrator has mixed non alpha numeric value(s) and alpha numeric value(s) in the name which isnot allowed.
D. The Administrator must bring the IBM Security QRadar SIEM V7.2.8 system first in edit mode beforechanges are allowed.

Answer: B

Explanation:

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

Referenceftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.1/QRadar/EN/
b_qradar_admin_guide.pdf

Question No : 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

Answer: A

Question No : 7

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.

Answer: D

Explanation:

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.

Referencehttps://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/

c_qradar_appliance_require.html

Question No : 8

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

A. 1
B. 5
C. 7
D. 10

Answer: B

Explanation:

There are five default dashboards:

1 – application overview

2 – compliance overview

3 – network overview

4 – system monitoring

5 – threat and security monitoring

Referenceftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_users_guide.pdf

Question No : 9

Where are the logs for QFlow stored on IBM Security QRadar SIEM V7.2.8?

A. /var/log/qflow.debug
B. /opt/var/log/qflow.debug
C. /opt/log/qradar/qflow.debug
D. /opt/qradar/log/qflow.debug

Answer: A

Explanation:

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 & License Mgmt > Actions > Collect Log Files.

Referencehttps://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.6/com.ibm.qradar.doc/
c_qradar_siem_inst_logs.html

Question No : 10

An Administrator needs to create a new user role in the IBM Security QRadar SIEM V7.2.8 system.

What steps need to be followed?

A. System Configuration tab -> Users and Roles -> Add New Role -> Add
B. Admin tab -> System Configuration -> User Management -> User Roles -> New
C. Admin tab -> System and Settings -> Users and Roles -> Role Management -> New
D. System Management tab -> System Configuration -> User Management -> User Roles -> New

Answer: B

Explanation:

By default, your system provides a default administrative user role, which provides access to all areas of
QRadar SIEM. Users who are assigned an administrative user role cannot edit their own account. This
restriction applies to the default Admin user role. Another administrative user must make any account
changes.
Referenceftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.1/QRadar/EN/
b_qradar_admin_guide.pdf