Vendor:IBM

Exam Code:C2150-624

Exam Name:IBM Security QRadar Risk Manager V7.2.6 Administration

Version: Demo

QUESTION 1

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 2

What is the difference between Flows and Event data collected by IBM Security QRadar SIEM V7.2.8?

A. Events are streamed each minute to the Event Processor. Flows are streamed immediately to the Flow Processor.

B. Flow data is collected from different log sources. Event data is collected from internal or external network sources.

C. An Event occurs at a specific time and is logged at that time. A Flow is a record of network activity that can last for seconds, minutes, hours, or days.

D. An Event can span time lasting seconds, minutes, hours depending on the duration of a network session. A Flow happens at a single point in time and then is complete.

Correct Answer: C

QUESTION 3

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 4

What key point should be understood about how flow information in IBM Security QRadar SIEM V7.2.8 is used?

A. Flow information generates the response that is configured in the custom rule.

B. Flow information is sent to QRadarQFlow Collector which normalizes raw log source events.

C. Flow information is actively gathered from the QRadar Event Collector and provides views, reports and alerts to the administrator.

D. Flow information is used to detect threats and other suspicious activity that might be missed if only event information were tracked.

Correct Answer: D

QUESTION 5

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 6

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to limit the networking team to see

just the Network Flow functions.

What should the Administrator do?

A. Create a user with access to the Log Activity tab.

B. Create a user role with Network Activity -> View Flow Content.

C. Create a user role with Network Activity -> View Reference: Data.

D. Create a user role which grants access to all the functions in the Network Activity tab.

Correct Answer: B

QUESTION 7

An Administrator working within IBM Security QRadar SIEM V7.2.8 has created a network hierarchy that includes the following groups and subgroups: Office #1 Group

-Miscellaneous 10.10.0.0/24

-Sales 10.10.8.0/24

-Marketing 10.10.1.0/24 Office #2 Group

-Miscellaneous 10.20.0.0/16

-Sales 10.20.8.0/24

-

Marketing 10.20.1.0/24 A new subgroup is added to Office #1 having a CIDR of 10.10.50.0/24. Offenses are being triggered and during the investigation, it is noticed the rule should not fire if traffic is L2L. The offense is being triggered on traffic from 10.10.4.17 to 10.20.1.8. Is this rule using the network hierarchy correctly?

A.

This rule is parsing the network hierarchy correctly, as the 10.10.4.17 address is not contained in a group, and therefore is remote.

B.

This rule is parsing the network hierarchy correctly, as the offices are both remotely geo-located, and connecting over the Internet, it is remote traffic.

C.

This rule isn\\'t parsing the network hierarchy correctly, as the network hierarchy contains the CIDR for

10.10.4.17 and 10.20.1.0/24, therefore being L2L traffic.

D.

This rule isn\\'t parsing the network hierarchy correctly, as the network hierarchy contains both subnets, but is viewing traffic between groups to be remote instead of local.

Correct Answer: A

QUESTION 8

An Administrator is unable to access the IBM Security QRadar SIEM V7.2.8 web GUI. What could the Administrator do to determine the reason for the issue?

A. Check the status of tomcat and httpd.

B. Check the status of ecs-ec and ecs-ep.

C. Check if the postgres database is running.

D. Check if the console is over the EPS and FPS license.

Correct Answer: A

QUESTION 9

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 10

When replacing a Console appliance in an IBM Security QRadar SIEM V7.2.8 deployment using a new IP address or host name, what must be the same on the two Console appliances?

A. The amount of storage must be the same.

B. The Basic and Upgrade license must be the same.

C. The software versions of both appliances must match.

D. The Network Configuration and Protocol must be the same.

Correct Answer: C

The software version of the new Console appliance must match the software version of the old Console appliance. QRadar does not allow appliances at different software versions in the deployment. Administrators might be required to reinstall an ISO for the appliance to downgrade or use a Fix Pack (SFS) to upgrade on the new appliance. The paperwork that came with your appliance lists the installed software version.

QUESTION 11

An IBM Security QRadar SIEM V7.2.8 Administrator wants to change the reference set type. What step(s) need to be taken to accomplish this?

A. Use the CLI with the ReferenceSetUtil.sh script

B. Recreate the reference set with the new data type

C. Admin tab -> System Configuration -> Reference: Set Management -> Edit

D. Admin tab -> System Configuration -> Reference: Set Type Management -> Edit

Correct Answer: C

QUESTION 12

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