C1000-026 Q&As

IBM Security QRadar SIEM V7.3.2 Fundamental Administration

Pass IBM C1000-026 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/c1000-026.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 needs to save the nightly QRadar backups on a network storage.

The administrator has established the connection to the network storage.

What should the administrator do next?

A. Change the Backup Repository Path to the network storage location using the Backup Recovery Configuration window.

B. Change the Backup Repository Path by adding a new Network Activity Rule.

C. Change the Backup Repository Path to the network storage location using the System Settings window.

D. Configure the new network storage using the Assets Manager

Correct Answer: A

Reference: http://ftpmirror.your.org/pub/misc/ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_admin_guide.pdf (146)

QUESTION 2

A custom rule is generating events reporting that a specific user is failing to login too many times in the last 5 minutes. The administrator opens the event details to investigate the anomaly associated with the events but finds that no Anomaly details pane is shown.

What is the reason?

The events were generated by:

A. a Behavioral Detection Rule

B. an Anomaly Detection Rule

C. a Threshold Detection Rule

D. a standard Custom Rule

Correct Answer: B

Reference: http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 3

An administrator would like to add a new managed host which uses an existing Network Address Translation (NAT).

Which parameters have to be provided if "Host is NATed" is chosen while adding a managed host?

A. Select Network Attached Telemetric, Enter MAC address of the server or appliance to add

B. Select NATed network, Enter public IP of the server or appliance to add

C. Select NATed network, Enter MAC address of the server or appliance to add

D. Select Network Attached Telemetric, Enter public IP of the server or appliance to add

Correct Answer: B

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=1andved=2ahUKEwihsu3Li5XmAhVYwAIHHeCLDtoQFjAAegQIBhACandurl=https%3A%2F%2Fwww.ibm.com%2Fdeveloperworks%2Fcommunity%2Fforums% 2Fajax%2Fdownload%2Fd5b20a5b-11bd-4a1d-b294-08ec138eb0e1%2F9d086dd8-eee9-4cbd-912d-26059ffdd0ca%2FQRadar_721_AdminGuide.pdfandusg=AOvVaw1GO4OmOjWV7uiyCLrdE0FV

QUESTION 4

A company has several appliances and the administrator needs to copy a file to all appliances to run some tests to verify the integrity of the processes. The /opt/qradar/support/all_servers.sh script can be used to issue commands to all QRadar appliances within the deployment.

What option must be used with the script to copy the file to all appliances in the deployment?

A. /opt/qradar/support/all_servers.sh -p

B. /opt/qradar/support/all_servers.sh -k

C. /opt/qradar/support/all_servers.sh -C

D. /opt/qradar/support/all_servers.sh -g

Correct Answer: A

Reference: https://www-01.ibm.com/support/docview.wss?uid=swg21998517

QUESTION 5

After fixing the assets that contributed to the asset growth deviation, an administrator needs to find the asset artifacts that have to be cleaned up.

What action should the administrator take to find the artifacts?

A. On the "Log Activity" tab, run the "Deviating Asset Growth: Asset Report event search"

B. On the Admin Tab, select System Configuration --> Asset Profiler Configuration

C. Run the ./cleanAssets.sh --list command

D. On the Asset tab, run the "Clean Assets" action

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_adm_assets_deleting_invalid_assets.html

QUESTION 6

An administrator needs to upgrade their QRadar environment. The administrator has downloaded the Patchupdate File from Fixcentral and transferred this Image to the Appliance.

Which commands does the administrator need to run to start the upgrade process?

A. 1. cd/medial/updates

2.

systemctl stop Qradar

3.

Qradar.sh upgrade all

4.

systemctl reboot

B. 1. mount –o loop –t squashfs XX_patchupdate.sfs /media/updates

2.

cd /media/updates

3.

/installer

C. 1. cd /media/updates

2. yum update XX_patchupdate.sfs

D. 1. patch XX_patchupdate.sfs

Correct Answer: B

QUESTION 7

An administrator needs to import data into QRadar for a specific use case.

The data that has been provided to the administrator is stored in records that map a key to a value.

Which type of data collection must the administrator create?

A. Reference set

B. Reference map of sets

C. Reference map

D. Reference map of maps

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/t_qradar_conifig_rul_resp_reference_set.html

QUESTION 8

An administrator logs into the QRadar Console to review the stored backup files. There is an exclamation mark beside some files.

What is the cause of this?

A. Canceled backup files

B. Missing backup files

C. Corrupted backup files

D. Incomplete backup files

Correct Answer: B

QUESTION 9

A QRadar user reported the following notification:

38750099 – The accumulator was unable to aggregate all events/flows for this interval

When does this message appear?

A. When the aggregate data view configuration that is in memory is unable to write data to the database

B. When the system is unable to accumulate data aggregations within 60 seconds

C. When aggregated data views are disabled

D. When search results is unable to return over 200 unique objects

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/38750099.html

QUESTION 10

An administrator enters the QRadar web console into a web browser but does not get a response. Which process is responsible for the QRadar GUI?

A. tomcat

B. consoled

C. magistrated

D. guid

Correct Answer: A

Reference: https://www.ibm.com/support/pages/qradar-core-services-and-impact-when-restarted