DUMPSARENA

IBM Security QRadar SIEM V7.3.2 Fundamental Administration

IBM C1000-026

Version Demo

Total Demo Questions: 8

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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

ANSWER: B

Explanation:

Reference:
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwihsu3Li5XmAhVYwAIHHeCLDtoQFjAAegQIBhAC&url=https%3A%2F%2Fwww.ibm.com%2Fdeveloperworks%2Fcommunity%2Fforums%2Fajax%

2Fdownload%2Fd5b20a5b-11bd-4a1d-b294-08ec138eb0e1%2F9d086dd8-eee9-4cbd-912d-26059ffdd0ca%2FQRadar_721_AdminGuide.pdf&usg=AOvVaw1GO4OmOjWV7uiyCLrdE0FV

QUESTION NO: 2

An administrator is about to integrate logs from a custom firewall in a QRadar deployment using syslog. The SIEM has two domains, namely Domain A and Domain

B. While reviewing the following sample logs, the administrator notices a “context” keyword:

May 14 11:05:01 192.168.1.23 20190514 11:05:00 context=contextA permit 192.168.1.24 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp; May 13 12:07:01 192.168.1.23 20190513 11:07:00 context=contextB permit 192.168.1.25 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp; Which options assign the “contextA” logs to DomainA and the “contextB” logs to domain B? (Choose two.)

A. Create a single log source, create a “Context” custom event property, and assign the log to both domains using a custom rule.

B. While reviewing the following sample logs, the administrator notices a “context” keyword:
May 14 11:05:01 192.168.1.23 20190514 11:05:00 context=contextA permit 192.168.1.24 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp; May 13 12:07:01 192.168.1.23 20190513 11:07:00 context=contextB permit 192.168.1.25 source: 10.10.1.15; source_port: 64094; destination: 10.10.13.34; service: 53; protocol: udp; Which options assign the “contextA” logs to DomainA and the “contextB” logs to domain B? (Choose two.)
Create two individual log sources by configuring a separated logging instance for each context on the firewall and assign each log source to the correct domain.

C. Create a single log source, create a “Context” custom event property, and assign the log to the correct domain using custom event property value.

D. Create two individual log sources using the context value as log source identifier and assign each log source to the correct domain.

E. Create a single log source, create a “Context” custom event property, and assign the log to the correct domain using a custom rule.

ANSWER: B D

QUESTION NO: 3

An administrator needs to collect logs from the Command Line Interface (CLI).

Which command should the administrator use?

A. /opt/bin/qradar/support/get_logs.sh

B. /opt/support/get_logs.sh

C. /opt/support/qradar/get_logs.sh

D. /opt/qradar/support/get_logs.sh

ANSWER: D

Explanation:

Reference: https://www.ibm.com/support/pages/getting-help-what-information-should-be-submitted-qradar-service-request

QUESTION NO: 4

Which event routing rule is required to add QRadar Data Store (QDS) capability to a deployment?

A. Log Only (exclude Analytics)

B. Delete data When storage space is required

C. Bypass Correlation

D. Delete data immediately after the retention period has expired

ANSWER: A

Explanation:

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

QUESTION NO: 5

A QRadar administrator added High Availability (HA) to the Event Processor and needs to verify the crossover link status between the primary and secondary hosts.

Which commands can be used to verify the crossover status? (Choose two.)

A. /opt/qradar/ha/bin/ha_getstate.sh

B. /opt/qradar/ha/bin/getStatus crossover

C. /opt/qradar/ha/bin/qradar_nettune.pl crossover status

D. /opt/qradar/ha/bin/qradar_nettune.pl linkaggr status

E. /opt/qradar/ha/bin/ha cstate

F. cat /proc/drbd

ANSWER: C F

Explanation:

Reference: https://www.ibm.com/developerworks/community/forums/html/topic?id=5c01c198-016d-461b-a648-a87cdc445768

QUESTION NO: 6

When an administrator attempts to edit a log source after upgrading QRadar, a Device Support Module (DSM), a protocol, or Vulnerability Information Services (VIS) components, the following error message appears.

An error has occurred. Refresh your browser (press F5) and attempt the action again. If the problem persists, please contact customer support for assistance.

What action should the administrator take to troubleshoot this issue? (Choose two.)

A. systemctl restart snmpd

B. systemctl restart iptables

C. systemctl restart ecs-ep

D. systemctl start tomcat

E. systemctl restart httpd

F. Clear browser cache

ANSWER: D F

Explanation:

Reference:
https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/t_QRadar_Troubleshooting_guide_PurgeFiles.html

QUESTION NO: 7

An administrator is tasked to reduce data volumes in the asset database and reduce stale data contributing to asset growth deviation.

How can the administrator tune the configuration of the Asset Profiler?

A. In the System Configuration section of the Admin, access the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save. Next, deploy the changes into the environment for the updates to take effect.

B. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save. Next, deploy the changes into the environment for the updates to take effect.

C. On the navigation menu, click Admin, click the Asset Profile Configuration and reduce the retention values for the Asset Profiler Retention Configuration and Save. On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

D. In the System Configuration section of the Admin, access the Asset Profile Configuration and increase the retention values for the Asset Profiler Retention Configuration and Save. On the navigation menu, click Admin and from the Advanced menu, click Restart Event Collection Services. Next, deploy the changes into the environment for the updates to take effect.

ANSWER: B

Explanation:

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

QUESTION NO: 8

An administrator needs to import a list of HR staff logins into a reference set.

Which file type can be used with the import function in the reference set editor window?

A. xml

B. csv

C. xls

D. json

ANSWER: B

Explanation:

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