Vendor:IBM

Exam Code:C1000-026

Exam Name:IBM Security QRadar SIEM V7.3.2 Fundamental Administration

Version: Demo

QUESTION 1

An administrator needs to combine multiple extraction and calculation-based properties into a single property.

Which Ariel Query Language (AQL) statement can be used?

A. AQL-based custom properties

B. AQL functions and SELECT, FROM, or database names

C. AQL functions and AQL-based custom properties

D. AQL functions

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_aql_whatsnew_731.html

---

QUESTION 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. 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.

Correct Answer: BD

QUESTION 3

Which app should be used for monitoring QRadar performance and health?

A. QRadar Deployment Intelligence

B. QRadar Monitoring Intelligence

C. QRadar Extension Management

D. QRadar Performance Overview

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/en/SSKMKU/com.ibm.QDIapp.doc/ c_qapps_QDI_intro.html

---

QUESTION 4

An administrator installed a new App Host and would like to move the existing applications from the Console to the App Host.

What steps should be performed?

A. Admin Tab > Extension Management > Click to change where apps are run

B. Admin Tab > System Settings > Move apps

C. Admin Tab > Extension Management > Move apps

D. Admin Tab > System and License Management > Click to change where apps are run

Correct Answer: D

QUESTION 5

A QRadar upgrade is planned and a maintenance window is scheduled. The administrator must stage the FIXPACK from IBM Fix Central.

Which QRadar FIXPACK file type must the administrator download?

A. RPM

B. IMG

C. SFS

D. XFS

Correct Answer: C

Reference: https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%
20Securityandproduct=ibm/Other+software/IBM+QRadar+Network
+Insightsandrelease=7.3.0andplatform=Linuxandfunction=all

QUESTION 6

What is a reason for restarting hostcontext service in QRadar?

A. A new user was created and it needs to be replicated

B. A new network hierarchy was uploaded

C. A new app was installed

D. The host is not responding to deploy requests

Correct Answer: D

Reference: https://www.ibm.com/support/pages/qradar-restarting-hostcontext-q-switch

---

QUESTION 7

An administrator has been tasked to create a saved search that shows a list of multiple login failures for a single user by username. The administrator has done the following:

1.

Selected Last Hour in the view option.

2.

In the Add filter window, selected the search parameter Custom Rule [Indexed].

3.

Selected Equals for Operator.

4.

Selected Authentication for Rule Group.

What is the next step the administrator needs to perform for the Rule option?

A. Select login failures followed by success to the same username

B. Select multiple login failures from the same source

C. Select multiple login failures to the same destination

D. Select multiple login failures for a single username

Correct Answer: C

QUESTION 8

An administrator has been asked to configure a new QRadar console high availability (HA) deployment. Both the primary and secondary consoles have been installed with the QRadar software.

What should the administrator do to complete the HA configuration?

A. Add the secondary console to the deployment, and then create the HA host.

B. Reinstall the QRadar software on the secondary console using an "HA Recovery Setup".

C. Select "Secondary Host" on the wizard when adding the secondary host to the deployment.

D. Create the HA host to add the secondary console to the deployment.

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/ b_qradar_ha_guide.pdf

---

QUESTION 9

An administrator has added a new Event Processor to a QRadar deployment.

How many events per second (EPS) are granted from the temporary license and how many days will those EPS last?

A. 10000 EPS for a 35 day period

B. 5000 EPS for a 45 day period

C. 10000 EPS for a 45 day period

D. 5000 EPS for a 35 day period

Correct Answer: D

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

---

QUESTION 10

Which event QID test is used to send an email as a rule response when disk usage reaches a threshold?

A. (38750076) Disk Sentry Reached Warn threshold

B. (38750076) Disk Sentry Disk Usage Exceeded Warning threshold levels

C. (38750076) Disk Usage Exceeded Warn threshold

D. (38750076) Disk Sentry Disk Usage Exceeded Warn threshold

Correct Answer: B

Reference: https://www.ibm.com/support/pages/qradar-configuring-qradar-remote-alerts-about-disk-usage

---

QUESTION 11

An administrator enabled the base license of QRadar Vulnerability Manager.

How many assets can be scanned using this license?

A. up to 128

B. up to 256

C. up to 100

D. up to 512

Correct Answer: B

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

---

QUESTION 12

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

Correct Answer: DF

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