EDUSUM

#1 Online Certification Guide

IBM C1000-026

IBM QRadar SIEM Fundamental Administration Certification Questions & Answers

Exam Summary – Syllabus –Questions

C1000-026

IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2

60 Questions Exam – 67% Cut Score – Duration of 90 minutes

Table of Contents:

Know Your C1000-026 Certification Well:

The C1000-026 is best suitable for candidates who want to gain knowledge in the IBM Security. Before you start your C1000-026 preparation you may struggle to get all the crucial QRadar SIEM Fundamental Administration materials like C1000-026 syllabus, sample questions, study guide.

But don't worry the C1000-026 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the C1000-026 syllabus?
- How many questions are there in the C1000-026 exam?
- Which Practice test would help me to pass the C1000-026 exam at the first attempt?

Passing the C1000-026 exam makes you IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2. Having the QRadar SIEM Fundamental Administration certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

IBM C1000-026 QRadar SIEM Fundamental Administration Certification Details:

Exam Name	IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2
Exam Code	C1000-026
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	60
Passing Score	67%
Books / Training	**IBM QRadar SIEM Foundations**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM QRadar SIEM Fundamental Administration Sample Questions**
Practice Exam	**IBM C1000-026 Certification Practice Exam**

C1000-026 Syllabus:

Topic	Details	Weights
Implementing	- Plan and design QRadar deployment. - Implement and install QRadar. - Add Managed Hosts.	8%
Migrating and upgrading	- Plan QRadar upgrade and migration. - Review documentation and release notes. - Perform QRadar updates, patches and upgrades. - Perform migration (e.g., backup and restore, import and export content).	12%
Configuring and administering tasks	- Configure event flow sources and custom properties. - Maintain configuration and data backups. - Create and administer users, user roles, and security profiles. - Manage the license per allocation. - Create, review and modify rules, building blocks and reference sets. - Configure and manage retention policies (i.e., data and assets). - Create and manage saved searches, index, global views, dashboards and reports. - Deploy and manage applications and content packages. - Configure global system notifications. - Configure and apply network hierarchy. - Configure and manage domain and tenants. - Use the asset database. - Schedule and run a VA scan.	42%
Monitoring	- Monitor QRadar Notifications and error messages. - Review and interpret system monitoring dashboards. - Verify QRadar processes and services. - Monitor QRadar performance. - Use apps and tools for monitoring (e.g., QDI, assistant app, incident overview, DrQ). - Check system maintenance and health of appliances. - Monitor offenses and detect anomalies.	25%
Troubleshooting	- Demonstrate knowledge of key commands to interpret QRadar services and processes. - Explain error messages and notifications. - Interpret the basic logs (e.g., qradar.error, qradar.log). - Use embedded troubleshooting tools and scripts.	13%

IBM C1000-026 Sample Questions:

Question: 1

An administrator wants to be notified when, during office hours, the number of connected users to a VPN is more than the 250 licensed VPN clients. The administrator wants to receive an email and see a corresponding event generated in the Log Activity tab. How can the administrator monitor this event?

a) From the Offenses tab select Rules and then click Actions, Create Common Rule and in the rule wizard setup select the test to count events showing successful logins to the VPN server during office opening hours. In the Rule Response dispatch a new event and then send an email entering the email of the analyst.
b) From the Log Activity tab select Rules and then click Actions, Create Event Rule and in the rule wizard setup select the test to count events showing successful logins to the VPN server during office opening hours. In the Rule Response dispatch a new event and then send an email entering the email of the analyst.
c) From the Network Activity tab select Rules and then click Actions, Create Flow Rule and in the rule wizard setup select the test to count events showing successful logins to the VPN server during office opening hours. In the Rule Response dispatch a new event and then send an email entering the email of the analyst.
d) From the Log Activity tab create and save a search filtered and grouped by the VPN log source successful connection events showing the Count Column, click Rules and select Add Threshold Rule, configure the test stack to trigger the rule when the counted properties is over 250 and it happens between the specified hours. In the Rule Response dispatch a new event and then send an email entering the email of the analyst.

Answer: d

Question: 2

An administrator has found an error in the QRadar logs, and has identified a particular classpath connected with the error. To further troubleshoot this error, the administrator needs to put it into debug mode. Which script should the administrator use to toggle debug mode for QRadar logging?

a) /opt/qradar/support/jmx.sh
b) /opt/qradar/support/threadtop.sh|
c) /opt/qradar/support/mod_log4j.pl
d) /opt/qradar/support/qapp_utils.py

Answer: c

Question: 3

An administrator is seeing large number of assets related to service accounts/automated services in the Assets tab. The administrator wants to minimize asset creation related to service accounts to enhance product performance. What should the administrator do to stop this asset growth deviation?

a) 1. Create a saved search where ‘Identity Username’ + ‘Is Any Of’ + ‘Anonymous logon’.
2. Add the search using Admin tab > Asset Profile Configuration > Manage Identity Exclusion > Add Saved Search

b) 1. Create a saved search where ‘Identity Username’ + ‘Is Any Of’ + ‘Anonymous logon’.
2. Add the search using Admin tab > Asset Database Configuration > Manage Database Exclusion > Add Saved Search

c) 1. Create a saved search where ‘Identity Services’ + ‘Is Any Of’ + ‘Administrator logon’.
2. Add the search using Admin tab > Asset Database Configuration > Manage Service Exclusion > Add Saved Search

d) 1. Create a saved search where ‘Identity Username’ + ‘Is Any Of’ + ‘Anonymous logon’.
2. Add the search using Admin tab > Asset Profile Configuration > Manage Asset Blacklist Exclusion > Add Saved Search

Answer: a

Question: 4

An administrator has a rule that populates a reference set with Source IPs. The administrator wants this reference set to contain just Source IPs seen in the last 30 days. How does the administrator configure the reference set?

a) Admin > Reference Set Management > Select Reference set > Edit > Time to Live of elements > uncheck lives forever > select since last seen > set 30 days

b) Admin > Reference Set Management > Select Reference set > Edit > Time to Live of elements > uncheck lives forever > select since first seen > set 30 days

c) Admin > Reference Set Management > Select Reference set > Edit > Time to Live of elements > check lives forever > select since first seen > set 30 days

d) Admin > Reference Set Management > Select Reference set > Edit > Time to Live of elements > check lives forever > select since last seen > set 30 days

Answer: a

Question: 5

To increase the search performance and storage capabilities of an existing distributed QRadar deployment, an administrator decided to install a QRadar Data Node appliance. Before the installation and deployment of the Data Node, what should the administrator check?
(Choose two)

a) Ensure the Event Processor and the Data Node are using the same hardware.
b) Ensure port 32006 between the Data Node and the Event Processor appliance is opened.
c) Ensure port 32011 between the Data Nodes and the Console's Event Processor is opened.
d) Ensure the existence of an IP Tables rule to permit the traffic between the Data Node and the QRadar Console
e) Ensure the SSH keys are available on both the Event Processor and the Data Node for the encryption tunnel to be configured.

Answer: b, c

Question: 6

What are two valid user responses for the following QRadar notification?
38750109 - A store and forward schedule finished while events were left on disk. These events will be stored on the local event collector until the next forwarding sessions begins
(Choose two.)

a) Wait until the next store and forward interval occurs
b) Decrease the event forwarding rate from the event collector
c) Increase the event forwarding rate from the event collector
d) Increase the time interval for the store and forward process
e) Increase the time interval that is configured for forwarding events

Answer: c, e

Question: 7

What is the recommended order of the directories to copy the SFS file in an upgrade process?

a) /storetmp, /store, /tmp
b) /storetmp, /store/transient, /tmp
c) /storetmp, /tmp/, /store/transient
d) /tmp, /store/transient. /storetmp

Answer: c

Question: 8

An administrator reviews a newsflash from IBM Support. It informs that the QRadar deployment has been security tested and is vulnerable against several known attacks, and that the vulnerabilities have been fixed in the latest patch. The administrator decides to update their QRadar installation.

In a distributed environment, which QRadar appliance must be updated first?

a) QRadar Console
b) QRadar Data Node
c) QRadar HA Console
d) QRadar Event/Flow Processor

Answer: a

Question: 9

An administrator wants to add a new Cisco ASA log source. What are the two protocols that Cisco ASA supports for collecting events?

(Choose two)

a) JDBC
b) SNMP
c) Syslog
d) Rest API
e) Cisco NSEL

Answer: c, e

Question: 10

An administrator receives a system notification stating: 'Performance degradation was detected in the event pipeline. Expensive Device Support Module (DSM) extensions were found'. Which QRadar service is having this pipeline issue?

a) ariel
b) ecs-ec
c) ecs-ep
d) hostcontext

Answer: b

Study Guide to Crack IBM QRadar SIEM Fundamental Administration C1000-026 Exam:

- Getting details of the C1000-026 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the C1000-026 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the IBM provided training for C1000-026 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the C1000-026 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on C1000-026 practice tests is must. Continuous practice will make you an expert in all syllabus areas.