EDUSUM

#1 Online Certification Guide

IBM C1000-026 STUDY GUIDE PDF

Grab the IBM QRadar SIEM Fundamental Administration Certification PDF Questions & Answers

Details of the Exam-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:

Get an Overview of the C1000-026 Certification:

Who should take the **C1000-026 exam**? This is the first question that comes to a candidate’s mind when preparing for the QRadar SIEM Fundamental Administration certification. The C1000-026 certification is suitable for candidates who are keen to earn knowledge on the IBM Security and grab their IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2 certification. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But C1000-026 study guide PDF is here to solve the problem. C1000-026 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the IBM C1000-026 Certification?

There are several reasons why one should grab the C1000-026 certification.

- The QRadar SIEM Fundamental Administration certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential employers.
- Thus earning the **IBM Certified Associate Administrator - IBM QRadar SIEM V7.3.2** is a powerful qualification for a prosperous career.

What is the IBM C1000-026 QRadar SIEM Fundamental Administration Certification Exam Structure?

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**

Enhance Knowledge with C1000-026 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 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

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: 7

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: 8

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

Question: 9

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: 10

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

What Study Guide Works Best in Acing the IBM C1000-026 QRadar SIEM Fundamental Administration Certification?

The C1000-026 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the QRadar SIEM Fundamental Administration exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don’t like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your study schedule must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

If there is related IBM training, don't miss out the chance to join. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the IBM C1000-026 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, C1000-026 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven C1000-026 Practice Test for Success!!!

Do you want to pass the C1000-026 exam on your first attempt? Stop worrying; [sitename] is here to provide you the best experience during your IBM Security QRadar SIEM V7.3.2 Fundamental Administration preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **C1000-026 practice tests**<link product page>. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.