



<http://www.ipass4sure.com>

# 000-196

**IBM**

*IBM Security QRadar SIEM V7.1 Implementation Exam*

The 000-196 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The 000-196 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently. The 000-196 exam is very challenging, but with our 000-196 questions and answers practice exam, you can feel confident in obtaining your success on the 000-196 exam on your FIRST TRY!

## IBM 000-196 Exam Features

- Detailed questions and answers for 000-196 exam
- Try a demo before buying any IBM exam
- 000-196 questions and answers, updated regularly
- Verified 000-196 answers by Experts and bear almost 100% accuracy
- 000-196 tested and verified before publishing
- 000-196 exam questions with exhibits
- 000-196 same questions as real exam with multiple choice options

Acquiring IBM certifications are becoming a huge task in the field of I.T. More over these exams like 000-196 exam are now continuously updating and accepting this challenge is itself a task. This 000-196 test is an important part of IBM certifications. We have the resources to prepare you for this. The 000-196 exam is essential and core part of IBM certifications and once you clear the exam you will be able to solve the real life problems yourself. Want to take advantage of the Real 000-196 Test and save time and money while developing your skills to pass your IBM 000-196 Exam? Let us help you climb that ladder of success and pass your 000-196 now!

**QUESTION: 1**

What are false positive rules?

- A. Rules that create offenses that the user should ignore.
- B. Rules that have matched could severely impact the environment.
- C. Rules that make use of the tests relation And Not. The test that follows this relation, if positively matched, will be negated and evaluated as not matched.
- D. They are mostly made out of building blocks and filtered out events or flows from the Correlation Rule Engine pipeline using selection criteria that deem the matching events or flows should not contribute to an offense.

**Answer: D**

**QUESTION: 2**

What must be done to obtain a token for an Authorized Service for WinCollect?

- A. Select Authorized Service under the WinCollect plug-in
- B. Add the service as an Authorized Service in the Admin tab
- C. Go to System and License Management and add an Authorized Service
- D. Go to Console Settings and add the already configured WinCollect as an Authorized Service

**Answer: B**

**QUESTION: 3**

What is a best practice when creating users and assigning roles?

- A. For one-off user creation or for a quick task, assign a user to the Admin role.
- B. Create a role for each user to make it easy to manage an individual's permissions.
- C. To make user management less time-consuming, create general user accounts with broad to specific permissions that can be shared between staff.
- D. Group users with like duties together and create roles with permissions that satisfy their business requirements; create roles for individuals only in cases of a special permission requirement.

**Answer: D**

**QUESTION: 4**

Which connection type to the console is required to run qchange\_netsetup?

- A. Local
- B. SSH
- C. RDP
- D. Telnet

**Answer: A**

**QUESTION: 5**

What will happen when a user sets a search as default?

- A. The search will be set as the user's default search.
- B. All IBM Security Qradar SIEM V7.1 (QRadar) users will have that search set as their default search.
- C. QRadar users will be able to select that search as their default from a list of searches.
- D. Only users with permission to view the data in the search results will see the search as an option.

**Answer: A**

**QUESTION: 6**

Which log file contains all of the relevant logging data for IBM Security Qradar SIEM V7.1?

- A. /var/log/qradar.txt
- B. /var/log/qradar.log
- C. /var/log/messages
- D. /var/log/qradar.error

**Answer: B**

**QUESTION: 7**

Which infrastructure components must be present before installing any of the virtual appliances?

- A. VMware ESX 3.7 with VMware vSphere client 3.9 fix pack 12
- B. VMware ESXi 4.0.8 with VMware Workstation 9.0 installed on the desktop
- C. VMware ESXi 4.1 with VMware vSphere client 4.1 installed on the desktop
- D. VMware Workstation 8.0.4 or above with VMware vSphere client 4.0 installed on the desktop

**Answer: C**

**QUESTION: 8**

On the Index Management page, what does the value of the Data Written column represent?

- A. The total amount of data the indexer has processed.
- B. The total amount of data consumed on disk by the index.
- C. The amount of data the indexer processed during the selected time range.
- D. The amount of data consumed on the disk by the index during the selected time range.

**Answer: D**

**QUESTION: 9**

What must be installed prior to using the Deployment Editor?

- A. Adobe Flash
- B. Microsoft ActiveX
- C. Oracle Java Runtime Environment
- D. Oracle Java Network Language Protocol

**Answer: C**



## Pass4sure Certification Exam Features;

- Pass4sure offers over **4500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **150** Global Certification Vendors Covered.
- Services of **Professional & Certified Experts** available via support.
- Free **90 days** updates to match real exam scenarios.
- **Instant Download Access!** No Setup required.
- Price as low as **\$19**, which is 80% more **cost effective** than others.
- **Verified answers** researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (**Android, iPhone, iPod, iPad**)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- **Guaranteed Success.**
- **Fast**, helpful support **24x7**.

View list of All certification exams offered;  
<http://www.ipass4sure.com/allexams.asp>

View list of All Study Guides (SG);  
<http://www.ipass4sure.com/study-guides.asp>

View list of All Audio Exams (AE);  
<http://www.ipass4sure.com/audio-exams.asp>

Download Any Certification Exam DEMO.  
<http://www.ipass4sure.com/samples.asp>

To purchase Full version of exam click below;  
<http://www.ipass4sure.com/allexams.asp>

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

and many others.. See complete list [Here](#)

