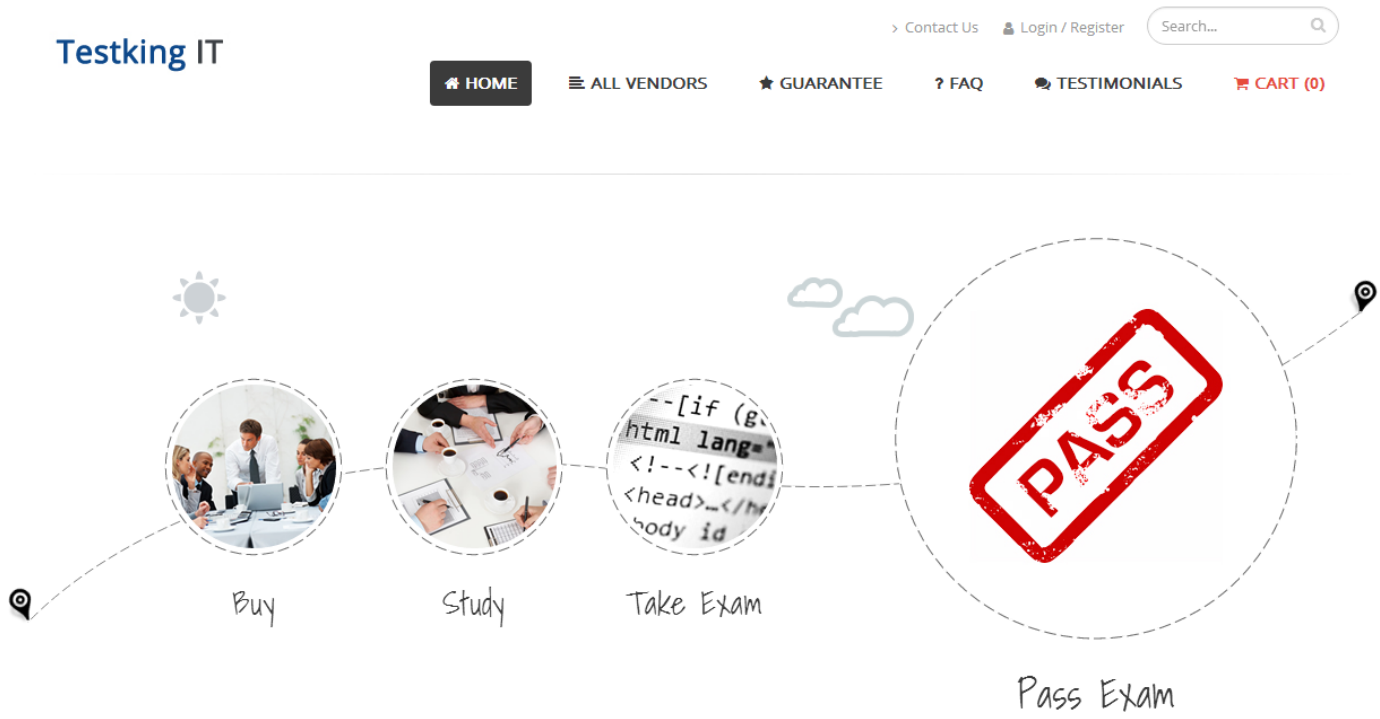
TestkingIT



Try **Desktop Test Engine** before you buy

We're not the only ones **happy** about TestKingsIT Practice Material ...

48236+ customers in 100+ countries use TestKingsIT Test Engine. Meet our customers.

iMessenger VOREED GetCustom JET ORANGE iCompany Paradoxx

http://www.testkingit.com/

Latest practice material - Exam Cram - TestKingIT

Exam : **C2150-624**

Title : IBM Security QRadar SIEM V7.2.8 Fundamental Administration

Vendor : IBM

Version : DEMO

NO.1 An Administrator working with IBM Security QRadar SIEM V7.2.8 only needs to remove a single host (10.1.95.142) from the reference set with the name "Asset Reconciliation IPv4 Whitelist" from the command line interface.
Which command would accomplish this task?
A. ./RefereceSetUtil.sh purge Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
B. ./RefereceSetUtil.sh delete Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
C. ./RefereceSetData.sh purge Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
D. ./RefereceSetData.sh delete Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
Answer: B
Explanation
The syntax for the command is:
ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP

NO.2 An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to delete a single value named User1 from a reference set with the name "Allowed Users" from the command line interface.
Which command will accomplish this?
A. ./UtilReferenceSet.sh purge "Allowed Users" User1
B. ./ReferenceSetUtil.sh purge "Allowed Users" User1
C. ./ReferenceSetUtil.sh delete "Allowed\ Users" User1
D. ./UtilReferenceSet.sh delete "Allowed\ Users" User1
Answer: B
Explanation
The Referencesetutil.sh purge is the correct syntax of the command. It deletes the specific user when you mention it within the reference set.

NO.3 When an IBM Security QRadar SIEM V7.2.8 distributed deployment requires scaling horizontally to achieve Event per Second (EPS) requirements, what QRadar Component needs to be added to meet the EPS demands?
A. Event Manager
B. Event Indexing
C. Event Collector
D. Event Processor
Answer: D
Explanation
The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:

NO.4 An Administrator working with a IBM Security QRadar SIEM V7.2.8 deployment needs to build an Ariel Query to find all events data received in the last 24 hours where the magnitude of the events is larger than 1 but smaller than 5.
What Query needs to be used?
A. SELECT * FROM events WHERE magnitude > 1 AND < 5 LAST 1 DAYS
B. SELECT * FROM events WHERE magnitude BETWEEN 1 AND 5 LAST 1 DAYS
C. SELECT * FROM eventstable WHERE magnitude BETWEEN 1 & 5 LAST 1 DAYS
D. SELECT * FROM eventstable WHERE magnitude BETWEEN 1 AND 5 LAST 1 DAYS

Answer: A

NO.5 How many dashboards come by default in IBM Security QRadar SIEM V7.2.8?
A. 1
B. 5
C. 7
D. 10
Answer: B
Explanation
There are five default dashboards:
1 - application overview
2 - compliance overview
3 - network overview
4 - system monitoring
5 - threat and security monitoring

NO.6 An Administrator using IBM Security QRadar SIEM V7.2.8 is using the RegEx syntax below:
(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)
What type of information is it designed to extract?
A. An IP Address
B. GPS Coordinates
C. A Telephone Number
D. A simple integer no longer than 4 digits
Answer: A
Explanation
Sample regular expressions:
* email: (.+@[^\.].*\.[a-z]{2,}$)
* URL: (http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\ S*)?$)
* Domain Name: (http[s]?://(.+?)["/?:])
* Floating Point Number: ([-+]?\d*\.?\d*$)
* Integer: ([-+]?\d*$)
* IP Address: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)
For example: To match a log that resembles: SEVERITY=43 Construct the following Regular Expression: SEVERITY=([-+]?\d*$)

NO.7 When upgrading IBM Security QRadar SIEM V7.2.8 in High Availability (HA) deployments, how can the upgrade be automatically applied to the associated secondary system(s)?
A. Issue the command on the primary system /media/updates/installer -HA
B. Confirm the system setting on both the primary and secondary systems are set to "Upgrade YES"
C. Make sure the primary system is the active system and the secondary system is in standby mode
D. Make sure the primary system is the active system and the secondary system is in failover mode
Answer: C

NO.8 An Administrator working with a customer looking to add IBM Security QRadar SIEM V7.2.8 into their network, has some requirements. The customer is looking to have 40Tb of raw storage

space for events and console data.
What appliances allow for this requirement to be met?
A. QRadar 3128 Console + QRadar 1410 Data Node
B. QRadar 3128 Console + QRadar 1400 Data Node
C. QRadar 3118 Console + QRadar 1410 Data Node
D. QRadar 3128 Console + QRadar Flow Processor 1728
Answer: B
Explanation
The IBM Security QRadar 1400 Data Node (MTM 4380-Q1E) appliance provides scalable data storage solution for QRadar deployments. The QRadar 1400 Data Node enhances data retention capabilities of a deployment as well as augment overall query performance