PrepAwayPDF

ONLINE TEST ENGINE

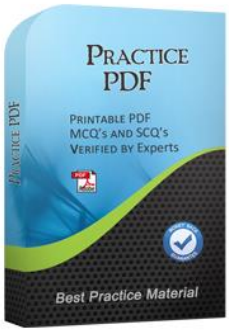
- Online Tool, Convenient, easy to study.
- Practice Online Anytime
- Instant Online Access
- Test History and Performance Review
- Supports All Web Browsers
- Supports Windows / Mac / Android / iOS, etc.

Online Test Engine

DESKTOP TEST ENGINE

- Installable Software Application
- Supports MS Operating System
- Simulates Real Exam Environment
- Two Modes For Practice
- Builds Exam Confidence
- Practice Offline Anytime

Desktop Test Engine



PDF PRACTICE Q&A'S

- Printable PDF Format
- Study Anywhere, Anytime
- Prepared by IT Experts
- 365 Days Free Updates
- Instant Access to Download
- Free PDF Demo Available

PDF Practice Q&A's

60920	59520	59062	59146
Demo Downloads	Successfull Cases	Satisfied Clients	The number of consulting

http://www.prepawaypdf.com/

Best Professional Test Guide Help You Pass and Provide Safe Shopping

Exam : **C1000-163**

Title : IBM Security QRadar SIEM V7.5 Deployment

Vendor : IBM

Version : DEMO

NO.1 To install the 7.x WinCollect Configuration Console, which of these actions is a prerequisite?
A. Install .net framework version 3.5
B. Install the WinCollect Agent SF bundle on QRadar
C. Add multiple destinations for the WinCollect agent
D. Generate an authentication token for the WinCollect agent
Answer: A

NO.2 When prioritizing offenses to investigate, what metric is provided on the Offenses tab specifically to help influence which offenses to investigate first?
A. Magnitude
B. Relevance
C. Severity
D. Credibility
Answer: A

NO.3 A company is developing a QRadar app. They are already running apps on an App Host. Which of these proposed scenarios do you suggest?
A. Run the new app on the console
B. Run the new app on the existing App Host
C. Add another App Host as a sandbox for the new application
D. Move running apps back to the Console and run the new app on the App Host
Answer: B

NO.4 Which statement is valid about the SAML authentication feature?
A. Users enter local credentials every time they access QRadar.
B. You cannot use the x509 certificate, only the provided QRadar_SAML certificate.
C. You can integrate QRadar with your corporate identity server to provide single sign-on.
D. Authentication is exchanged by using digitally signed HTML documents.
Answer: C

NO.5 What must a deployment professional select when defining a new flow source?
A. The destination port
B. The source IP address
C. The flow source type
D. The router brand
Answer: C

NO.6 What must be done on all managed hosts after the restoration of a config backup on a new console?
A. Restart the hostcontext service
B. Re-add all managed hosts
C. Restart the docker service
D. Delete all users

Answer: A

NO.7 How are extensions added to a QRadar deployment?
A. Import extensions by CSV file
B. Use the Extensions Management tool
C. Use Import Extensions under Admin tab
D. Download extensions from IBM X-Force App Exchange
Answer: B

NO.8 When multiple repositories are configured for authentication, what must a user do when they log in?
A. Specify which repository to use for authentication
B. Disable the admin account used to map the multiple repositories
C. Follow the QRadar prompts for the LDAP server to use for authentication
D. Specify the server addresses of the multiple repositories in the authentication group
Answer: A

NO.9 A deployment professional needs to migrate test rules developed in a test QRadar deployment to a production QRadar deployment.
Which approach can be used to migrate the rules?
A. Use the Use Case Manager to sync rules between the two deployments.
B. Use the Content Management Tool (CMT) to migrate the specific rules.
C. Use rsync to copy the /store/postgres/ directory that contains configurations.
D. Create a configuration backup, copy it to the production system, and import/restore the backup configuration.
Answer: B

NO.10 A QRadar deployment professional is asked to plan a hardware migration for an Event Processor in HA. Two new appliances are ready to be used, and they use the same IP addresses.
Which approach can be used to migrate the systems?
A. Use the QRadar config backup and restore process to transfer all configurations.
B. Use rsync to transfer the contents of the /store/postgres partition to the new system.
C. Remove HA on the EPs, migrate to the new primary, then add the new secondary back in.
D. Ensure both systems are built as appliance type 500 and add them into the deployment as replacements.
Answer: C

NO.11 To review the internal changes done in Qradar, what log source in log activity tab must be selected?
A. SIM Audit
B. Asset profile
C. System notification
D. SIM Generic events

Answer: A

NO.12 Which of the following are true about Data node?
A. A data node is an appliance that you can add to your event and flow processors to increase storage capacity and improve search performance.
B. Each data node can be connected to many processors.
C. Each data node can be connected to only one processor.
D. You can add an limited number of data nodes to your IBM QRadar deployment
Answer: AC

NO.13 What app can be used in QRadar to visualize offenses, network data, threats, and malicious behavior provide insights and analysis about a network?
A. Threat Intelligence
B. Use Case Manager
C. Pulse
D. Vulnerability Insights
Answer: B

NO.14 An analyst needs to preserve the data from a search to view later.
Which option should they select?
A. Save Criteria
B. Save Results
C. Save Data
D. Save Search
Answer: B

NO.15 Upon initial configuration, a company asks their deployment professional to move backups to an external device. They are concerned about the percentage of storage space that is used up on the volume, because QRadar no longer runs scheduled backups on this volume.
What percentage of the volume do they suspect is used?
A. 75%
B. 85%
C. 90%
D. 95%
Answer: A

NO.16 Which app can be used to find the state (active, standby, offline, or unknown) of each appliance, the number of notifications for each host, the host name and appliance type, disk usage, status, and time changed?
A. QRadar Operations
B. QRadar Deployment Monitoring
C. QRadar Performance Assistant
D. QRadar Deployment Intelligence

Answer: D

NO.17 Which of these is a tenant administrator responsible for?
A. Configure Domain Management
B. Collaborate with the MSSP administrator
C. Access or change the configuration for other tenants
D. Create roles and security profiles for tenant administrators and users
Answer: B

NO.18 What must be created before the Use Case Manager app can be used?
A. Authorized Service Token
B. Custom DSM
C. Security Profile
D. User roles
Answer: B