EXAMTOPICS

-Expert Verified, Online, **Free**.



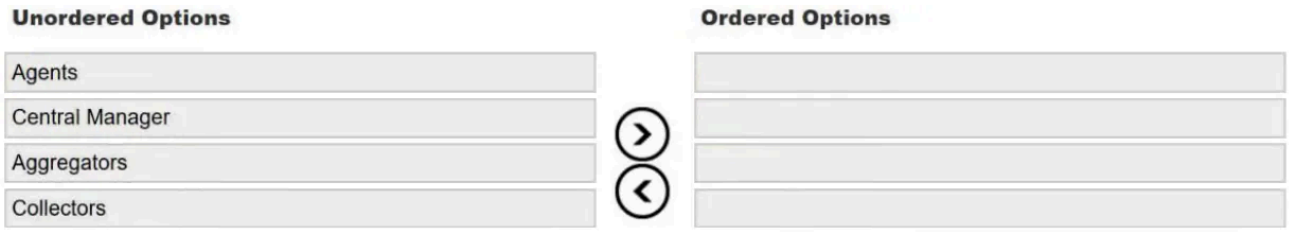
CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

DRAG DROP

What order is followed to successfully upgrade an environment with 1 Central Manager, 2 Aggregators, and 4 Collectors?



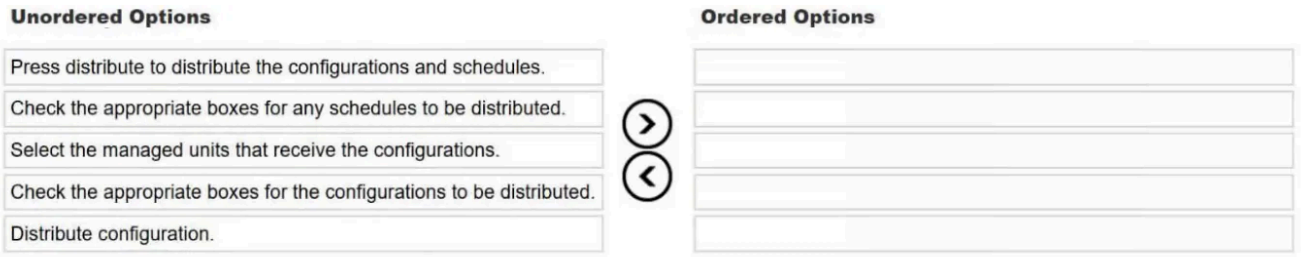
Suggested Answer:
Upgrade Collectors, then Aggregators, then Central Manager.

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

DRAG DROP

What is the correct order to distribute configurations and schedules from the Central Manager to its managed units?



Suggested Answer:
Select managed units, select configurations, select schedules, then distribute.

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

What is an accumulation interval in Correlation Alerts?

A. How often to send notifications from an alert.

B. How many events to accumulate before sending an alert.

C. How many alerts to accumulate before sending notification.

D. How far back to run the query in the alert definition.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

How is an SMTP configuration verified?

A. Checking the syslog messages via fileserver.

B. Running a test email using the iptraf command.

C. Reviewing the 'Failed Messages' report.

D. Testing the connection in the Alerter section.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which command should be started to upgrade a Windows S-TAP agent from the command line?

A. setup -NOAUTODISCOVERY

B. setup -UNATTENDED

C. setup -UPGRADE

D. setup -UPGRADESTAP

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Which component must be configured first to create Alert Builder e-mail notifications?

A. Alert Templates

B. Predefined Alerts

C. Syslog

D. SMTP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Which action is performed using Investigation Dashboard?

A. Creating, saving, and exporting investigation dashboards for forensic analysis.

B. Modifying Guardium's core analytics engine settings to enhance real-time processing.

C. Deleting Guardium audit logs to improve performance.

D. Disabling automatic recovery of critical security alerts.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which two (2) jobs does Database Auto-Discovery use to ensure that no database goes undetected in the environment? (Choose two.)

A. Discovery job

B. Scan job

C. Database job

D. Audit Process job

E. Probe job

Suggested Answer: *A, B*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Which component is recommended for the assessment tests and datasource definitions for Vulnerability Assessment in an Enterprise deployment?

A. Aggregator

B. Collector

C. Central Manager

D. CAS Server

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

What is the required step to ensure a successful restore when archived data is stored on an external EMC Centera storage, and the archive was created on a different Guardium system?

A. Import the EMC Centera storage configuration file using the CLI.

B. Upload the SFTP credentials directly to the Guardium appliance.

C. Ensure the system shared secret from the original system is available on the target system.

D. Run the delete_entry_location GuardAPI command on the target appliance.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which function improves data security?

A. Creating secure audit repository for large number of systems, networks, and databases.

B. Assessing network vulnerabilities and configuration flaws.

C. Tracking end user activity who never access data through enterprise applications.

D. Monitoring activity on sensitive data access, database changes, and privileged user actions.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which action is required after distributing the alerter configuration from the Central Manager to its managed units?

A. Unregister the registered managed unit

B. Reboot the managed unit

C. Refresh the managed unit

D. Restart the managed unit portal

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

What needs to be enabled to utilize the deployment health views?

A. Data imports and exports

B. Alerts in Policy actions

C. Unit utilization data

D. Enterprise S-TAP view report

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

What is the purpose of Domains in Query-Report Builder?

A. They organize related Entities and Attributes.

B. They store raw database logs before processing.

C. They act as predefined reports for compliance audits.

D. They define access control rules for user roles.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

A Guardium administrator has successfully installed an S-TAP agent for Informix. However, encrypted and shared memory traffic is not being collected.

Which monitoring mechanism captures this traffic when enabled?

A. PCAP

B. KTAP

C. ATAP

D. EXIT

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

What are two (2) types of rules within a data security policy? (Choose two.)

A. SQL

B. Extrusion

C. Access

D. Selective

E. Session

Suggested Answer: *B, C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Which CLI command checks if a Guardium appliance can communicate with the SMTP server?

A. support tcpdump -i host smtp_server_ip port port#

B. support store tcpdump interface smtp_server_ip port# tcp

C. support show port open smtp_server_ip port#

D. support netconnection --computername smtp_server_name port#

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Which operating system user is required to install the S-TAP client on a Linux database server?

A. guardium

B. root

C. admin

D. guardadmin

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which role allows performing routine maintenance on the system, such as restarting services, without granting access to sensitive data or configurations?

A. Admin-console-only

B. System-admin

C. Maintenance

D. Admin

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

Which two (2) components/artifacts are utilized by the Guardium Vulnerability Assessment? (Choose two.)

A. Workflow

B. Report

C. Test

D. Compliance

E. Datasource

Suggested Answer: *C, E*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Where are the must gather files stored when the support must_gather command is run?

A. Fileserver

B. Healthcheck log Page

C. Support Information Gathering Results Page

D. /tmp directory in the DB server

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which is the correct wildcard operator that is used in a query condition?

A. %ghdp%

B. jcfku*

C. aaa#

D. *c.c*

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

The customer has completed the Guardium and QRadar integration.

Which is true about Guardium policy where the new member is added to the associated group by the QRadar event?

A. The Guardium policy is automatically reinstalled.

B. The Guardium policy must be reinstalled manually.

C. The only one-way information flow is supported between Guardium and QRadar.

D. The generated GuardAPI script manually updates Guardium policy.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!