# Free Questions for Deep-Security-Professional by go4braindumps

## Shared by Schroeder on 15-04-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

A Deep Security administrator wishes to monitor a Windows SQL Server database and be alerted of any critical events which may occur on that server. How can this be achieved using Deep Security?

## Options:

**A-** The administrator could install a Deep Security Agent on the server hosting the Win-dows Server 2016 database and enable the Integrity Monitoring Protection Module. A rule can be assigned to monitor the Windows SQL Server for any modifications to the server, with Alerts enabled.

**B-** The administrator could install a Deep Security Agent on the server hosting the Win-dows Server 2016 database and enable the Log Inspection Protection Module. A rule can be assigned to monitor the Windows SQL Server for any critical events, with Alerts enabled.

**C-** The administrator could install a Deep Security Agent on the server hosting the Win-dows Server 2016 database and enable the Intrusion Prevention Protection Module. A Recommendation Scan can be run and any suggested rule can be assigned to monitor the Windows SQL Server for any vulnerabilities, with Alerts enabled.

**D-** This can not be achieved using Deep Security. Instead, the administrator could set up log forwarding within Window SQL Server 2016 and the administrator could monitor the logs within the syslog device.

## Answer:

B

# Question 2

**Question Type:** MultipleChoice

As the administrator in a multi-tenant environment, you would like to monitor the usage of security services by tenants? Which of the following are valid methods for monitoring the usage of the system by the tenants?

## Options:

**A-** Generate a Chargeback report in Deep Security manager Web console.

**B-** All the choices listed here are valid.

**C-** Use the Representational State Transfer (REST) API to collect usage data from the tenants.

**D-** Monitor usage by the tenants from the Statistics tab in the tenant Properties window.

## Answer:

B

## Explanation:

Deep Security Manager records data about tenant usage. This information is displayed in the Ten-ant Protection Activity widget on the Dashboard, the Statistics tab in tenant Properties, and the Chargeback report.

This information can also be accessed through the Status Monitoring REST API which can be enabled or disabled from the Administration > Advanced > System Settings > Advanced > Status Monitoring API.

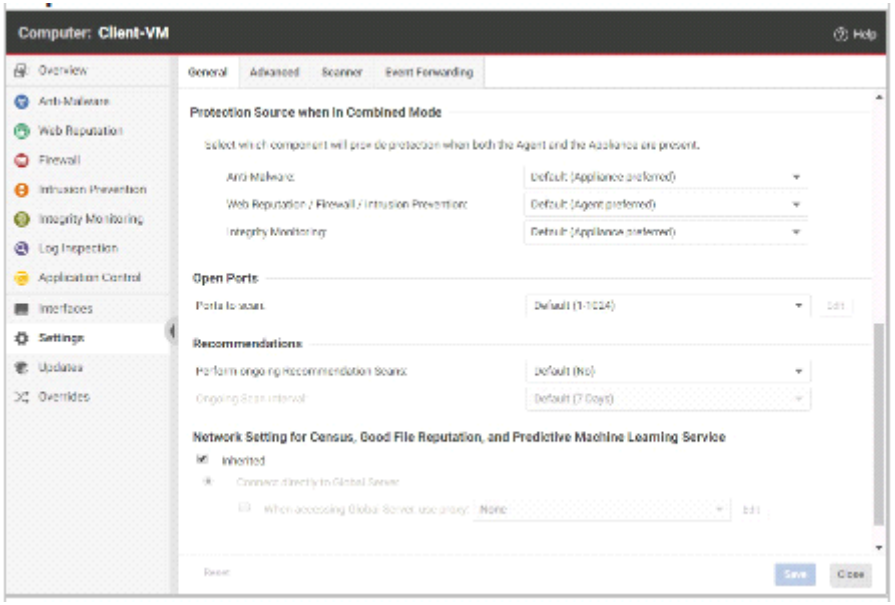
multi-tenancy

Explication: Study Guide - page (422)

# Question 3

**Question Type:** **MultipleChoice**

The "Protection Source when in Combined Mode" settings are configured for a virtual machine as in the exhibit. You would like to enable Application Control on this virtual machine, but there is no corresponding setting displayed. Why?




## Options:

**A-** In the example displayed in the exhibit, no activation code was entered for Application Control. Since the Protection Module is not licensed, the corresponding settings are not displayed.

**B-** These settings are used when both an host-based agent and agentless protection are available for the virtual machine. Since Application Control is not supported in agentless installations, there is no need for the setting.

**C-** In the example displayed in the exhibit, the Application Control Protection Module has not yet been enabled. Once it is enabled for this virtual machine, the corresponding settings are displayed.

**D-** In the example displayed in the exhibit, the VMware Guest Introspection Service has not yet been installed. This service is required to enable Application Control in agentless installations.

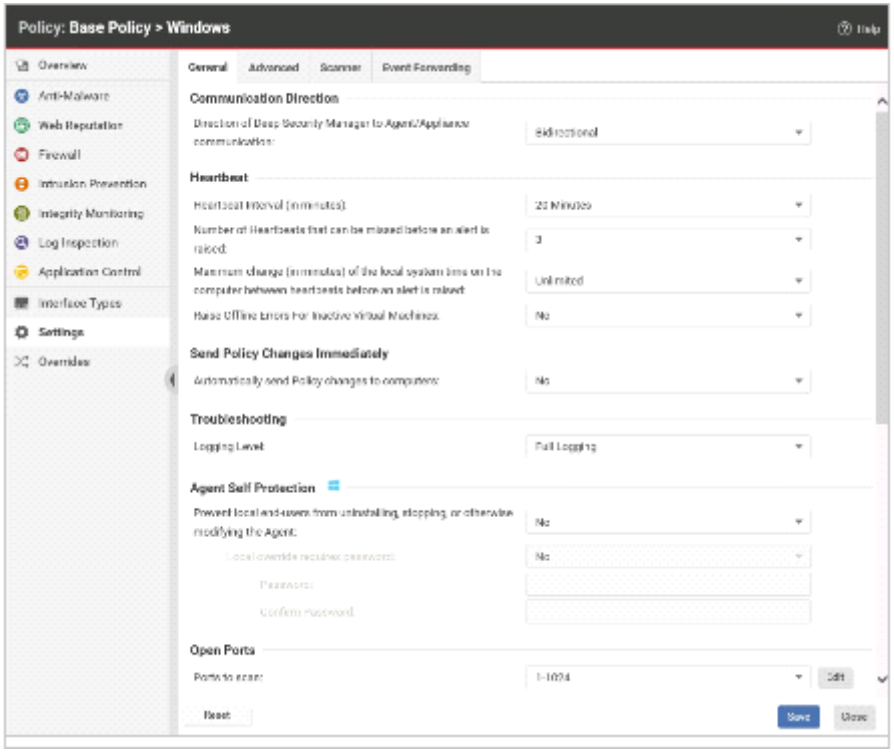
**Answer:**

B

# Question 4

**Question Type:** **MultipleChoice**

Based on the policy configuration displayed in the exhibit, which of the following statements is true?




## Options:

**A-** Changes to any of the Deep Security policies will be send to the Deep Security Agents as soon as the changes are saved.

**B-** Administrators with access to the protected Server will be able to uninstall the Deep Security Agent through Windows Control Panel.

**C-** Deep Security Agents will send event information to Deep Security Manager every 10 minutes.

**D-** If the Deep Security Manager does not receive a message from the Deep Security agent every 20 minutes, an alert will be raised.

## Answer:

B

# Question 5

**Question Type:** MultipleChoice

Which of the following statements is true regarding the Intrusion Prevention Protection Module?

## Options:

**A-** The Intrusion Prevention Protection Module blocks or allows traffic based on header information within data packets.

**B-** The Intrusion Prevention Protection Module analyzes the payload within incoming and outgoing data packets to identify content that can signal an attack.

**C-** The Intrusion Prevention Protection Module can identify changes applied to protected objects, such as the Hosts file, or the Windows Registry.

**D-** The Intrusion Prevention Protection Module can prevent applications from executing, allowing an organization to block unallowed software.

### Answer:

B

### Explanation:

deep-security-protection-modules

# Question 6

**Question Type:** MultipleChoice

Policies in Deep Security can include a Context value. Which of the following statements re-garding Context is correct?

### Options:

**A-** The Context provides Deep Security Agents with location awareness and are associated with Anti-Malware and Web Reputation Rules.

**B-** The Context provides Deep Security Agents with location awareness and are associated with Firewall and Intrusion Prevention Rules.

**C-** The Context provides Deep Security Agents with location awareness and are associated with Web Reputation Rules only.

**D-** The Context provides Deep Security Agents with location awareness and are associated with Log Inspection and Integrity Monitoring Rules.

### Answer:

B

### Explanation:

Contexts are designed to be associated with Firewall and Intrusion Prevention Rules. If the condi-tions defined in the Context associated with a rule are met, the rule is applied. To link a security rule to a Context, go to the Options tab in the Properties window for the rule and select the Context from the menu.

Explication: Study Guide - page (165)

## Question 7

**Question Type:** MultipleChoice

Which of the following statements is false regarding the Log Inspection Protection Module?

## Options:

**A-** Custom Log Inspections rules can be created using the Open Source Security (OSSEC) standard.

**B-** Deep Security Manager collects Log Inspection Events from Deep Security Agents at every heartbeat.

**C-** The Log Inspection Protection Module is supported in both agent-based and agentless environments.

**D-** Scan for Recommendations identifies Log Inspection rules that Deep Security should implement.

## Answer:

C

## Explanation:

Log Inspection requires running some analysis on the computer and is not supported in Agentless deployments.

Explication: Study Guide - page (310)

# Question 8

**Question Type:** MultipleChoice

Which of the following statements is true regarding Event Tagging?

## Options:

**A-** Adding a tag to an Event modifies the Event data by adding fields, including the name of the tag, the date the tag was applied, and whether the tag was applied manually or automatically

**B-** Only a single tag can be assigned to an Event.

**C-** Events can be tagged automatically if they are similar to known good Events.

**D-** Events can be automatically deleted based on tags.

## Answer:

C

# Question 9

**Question Type:** MultipleChoice

Which of the following operations makes use of the Intrusion Prevention Protection Module?

## Options:

**A-** Integrity scans

**B-** Port scans

**C-** Application traffic control

**D-** Stateful traffic analysis

## Answer:

D