



**Free Questions for Deep-Security-Professional by
braindumpscollection**

Shared by Walker on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following VMware components is not required to enable agentless protection using Deep Security.

Options:

- A- VMware NSX
- B- VMware ESXi
- C- VMware vRealize
- D- VMware vCenter

Answer:

C

Explanation:

Integrate with VMware vRealize Operations Manager

Question 2

Question Type: MultipleChoice

What is the purpose of the Deep Security Notifier?

Options:

- A-** The Deep Security Notifier is a application in the Windows System Tray that displays the Status of Deep Security Manager during policy and software updates.
- B-** The Deep Security Notifier is a server components that collects log entries from man-aged computers for delivery to a configured SIEM device.
- C-** The Deep Security Notifier is a server component used in agentless configurations to allow Deep Security Manager to notify managed computers of pending updates.
- D-** The Deep Security Notifier is a application in the Windows System Tray that com-municates the state of Deep Security Agents and Relays to endpoint computers.

Answer:

D

Explanation:

The Deep Security Notifier is a Windows System Tray application which provides local notification when malware is detected or malicious URLs are blocked.

It may be installed separately on protected virtual machines, however the Anti-Malware Protection Module must be licensed and enabled on the virtual machine for the Deep Security Notifier to display information.

The Notifier displays pop-up user notifications when the Anti-Malware module begins a scan, or blocks malware or access to malicious web pages. The Notifier also provides a console utility that allows the user to view events.

Explication: Study Guide - page (442)

Question 3

Question Type: MultipleChoice

Which of the following is not an operation that is performed when network traffic is intercepted by the network driver on the Deep Security Agent?

Options:

A- Analyze the packet within the context of traffic history and connection state.

B- Compare the data in the packet against the Anti-Malware Scan Configuration to verify whether any of the data related to files and

folders on the Exclusion list.

C- Verify the integrity of the packet to insure the packet is suitable for analysis.

D- Verify the packet is not part of a reconnaissance scan used to discover weaknesses on the Deep Security Agent host computer.

Answer:

B

Question 4

Question Type: MultipleChoice

How does Smart Scan vary from conventional pattern-based anti-malware scanning?

Options:

A- Smart Scan improves the capture rate for malware scanning by sending features of suspicious files to a cloud-based server where the features are compared to known malware samples.

B- Smart Scan shifts much of the malware scanning functionality to an external Smart Protection Server.

C- Smart Scan is performed in real time, where conventional scanning must be triggered manually, or run on a schedule.

D- Smart Scan identifies files to be scanned based on the content of the file, not the extension.

Answer:

B

Explanation:

Advantages of the Smart Scan pattern over the conventional pattern protection in OfficeScan (OSCE)

Question 5

Question Type: MultipleChoice

Multi-tenancy is enabled in Deep Security and new tenants are created. Where does the new tenant data get stored when using SQL Server as the Deep Security database?

Options:

- A-** The new tenant data is added to the existing SQL Server database.
- B-** An additional table is created for each new tenant in the existing database in the SQL Server database to store its data.
- C-** An additional database is created in SQL Server for each new tenant to store its data.
- D-** An additional user is created for each new tenant in the SQL Server database to store its data.

Answer:

C

Explanation:

With Microsoft SQL and PostgreSQL, there's one main database and an additional database for each tenant. With Oracle, all tenant information is in one Deep Security Manager database, but an additional user is created for each tenant. Each user has its own tables.

Explication: Study Guide - page (409)

Question 6

Question Type: MultipleChoice

Which of the following is NOT an operation that can be performed on Deep Security resources using the API?

Options:

A- GET

B- PUT

C- VIEW

D- POST

Answer:

C

Explanation:

Rest API

To Get Premium Files for Deep-Security-Professional Visit

<https://www.p2pexams.com/products/deep-security-professional>

For More Free Questions Visit

<https://www.p2pexams.com/trend/pdf/deep-security-professional>

