Free Questions for Deep-Security-Professional by ebraindumps

Shared by Medina on 29-01-2024

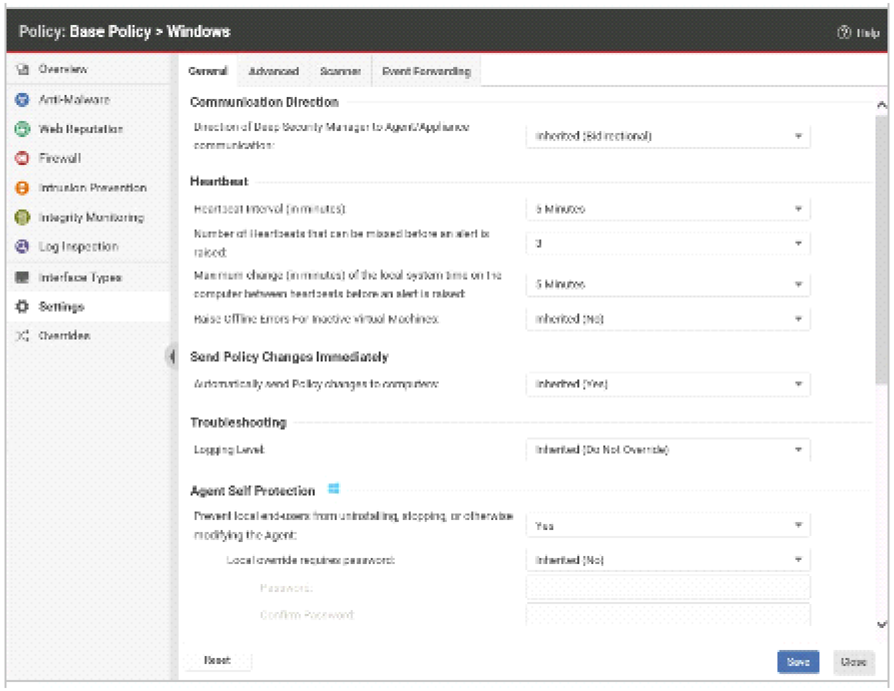
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following statements is correct regarding the policy settings displayed in the exihibit?



Communication Direction

Direction of Deep Security Manager to Agent/Appliance communication: Inherited (Bidirectional)

Heartbeat

Heartbeat Interval (in minutes): 5 Minutes

Number of Heartbeats that can be missed before an alert is raised: 3

Maximum change (in minutes) of the local system time on the computer between heartbeats before an alert is raised: 5 Minutes

Raise Offline Errors For Inactive Virtual Machines: Inherited (No)

Send Policy Changes Immediately

Automatically send Policy changes to computers: Inherited (Yes)

Troubleshooting

Logging Level: Inherited (Do Not Override)

Agent Self Protection

Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent: Yes

Local override requires password: Inherited (No)

Password:

Confirm Password:

Options:

A- The Heartbeat interval value displayed in this policy is inherited from the parent policy

B- Deep Security Agents using the displayed policy will send event details to Deep Security Manager every 5 minutes.

C- All Deep Security Agents will send event details to Deep Security Manager every 5 minutes.

D- Deep Security Manager will refresh the policy details on the Deep Security Agents using this policy every 5 minutes.

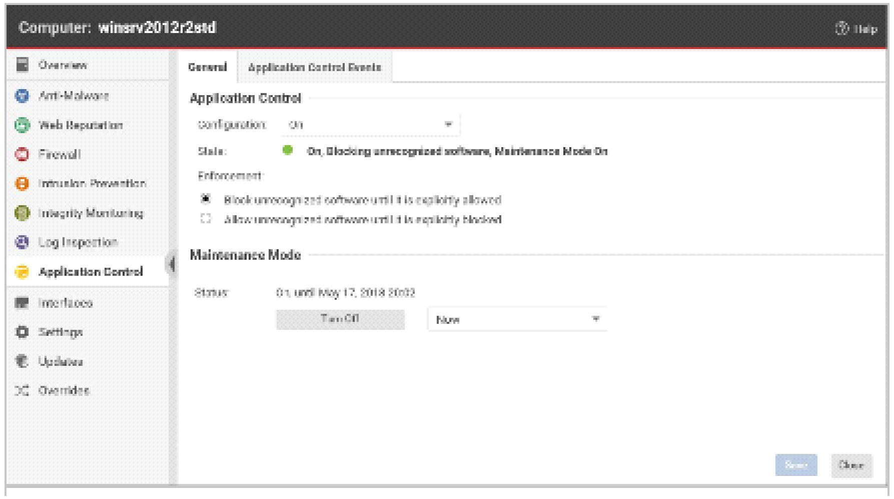
Answer:

C

Question 2

Question Type: **MultipleChoice**

Based on the following exhibit, what behavior would you expect for the Application Control Protection Module?



Application Control

Configuration: On

State: ● On, Blocking unrecognized software, Maintenance Mode On

Enforcement:

● Block unrecognized software until it is explicitly allowed

○ Allow unrecognized software until it is explicitly blocked

Maintenance Mode

Status: On, until May 17, 2018 20:02

Now

Options:

A- Since this computer is in Maintenance Mode, updates to the Application Control Pro-tection Module will be applied.

B- Since this computer is in Maintenance Mode, new or changed software will be auto-matically added to the list of Allowed software in the currently active ruleset.

C- Since this computer is in Maintenance Mode, Application Control will allow any Blocked software to temporarily run

D- Since this computer is in Maintenance Mode, Application Control will ignore any Blocked software in the currently active ruleset.

Answer:

A

Question 3

Question Type: MultipleChoice

Which of the following statements correctly describes Smart Folders?

Options:

A- Smart Folders identify the folders that will be scanned when a Real-Time, Manual or Scheduled malware scan is run.

B- Smart Folders are a collection of subfolders containing the policy settings that are ap-plied to child policies or directly to Computers.

C- Smart Folders act as a saved search of computers which is executed each time the folder is clicked to display its contents.

D- Smart Folders are the containers used to store the results of Recommendation Scans. Once a Recommendation Scan has completed, and administrator can click a Smart Folder and select which of the recommended rules to apply.

Answer:

C

Explanation:

Smart Folders are used to group your computers dynamically. The computers displayed in a Smart Folder are determined by a set of custom rules, that act as a saved search which is executed each time you click on the folder to display its contents. This allows administrators to easily filter and group computers by these defined properties.

Explication: Study Guide - page (127)

Question 4

Question Type: **MultipleChoice**

Which of the following statements is true regarding the use of the Firewall Protection Module in Deep Security?

Options:

A- The Firewall Protection Module can check files for certain characteristics such as compression and known exploit code.

B- The Firewall Protection Module can identify suspicious byte sequences in packets.

C- The Firewall Protection Module can detect and block Cross Site Scripting and SQL In-jection attacks.

D- The Firewall Protection Module can prevent DoS attacks coming from multiple systems.

Answer:

D

Question 5

Question Type: MultipleChoice

Which of the following statements is true regarding software inventories used as part of the Application Control Protection Module?

Options:

A- Disable the Application Control Protection Module when installing software upgrades, otherwise, the new software will be prevented from installing.

B- An administrator can view the list of allowed of software in the inventory from the De-tails tab for each individual Computer.

C- An administrator can share the inventory of allowed software with other computers protected by Deep Security Agents, by copying the inventory database file (ac.db) from the source computer.

D- When an administrator allows software that would be otherwise blocked by the En-forcement Mode, it isn't added to the inventory of approved software. Instead, it is added to that computer's white list.

Answer:

D

Question 6

Question Type: **MultipleChoice**

A Recommendation Scan is run to determine which Intrusion Prevention rules are appropriate for a Server. The scan is configured to apply the suggested rules automatically and ongoing scans are enabled. Some time later, an operating system patch is applied. How can you de-termine which Intrusion Prevention rules are no longer needed on this Server?

Options:

A- The READ ME file provided with the software patch will indicate which issues were addressed with this release. Compare this list to the rules that are applied to determine which rules are no longer needed and can be disabled.

B- Since the rules are being applied automatically, when the next Intrusion Prevention Recommendation Scan is run automatically, any rules that are no longer needed will be automatically unassigned. These are rules that are no longer needed as the vulnerability was corrected with the patch.

C- Since there is no performance effect when multiple Intrusion Prevention rules are ap-plied, there is no need to determine which rules are no longer needed. The original rec-ommended rules can remain in place without affecting the system.

C- Since the rules are being applied automatically, when the next Intrusion Prevention Recommendation Scan is run automatically, any rules that are no longer needed will be displayed on the Recommended for Unassignment tab in the IPS Rules. These are rules that are no longer needed and can be disabled as the vulnerability was corrected with the patch.

Answer:

B

Question 7

Question Type: **MultipleChoice**

What is the purpose of the Deep Security Relay?

Options:

A- Deep Security Relays distribute load to the Deep Security Manager nodes in a high-availability implementation.

B- Deep Security Relays forward policy details to Deep Security Agents and Virtual Ap-pliances immediately after changes to the policy are applied.

C- Deep Security Relays maintain the caches of policies applied to Deep Security Agents on protected computers to improve performance.

D- Deep Security Relays are responsible for retrieving security and software updates and distributing them to Deep Security Manager, Agents and Virtual Appliances.

Answer:

D

Question 8

Question Type: **MultipleChoice**

The Intrusion Prevention Protection Module is enabled and a Recommendation Scan is run to identify vulnerabilities on a Windows Server 2016 computer. How can you insure that the list of recommendations is always kept up to date?

Options:

A- Disabling, then re-enabling the Intrusion Prevention Protection Module will trigger a new Recommendation Scan to be run. New rules will be included in the results of this new scan.

B- Recommendation Scans are only able to suggest Intrusion Prevention rules when the Protection Module is initially enabled.

C- Enable 'Ongoing Scans' to run a recommendation scan on a regular basis. This will identify new Intrusion Prevention rules to be applied.

D- New rules are configured to be automatically sent to Deep Security Agents when Rec-ommendation Scans are run.

Answer:

C