Free Questions for Deep-Security-Professional by dumpshq

Shared by Franks on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following statements is true regarding Deep Security Relays?

Options:

A- Both 32-bit and 64-bit Deep Security Agents can be promoted to a Deep Security Relay.

B- Deep Security Agents promoted to Deep Security Relays no longer provide the security capabilities enabled by the Protection Modules.

C- Deep Security Relays are able to process Deep Security Agent requests during updates.

D- Deep Security Agents communicate with Deep Security Relays to obtain security up-dates.

Answer:

D

Question 2

Question Type: **MultipleChoice**

Your organization would like to implement a mechanism to alert administrators when files on a protected servers are modified or tampered with. Which Deep Security Protection Module should you enable to provide this functionality?

Options:

A- The Integrity Monitoring Protection Module

B- The File Inspection Protection Module

C- Deep Security can not provide this type of functionality

D- The Intrusion Prevention Protection Module

Answer:

A

Question 3

Question Type: **MultipleChoice**

What is IntelliScan?

Options:

A- IntelliScan is a method of identifying which files are subject to malware scanning as determined from the file content. It uses the file header to verify the true file type.

B- IntelliScan is a mechanism that improves scanning performance. It recognizes files that have already been scanned based on a digital fingerprint of the file.

C- IntelliScan reduces the risk of viruses entering your network by blocking real-time compressed executable files and pairs them with other characteristics to improve mal-ware catch rates.

D- IntelliScan is a malware scanning method that monitors process memory in real time. It can identify known malicious processes and terminate them.

Answer:

A

Question 4

Question Type: MultipleChoice

What is the result of performing a Reset operation on a Deep Security Agent?

Options:

A- A Reset operation generates Event information that can be used to troubleshoot Agent-to -Manager communication issues.

B- A Reset operation forces an update to the Deep Security Agent software installed on a managed computer.

C- A Reset operation forces the Deep Security Agent service to restart on the managed computer.

D- A Reset operation wipes out any Deep Security Agent settings, including its relationship with Deep Security Manager.

Answer:

D

Question 5

Question Type: **MultipleChoice**

What is the purpose of the override.properties file?

Options:

A- This file is used to transfer policy settings from one installation of Deep Security Man-ager to another

B- This file allows properties to be tested on Deep Security Manager without affecting the original configuration.

C- This file contains the original out-of-the-box configuration properties for Deep Security Manager. This file is renamed to dsm.properties upon initialization of Deep Security Manager.

D- This file allows Deep Security Agents to override enforced behavior by providing new policy configuration details.

Answer:

B

Explanation:

The properties specified in this configuration file override the properties specified in the dsm.properties file. This file can be created manually by a support engineer to modify product be-havior without affecting the original configuration.

Explication: Study Guide - page (42)

Question 6

Question Type: **MultipleChoice**

Which of the following Firewall rule actions will allow data packets to pass through the Firewall Protection Module without being subjected to analysis by the Intrusion Prevention Protection Module?

Options:

A- Deny

B- Bypass

C- Allow

D- Force Allow

Answer:

B

Question 7

Question Type: MultipleChoice

A collection of servers protected by Deep Security do not have Internet access. How can Smart Scan be used on these computers.

Options:

A- Install a Smart Protection Server in the environment and set it as the source for File Reputation information.

B- Smart Scan must contact the Smart Protection Network to function. Any servers without Internet access will be unable to use Smart Scan.

C- Promote one of the Deep Security Agents on the air gapped computers to become a Re-lay.

D- Smart Scan can be configured to use a local pattern file containing the same information as the Smart Protection Network.

Answer:

A

Explanation:

Agent-airgapped

Question 8

Question Type: **MultipleChoice**

Which of the following statements is true regarding Intrusion Prevention protection?

Options:

A- Intrusion Prevention protection can drop malicious packets but cannot reset the con-nection.

B- Intrusion Prevention protection only works in conjunction with the Anti-Malware Pro-tection Module.

C- Intrusion Prevention protection can only work on computers where a Deep Security Agent is installed; agentless protection is not supported.

D- Intrusion Prevention protection can drop or reset a connection.

Answer:

D

Question 9

Question Type: **MultipleChoice**

An administrator attempts to activate the Deep Security Agent installed on a server by typing the following command in the Command Prompt on the Deep Security Agent computer:

```
dsa_control -a dsm://server1.acme.com:4120
```

The Agent does not activate as expected. What is a valid reason for this issue?

Options:

A- The incorrect port was used. The correct command would be: dsa_control -a dsm://server1.acme.com:4118

B- Deep Security Agents can not be activated through the Command Prompt. They must be activated through the Deep Security Manager Web console or through a deployment script.

C- The command listed can only executed from the Command Prompt on the Deep Security Manager computer.

D- 'Allow Agent-Initiated Activation' is currently not enabled in Deep Security Manager.

Answer:

D

Explanation:

dsa_control -a dsm://<host or IP>:/

For the command-line Agent activation option to work, Deep Security Manager must be set to ac-cept Agent-Initiated Activations (AIA) commands. This method is particularly useful when using scripts or in Cloud environments like Amazon Web Services where Deep Security Manager can not typically connect to Deep Security Agents to activate them, but the Agents can connect to Deep Security Manager.

Explication: Study Guide - page (90)

Question 10

Question Type: MultipleChoice

What is the role of Apex Central in the Connected Threat Defense infrastructure?

Options:

A- Apex Central distributes Deep Security policies to Agents on the protected Servers.

B- Apex Central submits suspicious files to Deep Discovery Analyzer for further analysis.

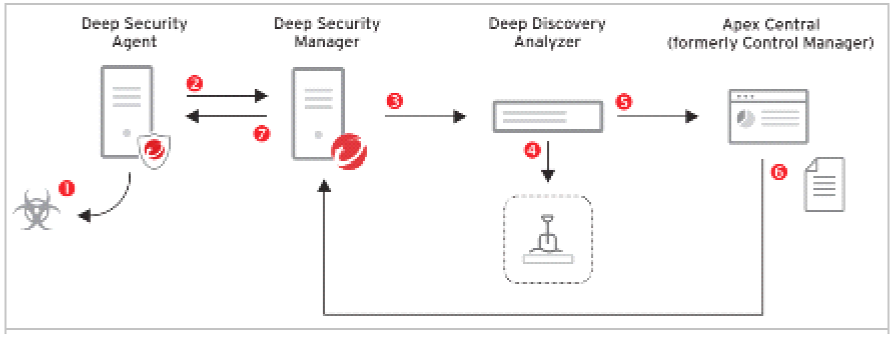
C- Apex Central stores suspicious files that are awaiting submission to the Deep Discovery Analyzer.

D- Apex Central compiles the Suspicious Objects List based on the result of file analysis in Deep Discovery Analyzer.

Answer:

D

Explanation:



1 Deep Security Agents are configured with rules to enable detection of malware on the protected computers.

2 Objects deemed to be suspicious are gathered and submitted to Deep Security Manager.

3 Deep Security Manager submits the suspicious objects to Deep Discovery Analyzer for analysis.

4 Deep Discovery Analyzer executes and observes the suspicious object in a secure, isolated virtual sandbox environment.

5 Deep Discovery Analyzer pushes the analysis results to Trend Micro Apex Central, where an action can be specified for the file based on the analysis. Once the action is specified, a list of emerging threats called a Suspicious Object List is created or updated. Other Trend Micro products, such as Apex One, Deep Discovery Inspector or Deep Discovery Email Inspector, may also be connected to Trend Micro Apex Central and be able to update the list.

6 Deep Security Manager receives the list of suspicious objects from Apex Central.

7 The list is forwarded to Deep Security Agents where protection against the suspicious object is applied. Anti-Malware policies define how suspicious objects are to be handled.

Explication: Study Guide - page (387)

Question 11

Question Type: MultipleChoice

What is the default priority assigned to Firewall rules using the Allow action?

Options:

A- Firewall rules using the Allow action always have a priority of 4.

B- Firewall rules using the Allow action can be assigned a priority between 0 and 4.

C- Firewall rules using the Allow action can be assigned a priority between 1 and 3.

D- Firewall rules using the Allow action always have a priority of 0.

Answer:

D

Explanation:

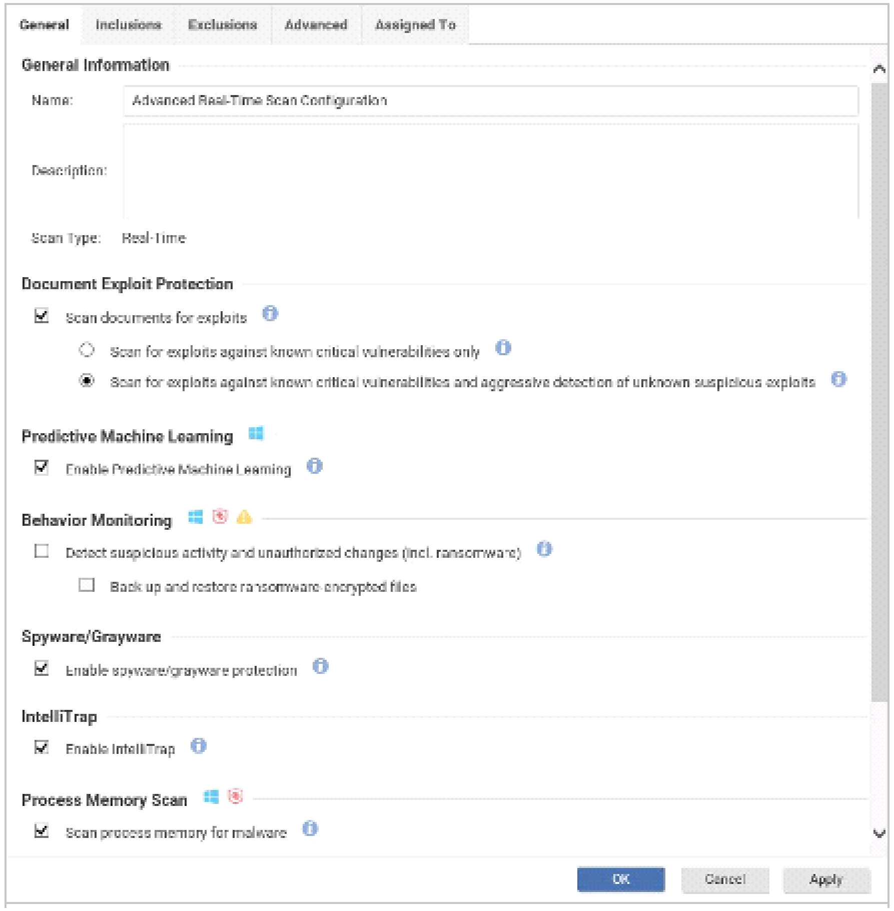
Firewall_rule_priorities

Explication: Study Guide - page (241)

Question 12

Question Type: MultipleChoice

Based on the Malware Scan Configuration displayed in the exhibit, which of the following statements is false.



General Information

Name: Advanced Real-Time Scan Configuration

Description:

Scan Type: Real-Time

Document Exploit Protection

☑ Scan documents for exploits

○ Scan for exploits against known critical vulnerabilities only

● Scan for exploits against known critical vulnerabilities and aggressive detection of unknown suspicious exploits

Predictive Machine Learning

☑ Enable Predictive Machine Learning

Behavior Monitoring

□ Detect suspicious activity and unauthorized changes (incl. ransomware)

□ Back up and restore ransomware-encrypted files

Spyware/Grayware

☑ Enable spyware/grayware protection

IntelliTrap

☑ Enable IntelliTrap

Process Memory Scan

☑ Scan process memory for malware

Options:

A- Any document files that display suspicious behavior will be submitted and executed in a sandbox environment on a Deep Discover Analyzer device.

B- Deep Security Agents using this Malware Scan Configuration will not monitor for compromised Windows processes.

C- Deep Security Agents will only be able to identify malware in files by using patterns downloaded from the Smart Protection Network.

D- Internet access is required to properly enable the features identified in this configuration.

Answer:

B

Explanation:

Configure Malware Scan