Free Questions for PSE-Endpoint by vceexamstest

Shared by Dillard on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator can check which two indicators to verity that Traps for Mac is running correctly on an installed endpoint? (Choose two.)

Options:

A) Use cytool from the command line interface to display the running Traps agent services.

B) In the Activity Monitor, verify that CyveraSecvice is running

C) Ping other Traps agents from the macOS agent

D) Verity that the Traps agent icon is displayed on the macOS finder bar.

Answer:

B, D

Question 2

Question Type: MultipleChoice

An administrator is installing ESM Core 4.0. The SQL Server is running on a non-standard port (36418). The database connection validation is failing. The administrator has entered the following information:

Server Name: ServernameInstance

Database: TrapsDB

User Name: DomainAccount

What is causing the failure?

Options:

A) The database name 'TrapsDB' is unsupported

B) The instance name should not be specified

C) The non-standard port needs to be specified in the format TrapsDB,36418

D) The destination port cannot be configured during installation

Answer:

B

Question 3

Question Type: **MultipleChoice**

An administrator is testing an exploit that is expected to be blocked by the JIT Mitigation EPM protecting the viewer application in use. No prevention occurs, and the attack is successful.

In which two ways can the administrator determine the reason for the missed prevention? (Choose two.)

Options:

A) Check in the HKLM\SYSTEM\Cyvera\Policy registry key and subkeys whether JIT Mitigation is enabled for this application

B) Check if a Just-In-Time debugger is installed on the system

C) Check that the Traps libraries are injected into the application

D) Check that all JIT Mitigation functions are enabled in the HKLM\SYSTEM\Cyvera\Policy\Organization\Process\Default registry key

Answer:

A, C

Question 4

Question Type: **MultipleChoice**

The ESM policy is set to upload unknowns to WildFire. However, when an unknown is executed the Upload status in ESM Console never displays "Upload in progress", and the verdict remains local analysis or unknown. Even clicking the upload button and checking in does not resolve the Issue. A line in the log file suggests not being able to download a file from "https:/ESMSERVER/BitsUploads/… to C:ProgramDataCyveraTemp..."

Which solution fixes this problem?

Options:

A) Restart BITS service on the endpoint

B) Restart BITS service on ESM

C) Remove and reinstall all the agents without SSL

D) In the ESM Console, use the FQDN in multi ESM

Answer:

B

Question 5

Question Type: **MultipleChoice**

An administrator receives a number of email alerts indicating WildFire has prevented a malicious activity. All the prevention events refer to launching an Install Wizard that has received a benign verdict from WildFire. All prevention events are reported on a subset of endpoints, that have recently been migrated Mom another Traps deployment.

Which two troubleshooting actions are relevant to this investigation? (Choose two.)

Options:

A) Check that the servers xml file has been cleared on the migrated endpoints.

B) Check that the ClientInfoHash tag has been cleared on the migrated endpoints.

C) Check that the actions xml file has not been cleared on the migrated endpoints.

D) Check that the WildFire cache has been cleared on the migrated endpoints.

Answer:

A, D

Question 6

Question Type: **MultipleChoice**

During installation of the ESM and the agent, SSL was enabled on an endpoint. However, the agent communication is failing. The services.log on the endpoint has the following error.

*An error occurred while making the HTTP request to https: //hostname:2125/CyveraServer/. This could be due to the fact that the server certificate is not configured property with HTTP SYS in the HTTPS case. This could also be caused by a mismatch of the security binding between the client and the server."

Which certificate can be imported on the endpoint to solve this issue? Assume the hostname is a valid FQDN and the ESM Server and Console have different certificates.

Options:

A) ESM Server Public Certificate

B) ESM Server Serf-Signed Certificate

C) ESM Console Self-Signed Certificate

D) ESM Console Public Certificate

Answer:

B