5V0-91.20$^{\text{Q\&As}}$

VMware Carbon Black Portfolio Skills

Pass VMware 5V0-91.20 Exam with 100% Guarantee

Following Questions and Answers are all new published by VMware Official Exam Center

QUESTION 1

Given the following query:

SELECT hostname, cpu_type, cpu_brand, cpu_physical_cores, cpu_logical_cores, cpu_microcode, (1.0 * physical_memory / (1000*1000*1000)) AS physical_mem_gb, hardware_vendor, hardware_model, hardware_version, hardware_serial FROM system_info;

Which statement Is correct?

A. This query combines data from several different tables.

B. This query customizes the results returned by the system.

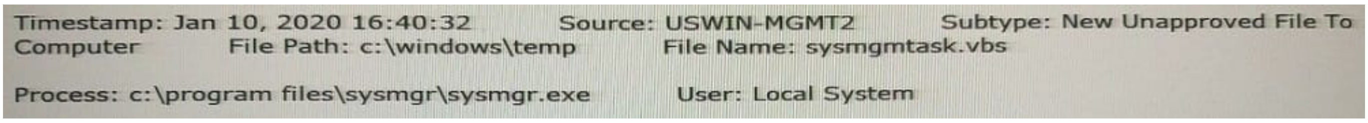
C. This query is missing a filter option.

D. This query shows data from the physical_mem_gb column.

Correct Answer: C

QUESTION 2

A process wrote an executable file as detailed in the following event:



```
Timestamp: Jan 10, 2020 16:40:32        Source: USWIN-MGMT2        Subtype: New Unapproved File To
Computer          File Path: c:\windows\temp          File Name: sysmgmtask.vbs

Process: c:\program files\sysmgr\sysmgr.exe          User: Local System
```

Which rule type should be used to ensure that files of the same name and path, written by that process in the future, will not be blocked when they execute?

A. Trusted Path

B. File Creation Control

C. Advances (Write-Ignore)

D. Trusted Publisher

Correct Answer: B

QUESTION 3

App Control System Health email alerts for excessive agent backlog are occurring hourly.

This is overwhelming the analysts, and they would like to reduce the notifications.

How can the analyst reduce the unneeded alerts?

A. Set the email address for subscribers to an invalid email.

B. Change reminder email to daily or disabled.

C. Disable the alert.

D. Delete the alert.

Correct Answer: B

QUESTION 4

An analyst on the security team noticed that several alerts are false positives within Enterprise EDR. The analyst disables the IOC within the report from those alerts.

Which statement correctly explains what disabling the IOC will accomplish?

A. That specific IOC in the report will no longer generate hits or alerts on the device from the alert.

B. The report will no longer generate hits or alerts on the device from the alert.

C. That specific IOC in the report will no longer generate hits or alerts.

D. The report will no longer generate hits or alerts.

Correct Answer: C

QUESTION 5

Which Live Query statement is properly constructed?

A. SELECT * FROM \\'users\\'

B. select * from *:

C. select from users;

D. SELECT * FROM users;

Correct Answer: D