



5V0-91.20^{Q&As}

VMware Carbon Black Portfolio Skills

Pass VMware 5V0-91.20 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/5v0-91-20.html>

100% Passing Guarantee
100% Money Back Assurance

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

What occurs when an administrator selects "Enable private logging level" in Sensor Settings under Policy?

- A. Delay execute for cloud scan is disabled.
- B. Script Files that have unknown reputations are not uploaded.
- C. Live Response is disabled.
- D. Domain names are obfuscated.

Correct Answer: B

QUESTION 2

An analyst is investigating a specific alert in Endpoint Standard. The analyst selects the investigate button from the alert triage page and sees the following:

TIME	TYPE	EVENT
10:59:16 am Jun 24, 2020	netconn	The script C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbcd8f4cc86\patchwindows_script.ps1 attempted to establish a TCP/80 connection to 169.254.169.254:80 (169.254.169.254) from 172.15.0.120:50155. The device was off the corporate network using the public address 34.225.43.220 (CBENT-WKSH2.ec2.internal, located in Ashburn VA, United States). The operation was blocked and the application terminated by Cb Defense. Policy Terminate Alert
10:59:15 am Jun 24, 2020	filemod	The file C:\windows\temp_psscriptpolicytest_bo100uen.5x4.ps1 was first detected on a local disk. The device was off the corporate network using the public address 34.225.43.220 (located in Ashburn VA, United States). The file is not signed. The file was created by the script C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbcd8f4cc86\patchwindows_script.ps1 Alert
10:59:15 am Jun 24, 2020	crossproc	The script C:\programdata\amazon\ssm\instancedata\i-009f0101ae42aca5d\document\orchestration\24c47c2a-50de-49b9-9e5c-dbcd8f4cc86\patchwindows_script.ps1 attempted to create a viewable window by calling the function 'CreateWindowExW'. The operation was successful. Alert
10:59:14 am Jun 24, 2020	filemod	The file C:\windows\temp_psscriptpolicytest_wnu140pe.wzg.ps1 was first detected on a local disk. The device was off the corporate network using the public address 34.225.43.220 (located in Ashburn VA, United States). The file is not signed. The file was created by the application C:\windows\system32\windowspowershell\v1.0\powershell.exe. Alert

Which statement accurately characterizes this situation?

- A. These events are tied to an observed alert within the user interface.
- B. The policy had no blocking and isolation rules set.
- C. The events shown will all have the same event ID, correlating them to the alert.
- D. Each event listed contributed to the overall alert score and severity.

Correct Answer: D



QUESTION 3

An Endpoint Standard administrator is working with an IT team to explicitly permit specific applications from the environment using both the IT Tools and Certs Approved List features.

Once applied, which reputation would these applications be classified under for processing?

- A. Trusted White
- B. Company White
- C. Local White
- D. Common White

Correct Answer: A

QUESTION 4

An administrator ran the following query.

```
SELECT name, VERSION, install_location, install_source, publisher, install_date, uninstall_string FROM  
programs WHERE publisher = "Microsoft Corporation";
```

The administrator notices a lot of installed programs are not returned.

How can the administrator alter the query to see all results?

- A. Edit the WHERE clause to remove the quotes
- B. Remove the WHERE clause
- C. Replace the = with LIKE
- D. Change the WHERE clause to = ""

Correct Answer: A

QUESTION 5

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

[5V0-91.20 VCE Dumps](#)

[5V0-91.20 Practice Test](#)

[5V0-91.20 Exam Questions](#)