VMware Carbon Black Cloud Enterprise EDR Skills

Exam Details (Last Updated: 01/09/2020)

The VMware Carbon Black Cloud Enterprise EDR Skills exam (5V0-94.22) which leads to VMware Carbon Black Cloud Enterprise EDR Skills badge is a 60-item exam, with a passing score of 300 using a scaled method. Exam time is 105. minutes.

Exam Delivery

This is a proctored exam delivered through Pearson VUE. For more information, visit the Pearson VUE website.

Certification Information

For details and a complete list of requirements and recommendations for attainment, please reference the VMware Education Services – Certification website.

Minimally Qualified Candidate

The minimally qualified candidate (MQC) should have attended the VMware Carbon Black Cloud Enterprise EDR course. The MQC should be a graduate of a cyber security degree or related program. The MQC should have 1 or more years of experience in IT security role. The MQC should be able to explain user, device, workload, and network security options. The MQC should be able to explain VMware Carbon Black security products, solutions, and architectures. The MQC should have knowledge of Windows, MacOS, and Linux operating systems. The MQC should possess knowledge of the objectives shown in the exam sections in this guide.

Exam Sections

VMware exam blueprint sections are now standardized to the seven sections below, some of which may NOT be included in the final exam blueprint depending on the exam objectives.

Section 1 – Architecture and Technologies

Section 2 – Products and Solutions

Section 3 – Planning and Designing

Section 4 – Installing, Configuring, and Setup

Section 5 – Performance-tuning, Optimization, and Upgrades

Section 6 – Troubleshooting and Repairing

Section 7 – Administrative and Operational Tasks

If a section does not have testable objectives in this version of the exam, it will be noted below, accordingly. The objective numbering may be referenced in your score report at the end of your testing event for further preparation should a retake of the exam be necessary.

Sections Included in this Exam

Section 1 –Architectures and Technologies

Objective 1.1 - Identify the architecture and data flows for Carbon Black Cloud Enterprise EDR communication.
Objective 1.2 Identify the notification capabilities within the VMware Carbon Black Cloud.

Objective 1.3 Identify the native integrations available within the VMware Carbon Black Cloud.

Section 2 – VMware Products and Solutions

Objective 2.1 Identify the response capabilities available in the VMware Carbon Black Cloud.

Objective 2.2 Identify where sensor status and sensor details exist.

Objective 2.3 Given the scenario including the status of a sensor, identify the correct action for a sensor.

Section 3 – Planning and Designing

Objective 3.1 Identify security benefits of using VMware Carbon Black Enterprise EDR.

Objective 3.2 Identify use cases of VMware Carbon Black Enterprise EDR

Section 4 – Installing, Configuring, and Setup

Objective 4.1 Identify how to create custom watchlists to detect suspicious activity in an environment

Objective 4.2 Identify how to manage a report within a watchlist to detect suspicious activity in an environment
Objective 4.3 Identify how to manage an IOC within a report to detect suspicious activity in an environment

Section 5 – Performance-tuning, Optimization, Upgrades

Objective 5.1 Given a scenario, identify how to fine tune the watchlist based on environmental information.

Section 6 – Troubleshooting and Repairing - There are no testable objectives for this section.

Section 7 – Administrative and Operational Tasks

Objective 7.1 Given a scenario about a suspicious behavior, identify how to perform a search across Enterprise EDR.

Objective 7.2 Given a scenario, identify how to subscribe to a watchlist.

Objective 7.3 Identify the impact of dismissing an alert within VMware Carbon Black Cloud Enterprise EDR
Objective 7.4 Given a scenario, identify how to monitor the status of the watchlist.

Objective 7.5 Given a security incident scenario, identify the first response that should be used within the VMware Carbon Black Cloud.

Objective 7.6 Identify the commands available within the Live Response features in the VMware Carbon Black Cloud.

Objective 7.7 Identify how to create alerts when malicious activity occurs on the endpoint in VMware Carbon Black Cloud Enterprise EDR

Objective 7.8 Given a scenario, identify events within a process.

Objective 7.9 Given a scenario, identify information available in the process analysis page.

Objective 7.10 Given a search, identify correct use of operators.

Objective 7.11 Identify the functionality of Advanced Queries.

Objective 7.12 Identify how to receive alerts notifications within the VMware Carbon Black Cloud Enterprise EDR

Recommended Courses

VMware Carbon Black Cloud Enterprise EDR

References

In addition to the recommended courses, item writers used the following references for information when writing exam questions. It is recommended that you study the reference content as you prepare to take the exam, in addition to the recommended training.

Name	Products
http://kb.vmware.com - [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud
http://www.vmware.com - [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud
https://blogs.vmware.com - [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud
https://docs.vmware.com - [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud
https://www.vmware.com/support/pubs - [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud
https://www.vmware.com/techpapers.html - [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud
http://pubs.vmware.com – [VMware Carbon Black Cloud Audit and Remediation]	VMware Carbon Black Cloud

*Carbon Black content in this exam is based on Carbon Black Audit and Remediation. Review all Carbon Black Audit and Remediation release notes and material for features and function.

Exam Content Contributors

Adam Bluhm
Kevin Evans
Kirk Hasty
Max Hondliik
Victor Monga

REV. 1/2022