

Associate VMware Security

Exam Details (Last Updated: 9/29/2020)

The Associate Security exam (1V0-81.20) which leads to VMware Certified Technical Associate – Security 2020 certification is a 55-item exam, with a passing score of 300 using a scaled scoring method. Candidates are given 120 minutes to complete the exam, which includes adequate time to complete the exam for non-native English speakers.

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) has basic experience in these areas: IT, network, virtualization, OS, and security. The MQC works in environments where VMware Carbon Black Cloud, NSX-T Data Center, and Workspace ONE solutions are present. The MQC is able to explain workspace, workload, and network security concepts to others. The MQC can explain the VMware security vision and describe at a high level, IT industry, networking, and endpoint security concepts. The MQC can perform basic navigation of the Carbon Black Cloud interface and identify its key components. The MQC can perform basic navigation of the NSX-T Data Center interface and view and understand the Security Tab. The MQC can perform basic navigation of Workspace One Monitor Overview and identify its key components. The MQC must possess all the knowledge contained in the sections included in this exam.

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 – VMware vSphere Architectures and Technologies

Objective 1.1 – Describe the anatomy and attack surfaces of a cyber attack

Objective 1.1.1 – Describe network based attacks

Objective 1.1.2 – Describe social engineering based attacks

Objective 1.1.3 – Describe hardware based attacks

Objective 1.1.4 – Describe software based attacks

Objective 1.2 – Identify common vulnerabilities of enterprise systems

Objective 1.3 – Explain common cyber-attack mitigation strategies

Objective 1.4 – Explain NSX high level architecture

Section 2 – VMware Products and Solutions

Objective 2.1 – Describe the VMware security vision

Objective 2.2 – Explain Zero-Trust User and device access

Objective 2.3 – Explain Zero-Trust for network security

Objective 2.4 – Describe Service-Defined Firewall

Objective 2.5 - Identify physical and virtual requirements for a defense-in-depth security deployment

Objective 2.5.1 - Identify network security requirements

Objective 2.5.2 - Identify application security requirements

Objective 2.5.3 - Identify endpoint security requirements (Audit & Remediation, EDR, NGAV)

Objective 2.6 - Describe the functionalities of VMware's security vision

Objective 2.6.1 - Explain the functionality of NSX gateway firewall and distributed firewall

Objective 2.6.2 - Explain the device posture based on network

Objective 2.6.3 - Explain the secure tunnel capabilities with Workspace ONE

Objective 2.6.4 - Explain the endpoint security capabilities of Carbon Black

Objective 2.6.5 - Explain CloudHealth and its role in multi-cloud security solution

Objective 2.7 - Describe the functions of edge firewall, internal firewall, and endpoint protection security mechanisms

Objective 2.8 - Differentiate between Layer 3 firewalls and Layer 7 firewalls

Objective 2.9 - Explain how Workspace ONE UEM facilitates endpoint security

Objective 2.10 - Describe how conditional access and modern authentication enforces security

Objective 2.11 - Explain how Workspace ONE Intelligence can be used to enforce endpoint security

Objective 2.12 - List the features of Workspace ONE Intelligence: Risk Score, CVE patch remediation, User experience, Intelligence SDK

Objective 2.13 - Differentiate between NGAV and traditional AV

Objective 2.14 - Describe the benefits and use case for Next Generation Anti-virus

Objective 2.15 - Describe the benefits and use case for VMware Carbon Black Cloud Enterprise EDR

Objective 2.16 - Explain the use case for Audit and Remediation

Objective 2.17 - Describe the different response capabilities in the VMware Carbon Black Cloud

Objective 2.18 - Differentiate between the types of reputations seen in the VMware Carbon Black Cloud

Section 3 – There are no testable objectives for this section.

Section 4 – There are no testable objectives for this section.

Section 5 – – There are no testable objectives for this section.

Section 6 – – Administrative and Operational Tasks

Objective 7.1 - Run compliance evaluation in Workspace ONE UEM against enrolled devices

Objective 7.2 - Examine the security violations for enrolled devices

Objective 7.3 - Examine compliance policies in Workspace ONE UEM console

Objective 7.4 - Identify the security factors configured in the access policies from Workspace ONE Access console

Objective 7.5 - Navigate the Workspace ONE Intelligence portal

Objective 7.6 - Interpret the dashboards and widgets in Workspace ONE Intelligence

Objective 7.7 - Use endpoint data collected in Workspace ONE Intelligence to investigate security issues

Objective 7.8 - Navigate the VMware Carbon Black Cloud

Objective 7.9 - Create watchlists in the VMware Carbon Black Cloud to detect threats

Objective 7.10 - Identify appropriate searches in the VMware Carbon Black Cloud

Objective 7.11 - Investigate an alert and describe appropriate response actions in the VMware Carbon Black Cloud

Objective 7.12 - Interpret and explain the impact of Rules in the VMware Carbon Black Cloud

Objective 7.13 - Perform recommended queries in the VMware Carbon Black Cloud

Objective 7.14 - Describe the different mechanisms to Allow-list applications to meet business requirements

Objective 7.15 - Perform device activation/enrollment for VMware devices and applications

Objective 7.16 - Identify preconfigured firewall rules for the NSX Security Tab

Objective 7.17 - Determine firewall rules action

Objective 7.18 - Verify validity of firewall rules

Recommended Courses

VMware Virtual Cloud Network: Core Technical Skills (Coming Soon!)

VMware Digital Workspace: Self-Paced (Coming Soon!)

VMware Carbon Black Cloud Audit and Remediation

VMware Carbon Black Cloud Endpoint Standard

VMware Carbon Black Cloud Enterprise EDR

References*

In addition to the recommended courses, item writers use 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 any recommended training.

Name	Products
http://www.vmware.com	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud
http://kb.vmware.com	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud
https://blogs.vmware.com	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud
https://docs.vmware.com	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud
https://www.vmware.com/support/pubs/	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud
https://www.vmware.com/techpapers.html	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud
http://pubs.vmware.com	NSX-T Data Center 3.0, Workspace ONE 20.01, VMware Carbon Black Cloud

*VMware NSX-T Data Center content in this exam is based on version 3.0. Review all 3.0 release notes and material for features and function.

*VMware Workspace ONE content in this exam is based on version 20.01. Review all 20.01 release notes and material for features and function.

Exam Content Contributors

Alex Sui

Arantxa Duque Barrachina

Benjamin Jacoby

Chris Gingolph

Christopher Garcia

Dunn Ryan

Erick Marshall

Frank Escaro-Buechsel

Jason Wiley

Keith Luck

Manny Duron

Michael Witte

Raymundo Escobar

Rich Perkins

Rohit Masand

Ryan Hendricks

Simeon Frank

Waldamar Pera



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
© 2020 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.