Professional VMware Security

Exam Details (Last Updated: 10/7/2020)
The Professional VMware Security exam (2V0-81.20) which leads to VMware Certified Professional – Security 2020 certification is a 70-item exam, with a passing score of 300 using a scaled scoring method. Candidates are given 130 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) possesses knowledge of vSphere, networking, and endpoint security. The MQC can explain VMware Security key features and functionality. The MQC can describe VMware’s Security architecture concepts. The MQC can explain the primary security features of VMware Carbon Black Cloud, NSX-T Data Center, and Workspace ONE, and how these VMware products interoperate with each other to deliver an intrinsic security solution. The MQC can describe use cases for VMware Security to others. The MQC has a minimum of 6 months hands-on experience configuring and managing VMware Security solutions and 1 year of experience working directly with VMware Carbon Black Cloud, NSX-T Data Center, and Workspace ONE. 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 – There are no testable objectives for this section.

Section 2 – There are no testable objectives for this section.

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

Section 4 – Installing, Configuring, and Setting

Objective 4.1 – Configure firewall rules to enable and secure Workspace ONE Components

Objective 4.2 – Configure and manage security groups and security policies in Carbon Black

Objective 4.3 – Configure compliance policies and profiles in Workspace ONE UEM

Objective 4.4 – Configure access policies in Workspace ONE Access

Objective 4.5 – Configure and administer endpoint management

Objective 4.6 – Deploy CB Defense sensors to endpoints

Objective 4.7 – Configure and administer identity providers in Workspace ONE Access

Objective 4.8 – Configure and administer authentication methods in Workspace ONE Access

Objective 4.9 – Deploy and configure NSX-T

Objective 4.10 – Outline the installation and preparation workflow of NSX-T data center

Objective 4.11 – Configure and manage firewalls rules for NSX-T

Objective 4.12 – Connect NSX-T Manager to User Directory for user based firewall rules

Objective 4.13 – Configure and manage security groups and security policies in NSX-T

Objective 4.14 – Install and configure Guest Introspection agent components in VMTools

Section 5 –

Section 6 – Troubleshooting and Repairing

Objective 6.1 – Compare and contrast tools available for troubleshooting (vRNI vs NSX Intelligence)

Objective 6.2 – Troubleshoot common NSX component issues

  Objective 6.2.1 – Troubleshoot common NSX installation and configuration issues

  Objective 6.2.2 – Troubleshoot common NSX firewall policy issues

Objective 6.3 – Troubleshoot common Carbon Black issues

Objective 6.4 – Troubleshoot Workspace ONE issues around endpoint security

Objective 6.5 – Troubleshoot connectivity issues

Objective 6.6 – Troubleshoot multi-cloud security issues

Objective 6.7 – Troubleshoot common physical infrastructure issues

Section 7 – Administrative and Operational Tasks

Objective 7.1 – Identify data center traffic flows

Objective 7.2 – Identify automation mechanisms for security policy configuration
Objective 7.3 – Manage firewall policies
Objective 7.4 – Monitor security for compliance and regulation assurance
Objective 7.5 – Manage security policies for business continuity and disaster recovery
Objective 7.6 – Perform patch management in Workspace ONE
Objective 7.7 – Manage access policies for Single Sign-On and third party Identity Provider federation

Recommended Courses
NSX-T Data Center Install, Config, Manage [3.X]
Workspace ONE Deploy and Manage [20.X]
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 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 any recommended training.

<table>
<thead>
<tr>
<th>Name</th>
<th>Products</th>
</tr>
</thead>
</table>

*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 Willey
Keith Luck
Manny Duron
Michael Witte
Raymundo Escobar
Rich Perkins
Rohit Masand
Ryan Hendricks
Simeon Frank
Waldamar Pera