BROADCOM®
SOFTWARE

Exam Study Guide

Exam 250-449: Symantec Cloud Workload Protection - R1 Technical Specialist

Exam Description

Candidates can validate technical knowledge and competency by becoming a Broadcom Technical Specialist (BTS) based on your specific area of Broadcom Software technology expertise. To achieve this level of certification, candidates must pass this proctored BTS exam that is based on a combination of Broadcom Software training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the Symantec Cloud Workload Protection product in a Security Operations role. This certification exam tests the candidate's knowledge on how Symantec Cloud Workload Protection provides cloud-native security with automatic discovery for public cloud workloads using a single security console that protects workloads across heterogeneous multi-cloud and hybrid cloud environments. For more information about Broadcom Software's certification program, see

https://www.broadcom.com/support/education/software/certification/all-exams

Recommended Experience

It is recommended that the candidate has at least 3-6 months experience working with Cloud Workload Protection in a production or lab environment.

Study References

Courses

Web-Based Training

Cloud Workload Protection R1 Basic Administration

- Introduction to Cloud Workload Protection
- Getting Started Using the Wizard
- Setup and Deployment of Agents
- Managing Policies
- Monitoring Cloud Workload Protection
- Managing Events
- Troubleshooting
- Cloud Workload Protection for Storage

Documentation

https://support.broadcom.com/security

- Cloud Workload Protection Documentation
  https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/cloud-workload-protection/1-0.html
- Cloud Workload Protection for Storage Documentation
  https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/cloud-workload-protection-for-storage/1-0.html

Website

- https://www.broadcom.com/support/education/software/training-courses
- https://www.broadcom.com/support/education/symantec/elibrary
- Symantec Cloud Workload Protection Landing Page
- Symantec Cloud Workload Protection Cloud Help

Exam Objectives

The following tables list the Broadcom Software SCS Certification exam objectives for the exam and how these objectives align to the corresponding Symantec course topics and their associated lab exercises as well as the referenced product documentation.

It is strongly recommended that all candidates complete all applicable lab exercises in preparation for the exam.

Introduction to Cloud Workload Protection

Exam Objectives	Applicable Web Based Content
Describe how Cloud Workload Protection protects the enterprise	**Cloud Workload Protection Basic Administration R1** • Introduction to Cloud Workload Protection
Describe the features and functionality of Symantec Cloud Workload Protection	
Describe the functionality of Cloud Workload Assurance	
Describe the Symantec Cloud Workload Protection architecture components	

Getting Started Using the Wizard

Exam Objectives	Applicable Web Based Content
Describe the Getting Started Wizard and it's use	**Cloud Workload Protection Basic Administration R1** • Getting Started Using the Wizard
Describe how to deploy Symantec Cloud Workload Protection components	

Setup and Deployment of Agents

Exam Objectives	Applicable Web Based Content
Describe Symantec Cloud Workload Protection deployment options	**Cloud Workload Protection Basic Administration R1** • Setup and Deployment of Agents
Describe Cloud Workload Protection Agent installation and management	

Managing Policies

Exam Objectives	Applicable Web Based Content
Describe Symantec Cloud Workload Protection policy types and supported platforms	**Cloud Workload Protection Basic Administration R1** • Managing Policies
Describe the predefined Prevention, Malware, and Detection policies	
Describe how to apply Prevention, Malware, and Detection policies	
Describe how to customize the predefined Prevention, Malware, and Detection policies	

Monitoring Cloud Workload Protection

Exam Objectives	Applicable Course Content
Describe how to navigate and use the Symantec Cloud Workload Protection Management console	**Cloud Workload Protection Basic Administration R1** • Monitoring Cloud Workload Protection
Describe how to use the Cloud Workload Protection dashboard	
Describe how to use the Cloud Workload Protection Threat Map and vulnerabilities	
Describe how to monitor instances and the Instances Map in Cloud Workload Protection	

Managing Events

Exam Objectives	Applicable Web Based Content
Describe how to create custom alerts and notifications based on filters and thresholds	**Cloud Workload Protection Basic Administration R1** • Managing Events
Describe how to locate and analyze Cloud Workload Protection alerts, events, jobs and notifications	

Troubleshooting

Exam Objectives	Applicable Web Based Content
Describe how to use Symantec Cloud Workload Protection Help Center	**Cloud Workload Protection Basic Administration R1** • Troubleshooting

Cloud Workload Protection for Storage

Exam Objectives	Applicable Web Based Content
Describe the functionality of Cloud Workload Protection for Storage	**Cloud Workload Protection Basic Administration R1** • Cloud Workload Protection for Storage

Sample Exam Questions

Review the following sample questions prior to taking an exam to gain a better understanding of the types of questions asked.

1. What is the name of the included command-line utility in Cloud Workload Protection for Storage?

A. Command Gateway
B. API Index
C. Command Module
D. Launch Pad

2. Which control is used to configure an application policy for assignment to a target computer?

A. Policy commands
B. Policy options
C. Rules Wizard
D. Sandbox rules

3. What differentiates a Full Closed policy from a Full Open policy for a custom application?

A. The Full Open policy enforces maximum restriction, while the Full Closed policy does not offer restriction
B. The Full Closed policy cannot be tuned, while the Full Open policy allows for additional tuning.
C. The Full Closed policy enforces maximum restriction, while the Full Open policy does not offer restriction
D. The Full Closed policy does not allow write access, while the Full Open policy allows for both read and write access

4. Where are specific Domain Controller protection settings found in Cloud Workload Protection?

A. Global System Settings
B. Default OS Policy
C. Cloud Formation Template
D. The Windows OS Policy

5. What is one use of the Windows Global Policy Agent Tools?

A. Allows Configuration Tools to run with full privileges for the root user.
B. Elevates privileges for all install agents.
C. Allows Configuration Tools to run with full privileges for specific users.
D. Removes agents from all Windows devices.

6. How can an administrator segregate organizational data in a Cloud Workload Protection account?

A. With the use of additional Domains
B. With the use of Isolation Policies
C. With the use of Sandboxed Applications
D. With the use of License Separation

7. How quickly are assets scanned when using Near real-time scan for Storage?

A. According to the schedule set in the global system policy
B. Immediately after an object is added or updated
C. After system update and reboot
D. Every time the agent checks in for updates

8. A network rule for the DNS service that is specified under the Windows OS and Modules sandbox *allows* inbound connections from all IP addresses on the DNS port. This connection is *denied* in the Global policy. Why does an inbound IP connection reach the protected instance?

A. The sandbox policy rules supersede the global policy rules
B. Given contradicting policy rules, allow is the default behavior
C. The global policy rules supersede the sandbox policy rules
D. The global denial will apply only if there are no contradicting sandbox-specific rules

9. Where can an administrator quickly see a count of software services and platforms that are exposed to any potential threats?

A. Threat Widget
B. Exposed Instance Events page
C. Threat Exposure Dashboard
D. Admin Notifications

10. What is required to successfully complete a Cloud Workload Protection agent installation?

A. Delete the agent enrollment keys
B. Restart the instance
C. Remove the instance token
D. Re-deploy the instance

Sample Exam Answers:

1. A
2. B
3. C
4. D
5. C
6. A
7. B
8. D
9. C
10. B