BROADCOM®
SOFTWARE

Exam 250-586
Symantec Endpoint Security Complete Implementation Technical Specialist

Exam Study Guide v. 1.0

Exam Description

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

This exam targets IT Professionals implementing the Symantec Endpoint Security Complete product in a consultative or support role. This certification exam tests the candidate's knowledge on how to assess, design, implement and manage a Symantec Endpoint Security Complete solution design that will provide comprehensive endpoint security with multilayered defense and single agent/single console management with AI-guided policy updates to our customers.

Recommended Experience & Enablement Prerequisites

It is recommended that the candidate has at least 3-6 months experience working with Symantec Endpoint Security Complete in a production or lab environment and have attended the following training courses:

Self-Paced

Symantec Endpoint Security Complete – Basic Administration Internal Link | External Link

This self-paced course serves as a prerequisite to the Symantec Endpoint Security Complete Administration Instructor-led training course. The material covers the basics of the modern threat landscape and how SESC's layered approach to endpoint protection keeps pace. It introduces how administrators access the ICDm and how they use it to configure their endpoint protection environment. It covers device enrollment, policy assignment, and the use of threat response tools. Finally, it outlines the process of moving an on-prem environment to the Cloud.

Instructor Led

https://www.broadcom.com/support/symantec/services/education

Symantec Endpoint Security Complete Administration (Course Description)

The Symantec Endpoint Security Complete Administration course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-day operation of a SESC endpoint security environment. The course focuses on SES Complete cloud-based management using the ICDm management console.

Symantec Endpoint Protection 14.x Administration (Course Description)

The Symantec Endpoint Protection 14.x Administration R1 course is designed for the network, IT security, and systems administration professional in a Security Operations position tasked with the day-to-day operation of the SEPM on-premises management console and with configuring optimum security settings for endpoints protected by Endpoint Protection.

Exam Study References

Self-Paced

Symantec Endpoint Security Complete Implementation Curriculum

Architecture and Design Essentials: Internal Link | External Link
The resources in this training deliver exhaustive instruction on the design and architecture of a SES Complete solution, encompassing the structure and interplay of the principal software components.

Assessing the Customer Environment and Objectives: Internal Link | External Link
This training imparts the necessary guidance for assessing and comprehending customer networks. It equips you with the ability to offer strategic counsel for planning and preemptively identifying potential issues prior to conceptualizing a Symantec solution implementation within a customer's environment.

Designing the Solution: Internal Link | External Link
This constitutes a comprehensive training program focused on Symantec solution design. It provides an extensive examination of the design process, starting from the interpretation of client requirements gleaned during the assessment phase, to the creation of bespoke solution designs that meet the unique needs of each customer.

Implementing the Solution: Internal Link | External Link
The materials encompassed in this training equip you with the necessary knowledge and expertise to deploy Symantec solutions within a customer's network infrastructure.

Managing the Ongoing Customer Relationship: Internal Link | External Link
This training addresses the critical elements of relationship management and explores strategies for ongoing support, handling feedback, and upselling or cross-selling including recommending customer workshops.

Documentation

https://support.broadcom.com/security

- **Symantec Endpoint Security Documentation** (Link)
- **Symantec Endpoint Protection Documentation** (Link)
- **Symantec Endpoint Protection Installation and Administration Guide** (Link)
- **Related Documents** (Includes the following)**:** (Link)
  - Symantec Endpoint Protection Client Guides
  - Release Notes
  - Sizing and Scalability Best Practices Whitepaper
  - Quick Start

Exam Objectives

The following tables list the objectives for the exam and how these objectives align to the corresponding Symantec course topics as well as the referenced product documentation.

For more information on the Broadcom Certification Program, visit:
https://www.broadcom.com/support/education/software/certification

Architecture & Design Essentials

EXAM OBJECTIVES	APPLICABLE COURSE CONTENT
Describe the available architecture types and benefits provided by SES Complete	• **SESC Implementation Curriculum** ○ *Architecture and Design Essentials* • **Symantec Endpoint Security Documentation** • **Symantec Endpoint Protection Documentation** • **Symantec Endpoint Protection Installation and Administration Guide** • **SEP Sizing and Scalability Best Practices Whitepaper**
Understand architectural design considerations and constraints of SES Complete	
Describe the components, structure, and communication flow of a SES Complete cloud infrastructure design	
Describe the components, structure and operation and communication flow of a SES Complete hybrid or on-premises infrastructure design	
Describe the migration planning & design process	

Assessing the Customer Environment and Objectives

EXAM OBJECTIVES	APPLICABLE COURSE CONTENT
Understand the phases and stages of the SES Complete Implementation Framework	• **SESC Implementation Curriculum** ○ *Assessing the Customer Environment and Objectives* • **Symantec Endpoint Security Documentation** • **Symantec Endpoint Protection Documentation**
Describe the actions performed in executing the Assessment phase	
Describe the steps required in determining functional requirements based on SES Complete use cases	
Describe the methods used in the development the SESC Solution Proposal	
Understand the actions performed in the production and presentation of the SES Complete Solution Proposal for validation	

Designing the Solution

EXAM OBJECTIVES	APPLICABLE COURSE CONTENT
Describe the actions performed in executing the Design Phase	• **SESC Implementation Curriculum** ○ Designing the Solution • **Symantec Endpoint Security Documentation** • **Symantec Endpoint Protection Documentation** • **Symantec Endpoint Protection Installation and Administration Guide** • **SEP Sizing and Scalability Best Practices Whitepaper**
Describe the steps required to develop the Solution Infrastructure Design	
Describe the steps required to develop the Solution Configuration Design	
Describe the methods used in the development of the Solution Test Plan	
Understand the actions performed in the production and presentation of the SESC Solution Design	

Implementing the Solution

EXAM OBJECTIVES	APPLICABLE COURSE CONTENT
Describe the actions performed in executing the Implement Phase	• **SESC Implementation Curriculum** ○ *Managing the Ongoing Customer Relationship* • **Symantec Endpoint Security Documentation** • **Symantec Endpoint Protection Documentation** • **Symantec Endpoint Protection Installation and Administration Guide**
Describe the steps required to implement the Solution Infrastructure Design	
Describe the steps required to implement the Solution Configuration Design	
Describe the methods used in the execution of the Pilot Deployment	
Understand the actions performed when finalizing the SES Complete Implementation engagement	

Managing the Ongoing Customer Relationship

EXAM OBJECTIVES	APPLICABLE COURSE CONTENT
Describe the actions performed in executing the Manage Phase	• **SESC Implementation Curriculum** ○ *Managing the Ongoing Customer Relationship*
Describe the steps required to assess the current state of the SES Complete Solution	
Describe the methods used when analyzing the current state of the SES Complete Solution	
Understand the actions performed when apprising the Customer of available SES Complete enablement, education, support, and documentation	

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 protection technologies should be enabled to protect against Ransomware attacks?**
   a. Firewall, Host Integrity, System Lockdown.
   b. IPS, SONAR, and Download Insight.
   c. IPS, Firewall, System Lockdown.
   d. SONAR, Firewall, Download Insight.

2. **What should be understood regarding the differences between a Domain and a Tenant in ICDm?**
   a. A domain can contain multiple tenants.
   b. A tenant can contain multiple domains.
   c. Each customer can have one tenant and no domains.
   d. Each customer can have one domain and many tenants.

3. **Why is it important to research the customer prior to arriving onsite?**
   a. To review the supporting documentation.
   b. To understand recent challenges.
   c. To align client expectations with consultant expectations.
   d. To understand the customer and connect their needs to technology.

4. **What does the Base Architecture section of the Infrastructure Design provide?**
   a. A mapping of the chosen implementation model.
   b. The methods for consistent and reliable delivery of agent installation packages.
   c. The approach to endpoint enrollment or agent installation.
   d. The illustration of the solution topology and component placement.

5. **What is the main objective of Network Integrity Configuration testing?**
   a. To validate the downloading and execution of the Breach Assessment Tool.
   b. To test the advanced settings for Intrusion Prevention Policies.
   c. To ensure that the 'Auto Tuning' of zero prevalence behaviors to deny is operational.
   d. To test the remediation behavior of the agent when a network is deemed suspicious.

6. **What is the purpose of the Solution Configuration Design in the Implement phase?**
   a. To provide a brief functional overview of the component placement in the environment.
   b. To outline the hardware requirements for on-premises components.
   c. To guide the implementation of features and functions.
   d. To detail the storage estimates and hardware configuration.

7. **What is implemented after the SES Complete Base architecture in the Implement phase?**
   a. Implement the Logical Design.
   b. Sign into Symantec Security Cloud page.
   c. Create administrative accounts.
   d. Endpoint Enrollment and Distribution.

8. **What is the purpose of the 'Evaluation' agenda item in a project close-out meeting?**
   a. To provide a project overview
   b. To gather insights and derive practical lessons from the project.
   c. To discuss the next steps and any possible outstanding project actions.
   d. To confirm project closure with all stakeholders.

9. **What is the purpose of evaluating default or custom Device/Policy Groups in the Manage Phase?**
    a. To understand how resources are managed and assigned.
    b. To validate replication between sites.
    c. To analyze the Solution Test Plan.
    d. To validate Content Delivery configuration.

10. **Where can information about the validation of in-use features/functions be found during the Manage phase?**
    a. Solution Infrastructure Design.
    b. Solution Configuration Design.
    c. Test Plan.
    d. Business or Technical Objectives.

Sample Exam Answers:

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