BROADCOM

250-580:
Symantec Endpoint Security Complete Administration R2

Exam Study Guide v. 1.2

Exam Description

Candidates can validate technical knowledge and competency by becoming a Symantec Certified Specialist (SCS) based on your specific area of Symantec technology expertise. To achieve this level of certification, candidates must pass this proctored SCS 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 using the Symantec Endpoint Security Complete product in a Security Operations role. This certification exam tests the candidate's knowledge on how Symantec Endpoint Security Complete provides comprehensive endpoint security with multilayered defense and single agent/single console management with AI-guided policy updates.

Recommended Experience

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.

Study References

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

Symantec Endpoint Security Complete Administration

(5-Day Classroom/Virtual)

- Introduction to Symantec Endpoint Security Complete
- Configuring SES Complete Security Controls
- Responding to Threats with ICDm
- Endpoint Detection and Response
- Attack Surface Reduction
- Mobile and Modern Device Security
- Threat Defense for Active Directory
- Working with a Hybrid Environment

Symantec Endpoint Protection 14.x Administration

(5-Day Classroom/Virtual)

- Managing Console Access and Delegating Authority
- Managing Client-to-Server Communication
- Managing Client Architecture and Active Directory Integration
- Managing Clients and Responding to Threats
- Monitoring the Environment and Responding to Threats
- Creating Incident and Health Status Reports
- Introducing Content Updates Using LiveUpdate
- Analyzing the SEPM Content Delivery System
- Managing Group Update Providers
- Manually Downloading Certified and Rapid Release Definitions

- Protecting Against Network Attacks and Enforcing Corporate Policies using the Firewall Policy
- Blocking Network Threats with Intrusion Prevention
- Protecting Against Memory-Based Attacks
- Preventing Attacks with SEP Layered Security
- Securing Windows Clients
- Securing Linux Clients
- Securing Mac Clients
- Providing Granular Control with Host Integrity
- Controlling Application and File Access
- Restricting Device Access for Windows and Mac Clients
- Hardening Clients with System Lockdown
- Customizing Protection Based on User Location
- Managing Security Exceptions

Symantec Endpoint Protection 14.2 Maintain and Troubleshoot

(3-Day Classroom/Virtual)

- Troubleshooting Techniques and Tools
- Troubleshooting the Console
- Installation and Migration Issues
- Client Communication Issues
- Content Distribution Issues
- Extending the SEP infrastructure
- Responding to a Security Incident
- Performance Issues

Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration

(3-Day Classroom/Virtual)

- Introduction to Symantec Endpoint Detection and Response
- Architecture and Sizing
- Implementation
- Detecting Threats
- Investigating Threats
- Responding to Threats
- Reporting on Threats

Self-Paced https://brocade.csod.com/ui/lms-learning-details/app/video/e595bd09-

Symantec Endpoint Security Complete – Basic Administration*

- Understanding Suspicious and Malicious activity using the MITRE ATT&CK Framework
- Integrated Cyber Defense Manager console tour
- Policy assignment
- Threat response tools overview

* This self-paced course is a prerequisite to the instructor led version of the Symantec Endpoint Security Complete Administration course and is recommended study by the exam candidate as some of the questions were derived from this courseware

Symantec Endpoint Protection 14.x Planning and Implementation

(4-Hour Self-Paced eLearning)

- Architecting and Sizing the SEP Implementation
- Installing the Symantec Endpoint Protection Manager
- Benefiting from a SEPM Disaster Recovery Plan
- Managing Replication and Failover
- Deploying Windows Clients
- Deploying Linux Clients
- Deploying Mac Clients
- Upgrading and Cloud Enrollment

Documentation https://support.broadcom.com/security

- Symantec Endpoint Security Documentation
  https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud.html
    - Symantec Endpoint Protection Installation and Administration Guide:
      https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all.html
- Related Documents (Includes the following):
    - Symantec Endpoint Protection Client Guides
    - Release Notes
    - Sizing and Scalability Best Practices Whitepaper
    - Quick Start
    - REST API Reference Guide

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Related-Documents.html

- Symantec Endpoint Detection and Response Documentation
  https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-6.html

Symantec Websites

- Symantec Endpoint Security Product Page
- Symantec Endpoint Security Cloud Help

Exam Objectives

The following tables list the Symantec 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.

Candidates are encouraged to complete applicable lab exercises as part of their preparation for the exam.

For more information on the Symantec Certification Program, visit https://www.broadcom.com/support/symantec/services/education/certification.

Introduction to Symantec Endpoint Security Complete

Exam Objectives	Applicable Course Content
Understand SES Complete Architecture.	**Symantec Endpoint Security Complete Administration** • Module: Introduction to Symantec Endpoint Security Complete
Describe the benefits of SES Complete Cloud-based management.	
Describe the various methods for enrolling SES endpoint agents.	

Configuring SES Complete Security Controls

Exam Objectives	Applicable Course Content
Understand how policies are used to protect endpoint devices.	

Exam Objectives	Applicable Course Content
Understand the Threat landscape and the MITRE ATT&CK Framework.	**Symantec Endpoint Security Complete Administration** • Module: Configuring SES Complete Security Controls
Describe how SES Complete can be used in preventing an attacker from accessing the environment.	
Describe how SES Complete prevents threat execution.	
Describe how SES Complete prevents threat persistence.	
Describe how SES Complete prevents privilege escalation.	
Describe how SES Complete prevents defense evasion.	
Describe how SES Complete prevents device discovery.	
Describe how SES Complete blocks Command & Control communication.	
Describe how SES Complete works to block data exfiltration.	
Describe SES Complete content update types and how they are distributed to endpoints.	
Describe SES Complete policy versioning and its use.	

Responding to Threats with ICDm

Exam Objectives	Applicable Course Content
Describe the ICDm security control dashboards and their use.	**Symantec Endpoint Security Complete Administration** • Module: Responding to Threats with ICDm
Understand how ICDm is used to identify threats in the environment.	
Describe the incident lifecycle and steps required to identify a threat.	
Describe the ways in which ICDm can be used to remediate threats.	

Exam Objectives	Applicable Course Content
Describe how to use ICDm to configure administrative reports.	

Endpoint Detection and Response

Exam Objectives	Applicable Course Content
Describe the requirements to enable Endpoint Detection and Response in the ICDm management console.	**Symantec Endpoint Security Complete Administration** • Module: Endpoint Detection and Response
Describe how EDR assists in identifying suspicious and malicious activity.	
Describe how EDR aids in investigating potential threats.	
Describe the configuration and use of the Endpoint Activity Recorder.	
Understand the use of LiveShell for incident response.	
Describe how to use EDR to retrieve and submit files for analysis.	
Describe how EDR can be used to quarantine endpoint devices.	
Describe how EDR can be used to block and quarantine suspicious files.	

Attack Surface Reduction

Exam Objectives	Applicable Course Content
Describe Behavior Prevalence the use of the SES Complete Behavioral Insights and Policy Tuning Widget.	**Symantec Endpoint Security Complete Administration** • Module: Attack Surface Reduction
Describe how the SES Complete Heatmap can be used to prevent unwanted application behaviors.	
Describe SES Complete policy adaptations and behavioral tuning.	

Exam Objectives	Applicable Course Content
Describe the SES Complete policy and device groups and how they are used.	
Describe the requirements to enable App Control in the ICDm management console.	
Describe the process of monitoring drift to further tune App Control policies.	

Mobile and Modern Device Security

Exam Objectives	Applicable Course Content
Describe the requirements to enable Network Integrity in the ICDm management console.	**Symantec Endpoint Security Complete Administration** • Module: Mobile and Modern Device Security
Describe Network Integrity Policy Configuration and its use.	
Describe how Network Integrity works to remediate threats.	
Describe how SES Complete's mobile technologies protection against malicious apps.	
Describe how SES Complete's mobile technologies protection against malicious networks.	

Threat Defense for Active Directory

Exam Objectives	Applicable Course Content
Describe the requirements for Threat Defense for Active Directory Installation and Configuration.	**Symantec Endpoint Security Complete Administration** • Module: Threat Defense for Active Directory
Describe the Threat Defense Active Directory policy and its use.	
Describe how Threat Defense for Active Directory is used to identify threats.	
Describe how Threat Defense for Active Directory protects against misconfigurations and vulnerabilities in an environment.	

Working with a Hybrid Environment

Exam Objectives	Applicable Course Content
Describe the process for policy migration from SEPM to the ICDm console.	**Symantec Endpoint Security Complete Administration** • Module: Working with a Hybrid Environment
Describe policy precedence in a hybrid configuration.	
Understand how Sites and Replication are impacted in a Hybrid environment.	
Describe the requirements and process for SEPM integration with the ICDm platform used in a SES Complete Hybrid architecture.	

Architecting and Sizing the SEP Implementation

Exam Objectives	Applicable Course Content
Describe the Symantec Endpoint Protection components	**Symantec Endpoint Protection 14.x Planning and Implementation** • Module: Architecting and Sizing the SEP Implementation
Determine proper placement for GUP, SEPM, and LUA for communication and content deployment	

Preventing File-Based Attacks with SEP Layered Security

Exam Objectives	Applicable Course Content
Explain common threats and security risks to the endpoint	**Symantec Endpoint Protection 14.x Administration** • Module: Preventing File-Based Attacks with SEP Layered Security

Managing Client Architecture and Active Directory Integration

Exam Objectives	Applicable Course Content
Explain how policies and concepts relate to the Symantec Endpoint Protection architecture	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Client Architecture and Active Directory Integration
Describe how to configure communication, general, and security settings	

Managing Client-to-Server Communication

Exam Objectives	Applicable Course Content
Identify how to verify client connectivity and find clients in the console	**Symantec Endpoint Protection 14.x Administration** **and** **Symantec Endpoint Protection 14.2 Maintain and Troubleshoot** • Module: Managing Client-to-Server Communication (Administration) and Client Communication Issues (Maintain and Troubleshoot)

Introducing Content Updates Using LiveUpdate

Exam Objectives	Applicable Course Content
Describe how to configure LiveUpdate policies	**Symantec Endpoint Protection 14.x Administration** • Module: Introducing Content Updates Using LiveUpdate

Managing Security Exceptions

Exam Objectives	Applicable Course Content
Describe when and how to configure exceptions	**Symantec Endpoint Protection 14.x Administration** **and** **Symantec Endpoint Protection 14.2 Maintain and Troubleshoot** • Module: Managing Security Exceptions (Administration) and Responding to a Security Incident (Maintain and Troubleshoot)
Explain the remediation actions for infected files	

Preventing Attacks with SEP Layered Security

Exam Objectives	Applicable Course Content
Describe how protection technologies interact and their dependencies	**Symantec Endpoint Protection 14.x Administration** • Module: Preventing Attacks with SEP Layered Security
Describe how to customize Firewall, Intrusion Prevention and Application and Device Control policies	

Securing Windows Clients

Exam Objectives	Applicable Course Content
Describe how to configure scheduled and on-demand scans	**Symantec Endpoint Protection 14.x Administration** **and** **Symantec Endpoint Protection 14.2 Maintain and Troubleshoot** • Module: Securing Windows Clients (Administration) and Responding to a Security Incident (Maintain and Troubleshoot)
Describe how to configure Auto-Protect for file systems/email clients	
Describe how to configure Insight and Download Insight	
Describe how to configure SONAR	

Protecting Against Network Attacks and Enforcing Corporate Policies using the Firewall Policy

Exam Objectives	Applicable Course Content
Describe how to configure the Firewall policy	**Symantec Endpoint Protection 14.x Administration** • Module: Protecting Against Network Attacks and Enforcing Corporate Policies using the Firewall Policy

Blocking Network Threats with Intrusion Prevention

Exam Objectives	Applicable Course Content
Describe how to configure Intrusion Prevention policies	**Symantec Endpoint Protection 14.x Administration** • Module: Blocking Network Threats with Intrusion Prevention

Controlling Application and File Access and Restricting Device Access for Windows and Mac Clients

Exam Objectives	Applicable Course Content
Describe how to configure Application and Device Control policies	**Symantec Endpoint Protection 14.x Administration** • Module: Controlling Application and File Access and Restricting Device Access for Windows and Mac Clients

Installing the Symantec Endpoint Protection Manager

Exam Objectives	Applicable Course Content
Explain when to install additional Symantec Endpoint Protection Managers and sites	**Symantec Endpoint Protection 14.x Planning and Implementation** • Module: Installing the Symantec Endpoint Protection Manager

Managing Replication and Failover

Exam Objectives	Applicable Course Content
Describe how to edit server and site properties	**Symantec Endpoint Protection 14.x Planning and Implementation** • Module: Managing Replication and Failover

Benefiting from a SEPM Disaster Recovery Plan

Exam Objectives	Applicable Course Content
Explain the procedures for Symantec Endpoint Protection database management, backup, restore and Symantec Endpoint Protection disaster recovery	**Symantec Endpoint Protection 14.x Planning and Implementation** • Module: Benefiting from a SEPM Disaster Recovery Plan

Monitoring the Environment and Responding to Threats

Exam Objectives	Applicable Course Content
Describe how to create, view, and manage notifications	**Symantec Endpoint Protection 14.x Administration** • Module: Monitoring the Environment and Responding to Threats

Managing Console Access and Delegating Authority

Exam Objectives	Applicable Course Content
Describe how to manage administrator accounts and delegation of roles	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Console Access and Delegating Authority

Endpoint Detection and Response – Architecting and Sizing

Exam Objectives	Applicable Course Content
Given a scenario, demonstrate knowledge of SEDR Architecture and Sizing considerations.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration** • Module: Architecture and Sizing
Describe the capabilities and functions of Symantec EDR.	

Implementation

Exam Objectives	Applicable Course Content
Given a scenario, define the discrete components found within SEDR.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration** • Module: Implementation
Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats.	

Detecting Threats

Exam Objectives	Applicable Course Content
Describe installation prerequisites, minimum solution configuration and installation procedures required to identify threats.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration** • Module: Detecting Threats
Describe the challenges faced when threat hunting in the environment and their resultant business objectives.	

Investigating Threats

Exam Objectives	Applicable Course Content
Describe the methods used to identify evidence of suspicious and malicious activity.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration**
Describe the various types of Indicators of Compromise (IoC) found in a typical environment.	

Exam Objectives	Applicable Course Content
Describe the methods used to search for IOCs using SEDR.	• Module: Investigating Threats

Responding to Threats

Exam Objectives	Applicable Course Content
Describe the methods SEDR uses to respond to threats in a typical environment.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration** • Module: Responding to Threats
Describe installation prerequisites, minimum solution configuration and installation procedures required to isolate threats.	

Reporting on Threats

Exam Objectives	Applicable Course Content
Describe the methods used to create post incident reports and the benefits to forensic analysis it provides.	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration** • Module: Reporting on Threats
Given a scenario, determine the appropriate method to create a post incident report using SEDR.	

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. Which Windows component needs to be tuned using a registry key change to enable SES remote push?

A. Windows Firewall
B. User Access Control
C. Group Policies
D. Local Policies

2. Which MITRE ATT&CK framework step includes destroying data and rendering an endpoint inoperable?

A. Rampage
B. Kill Chain
C. Exfiltration
D. Impact

3. Which SES Policy controls port scan detection?

A. IPS
B. Firewall
C. Device Control
D. Exploit Mitigation

4. Which type of endpoint connectivity requires low bandwidth mode for LiveUpdate?

A. 4G
B. Wifi
C. VPN
D. Satellite

5. Using the ICDm console, a SES administrator issues a device command. When will the command be executed on the endpoint?

A. At the next heartbeat
B. When the user is idle
C. Immediately
D. When the endpoint reboots

6. Which antimalware engine detects attacks coded in JavaScript?

A. Emulator
B. Sapient
C. Core3
D. SONAR

7. When an endpoint is compromised and quarantined, which online resource is available to remediate the infection?

A. Windows Update
B. LiveUpdate
C. Security Response
D. SymDiag

8. Which auto management task is created when a malicious file generates malicious outbound traffic?

A. Deny list file
B. Allow list file
C. Enable IPS audit
D. Quarantine file

9. Which report format is supported in Symantec Endpoint Security?

A. Text
B. HTML
C. XML
D. PDF

10. What is the recommended first step for an administrator to perform when beginning a discover and deploy campaign?

A. Configure the registry
B. Configure the SES policies and Groups
C. Disable the Windows firewall
D. Install the first SES agent in the subnet

Sample Exam Answers:

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