BROADCOM

250-605:
Symantec Endpoint Protection 14.x Admin R2 Technical Specialist

Exam Study Guide v. 1.0

Exam Description

Candidates can validate technical knowledge and competency by becoming a Broadcom Technical Specialist (BTS) 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 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 Protection 14.x Administration

(4-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
- Restricting Device Access for Windows and Mac Clients
- Hardening Clients with System Lockdown
- Customizing Protection Based on User Location
- Managing Security Exceptions

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
- Managing System Settings

Self-Paced https://www.broadcom.com/support/education/elibrary

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

Symantec Endpoint Protection 14.x Maintain and Troubleshoot

(3-Hour Self-Paced eLearning)

- 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 Protection 14.x Basic Administration

(1.5-Hour Self-Paced eLearning)

Symantec Endpoint Detection and Response 4.x Basic Administration

(45-Minute Self-Paced eLearning)

Note: Exam questions are based on content from the Instructor-Led courses. Exam candidates can use the Self-Paced content to enhance their understanding of SEP/EDR principles and as supplemental exam preparation.

Documentation

- Symantec Endpoint Protection Documentation
- Symantec Endpoint Detection and Response Documentation

Symantec Websites

- Symantec Endpoint Security Product Page
- Symantec Endpoint Protection Related Documents
- Symantec Endpoint Detection and Response Related Documents
- Broadcom Support Portal

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.

Managing Console Access and Delegating Authority

Exam Objectives	Applicable Course Content
Describe Administrator Accounts	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Console Access and Delegating Authority
Understand Directory Server Authentication for an Administrator Account	

Managing Client to Server Communication

Exam Objectives	Applicable Course Content
Describe Client-to-SEPM Communication	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Client to Server Communication

Managing Client Architecture and Active Directory Integration

Exam Objectives	Applicable Course Content
Describe the Interaction Between Sites, Domains, and Groups	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Client Architecture and Active Directory Integration
Understand Groups, Locations, and Policy Inheritance Management	
Describe Importing Organizational Units from Active Directory	

Managing Clients and Responding to Threats

Exam Objectives	Applicable Course Content
Understand the Clients View	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Clients and Responding to Threats

Monitoring the Environment and Responding to Threats

Exam Objectives	Applicable Course Content
Understand Critical Data Using the Summary Page	**Symantec Endpoint Protection 14.x Administration** • Module: Monitoring the Environment and Responding to Threats
Describe New Incidents Using the Logs Page	
Understand How Actions Sent to Clients Using the Command Status View are Monitored	
Describe How to Configure Notifications	

Creating Incident and Health Status Reports

Exam Objectives	Applicable Course Content
Describe How to Monitor Critical Data Using the Reports Page	**Symantec Endpoint Protection 14.x Administration** • Module: Creating Incident and Health Status Reports
Describe How to Identify New Incidents Using Quick Reports and Filters	
Describe how to Configure Scheduled Reports	

Introducing Content Updates Using LiveUpdate

Exam Objectives	Applicable Course Content
Describe the LiveUpdate Ecosystem	**Symantec Endpoint Protection 14.x Administration** • Module: Introducing Content Updates Using LiveUpdate
Describe How to Configure LiveUpdate	
Understand the Need for an Internal LiveUpdate Administrator Server	
Describe how to Configure an Internal LiveUpdate Administrator Server	

Analyzing the SEPM Content Delivery System

Exam Objectives	Applicable Course Content
Describe Content Updates	**Symantec Endpoint Protection 14.x Administration** • Module: Analyzing the SEPM Content Delivery System
Describe how to Manage Content on the SEPM	
Understand how to Monitor Content Distribution to the Clients	

Managing Group Update Providers

Exam Objectives	Applicable Course Content
Describe Group Update Providers	**Symantec Endpoint Protection 14.x Administration** • Module: Managing Group Update Providers
Describe how to Add Group Update Providers	
Describe how to Monitor Group Update Providers	

Manually Downloading Certified and Rapid Release Definitions

Exam Objectives	Applicable Course Content
Describe how to Download Certified SEPM Definitions from Symantec Security Response	**Symantec Endpoint Protection 14.x Administration** • Module: Manually Downloading Certified and Rapid Release Definitions
Describe how to Download Rapid Release Definitions from Symantec Security Response	
Describe how to Locate Statically Named Definitions	

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

Exam Objectives	Applicable Course Content
Understand how to Prevent Network Attacks	**Symantec Endpoint Protection 14.x Administration** • Module: Protecting Against Network Attacks and Enforcing Corporate Policies Using the Firewall Policy
Examine Firewall Policy Elements	
Describe How to Create Custom Firewall Rules	
Describe Advanced Firewall Features	

Blocking Network Threats with Intrusion Prevention

Exam Objectives	Applicable Course Content
Describe Intrusion Prevention Technologies	**Symantec Endpoint Protection 14.x Administration** • Module: Blocking Network Threats with Intrusion Prevention
Describe how to Configure the Intrusion Prevention Policy	
Understand how to Manage Custom Signatures	
Describe how to Monitor Intrusion Prevention Events	

Protecting Memory with Memory Exploit Mitigation

Exam Objectives	Applicable Course Content
Describe Memory Exploit Mitigation	**Symantec Endpoint Protection 14.x Administration** • Module: Protecting Memory with Memory Exploit Mitigation

Preventing File-Based Attacks with SEP Layered Security

Exam Objectives	Applicable Course Content
Describe Virus and Spyware Protection	**Symantec Endpoint Protection 14.x Administration** • Module: Preventing File-Based Attacks with SEP Layered Security
Understand File Reputation	
Describe Insight Lookup	
Describe the Emulator and Machine Learning Engine	
Understand Download Insight	
Understand Auto-Protect Scans	

Describe SONAR	
Understand Administrator-Defined Scans	

Securing Windows Clients

Exam Objectives	Applicable Course Content
Describe the Windows Virus and Spyware Protection Policy	**Symantec Endpoint Protection 14.x Administration** Module: Securing Windows Clients
Describe how to Tailor Scans to Meet an Environment's Needs	
Describe how to Ensure Real-Time Protection for Clients	
Understand Detecting and Remediating Risks in Downloaded Files	
Describe how to Identify Zero-Day and Unknown Threats	
Describe how to Prevent Email from Downloading Malware	
Describe how to Configure Advanced Options	
Describe how to Monitor Virus and Spyware Activity	

Restricting Device Access for Windows and Mac Clients

Exam Objectives	Applicable Course Content
Describe Windows and Mac Device Control Concepts	**Symantec Endpoint Protection 14.x Administration** Module: Restricting Device Access for Windows and Mac Clients
Understand How to Configure Device Control	

Understand How to Monitor Device Control Events	

Hardening Clients with System Lockdown

Exam Objectives	Applicable Course Content
Describe System Lockdown	**Symantec Endpoint Protection 14.x Administration** Module: Hardening Clients with System Lockdown
Understand How to Create the File Fingerprint List	
Describe System Lockdown Use Cases	

Customizing Protection Based on User Location

Exam Objectives	Applicable Course Content
Understand How to Create Locations	**Symantec Endpoint Protection 14.x Administration** Module: Customizing Protection Based on User Location
Describe Adding Policies to Locations	
Understand How to Monitor Location Awareness	

Managing Security Exceptions

Exam Objectives	Applicable Course Content
Describe Security Exceptions	**Symantec Endpoint Protection 14.x Administration** Module: Managing Security Exceptions
Describe Exclusions	
Understand How to Manage Exceptions	
Understand How to Monitor Security Exceptions	

Endpoint Detection and Response – Introduction

Exam Objectives	Applicable Course Content
Describe Symantec Endpoint Detection and Response Business Objectives	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Introduction
Describe the Components of Symantec Endpoint Detection and Response	
Describe SEDR Shared Technologies	

Architecting and Sizing

Exam Objectives	Applicable Course Content
Understand SEDR Architecture and Sizing	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Architecture and Sizing

Implementation

Exam Objectives	Applicable Course Content
Describe SEDR System Requirements	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Implementation
Understand SEDR Installation Considerations	
Describe the SEDR Management Console	
Describe SEDR User Accounts and Roles	
Understand SEDR Integration with Symantec Endpoint Protection	

Detecting Threats in the Environment

Exam Objectives	Applicable Course Content
Understand Suspicious & Malicious Activity with SEDR	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Detecting Threats in the Environment
Describe Prerequisite SEDR Threat Detection Configuration	
Identify evidence of suspicious/malicious activity with SEDR	

Investigating Threats in the Environment

Exam Objectives	Applicable Course Content
Search for indicators of Compromise with SEDR	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Investigating Threats in the Environment
Analyze Endpoint Activity Recorder Data	
Describe Additional SEDR Investigation Tools	

Responding to Threats in the Environment

Exam Objectives	Applicable Course Content
Understand Threat Response in the Cybersecurity Framework for use with SEDR	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Responding to Threats in the Environment
Isolate/Deny/Remove Threats in the Environment with SEDR	
Tune the SEDR Environment	

Reporting on Threats in the Environment

Exam Objectives	Applicable Course Content
Understand SEDR Incident Reporting	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Reporting on Threats in the Environment

Managing System Settings

Exam Objectives	Applicable Course Content
Understand user managed certificates in the SEDR environment	**Symantec Endpoint Detection and Response 4.x Planning, Implementation, and Administration R1** Module: Managing System Settings
Understand SEDR event and incident forwarding	
Describe Splunk integration with 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 SEPM view determines which computers have the latest policies and virus definitions?

A. The Client view
B. The Summary view
C. The Policies view
D. The Health Check view

2. Which LiveUpdate policy type provides options for configuring a LiveUpdate delivery schedule?

A. LiveUpdate Content
B. LiveUpdate Schedule
C. LiveUpdate Settings
D. Content Delivery

3. Which policy component includes lists of approved applications that are allowed to run on client computers?

A. Host Group Lists
B. File Fingerprint Lists
C. Approved Application Lists
D. Allow Lists

4. Which feature makes it possible to insert a warning message into an infected email message?

A. Microsoft Outlook Auto-Protect
B. Internet Email Auto-Protect
C. Internet Email Anti-Malware Protection

D. Microsoft Exchange Anti-Malware

5. Which Clients page view is used see when the most recent scan started on protected endpoints?

A. Protection Technology
B. Client Status
C. Client System
D. Default

6. Which feature is a subset of Application and Device Control that can be used by itself or in conjunction with Application and Device Control?

A. Allow Lists
B. Custom AD Control
C. Application Monitoring
D. System Lockdown

7. Which feature excludes files and folders from various scan types so that scans do not interfere with daily business operations?

A. Allow Lists
B. Scan Overrides
C. Exceptions
D. Security Overrides

8. What is the correlation engine that allows for faster, confident responses to security incidents?

A. Insight
B. Skeptic
C. Synapse
D. SONAR

9. What is the timeout for the file deletion command in SEDR?

A. 2 Days
B. 7 Days
C. 72 Hours
D. 5 Days

10. What priority would an incident that may have an impact on business be considered?

A. Low
B. Medium
C. High
D. Critical

Sample Exam Answers:

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