BROADCOM®

250-611: Symantec Data Center Security - Server Advanced 6.x 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 technology expertise. To achieve this level of certification, candidates must pass this proctored exam that is based on a combination of training material, commonly referenced product documentation, and real-world job scenarios.

This exam targets IT Professionals using the Data Center Security: Server Advanced product in an Operations role. This certification exam tests the candidate's knowledge on how to how to install, configure and administer Symantec Data Center Security: Server Advanced.

Recommended Experience

It is recommended that the candidate has at least 3-6 months' experience working with Data Center Security: Server Advanced in a production or lab environment.

Study References

Instructor Led	https://www.broadcom.com/support/education/software/training-courses

Symantec Data Center Security Server Advanced 6.x Administration R2
(3 Day Instructor-Led)

- Introduction to Security Risks and Risk
- SDCS: Server Advanced Overview
- Installation and Deployment
- Configuring Agents
- Policy Overview
- Windows Prevention Policies
- UNIX and Legacy Prevention Policies
- Advanced Prevention
- Detection Policies
- Event Management
- Agent Management and Troubleshooting
- System Management

Documentation

- **Symantec Data Center Security: Server Advanced Documentation**

Product Websites

- **Symantec Data Center Security Product Page**
- **Symantec Data Center Security Related Documents**
- **Broadcom Support Portal**

Exam Objectives

The following tables list the Certification exam objectives for the exam and how these objectives align to the corresponding course topics and their associated lab exercises.

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

For more information on the Certification Program, visit

https://www.broadcom.com/support/education/software/certification

Exam Objectives	Topics from *Symantec Data Center Security: Server Advanced 6.x Administration R2*
Describe Modern Security Risks	• **Lesson**: Introduction to Security Risks
Describe Symantec Data Center Security: Server Advanced Protection Concepts	• **Lesson**: SDCS:SA Overview
Describe Symantec Data Center Security: Server Advanced Installation and Deployment	• **Lesson**: Installation and Deployment
Describe Symantec Data Center Security: Server Advanced Agent Configuration	• **Lesson**: Configuring Agents
Describe Symantec Data Center Security: Server Advanced Policy Concepts	• **Lesson**: Policy Overview

Exam Objectives	Topics from *Symantec Data Center Security: Server Advanced 6.x Administration R2*
Describe Symantec Data Center Security: Server Advanced Windows Prevention Policies	• **Lesson**: Windows Prevention Policies
Describe Symantec Data Center Security: Server Advanced Unix and Lagacy Prevention Policies	• **Lesson**: Unix and Lagacy Prevention Policies
Describe Symantec Data Center Security: Server Advanced Advanced Prevention	• **Lesson**: Advanced Protection
Describe Symantec Data Center Security: Server Advanced Detection Policies	• **Lesson**: Detection Policies
Describe Symantec Data Center Security: Server Advanced Event Management	• **Lesson**: Event Management
Describe Symantec Data Center Security: Server Advanced Agent Management and Troubleshooting	• **Lesson**: Agent Management and Troubleshooting
Describe Symantec Data Center Security: Server Advanced System Management	• **Lesson**: System Management

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 statement describes a benefit of a Host Intrusion Prevention System?**

    a. Real-time proactive enforcement
    b. Monitor-less administration
    c. Constant signature updates
    d. Regular operating system patch maintenance

2. **What information is used to determine which sandbox a program is assigned to?**

    a. Behavior Control Descriptors
    b. Process Binding Rules
    c. Access Control Lists
    d. Least Privilege Access Lists

3. **How many instances of the DCS management server should an administrator install in a large deployment?**

    a. One for every 5,000 agents
    b. One for every 10,000 agents
    c. One for every 50,000 agents
    d. One for every 100,000 agents

4. **What Management Console view would you access to add a new DCS administrator to the system?**

    a. Users
    b. Integration
    c. Administration
    d. Settings

5. **What SDCS:SA policy type uses code segment collectors to acquire information from the host system such as recorded security events, log creation, and registry key modifications?**

    a. Detection
    b. Prevention
    c. System
    d. Configuration

Sample Exam Answers:

1. A
2. B
3. B
4. D
5. A