BROADCOM®

250-587
Symantec Data Loss Prevention 16.x Administration 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 using Data Loss Prevention product suite in an administrative role (including though knowledge of policy authoring and incident reporting). This certification exam texts the candidate's knowledge on how to plan, implement, and administer Symantec Data Loss Prevention.

Recommended Experience

It is recommended that the candidate has 6-9 months' regular experience working with the entire Symantec Data Loss Prevention product suite in a production or lab environment.

Study References

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

Symantec Data Loss Prevention 16.x Administration

(5-Day Classroom/Virtual)

- Data Loss Prevention Landscape
- Overview of Symantec Data Loss Prevention
- Identifying and Describing Confidential Data
- Locating Confidential Data Stored on Premises and in the Cloud
- Understanding How Confidential Data is Being Used
- Educating Users to Adopt Data Protection Practices
- Preventing Unauthorized Exposure of Confidential Data
- Remediating Data Loss Incidents and Tracking Risk Reduction
- Enhancing Data Loss Prevention with Integrations

Self-Paced Learning@Broadcom- DLP 16.x Basic Administration

Symantec Data Loss Prevention 16.x – Basic Administration

- Data Loss Prevention Overview
- Detection Basics
- Locating and Protecting Confidential Data
- Incident Reporting

Documentation

https://techdocs.broadcom.com/us/en/symantec-security-software.html

- Symantec Data Loss Prevention Documentation
  https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0-1.html

Symantec Websites

- Symantec Information Security Product Page

Exam Objectives

The following tables list the Broadcom BTS 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.

As mentioned above, beyond mastery of the administration course and familiarity with product documentation, it is recommended to have 6-9 months regular experience working with the entire Symantec Data Loss Prevention product suite in a production or lab environment.

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

Data Loss Prevention Landscape

Exam Objectives	Applicable Course Content
Describe Data Loss Prevention as it pertains to the industry.	**Symantec Data Loss Prevention 16.x Administration** • **Module**: Data Loss Prevention Landscape
Given a scenario, determine how to reduce risk over time.	**Symantec Data Loss Prevention 16.x Administration** • **Module**: Data Loss Prevention Landscape

Overview of Symantec Data Loss Prevention

Exam Objectives	Applicable Course Content
Describe the features and functionality of Symantec Data Loss Prevention.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Overview of Symantec Data Loss Prevention ○ Identifying and Describing Confidential Data ○ Understanding How Confidential Data is Being Used ○ Preventing Unauthorized Exposure of Confidential Data
Describe the Symantec Data Loss Prevention architecture including each product's architecture.	**Symantec Data Loss Prevention 16.x Administration** • **Module**: Overview of Symantec Data Loss Prevention

Identifying and Describing Confidential Data

Exam Objectives	Applicable Course Content
Given a scenario, determine how to configure policies to effectively capture incidents, including all detection methods.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Identifying and Describing Confidential Data ○ Understanding How Confidential Data is Being Used ○ Preventing Unauthorized Exposure of Confidential Data

Exam Objectives	Applicable Course Content
Describe how to manage and maintain policies.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Identifying and Describing Confidential Data ○ Understanding How Confidential Data is Being Used ○ Preventing Unauthorized Exposure of Confidential Data

Locating Confidential Data Stored on Premises and in the Cloud

Exam Objectives	Applicable Course Content
Describe how to configure Network Discover targets (repositories) to capture incidents and configure Network Protect actions.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Locating Confidential Data Stored on Premises and in the Cloud ○ Preventing Unauthorized Exposure of Confidential Data
Describe how to configure Symantec Data Loss Prevention endpoint agents to perform endpoint actions and configure Endpoint Discover targets to capture endpoint incidents.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Locating Confidential Data Stored on Premises and in the Cloud ○ Understanding How Confidential Data is Being Used ○ Preventing Unauthorized Exposure of Confidential Data

Understanding How Confidential Data is Being Used

Exam Objectives	Applicable Course Content
Describe how to configure Network Prevent with appropriate MTAs or web proxies to capture incidents and block network communications.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Understanding How Confidential Data is Being Used ○ Preventing Unauthorized Exposure of Confidential Data
Given a scenario, describe and apply the various tasks and tools associated with server and system administration.	For this objective, it is important to have experience with the product and to be familiar with product documentation.
Describe how to manage DLP Agents.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Locating Confidential Data Stored on Premises and in the Cloud ○ Understanding How Confidential Data is Being Used ○ Preventing Unauthorized Exposure of Confidential Data
Describe how to configure Network Monitor to capture network incidents.	**Symantec Data Loss Prevention 16.x Administration** • **Module**: Understanding How Confidential Data Is Being Used

Preventing Unauthorized Exposure of Confidential Data

Exam Objectives	Applicable Course Content
Given a scenario, describe how to configure and manage automated and smart response rules to appropriately remediate specific types of incidents.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Preventing Unauthorized Exposure of Confidential Data ○ Remediating Data Loss Incidents and Tracking Risk Reduction

Remediating Data Loss Incidents and Tracking Risk Reduction

Exam Objectives	Applicable Course Content
Describe how to create, use, and distribute reports in DLP using the available tools (Enforce GUI, Reporting and Update API, and Incident Data Access Views).	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Remediating Data Loss Incidents and Tracking Risk Reduction ○ Enhancing Data Loss Prevention with Integrations
Describe how to remediate incidents effectively including use of role-based access control.	**Symantec Data Loss Prevention 16.x Administration** • **Module (including labs)**: Remediating Data Loss Incidents and Tracking Risk Reduction

Enhancing Data Loss Prevention with Integrations

Exam Objectives	Applicable Course Content
Given a scenario, describe how to integrate DLP with other Symantec products and third-party products.	**Symantec Data Loss Prevention 16.x Administration** • **Modules (including labs)**: ○ Understanding How Confidential Data Is Being Used (section on CloudSOC) ○ Locating Confidential Data Stored on Premises and in the Cloud (section on CloudSOC) ○ Enhancing Data Loss Prevention with Integrations

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 Symantec Data Loss Prevention product can monitor and block FTP transmissions?
   A. Network Monitor
   B. Network Prevent for Web
   C. Network Prevent for Email
   D. Network Discover

2. An organization wants to implement Endpoint Prevent and Endpoint Discover for 120,000 endpoint computers using transient connections. What is the minimum number of Endpoint Servers that an organization would need to install??
   A. 4
   B. 6
   C. 8
   D. 10

3. In which two (2) ways can the default listener port for a detection server be modified? (Select two.)
   A. Through the Enforce user interface under System > Overview
   B. By editing the Communication.properties file on a detection server
   C. Through the Enforce user interface under Manage > Policies
   D. By editing the MonitorController.properties file on a detection server
   E. By editing the model.notification.port file on a detection server

4. A state governmental agency has digitized paper applications received from residents over the past several years, and recently the agency deployed a Form Matching policy to prevent these completed applications from leaving their network. However, when employees try to send official publications, blank application forms, or other non-confidential PDF documents externally, the Form Matching process seems to run much slower than expected.

What can the agency do to improve Form Matching performance??
   A. Replace all the files in the Form Matching profile's image gallery with higher resolution PDFs.
   B. Reduce the Filling Threshold setting in the Form Matching policy's rules to a value of 4 or less.
   C. Create fewer Form Matching profiles with a larger number of blank forms in each image gallery.
   D. Protect the files with an EDM policy instead because EDM is inherently more efficient.

5. An organization is monitoring email based on DLP policies but is now ready to implement automated blocking. As part of the designed incident response process, the Incident Response team wants to foster awareness among end users by keeping them informed of any email that is blocked.

Which response rule configuration will allow a DLP Administrator to block the email while providing context and incident information to the email sender?
   A. Combine a Block SMTP Message with an Add Note action that includes incident variables
   B. Combine a Modify SMTP Message with an Add Note action that includes incident variables
   C. Create Block SMTP Message and include incident variables in the Bounce Message to Sender field
   D. Combine a Block SMTP with a Send Email notification action that includes incident variables

6. Which two (2) incident conditions are available to configure Automated Response Rules? (Select two.)

A. Incident Status
B. Sender Groups
C. Protocol or Endpoint Destination
D. Incident Match Count
E. File Size

7. Which response rule action will be ignored when using an Exact Data Matching (EDM) policy?

A. Network Prevent: Remove HTTP/HTTPS Content
B. All: Send Email Notification
C. Network Protect: Copy File
D. Endpoint Prevent: Notify

8. Which two (2) steps should an DLP Administrator take to analyze traffic over port 578 TCP? (Select two.)

A. Create the port 578 under System > Settings > Protocols > Add Protocol.
B. Add port 578 to the existing signature-based HTTP protocol under System > Settings > Protocols > HTTP.
C. Create port 578 under System > Servers and Detectors > Traffic > Add Protocol.
D. Enable Network Monitor detection for port 578 under System > Servers and Detectors > Overview Server > Detector Detail > Configure.
E. Enable Network Monitor detection for port 578 with a detection rule assigned to an active policy under Manage > Policy > Policy List.

9. A Chief Information Security Officer (CISO) wants to consolidate DLP Incident Remediation triage and follow up using a third-party Help Desk through Web Services.

Which document advertises all of the available operations in the Incident Reporting and Update API?

A. Simple Object Access Protocol (SOAP)
B. Web Services Description Language (WSDL)
C. Simple Oriented Access Protocol (SOAP)
D. Web Services Definition Language (WSDL)

10. An incident responder is viewing a discover incident snapshot and needs to determine which information to provide to the next level responder.

Which information would be most useful in assisting the next level responder with data cleanup??

A. Incident Details: Message Body content
B. Data Owner: From Data Insight
C. Incident Details: File Owner metadata
D. Access Information: File Permissions

Sample Exam Answers:

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