Symantec™
A Division of Broadcom

250-438: Symantec Data Loss Prevention Administration – 15.5

Exam Study Guide v2.0

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 Data Loss Prevention product suite in an administrative role (including thorough knowledge of policy authoring and incident reporting). This certification exam tests the candidate's knowledge on how to plan, implement, and administer Symantec Data Loss Prevention.

For more information about the SCS program, see
https://www.broadcom.com/support/symantec/services/education/certification .

Recommended Experience

It is very strongly 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

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

Data Loss Prevention 15.5 Administration

(5-Day Instructor-Led with hands-on labs)

- 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

Data Loss Prevention 15.5 Planning and Implementation

(1-Day Instructor-Led with hands-on labs)

- Overview of Symantec Data Loss Prevention Products and Architecture
- Design Considerations for Implementing Symantec Data Loss Prevention
- Installing Symantec Data Loss Prevention

Data Loss Prevention 15.0 Differences

(eLearning)

- DLP 15.0: Differences Training – Endpoint Enhancements
- DLP 15.0: Differences Training – CloudSOC Integration
- DLP 15.0: Differences Training – Discover
- DLP 15.0: Differences Training – Enforce
- DLP 15.0: Differences Training – Appliance
- DLP 15.0: Differences Training – Appliance Demo

Documentation

https://support.broadcom.com/security

- **Symantec Data Loss Prevennton 15.5 Product Documentation**: https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/information-security/data-loss-prevention/15-5.html

Product documentation referenced in this exam:

- Symantec Data Loss Prevention Administration Guide
- Symantec Data Loss Prevention System Requirements and Compatibility Guide
- Symantec Data Loss Prevention System Maintenance Guide
- Symantec Data Loss Prevention Installation Guide (Windows or Linux)
- Symantec Data Loss Prevention Upgrade Guide (Windows or Linux)
- Symantec Data Loss Prevention Cloud Prevent for Microsoft Office 365 Implementation Guide
- Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide
- Symantec Data Loss Prevention Cloud Detection Service Getting Started Guide
- Symantec Data Loss Prevention Oracle 12c Enterprise Implementation Guide

Symantec Websites

- **Symantec Data Loss Prevention landing page:** https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention

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 strongly recommended to complete all applicable lab exercises in preparation for the exam.

Data Loss Prevention Architecture and Overview

Exam Objectives	Applicable Course Content and Product Documentation
Describe Data Loss Prevention as it pertains to the industry.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Data Loss Prevention Landscape **Documentation**: Symantec Data Loss Prevention 15.5 Administration Guide • Introducing Symantec Data Loss Prevention

Describe the features and functionality of Symantec Data Loss Prevention.	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Module**: Overview of Symantec Data Loss Prevention
	• **Course Labs**:
	  ○ Identifying and Describing Confidential Data (Policy Configurations)
	  ○ Understanding How Confidential Data is Being
	  ○ Preventing Unauthorized Exposure of Confidential Data
	Documentation: Symantec Data Loss Prevention 15.5 Administration Guide
	• Introducing Symantec Data Loss Prevention
	• Detection Server Technologies
	• Deploying the Cloud Detection Service
	• Implementing and working with Appliances
	• Working with Information Centric Encryption
	• Endpoint Agent Capabilities (Protect and Discover)
	• Other chapters with overviews of products in the Symantec Data Loss Prevention product suite

Exam Objectives	Applicable Course Content and Product Documentation
Describe the Symantec Data Loss Prevention architecture including each product's architecture.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Overview of Symantec Data Loss Prevention **Documentation**: Symantec Data Loss Prevention 15.5 Administration Guide • Introducing Symantec Data Loss Prevention • Installing and Implementing Detection Servers • Optical Character Recognition • Network/Endpoint Discover • Other chapters with overviews of products in the Symantec Data Loss Prevention product suite Symantec Data Loss Prevention 15.5 System Requirements and Compatibility Guide • Hardware Requirements

Data Loss Prevention Installation and Configuration

Exam Objectives	Applicable Course Content
Describe how to install Data Loss Prevention.	**Documentation**: Symantec Data Loss Prevention Administration Guide Install additional Detection capabilities • Managing Enforce Server services and settings Symantec Data Loss Prevention Installation Guide (Windows or Linux) • Planning a DLP Install

Exam Objectives	Applicable Course Content

Describe the process for installing and/or registering DLP components in the cloud.	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Modules**:
	  ○ Locating Confidential Data Stored on Premises and in the Cloud
	  ○ Understanding How Confidential Data is Being Used
	Documentation:
	Symantec Data Loss Prevention Administration Guide
	• Installing and managing detection servers and cloud detectors
	Symantec Data Loss Prevention Cloud Prevent for Microsoft Office 365 Implementation Guide
	Symantec Data Loss Prevention Installation Guide
	• Security Configurations
	• Understanding Post-Install Tasks

Given a scenario, determine how to configure policies to effectively capture incidents, including all detection methods.	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Module**: Identifying and Describing Confidential Data
	• **Course Labs:**
	  ○ Identifying and Describing Confidential Data (Policy Configurations)
	  ○ Understanding How Confidential Data is Being
	  ○ Preventing Unauthorized Exposure of Confidential Data
	Documentation:
	Symantec Data Loss Prevention Administration Guide
	• Detection Technologies (DCM, EDM, IDM, VML, etc.)
	• Testing and Tuning
	• Authoring policies

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.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Preventing Unauthorized Exposure of Confidential Data • **Course Labs**: ○ Remediating Data Loss Incidents and Tracking Risk Reduction **Documentation**: Symantec Data Loss Prevention Administration Guide • Configuring policy response rules and actions
Describe how to configure Network Prevent with appropriate MTAs or web proxies to capture incidents and block network communications.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Understanding How Confidential Data is Being Used • **Course Labs**: ○ Understanding How Confidential Data is Being Used **Documentation**: Symantec Data Loss Prevention Administration Guide • Configuring policy response rules and actions
Describe how to configure Network Discover/Cloud Storage targets (repositories) to capture incidents and configure Network Protect actions.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Locating Confidential Data Stored on Premises and in the Cloud • **Course Labs**: ○ Understanding How Confidential Data is Being Used **Documentation**: Symantec Data Loss Prevention Administration Guide • Discovering where confidential data is stored • Working with Information Centric Encryption

Exam Objectives	Applicable Course Content

Describe how to configure Endpoint Prevent agents to perform endpoint actions and configure Endpoint Discover targets to capture endpoint incidents.	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Modules**:
	  ○ Understanding How Confidential Data is Being Used
	  ○ Locating Confidential Data Stored on Premises and in the Cloud
	• **Course Labs**:
	  ○ Locating Confidential Data Stored on Premises and in the Cloud
	Documentation:
	Symantec Data Loss Prevention Administration Guide
	• Using Endpoint Prevent
	• Discovering and preventing data loss on endpoints
	• Working with Information Centric Encryption
	• Configuring policy response rules and actions
	• Working with Agent Configurations and Devices

Given a scenario, describe how to use APIs to integrate DLP with other Symantec solutions (such as CloudSOC and ICE) and third-party products.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Enhancing Data Loss Prevention with Integrations **Documentation**: Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide • About the Update and Reporting API

Data Loss Prevention Managing and Reporting

Exam Objectives	Applicable Course Content
Given a scenario, describe and apply the various tasks and tools associated with server and system administration.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Course Labs**: ○ Understanding How Confidential Data is Being Used **Documentation**: Symantec Data Loss Prevention Administration Guide • Managing the Enforce Server platform • Installing and managing detection servers and cloud detectors • Advanced Server Settings

Describe how to manage DLP Agents.	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Modules**:
	  ○ Locating Confidential Data Stored on Premises and in the Cloud
	  ○ Understanding How Confidential Data Is Being Used
	• **Course Labs**:
	  ○ Understanding How Confidential Data Is Being Used
	Documentation:
	Symantec Data Loss Prevention Administration Guide
	• Managing Agents
	• Agent Configurations
	• Application Monitoring

Exam Objectives	Applicable Course Content

Describe how to create, use, and distribute reports in DLP using the available tools (Enforce GUI, IT Analytics, Reporting and Update API, and Incident Data Access Views).	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Modules**:
	  ○ Remediating Data Loss Incidents and Tracking Risk Reduction
	  ○ Enhancing Data Loss Prevention with Integrations
	• **Course Labs**:
	  ○ Remediating Data Loss Incidents and Tracking Risk Reduction
	Documentation:
	Symantec Data Loss Prevention Administration Guide
	• Remediating and managing incidents

Describe how to remediate incidents effectively including use of role-based access control.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Remediating Data Loss Incidents and Tracking Risk Reduction • **Course Labs**: ○ Remediating Data Loss Incidents and Tracking Risk Reduction **Documentation**: Symantec Data Loss Prevention Administration Guide • Remediating and managing incidents • Managing roles and users

Exam Objectives	Applicable Course Content

Describe how to manage and maintain policies.	**Course**: Symantec Data Loss Prevention 15.5 Administration
	• **Modules**:
	  ○ Identifying and Describing Confidential Data
	  ○ Preventing Unauthorized Exposure of Confidential Data
	• **Course Labs**:
	  ○ Remediating Data Loss Incidents and Tracking Risk Reduction
	Documentation:
	Symantec Data Loss Prevention Administration Guide
	• Authoring policies
	• Configuring policy response rules
	• Data Retention

Given a scenario, determine how to reduce risk over time.	**Course**: Symantec Data Loss Prevention 15.5 Administration • **Module**: Data Loss Prevention Landscape **Documentation**: Symantec Data Loss Prevention Administration Guide

Data Loss Prevention Basic Troubleshooting

Exam Objectives	Applicable Course Content
NOTE: For each exam objectives in this table, please familiarize yourself with the relevant articles in the Tech Support Knowledge Base (in addition to the particular documentation specified for each objective). To access KB articles, go to **https://support.broadcom.com/security** , click on **Product Information**, and search for products in the Data Loss Prevention suite. (KB articles are grouped by individual products in the suite.)	

Exam Objectives	Applicable Course Content
Given a scenario, identify database issues in Symantec Data Loss Prevention.	**Documentation**: Symantec Data Loss Prevention Oracle 12c Enterprise Installation Guide • Installing Oracle 12c • Verifying Database readiness Symantec Data Loss Prevention System Maintenance Guide
Given a scenario, troubleshoot Enforce issues in Symantec Data Loss Prevention.	**Documentation**: Symantec Data Loss Prevention Administration Guide • Various Detection Server Knowledge • Working with User Risk • Accessing the Enforce Console
Given a scenario, troubleshoot endpoint agent issues in Symantec Data Loss Prevention.	**Documentation**: Symantec Data Loss Prevention Administration Guide • Manage DLP Agents (Installation / Removal) Symantec Data Loss Prevention System Maintenance Guide
Given a scenario, troubleshoot detection issues in Symantec Data Loss Prevention.	**Documentation**: Symantec Data Loss Prevention Administration Guide • Installing and Manage Detection/Cloud detection servers • Detection Servers Basic Configuration Symantec Data Loss Prevention System Maintenance Guide
Given a scenario, troubleshoot detection server issues in Symantec Data Loss Prevention.	**Documentation**: Symantec Data Loss Prevention Administration Guide • Enforce and Detection Server Services Symantec Data Loss Prevention System Maintenance Guide

Exam Objectives	Applicable Course Content
Troubleshoot the installation/upgrade process using Symantec tools.	**Documentation**: Symantec Data Loss Prevention Upgrade Guide • Upgrade Phases • Database preparation Symantec Data Loss Prevention Installation Guide
Describe how to configure Cloud Detection Service and integrate it with Symantec CloudSOC to monitor and protect data in motion and data at rest in cloud applications.	**Documentation**: Symantec Data Loss Prevention Administration Guide • Working with Cloud Connectors • Application Detection Symantec Data Loss Prevention Installation Guide • Installing an Enforce Server

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

11. **A DLP Administrator is creating a role that contains an incident access condition that restricts users from viewing specific incidents.**

    Which two (2) conditions can the administrator specify when creating the incident access condition in a role? (Select two.)

    A. File type
    E. Custom attribute
    F. Recipient
    G. File size
    H. Policy group

12. **An incident responder sees basic incident data but is unable to view specific details of the incident.**

    What could be wrong with the configuration in the incident responder's role?

    A. View option is selected, and all display attributes are deselected.
    B. Incident Access tab conditions are specified.
    C. Available Smart Response rules are deselected.
    D. Server administration rights are deselected.

13. **Which detection method should a DLP Administrator utilize to block files containing credit card numbers from being transferred from an endpoint computer to an external USB drive?**

    A. Keywords
    B. Exact Data Matching
    C. Vector Machine Learning
    D. Data Identifier

14. A Network Monitor server has been installed. The server is receiving traffic but Enforce is NOT showing incidents. Running Wireshark indicates that the desired traffic is reaching the detection server.

What is the most likely cause for this behavior?

A. The mirrored port is sending corrupted packets.
B. The wrong interface is selected in the configuration.
C. The configuration is set to process GET requests.
D. The communication with Enforce is interrupted.

15. Which two (2) pieces of system information are collected by Symantec Data Loss Prevention Supportability Telemetry? (Select two.)

A. Currently installed version of the Enforce Server
B. Number of policies currently deployed
C. Cumulative statistics regarding network traffic
D. File types for which there are incidents
E. Number of system alerts generated daily

16. Under which circumstances does CloudSOC refer a file for DLP Scanning?

A. When it matches parameters configured in Application Detection Configuration
B. When it matches parameters configured in the Enforce policy
C. When it matches parameters configured in Cloud Detection Service
D. When it matches parameters configured in CloudSOC

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
11. B, E
12. A
13. D
14. D
15. A, D
16. A