Administration of Symantec™ Data Loss Prevention 12
Sample Exam

Contents

Sample Questions

1. What are two reasons why a company should implement data loss prevention? (Select two.)

   a. prevent the threat of malware
   b. demonstrate regulatory compliance
   c. protect the CISO from liability due to a security breach
   d. prevent employee malicious activity
   e. protect brand and reputation

2. Which product must run on a physical server?

   a. Endpoint Prevent
   b. Network Monitor
   c. Enforce
   d. Network Prevent

3. How can a DLP administrator hide the agent from registering itself in the Windows control panel when manually installing the Symantec DLP Agent?

   a. add `ARPSYSTEMCOMPONENT="1"` to the installer file
   b. select the "Hide from Control Panel" checkbox in the installation user interface
   c. add `HIDECONTROLPANEL="YES"` to the installer file
   d. add `ARPSYSTEMCOMPONENT="0"` to the installer file

4. Which two identifiers can a detection server match with a recipient matches pattern rule? (Select two.)

   a. IP address
   b. Windows username
   c. Yahoo IM Name
   d. AOL IM Name
   e. URL Domain

5. Which two remediation actions are available for Network Protect? (Select two.)

   a. Copy
   b. Move
   c. Block
   d. Encrypt
   e. Quarantine

6. What is the purpose of the File Recovery Area Location option?

   a. secure filestore of incidents and data while agents are offline
   b. location of files quarantined through Endpoint Discover scans
   c. temporary backup location of blocked files
   d. location of files marked for retention after deleting incidents

7. Which feature should an incident responder use to investigate where an attachment has created other violations?

   a. Report Filters
   b. Incident History
   c. Incident Details
   d. Policy Matches

8. A role is configured for XML export and a user executes the export XML incident action. The exported incidents are missing prior incident information.

   What must be done to display this information in the XML export?

   a. A remediator must take an action on the incident.
   b. IncidentHistory option on System Overview / Configure page must be enabled.
   c. Incident history must be enabled in the user's role.
   d. The manager.properties must be configured for historical export.

9. A DLP Agent is connected to the corporate network through a VPN. An administrator sees a Warning icon associated with the agent on the Agent Overview page. The administrator determines the warning is related to a failure to update Active Directory group membership.

   What should the administrator do to clear the warning?

   a. disconnect and reconnect the VPN connection
   b. restart the DLP Agent
   c. reboot the Endpoint computer
   d. refresh the Active Directory services

10. An administrator is completing an example document training process, but is having difficulty deciding whether to accept a Vector Machine Learning profile. The administrator needs to perform a detailed review of the quality of each training set at a granular, per-fold level.

    Where can the administrator find the information to perform this review?

    a. machinelearning_training_process.log
    b. machinelearning_native_filereader.log
    c. machinelearning_training.log
    d. machinelearning_training_native_manager.log

11. Which product should the customer use to block outgoing mobile traffic?

    a. Mobile Email Monitor
    b. Network Prevent for Email
    c. Mobile Prevent
    d. Network Discover

12. An enterprise architect is designing a Symantec Data Loss Prevention Solution that needs to leverage a hosted service provider's infrastructure.

    Which two Symantec Data Loss Prevention products can be hosted in the service provider's environment? (Select two.)

    a. Mobile Prevent
    b. Mobile Email Monitor
    c. Network Prevent for Email
    d. Network Prevent for Web
    e. Network Monitor

13. Which database is used to store DLP incidents, users, and Enforce policies?

    a. MySQL
    b. Oracle
    c. IBM DB2
    d. SAP

14. Which two standard checks does the Environment Check Utility (ECU) perform? (Select two.)

    a. amount of traffic sent to the servers daily
    b. status of the DLP services
    c. number of days the DLP system has been operational
    d. database parameters that are required for DLP

e. list of Microsoft patches applied to the Enforce server

15. A Symantec Data Loss prevention customer has two proxy servers connected to a single Mobile Email Monitor. The customer determines that ICAP streams are timing out. What should an administrator increase to resolve this issue?

a. Maximum Number of responses
b. Icap.Buffersize
c. Maximum Number of requests
d. RequestProcessor.RPLTimeout

16. What is the correct traffic flow for the Symantec Data Loss Prevention Mobile Email Monitor?

a. Exchange ActiveSync Server > Web proxy (REQMOD) > Mobile Email Monitor Server > VPN . iOS device
b. Exchange ActiveSync Server > Web proxy (RESPMOD) > Mobile Email Monitor Server > VPN > iOS device
c. Exchange ActiveSync Server > Web proxy (REQMOD) > Mobile Email Monitor Server > iOS device
d. Exchange ActiveSync Server > Web proxy (RESPMOD) > Mobile Email Monitor Server > iOS device

17. Which two actions must a DLP administrator take to implement Endpoint FlexResponse? (Select two.)

a. enable credentials to be saved on the endpoint in general settings
b. enable Endpoint FlexResponse in the Agent Configuration
c. enable Endpoint FlexResponse as a Smart Response rule action
d. use Flrinst.exe to install the Endpoint FlexResponse plug-in
e. use AgentInstall.msi with the correct switch to install Endpoint FlexResponse

18. What is the correct processing flow for data loss prevention policies?

    a. evaluate detection rules > process user exceptions > execute response rules
    b. execute response rules > process user exceptions > evaluate detection rules
    c. evaluate detection rules > execute product specific response rules > execute general response rules
    d. execute general response rules > execute product specific response rules > evaluate detection rules

19. What are two types of metrics collected when participating in Supportability Telemetry? (Select two.)

    a. total count of different Detection server versions
    b. current installed version of Enforce
    c. complete list of protocols monitored
    d. customer contact name and email address
    e. total count of different file types that occurred in incidents

20. What is the minimum recommended number of columns that should be used in an Exact Data Matching (EDM) profile to achieve the greatest accuracy?

    a. 2
    b. 3
    c. 4
    d. 5

Answers

1-b&e, 2-b, 3-a, 4-a&e, 5-a&e, 6-c, 7-a, 8-c, 9-b, 10-c, 11-c, 12-c&d, 13-b, 14-b&d, 15-a, 16-d, 17-a&d, 18-a, 19-b&e, 20-b

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright (c) 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.