IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **ST0-075**

Title : Symantec Data Loss Prevention 9.0 (STS)

Version : DEMO

1. What is a three-tier Symantec Data Loss Prevention 9.0 deployment?
A.two Enforce Servers deployed on the same host as the database
B.three different detection servers deployed on separate hosts
C.Enforce Server and a detection server deployed on the same host as the database
D.Enforce Server, detection servers, and the database deployed on separate hosts
ANSWER: D

2. A policy manager wants to apply policies only to certain employees with a specific classification level. Which TrueMatch detection method can help accomplish this?
A.Directory Group Matching (DGM)
B.Exact Data Matching (EDM)
C.Described Content Matching (DCM)
D.Indexed Document Matching (IDM)
ANSWER: A

3. Which component of Microsoft Outlook Personal Folder (.pst) files does Network Discover apply filters to?
A.individual emails in the .pst file
B.the entire .pst file
C.attachments in the .pst file
D.folders in the .pst file
ANSWER: B

4. Which three are valid Scanned Content filter types for the Discover File System target? (Select three.)
A.Exclude filter
B.File Size filter
C.Read ACL filter
D.File Owner filter
E.File Date filter
ANSWER: ABE

5. Which three statements apply to communication between the Enforce Server and detection servers? (Select three.)
A.By default, the Enforce Server and the detection servers communicate over port 8100.
B.Port 3389 must be open between the Enforce Server and the detection servers.
C.The same port number must be used for all detection servers.
D.The servers can be configured to use any port higher than 1024.
E.IPSec must be configured on the Enforce Server and the detection servers.
ANSWER: ACD
6. What must a system administrator do for Network Monitor filter configuration changes to take effect?
A.recycle VontuManager and VontuMonitorController services on Enforce

B.recycle PacketCapture process on the Network Monitor
C.recycle VontuNotifier service to propagate changes to Network Monitor
D.recycle Network Monitor server from the Server Detail page
ANSWER: D

7. Why do companies deploy data loss prevention solutions? (Select two.)
A.to protect their perimeters from external threats
B.to help protect their brands and reputations
C.to prevent employee access to undesirable websites
D.to encrypt sensitive data to ensure secure transmission
E.to reduce the likelihood of data breaches and related costs
ANSWER: BE

8. What are three benefits that data loss prevention solutions provide that other security technologies or tools do not? (Select three.)
A.give visibility into where sensitive data is stored
B.give insight into capacity planning for sensitive data
C.identify who has access to sensitive data
D.indicate where sensitive data is being sent
E.measure encryption strength for sensitive data
ANSWER: ACD

9. Which three are examples of confidential data? (Select three.)
A.national ID numbers
B.published press releases
C.health information
D.CAD drawings
E.manufacturing plant locations
ANSWER: ACD

10. What does a data loss prevention solution help an organization identify? (Select three.)
A.employee education opportunities
B.risk of virus infection
C.unprotected content on laptops
D.illegally obtained software on desktops
E.encryption enforcement opportunities
ANSWER: ACE

11. Which three describe an effective data loss prevention (DLP) program? (Select three.)
A.DLP is a company-wide initiative.
B.DLP is primarily driven by Information Security.
C.DLP is primarily driven by the Incident Response Team.
D.Employee participation is important.
E.Business stakeholders are held accountable for risk reduction.

ANSWER: ADE

12. Which two products are required for quarantining confidential files residing inappropriately on a public file share? (Select two.)
A.Network Discover
B.Endpoint Discover
C.Network Monitor
D.Network Prevent
E.Network Protect
ANSWER: AE

13. Which product can replace a confidential document residing on a public share with a Marker File explaining why the document was removed?
A.Network Prevent
B.Network Protect
C.Network Monitor
D.Network Discover
ANSWER: B

14. Which product lets an incident responder see who has access to confidential files on a public file share?
A.Network Protect
B.Network Monitor
C.Network Prevent
D.Network Discover
ANSWER: D

15. Where does an incident responder find the exact matches that triggered an incident?
A.Dashboard report
B.Incident Snapshot
C.Incident List
D.System Events report
ANSWER: B

16. Under which high-level node in the left navigation panel can administrators find the System Events report?
A.Reports
B.Policy
C.System Health
D.Administration
ANSWER: D

17. Under which high-level node in the left navigation panel can administrators find the Discover Targets

page?
A.Policy
B.Reports
C.Administration
D.Data at Rest
ANSWER: A

18. Which products run on the same detection server?
A.Network Protect and Network Discover
B.Endpoint Discover and Network Discover
C.Network Monitor and Network Prevent
D.Network Discover and Network Monitor
ANSWER: A

19. What is a function of the Enforce Server?
A.provides a GUI for policy creation
B.detects incidents
C.writes incidents to all detection servers
D.deploys agents to endpoint computers
ANSWER: A

20. Which database does Symantec Data Loss Prevention 9.0 support for incident and policy storage?
A.Oracle 10g version 10.2.0.4
B.any version of Oracle 10g
C.Oracle 10g version 10.2.0.1
D.Microsoft SQL Server
ANSWER: A