Symantec

Exam ST0-237

Symantec Data Loss Prevention 12 Technical Assessment

Version: 8.0

[Total Questions: 362]

Topic 1, Volume A

Question No : 1 - (Topic 1)

You are turning on the quota on a file system for the first time.You want to ensure you are ableto establish quota for a group of users named finance.

What should you do?

A. Create a file named quota and assign it to the finance group.
B. Create a file named quota and place it in the root directory of the file system.
C. Create a file named quota.grp and assign it to the group of users.
D. Create a file named quota.grp that is owned by the root of the file system.

Answer: D

Question No : 2 - (Topic 1)

What is the main difference between data loss prevention and other security technologies?

A. It is designed to take a content aware approach to security.
B. It determines the data owner of inbound sensitive information.
C. It quarantines adware before it is able to extract confidential information.
D. It is designed to give visibility into where the company's least sensitive data is stored.

Answer: C

Question No : 3 - (Topic 1)

You move a set of files from a VxFS file system to another file system. When the files are moved, the extent attributes are not moved along with the files and are lost during the migration.

What could be a possible cause for this problem?

A. The target file system is not a VxFS type file system.
B. There is a variation in the block size of source and target VxFS file system.
C. The target VxFS file system does not have enough free space to accommodate the

extent attributes.
D. The target VxFS file system uses mixed block size.

Answer: A

Question No : 4 - (Topic 1)

What causes the majority of data loss prevention violations?

A. hackers exploit vulnerabilities and exfiltrate confidential data
B. companies lack security policies to prevent loss of confidential data
C. employees unintentionally expose confidential data
D. system backups are performed improperly

Answer: C

Question No : 5 - (Topic 1)

You execute the command ps –ef | grep vxatd.

What is the expected output of this command?

A. The command verifies the Fully Qualified Host Name.
B. The command verifies the status of Symantec Authentication service.
C. The command verifies the status of Root Broker.
D. The command verifies the status of Authentication Broker.

Answer: B

Question No : 6 - (Topic 1)

What is the minimum number of plexes required for true mirroring to provide redundancy of data?

A. One
B. Two
C. Three

D. Four

Answer: B

Question No : 7 - (Topic 1)

Which product can replace a confidential document residing on a share with a marker file explaining why the document was removed?

A. Network Discover
B. Network Protect
C. Mobile Prevent
D. Endpoint Discover

Answer: B

Question No : 8 - (Topic 1)

Which command will you use to determine the operating mode of vxconfigd?

A. vxdctl enable
B. vxdctl mode
C. vxmode
D. ps –ef |grep vxconfig

Answer: B

Question No : 9 - (Topic 1)

Which structures are parts of the Cross-platform Data Sharing (CDS) format?

A. An Operating System-reserved area
B. A directory area
C. A private region
D. A public region
E. A Bad Block Relocation Area

Answer: A,C,D

Question No : 10 - (Topic 1)

Which two components can perform a scan of a workstation? (Select two.)

A. Endpoint Server
B. DLP Agent
C. Network Prevent
D. Enforce Server
E. Discover Server

Answer: B,E

Question No : 11 - (Topic 1)

While accessing a node in the Dynamic Multipathing (DMP) database you get an error "VxVM vxdmp NOTICE V-5-0-111 disabled dmpnode dmpnode_device_number".

How will you resolve this error? (Each correct answer presents part of the solution. Select two.)

A. Enable the appropriate controllers to allow at least one path under this DMP node.
B. Check the underlying hardware to recover the desired path.
C. If possible correct the hardware failures Then, recover the volume using the vxrecover command.
D. Replace the hardware because there may be a problem with host-bus adapter.

Answer: A,B

Question No : 12 - (Topic 1)

How many free partitions do you need to encapsulate a boot disk?

A. 1
B. 2

C. 3
D. 4

Answer: B

Question No : 13 - (Topic 1)

Which user store is essential for using the user risk summary feature?

A. Tomcat
B. Active Directory
C. MySQL
D. Samba

Answer: B

Question No : 14 - (Topic 1)

When you are mounting a file system, which mode sets the policy for handling I/O errors on mounted file system?

A. disable
B. ioerror
C. cio
D. minicache

Answer: B

Question No : 15 - (Topic 1)

In which two 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

Answer: A,B

What is the correct traffic flow for the Symantec Data Loss Prevention for Mobile Prevent?

A. mobile device (iOS) > VPN > Mobile Prevent Server > Web proxy > Enforce Server > final destination
B. mobile device (iOS) > VPN > Web proxy > Mobile Prevent Server > final destination
C. mobile device (iOS) > VPN > Web proxy > Mobile Prevent Server > Enforce Server > final destination
D. mobile device (iOS) > VPN > Mobile Prevent Server > Web proxy > final destination

Answer: B

Which detection server requires two physical network interface cards?

A. Network Protect
B. Network Discover
C. Endpoint Discover
D. Network Monitor

Answer: B

Which option describes the three-tier installation type for Symantec Data Loss Prevention?

A. Install the database, the Enforce Server, and a detection server all on the same computer.
B. Install the Oracle database and the Enforce Server on the same computer, then install detection servers on separate computers.
C. Install the Oracle Client (SQL*Plus and Database Utilities) on three detection servers.

D. Install the Oracle database, the Enforce Server, and a detection server on separate computers.

Answer: C

Question No : 19 - (Topic 1)

Which interface provides single sign-on access for the purpose of administering Data Loss Prevention servers, managing policies, and remediating incidents?

A. Symantec Information Manager
B. Symantec Protection Center
C. Symantec Data Insight
D. Symantec Messaging Gateway

Answer: B

Question No : 20 - (Topic 1)

Which two operating systems are supported for Symantec Data Loss Prevention 12 servers? (Select two.)

A. Windows 2003 Enterprise Edition 64-bit
B. Red Hat Linux 5 Enterprise 64-bit
C. Windows 2008 Server 32-bit
D. Red Hat Linux 6 Enterprise 64-bit
E. Windows 2008 R2 Enterprise Edition 64-bit

Answer: B,E

Question No : 21 - (Topic 1)

Which is the correct installation sequence?

A. Enforce > Oracle > detection server > Solution pack
B. Oracle > Enforce > Solution pack > detection server
C. Oracle > Enforce > detection server > Solution pack

D. Enforce > Oracle > Solution pack > detection server

Answer: B

Question No : 22 - (Topic 1)

A company needs to secure the content of all Mergers and Acquisitions Agreements. However, the standard text included in all company literature needs to be excluded.

How should the company ensure that this standard text is excluded from detection?

A. create a whitelisted.txt file after creating the Vector Machine Learning (VML) profile
B. create a whitelisted.txt file before creating the Exact Data Matching (EDM) profile
C. create a whitelisted.txt file after creating the Indexed Document Matching (IDM) profile
D. create a whitelisted.txt file before creating the Indexed Document Matching (IDM) profile

Answer: D

Question No : 23 - (Topic 1)

A policy template called Customer Credit Card Numbers is being imported into the system.

What is the default result for this action?

A. the policy template will be listed under US Regulatory Enforcement Templates and be available
B. the policy template will be enabled by default
C. the policy template will be available after logging off and on to Enforce
D. the policy template will be listed under Imported Templates

Answer: D

Question No : 24 - (Topic 1)

You are not able to find a physical device corresponding to the disk ID in the disk media record when one of the subdisks associated with the plex fails. You need to check the plex state to solve the problem. What will be the status of the plex in this situation?

A. UNENABLED
B. NODEVICE
C. DISCONNECTED
D. INACTIVE

Answer: B

Question No : 25 - (Topic 1)

A software company needs to protect its source code including new source code between indexing times.

Which detection method should the company use to meet this requirement?

A. Exact Data Matching (EDM)
B. Described Content Matching (DCM)
C. Indexed Document Matching (IDM)
D. Vector Machine Learning (VML)

Answer: D

Question No : 26 - (Topic 1)

An organization needs to determine whether at least 50% of a sensitive document is being sent outside the organization. Which action should the company take to accomplish this?

A. use a whitelisted.txt document
B. use match on selected fields
C. use match count
D. use minimum document exposure

Answer: D

Question No : 27 - (Topic 1)

A company needs to implement Data Owner Exception so that incidents are avoided when employees send or receive their own personal information.