TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **ST0-116**

Title : Symantec Data Loss Prevention 11 Technical Assessment

Version : Demo

1.How can an administrator validate that once a policy is updated and saved it has been enabled on a specific detection server?
A. check the status of the policy on the policy list page
B. check to see whether the policy was loaded under System > Servers > Alerts
C. check the policy and validate the date and time it was last updated
D. check to see whether the policy was loaded under System > Servers > Events
Answer: D

2.An administrator is running a Discover Scanner target scan and the scanner is unable to communicate back to the Discover Server. Where will the files be stored.?
A. Discover Server incoming folder
B. scanner's outgoing folder
C. scanner's incoming folder
D. Enforce incident persister
Answer: B

3.Which two remediation actions are available for Network Protect? (Select two.)
A. Copy
B. Move
C. Block
D. Rename
E. Quarantine
Answer: A, E

4.A company needs to scan all of its file shares on a weekly basis to make sure sensitive data is being stored correctly. The total volume of data on the file servers is greater than 1 TB . Which approach will allow the company to quickly scan all of this data on a weekly basis?
A. run an initial complete scan of all the file shares, then modify the scan target to add date filters and exclude any files created or modified before the initial scan was run
B. run an initial complete scan of all the file shares, then modify the scan target to an incremental scan type
C. create a separate scan target for each file share and exclude files accessed before the start of each scan
D. run an initial complete scan of all file shares, create a summary report of all incidents created by the scan, then run weekly scans and compare incidents from weekly scans to incidents from the complete scan
Answer: B

5.Which Network Discover option is used to determine whether confidential data exists without having to scan the entire target?
A. Byte Throttling
B. File Throttling
C. Match Thresholds
D. Inventory Mode Scanning

Answer: D

6.A Data Loss Prevention administrator notices that several errors occurred during a Network Discover scan. Which report can the administrator use to determine exactly which errors occurred and when?
A. Discover Incident report sorted by target name and scan
B. Full Activity report for that particular scan
C. Server Event report from Server Overview
D. Full Statistics report for that particular scan
Answer: B

7.What must a policy manager do when working with Exact Data Matching (EDM) indexes?
A. re-index large data sources on a daily or weekly basis
B. index the original data source on the detection server
C. deploy the index only to specific detection servers
D. create a new data profile if data source schema changes
Answer: D

8.Which two policy management actions can result in a reduced number of incidents for a given traffic flow? (Select two.)
A. adding additional component matching to the rule
B. adding data owner exceptions
C. deploying to additional detection servers
D. increasing condition match count
E. adding additional severities
Answer: B, D

9.What is a feature of keyword proximity matching?
A. It will match on whole keywords only.
B. It has a maximum distance between keywords of 99.
C. It only matches on message body.
D. It evaluates each keyword pair independently.
Answer: D

10.The database is full and the Incident Persister is unable to process incidents. Which two file types could be present in Vontu/protect/incidents? (Select two.)
A. .idx
B. .edc
C. .idc
D. .inc
E. .bad
Answer: C, E

11.A role is configured for XML export and a user executes the export XML incident action. What must be done before history information is included in the export?

A. A remediator must take an action on the incident.
B. History must be enabled as a tab or panel in the incident snapshot layout.
C. Incident history must be enabled in the user's role.
D. The manager.properties must be configured for XML export.
Answer: C

12.A user is unable to log in as sysadmin. The Data Loss Prevention system is configured to use Active Directory authentication. The user is a member of two roles, sysadmin and remediator. How should the user log in to the user interface in the sysadmin role?
A. sysadmin\username@domain
B. sysadmin\username
C. domain\username
D. sysadmin\username\domain
Answer: B

13.Which product provides support for the Citrix XenApp virtualization platform?
A. Endpoint Prevent
B. Network Discover
C. Network Protect
D. Network Prevent
Answer: A

14.What are two benefits of the Symantec Data Loss Prevention 11 security architecture? (Select two.)
A. Communication is initiated by the detection servers inside the firewall.
B. SSL communication is used for user access to the Enforce Platform.
C. Endpoint Agent to Endpoint Server communication uses the Triple Data Encryption Standard (Triple DES).
D. Confidential information captured by system components is stored using Advanced Encryption Standards (AES) symmetric keys.
E. All indexed data uploaded into the Enforce Platform is protected with a two-way hash.
Answer: B, D

15.Which two functions of the communications architecture ensure that the system will automatically recover if a network connectivity failure occurs between the detection servers and the Enforce Server? (Select two.)
A. Oracle database backup
B. detection server autonomous monitoring
C. Enforce Server offline alert notification
D. detection server incident queuing
E. detection server alert archiving
Answer: B, D

16.Where should the Network Discover detection server be placed in a corporate network architecture?
A. inside the DMZ

B. on the same virtual LAN as the proxy server
C. inside the corporate network
D. on the same switch as the Oracle database server
Answer: C

17.Which DLP Agent task is unique to the Symantec Management Platform and is unavailable through the Enforce console?
A. Change Endpoint server
B. Restart agent
C. Pull agent logs
D. Set log level
Answer: D

18.After installing several new DLP Agents, the Data Loss Prevention administrator discovers that none of the endpoint agents are appearing on the Agent Overview page. After refreshing the page several times, and determining that the equipment is powered on and connected to the network, the Agent Overview page still fails to display the new agents. What is a possible cause for this issue?
A. The DLP Agents need to be added manually through the Symantec Management Platform.
B. The DLP Agents were installed with the incorrect Endpoint server IP address.
C. The assigned Endpoint server needs to be recycled in order to detect the new DLP Agents.
D. The Endpoint Location is set to "Manually" instead of "Automatically" in the Enforce user interface.
Answer: B

19.To manually troubleshoot DLP Agent issues, the database and log viewer tools must be executed in which location?
A. in the same location as the dcs.ead file location
B. in the same location as the cg.ead file location
C. in the same location as the ks.ead file location
D. in the same location as the is.ead file location
Answer: C

20.A divisional executive requests a report of all incidents generated by a particular region, summarized by department. What must be populated to generate this report?
A. remediation attributes
B. sender correlations
C. status groups
D. custom attributes
Answer: D