Symantec

Exam 250-511

Administration of Symantec Data Loss Prevention 11

Version: 6.0

[Total Questions: 176]

Topic 1, Volume A

Question No : 1 - (Topic 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

Question No : 2 - (Topic 1)

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

Question No : 3 - (Topic 1)

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

A. Copy
B. Move
C. Block
D. Rename
E. Quarantine

Answer: A,E

Question No : 4 - (Topic 1)

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

Question No : 5 - (Topic 1)

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

Question No : 6 - (Topic 1)

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

Question No : 7 - (Topic 1)

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

Question No : 8 - (Topic 1)

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

Question No : 9 - (Topic 1)

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

Question No : 10 - (Topic 1)

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

Question No : 11 - (Topic 1)

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

Question No : 12 - (Topic 1)

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

Question No : 13 - (Topic 1)

Which product provides support for the Citrix XenApp virtualization platform?

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

Answer: A

Question No : 14 - (Topic 1)

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

Question No : 15 - (Topic 1)

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

Question No : 16 - (Topic 1)

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

Question No : 17 - (Topic 1)

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

Question No : 18 - (Topic 1)

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

Question No : 19 - (Topic 1)

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

Question No : 20 - (Topic 1)

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

Question No : 21 - (Topic 1)

Which report helps a compliance officer understand how the company is complying with its data security policies over time?

A. Policy Trend report, summarized by policy, then quarter
B. Policy Trend report, summarized by policy, then severity
C. Policy report, filtered on quarter, and summarized by policy
D. Policy report, filtered on date, and summarized by policy

Answer: A

Question No : 22 - (Topic 1)

Which Network incident report indicates where employees are most often sending emails in violation of policies?

A. Location Summary
B. Status by Target
C. Top Recipient Domains
D. Destination Summary

Answer: C

Question No : 23 - (Topic 1)

When reviewing an SMTP incident snapshot, which reporting feature would a Data Loss Prevention administrator use to quickly find recent incidents with the same subject and sender?

A. Incident History
B. Incident Summary report
C. Incident Notes
D. Incident Correlations

Answer: D

Question No : 24 - (Topic 1)

When deploying the Symantec Data Loss Prevention 11 solution on multiple servers, which mix of operating systems is supported?

A. All detection servers need to be on the same supported operating system, but the Enforce Server can be on a different supported operating system.
B. The Enforce Server must be on a supported Linux operating system and the detection servers can be on any supported operating system.
C. Any mix of supported Linux and Windows operating systems is allowed.
D. The Enforce Server must be on a supported Windows operating system and the detection servers can be on any supported operating system.

Answer: C

Question No : 25 - (Topic 1)

How is a policy applied to Network Discover scans?

A. by assigning policy groups to the scan target
B. by choosing the correct policies in the scan target
C. by assigning policies to the Network Discover Server
D. by choosing the correct targets to run the policies

Answer: A

Question No : 26 - (Topic 1)

On which protocols does Symantec Data Loss Prevention 11 use port-based protocol recognition?

A. secure tunnelling protocols
B. user-defined IP protocols
C. user-configured TCP protocols
D. system-defined UDP and TCP protocols

Answer: C

Question No : 27 - (Topic 1)

Which Oracle utility can be run from the Enforce box to test network connectivity between Enforce and the Oracle database?