Veritas

Exam ASC-093

ASC Data Loss Prevention 2010

Version: 6.0

[Total Questions: 70]

Question No : 1

Data Loss Prevention (DLP) can use custom SSL certificates to secure communication between the Endpoint server and Endpoint agents. What is the name of the tool that is used to create these certificates?

A. endpointssl.exe
B. endpointkeytool.exe
C. sslkeytool.exe
D. endpointsslkey.exe

Answer: B

Question No : 2

Symantec Data Loss Prevention can be configured to populate custom attributes pulled from a Lightweight Directory Access Protocol (LDAP) server. In addition to LiveLdapLookup.properties, which other file must be modified to configure custom attributes?

A. Plugins.properties
B. Manager.properties
C. Jdbc.properties
D. Aggregator.properties

Answer: A

Question No : 3

What is a best practice to be used for monitoring mail traffic in an environment that uses Transport Layer Security (TLS) for their outbound email?

A. deploy Network Prevent for Email
B. turn TLS off on the outbound email server
C. import the TLS certificate from the outbound email server onto the Network Monitor detection server
D. Data Loss Prevention is not capable of viewing TLS traffic.

Answer: A

Question No : 4

If an Enforce server is configured to use Active Directory (AD) authentication for logins, which statement is true?

A. Any user that has an account in AD can log in to Enforce as long as they have been assigned a role.
B. Any user that has an account in AD can log in to Enforce as long as they have been added to the krb5.ini or krb5.conf file.
C. Any user that has an account in AD can log in to Enforce as long as their Organizational Unit has been assigned to a Policy Group.
D. Any user that has an account in AD can log in to Enforce as long as they have a matching user name in Enforce.

Answer: D

Question No : 5

A user has determined that many incidents are showing 100 matches per incident from the default PCI policy template. The user needs to increase this limit to better reflect the most critical files with the most violations. Which change will increase the number of maximum matches per incident?

A. change the value for DI.MaxViolations
B. change the value for IncidentDetection.patternConditionMaxViolations
C. change the value for EDM.MaximumNumberOfMatchesToReturn
D. change the value for Incident Threshold within the relevant policy

Answer: A

Question No : 6

When implementing an automated response rule, what must be done to make the rule execute?

A. select Incident-All and click the Response Rule button to execute

B. enable response rules from the Settings page
C. add the response rule to the appropriate policy
D. Automated response rules are effective as soon as they are created

Answer: C

Question No : 7

Data Loss Prevention (DLP) Network Prevent supports load balancing among multiple Prevent servers in high volume networks. In the absence of a network load balancing device, what is the best practice for enabling load balance among multiple Prevent servers?

A. enable Load Balancing in the Settings, Servers Overview page
B. In the case of Network Prevent for Email, the upstream MTA is configured with the IP address of each Prevent server. This is done in a similar fashion for the web proxy server(s) with the IP address of each Network Prevent for web server.
C. A third Network Interface Card (NIC) is required for each Prevent server to be used as a "heartbeat monitor" to the other Prevent servers. Once installed and configured, the Prevent servers act as a virtual cluster.
D. configure a DNS alias to point to the IP address of each Prevent server, also known as a DNS Round Robin

Answer: D

Question No : 8

What needs to be done with unused Network Interface Cards (NIC) on the Enforce server?

A. They need to be configured to utilize Dynamic Host Configuration Protocol (DHCP).
B. They need to be disabled.
C. They need to be configured with a static IP address.
D. They need to be assigned with 127.0.0.1 as their IP address.

Answer: B

Question No : 9

Endpoint agents CANNOT monitor data copies to what?

A. CD/DVD
B. network shares
C. USB (for example, thumb drives)
D. printers/faxes

Answer: B

Question No : 10

What is the best method for deploying a policy to Endpoint agents that makes use of Index Matching.

A. create the policy using Described Content, then "and" the Index Matching statement into the policy
B. Policies that use Index Matching cannot be deployed to Endpoint agents.
C. create the policy using the Index Matching statement, then "and" a Described Content statement into the policy
D. combine all Index Matching statements that are to be deployed to Endpoint agents into one single policy

Answer: A

Question No : 11

An administrator is deploying a Data Loss Prevention Network Monitor detection server to monitor network traffic on a very high performance network (>100 Mbps). Which technique allows them to best capture traffic without dropping packets?

A. implement a Windows 2003 Enterprise Server, and uninstall all unnecessary applications to improve system performance
B. implement a Network Monitor detection server that has more than two Network Interface Cards (NIC), use one NIC for communication between
the Network Monitor and Enforce, then use all of the remaining NICs on multiple SPAN ports
C. install a host-based firewall on the Network Monitor detection server to filter out any unwanted traffic
D. have the SPAN port configured to only forward protocols that the administrator wishes to