Veritas

Exam ASC-090

ASC IT Compliance 2010

Version: 6.0

[Total Questions: 69]

Question No : 1

A Symantec Security Information Manager (SSIM) administrator has written a simple Perl script to convert HEX format to a dotted decimal number to aid forensic analysis of attack packets recorded by the Network Intrusion Detection system. They have used this script in a user action. However, the user action is failing. What is the problem?

A. Only shell scripts are supported for custom user actions.
B. Perl interpreter is not installed on the Archive Server.
C. Only Java scripts are supported for custom user action.
D. Perl interpreter is not installed on the SSIM client machine.

Answer: D

Question No : 2

A company is receiving "disk full" errors on the volume hosting the RMS Information server database. They are running native RMS queries and saving the historical reports. What is the process for deleting outdated RMS historical data sets?

A. from the Control Compliance Suite Console, under the System > General > Data Purge menu, configure the Purge Settings to run a data purge job
B. from the RMS console, run an RMS Query using the "Show Advanced Data Sources" option, and use Active Admin to delete historical data
C. on the Information server, stop the BVProcessManager Service, then stop and restart the SQL Server Service, then restart the BVProcessManager Service
D. on the Information server, stop all RMS Services, and then use the Microsoft command-line tool "OSQL.EXE" to purge the "QUERY_RESULTS" table

Answer: B

Question No : 3

In Control Compliance Suite (CCS) Reporting and Analytics, where do administrators add content for new regulations not already included?

A. from the CCS Console, in "Manage > Polices" select "New Regulation"
B. in Content Studio, choose "Mandates", right-click, and then choose "New Regulation"
C. New regulations cannot be added to Reporting and Analytics.

D. from a SQL script, write an INSERT statement to create the new content on the SQL Database Server

Answer: B

Question No : 4

An administrator sees the following in the agent log:

ERROR [Logging] com.symantec.management.security.

HostnameVerificationFailureException SESA Agent Symc_ConfigProvider: Failed to bootstrap to primary management server https:

What are two reasons for this? (Select two.)

A. The name resolution is not working.
B. Agent failed to download the SSL certificate.
C. There is a hostname mismatch with the SSL certificate.
D. Another host with same hostname is already registered.
E. Bootstrapping is disabled on the Information Manager.

Answer: A,E

Question No : 5

A company reports that Windows Data Collection jobs using the RMS data collector never complete. UNIX Data Collection jobs complete normally. The administrator suspects that one of the Slave Query Engines might be failing to respond. Which troubleshooting step should be used to determine which Slave Query Engine might be hanging?

A. from the RMS Console, log in under the Data Processor Service Account, and check the "Task Status" screen
B. on the Information server, review the Application log
C. in bv-Config, check the "Query Engine Diagnostics- Master" for Slave Query Engine job statuses
D. in the Control Compliance Suite Console, on the Settings > System Topology Menu, Choose "Monitor System Jobs"

Answer: C

Question No : 6

In the Control Compliance Suite Asset System, "Asset Custodian" is an example of an asset _____?

A. tag
B. permission
C. property
D. view

Answer: C

Question No : 7

A policy has been submitted for review. Reviewers have made change requests to the policy, and the policy review deadline has passed. What is the status of the policy?

A. In Review
B. Pending Approval
C. Draft
D. Approved

Answer: C

Question No : 8

What is the objective of the Control Compliance Suite Implementation customer planning call?

A. to review customer information and history
B. to discuss engagement needs
C. to identify the project team members
D. to review essential tasks

Answer: C

Question No : 9

Which of the following is an example of a customer challenge that the SSIM addresses?

A. There is an increasing need to generate complex reports about incidents, threats and the security posture
B. Organizations only use one vendor for security products
C. Organizations have only one security policy to report against
D. There is an increasing number of vendor patches to monitor for vulnerabilities and apply

Answer: A

Question No : 10

When deploying Symantec Security Information Manager (SSIM) collectors for a product, what are two reasons that could necessitate using an additional off-box SSIM agent server independent of the SSIM server or point product server? (Select two.)

A. The endpoint product uses syslog over 514/UDP to export its logs.
B. The endpoint product saves its log files locally.
C. The collector is not designed for operation on the SSIM collector server.
D. The endpoint product runs on a proprietary or unsupported operating system.
E. The collector is designed to install directly onto the point product server.

Answer: C,D

Question No : 11

When planning a new data collection job on a system already working in production, which factor would influence the data collection job?

A. The client requires change control on all production systems.
B. The client operates multiple child Windows domains in the same forest.
C. The client only allows data collection to occur during defined maintenance windows.
D. The client operates a centrally-managed global infrastructure over high-speed WAN links.

Answer: C

Question No : 12