Exam Code: 000-937

Exam Name: IBM Tivoli Compliance Insight Manager V8.5 Implementation

Vendor: IBM

Version: DEMO

Part: A

1: On a Microsoft Windows platform, which three types of activity can be audited? (Choose three.)
A.Runas Actions
B.Object Access
C.Network Activity
D.System Registry
E.Privileged User Activity
F.Hardware Configuration
Correct Answers: B D E

2: What question would a customer answer to determine basic generation of reporting needs?
A.How many copies will you be printing?
B.How often will your users access the reports?
C.What size would you need your reports to be?
D.When do you need to run your reports and who will receive them?
Correct Answers: D

3: What are two valid steps in the process of implementing a report? (Choose two.)
A.Verify connectivity with the event sources.
B.Make one change at a time in each report.
C.Create and define a proper group used in a report.
D.Verify that privileges are set for the user receiving the report.
E.Identify the schedule of the managers who will be receiving them.
Correct Answers: B C

4: Which elements match the W7 model What?
A.Logon, Logoff, Write, Read
B.Opening hours, closing hours, holidays
C.Platform XYZ, Workstation X, Workstation Z
D.Workstation ABC, File X, C:/filepath/file, Printer Z
Correct Answers: A

5: When should the report distribution be scheduled?
A.After the GEM database has successfully loaded
B.As soon as the audit trails have been successfully collected
C.With data processing configured at load-time, after the bulk load phase has completed successfully
D.With data processing configured at collect-time, after the mapping process has completed successfully
Correct Answers: A

6: What is required to install the management console on a machine other than a standard or

enterprise server?
A.Java SDK
B..NET Framework
C.Point of presence
D.Internet Explorer 6.0 or higher
Correct Answers: C

7: Which process normalizes and stores the data in the GEM database?
A.load
B.mapping
C.aggregation
D.consolidation
Correct Answers: A

8: Which port must be available for communication between IBM Tivoli Directory Server (ITDS) and the standard server?
A.139
B.389
C.5992
D.50001
Correct Answers: B

9: What is the advantage of collect-time data processing for a GEM database?
A.Chunks are mapped as soon as they are collected.
B.Chunks are mapped and loaded as soon as they are collected.
C.Reports are readily available in iView as soon as the chunks are collected.
D.Processing of chunks is performed at collection time to prevent loss of information if the standard server is accidentally rebooted.
Correct Answers: A

10: What is mandatory in order to collect Oracle fine-grained audit events?
A.A point of presence on a z/OS system
B.A point of presence on a Solaris server
C.An ODBC connection to the Oracle DB
D.A point of presence on any UNIX platform
Correct Answers: C

11: Which statement is true about attention rules?
A.Attention rules indicate policy exceptions.
B.Attention rules can be defined for any event.
C.Attention rules cannot be defined for allowed events.
D.Attention rules are combinations of W7 elements that indicate allowable events.
Correct Answers: B

12: What are two advantages of using remote syslog collection with optional syslog-ng? (Choose two.)
A.Can receive syslogs over reliable TCP
B.Does not require any ports to be open
C.Can be configured to collect SNMP real-time messages
D.Can be used to consolidate syslogs from multiple real-time devices
E.Can have a point of presence installed to reliably transmit security logs to the standard server
Correct Answers: A D

13: Which component provides the ability to perform depot forensic searches of collected audit data?
A.actuator
B.standard server
C.enterprise server
D.point of presence
Correct Answers: C

14: When configuring SSH collection on an AIX audited machine, to which three groups must the IBM Tivoli Compliance Insight Manager user be assigned in order to be able to collect? (Choose three.)
A.Root
B.Audit
C.Users
D.System
E.Security
F.Administrators
Correct Answers: B D E

15: To calculate the number of grouping user information sources, which question would be appropriate to ask the customer?
A.Is there a need to monitor any mobile users?
B.Are the Windows 2003 servers behind a firewall?
C.How many PCs are running Windows XP Professional?
D.What is the number of domains in the Active Directory forest?
Correct Answers: D

16: According to the IBM Tivoli Compliance Insight Manager installation guide, what is the global formula used to calculate the repository size?
A.1.5 * (total GB of daily logs/10 compression factor) * number of days to keep in repository + 25 GB for program files, temp files, databases
B.2.5 * (total GB of daily logs/10 compression factor) * number of days to keep in repository + 15 GB for program files, temp files, databases
C.total GB of daily logs * number of standard servers * number of days to keep in repository + 25 GB for program files, temp files, databases

D.total GB of daily logs * number of standard servers * number of days to keep in repository + 15 GB for program files, temp files, databases

Correct Answers: A

17: Which components require DB2 database communication over default port 50001?

A.the enterprise server and standard server

B.the standard server and the Syslog collector

C.the standard server and the point of presence

D.the Syslog collector and the point of presence

Correct Answers: A

18: What is the purpose of Policy rules?

A.To define all security violations

B.To define all allowable audited activity

C.To define all disallowed audited activity

D.To define high-severity security violations

Correct Answers: B

19: Which tool can be used to install an actuator on the AIX platform?

A.SMIT

B.pkgmgr

C.swinstall

D.admintool

Correct Answers: A

20: When performing a remote installation of an actuator, what does the error Not Resolved signify?

A.Port 5992 is in use on the remote system.

B.The remote system is not reachable using NetBIOS.

C.The SSH server on the remote system is not properly configured.

D.The administrator account specified does not have the appropriate rights to access the remote system.

Correct Answers: B