

IBM 000-937

**000-937 IBM Tivoli Compliance Insight Manager V8.5
Implementation
Practice Test
Version 1.1**

QUESTION NO: 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

Answer: B,D,E

QUESTION NO: 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?

Answer: D

QUESTION NO: 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.

Answer: B,C

QUESTION NO: 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

Answer: A

QUESTION NO: 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

Answer: A

QUESTION NO: 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

Answer: C

QUESTION NO: 7

Which process normalizes and stores the data in the GEM database?

- A. Load
- B. Mapping
- C. Aggregation
- D. Consolidation

Answer: A

QUESTION NO: 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

Answer: B

QUESTION NO: 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.

Answer: A

QUESTION NO: 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

Answer: C

QUESTION NO: 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.

Answer: B

QUESTION NO: 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

Answer: A,D

QUESTION NO: 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

Answer: C

QUESTION NO: 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

Answer: B,D,E

QUESTION NO: 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?

Answer: D

QUESTION NO: 16

According to the IBM Tivoli Compliance Insight Manager installation guide, what is the global formula used to calculate the repository size?

- A. $1.5 * (\text{total GB of daily logs} / 10 \text{ compression factor}) * \text{number of days to keep in repository} + 25$ GB for program files, temp files, databases
- B. $2.5 * (\text{total GB of daily logs} / 10 \text{ compression factor}) * \text{number of days to keep in repository} + 15$ GB for program files, temp files, databases
- C. $\text{total GB of daily logs} * \text{number of standard servers} * \text{number of days to keep in repository} + 2$ GB for program files, temp files, databases
- D. $\text{total GB of daily logs} * \text{number of standard servers} * \text{number of days to keep in repository} + 15$ GB for program files, temp files, databases

Answer: A

QUESTION NO: 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

Answer: A

QUESTION NO: 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

Answer: B

QUESTION NO: 19

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

- A. SMIT
- B. pkgmgr
- C. swinstall
- D. admintool

Answer: A

QUESTION NO: 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.

Answer: B

QUESTION NO: 21

Which actuator has a component called "WatchDog Timer" or "CEAWatchdog" that restarts the actuator process when it is terminated?

- A. AIX
- B. HP-UX
- C. Solaris
- D. Windows NT/2000/XP/2003

Answer: C

QUESTION NO: 22

Which command-line parameter is used to add a standard server to a cluster?

- A. setsrv
- B. addsrv
- C. cluseradd
- D. newmember

Answer: A

QUESTION NO: 23

What is the default database connection port for IBM Tivoli Directory Server when upgrading to IBM Tivoli Compliance Insight Manager V8.5?

- A. 139
- B. 389
- C. 5992
- D. 50000

Answer: D

QUESTION NO: 24

Which two statements about Compliance Management Modules are true? (Choose two.)

- A. Compliance Management Modules are enterprise servers without Consolidation servers.
- B. Compliance Management Modules provide optional sets of capabilities that can be installed if required.
- C. Compliance Management Modules allow a customer to monitor and maintain compliance with selected standards.
- D. Compliance Management Modules manage and configure the IBM Tivoli Compliance Insight Managersystem configuration.
- E. Compliance Management Modules are systems on which an IBM Tivoli Compliance Insight Manager actuator is installed to collect the audit data.

Answer: B,C

QUESTION NO: 25

Which of the following actions occurs with a UNIX hotfix installation?

- A. File modifications are rolled back when the hotfix installation fails.
- B. The hotfix script aborts when a higher hotfix has already been installed.
- C. The hotfix number in the register.ini is registered in the point of presence installation folder.
- D. The register.ini updates on the IBM Tivoli Compliance Insight Manager server after the hotfix installation completes successfully.

Answer: A

QUESTION NO: 26

What is the correct default installation path for the DB2 software that is used for centralized user management?

- A. C:\Program files\IBM\ldap\V6.1
- B. C:\Program Files\IBM\tcimum85
- C. C:\Program Files\IBM\tdsdb2V91
- D. C:\Program Files\IBM\tcim85\security

Answer: C

QUESTION NO: 27

Which account is used to invoke the remote installation of a Windows point of presence?

- A. Windows SYSTEM account
- B. IBM Tivoli Compliance Insight Manageradministrator (default is cifowner)
- C. A user-defined account with administrative authority on the target machine
- D. IBM Tivoli Compliance Insight Manager Server service runs as account (default is DOMAIN\cifadmin)

Answer: C

QUESTION NO: 28

Which service would be running after a successful installation of standard server?

- A. DB2CSService
- B. IBM Tivoli Compliance Insight ManageriView