Exam Code: 000-896

Exam Name: IBM Tivoli Compliance Insight Manager V8.0 Implementation

Vendor: IBM

Version: DEMO

Part: A

1: After IBM Tivoli Compliance Insight Manager is configured on an AIX platform, what is the default location for the audit trail files?
A./var/audit
B./var/log/audit
C./var/log/eprise
D./var/audit/eprise
Correct Answers: C

2: What is the purpose of scoping?
A.to regulate access to GEM databases
B.to regulate access to policies in the policy explorer
C.to regulate access to information generated in reports
D.to regulate access to the Tivoli Compliance Insight Manager Web portal
Correct Answers: C

3: 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 when the IBM Tivoli Compliance Insight Manager server is accidentally rebooted.
Correct Answers: A

4: Which components are installed by default for a Standard server?
A.Tivoli Compliance Insight Manager server, Tivoli Compliance Insight Manager Management Console, and Tivoli Compliance Insight Manager Consolidation
B.Tivoli Compliance Insight Manager server, Tivoli Compliance Insight Manager Web Applications, and Tivoli Compliance Insight Manager Management Console
C.Tivoli Compliance Insight Manager server, Tivoli Compliance Insight Manager Web Applications, Tivoli Compliance Insight Manager Management Console, and Tivoli Compliance Insight Manager Actuator
D.Tivoli Compliance Insight Manager server, Tivoli Compliance Insight Manager Web Applications, Tivoli Compliance Insight Manager Management Console, and Tivoli Compliance Insight Manager Consolidation
Correct Answers: B

5: From which two Tivoli products can IBM Tivoli Compliance Insight Manager v8.0 retrieve information using User Information Source? (Choose two.)
A.Tivoli Identity Manager
B.Tivoli Access Manager
C.Tivoli Directory Integrator
D.Tivoli Security Operations Manager

E.Tivoli Access Manager for Enterprise Single Sign-On
Correct Answers: A B

6: A customer wants to use several groups from an Active Directory User Information Source to define the policy. How can this goal be accomplished?
A.Drag Active Directory Groups from the View Automatic Policy.
B.Collect the grouping information from the Active Directory using W7 Log and use them in the policy.
C.Copy and paste the name of the Groups from the Domain Controller Users and Group Management view.
D.Import the Active Directory group names into the Grouping Wizard by using an LDAP data interchange format (LDIF) file.
Correct Answers: A

7: Which IBM Tivoli Compliance Insight Manager component provides the capability to report against the ISO 17799 standard?
A.Audit policy
B.Log Manager
C.Compliance module
D.Management Console
Correct Answers: C

8: What is the procedure to verify that the diagnostics file has been successfully generated?
A.Run the Diagnostics under the Administrator account.
B.The only method is to check whether the Diagnostics Application ended without reporting any message.
C.Check whether a fresh copy of Diagnostics file with the correct file extension has been created in the destination folder.
D.Check whether the Diagnostics Application has provided a dialog message reporting that the diagnostics file was successfully generated.
Correct Answers: C

9: What does the error retention property in the z/OS event source define?
A.sets of error files maintained in each *.err directory
B.sets of error files maintained in each *.etc directory
C.sets of log files maintained in each *.props directory
D.sets of log files maintained in each *.property directory
Correct Answers: C

10: What are two advantages of using Secure Shell (SSH) remote collection? (Choose two.)
A.Can have an SSH Collection user as a non-root account
B.Can be used to collect logs remotely from any event source
C.Uses secure user name-password authentication during collection
D.Reduces maintenance costs in terms of agent installation and upgrade

E.Requires less number of ports to be opened on the firewall when compared to IBM Tivoli Compliance Insight Manager-point of presence communication port requirements
Correct Answers: A D

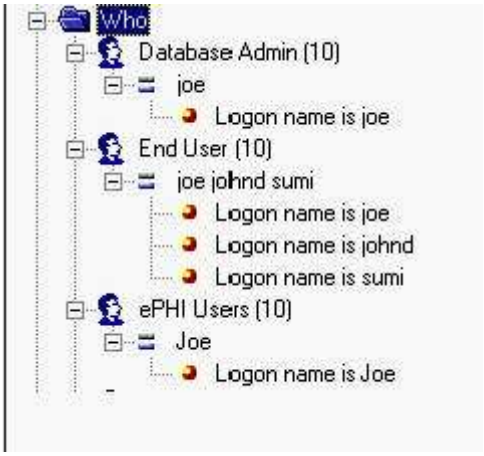
11: What action could be performed to determine if the point of presence is listening?
A.From the Management Console, click Test IP and Port.
B.From the Management Console, double-click machine plus Network.
C.From a command window, execute the tracer machine 5992 command.
D.From a command window, execute the ping command to the point of presence.
Correct Answers: A

12: When are the alert events processed and delivered?
A.when a Windows scheduled task is run
B.when the Event source log files are collected
C.when the mainmapper process maps collected events during a manual load
D.when the mainmapper maps the collected events for a scheduled GEM database
Correct Answers: D

13: Which statement about the universal event source (w7Log) is true?
A.Uses the getnewrecs script to collect the audit trail.
B.Keeps track of the last record read in the audit trail.
C.A regular expression is used to specify the path to the log file.
D.Provides the ability to collect, load, and map a custom audit trail.
Correct Answers: D

14: On which systems can an IBM Tivoli Compliance Insight Manager Compliance Module be installed?
A.on a system where an IBM Tivoli Compliance Insight Manager Management Console is installed
B.on a system where an IBM Tivoli Compliance Insight Manager point of presence has been installed
C.on any HTTP server where the IBM Tivoli Compliance Insight Manager Runtime environment has been installed
D.on any system where IBM Tivoli Compliance Insight Manager Web Applications components have been installed
Correct Answers: D

15: Click the Exhibit button.
An event initiated by a user with the logon name joe will be categorized under which Who group or groups?



A.Database Admin
B.End User, ePHI Users
C.Database Admin, End User
D.Database Admin, End User, ePHI Users
Correct Answers: A

16: Which account is used to invoke the remote installation of a Windows Point of Presence?
A.Windows SYSTEM account
B.IBM Tivoli Compliance Insight Manager administrator (default is cearoot)
C.A user defined account with administrative authority on the target machine
D.IBM Tivoli Compliance Insight Manager Server service runas account (default is DOMAIN\cearoot)
Correct Answers: C

17: Which configuration file contains entries for the Standard servers that are registered with an Enterprise server?
A.beat.ini
B.cluster.ini
C.aggregation.ini
D.consolidation.ini
Correct Answers: A

18: On a Microsoft Windows platform, what is the main weakness in the audit system?
A.User access to files is not logged.
B.Administrator access to files is not logged.
C.File open and closes are logged, but file read and writes are not.
D.File read and writes are logged, but file open and closes are not.
Correct Answers: C

19: Which two options are valid data-processing properties? (Choose two.)
A.scheduled load
B.load time mapping
C.collect size mapping

D.collect time mapping
E.selective sources load
Correct Answers: B D

20: A Cisco PIX Syslog real-time event source has the Source Address property set to the asterisk (*). Which statement is true?
A.The point of presence can receive SNMP messages from Cisco PIX devices.
B.The point of presence can receive real-time messages from any Cisco PIX device.
C.No syslog messages are received because * (asterisk) is not a valid IP address or host name.
D.The point of presence can receive reliable syslog messages from Cisco PIX devices over TCP.
Correct Answers: B