KTest

高品質　より良いサービス



練習問題

https://www.ktest.jp

1年間無料アップデート

Exam : **000-020**

Title : IBM Tivoli Access Manager for Enterprise Single Sign-On V8.0.1 Implementation

Version : DEMO

1. An organization has decided to deploy an IBM Tivoli Access Manager for Enterprise Single-on solution to help address security and productivity issues. Per their corporate security policy, the organization has detailed requirements related to password management for their enterprise applications.
Which password requirements need to be captured?
A. details related to application user ID requirements
B. policy requirements related to the number of applications that a user can access
C. policy requirements for application and user initiated password resets and password complexity
D. do nothing as password policy requirements are best addressed within the application space rather than
in an Enterprise Single Sign-On project
Answer: C

2. Which operator allows specification of a case-sensitive regular expression comparison for attributes in an AccessProfile signature?
A. Tilde (~)
B. Hash (#)
C. Equals (=)
D. Asterisk (*)
Answer: A

3. What are the directory details of Relational Database backup files created by IBM Tivoli Access Manager for Enterprise Single Sign-On V8.0.1 housekeeping?
A. The directory must exist with one subdirectory (general).
B. The directory must exist with two subdirectories (daily, weekly).
C. The directory must exist with three subdirectories (daily, weekly, monthly).
D. The directory must exist with four subdirectories (general, daily, weekly, monthly).
Answer: C

4. System, machine, and user policies can be configured though AccessAdmin. How are changes synchronized with the AccessAgent?
A. written by the Administrators on the INI files
B. propagated only with the Active Directory network service
C. propagated to the clients on the next Administrator access
D. propagated to clients the next time AccessAgent synchronizes with the IMS Server
Answer: D

5. An SSL VPN can be used in conjunction with IBM Tivoli Access Manager for Enterprise Single Sign-On to provide remote access to business critical information. Which statement is true about the Mobile ActiveCode (MAC) when it is used with a VPN Solution for remote access?
A. The MAC can only be delivered to a mobile phone and is good for a single use only.
B. The MAC can be delivered by mobile phone, e-mail, or fax, and it is good for one time authentication only.
C. The MAC can only be delivered to a mobile phone and it is good until the expiration time is reached, as set by an administrator.

D. The MAC can be delivered by mobile phone, email, or fax, and it is good until the expiration time is reached, as set by an administrator.
Answer: B

6. An application is upgraded and it has been determined that the AccessAgent no longer properly responds to the application. It is understood that for a certain amount of time both the current version and the upgraded version of the application will be used by the end-users. The executables for both versions are the same. What should be the next step?
A. Open AccessStudio and change the existing AccessProfile to use only the new signatures for Windows, control IDs, or HTML elements.
B. Open AccessStudio and create a new AccessProfile for the upgraded version and overwrite the existing AccessProfile on the IMS Server.
C. Open AccessStudio and edit the existing AccessProfile by using new triggers/actions associated with the new signatures for Windows, control IDs, or HTML elements.
D. Open AccessStudio and create a new AccessProfile for the upgraded version and upload it to the IMS Server so that two separate AccessProfiles may be used by the AccessAgent.
Answer: C

7. Which type of IBM Tivoli Access Manager for Enterprise Single Sign-On built-in application connector should be used to integrate with Novell eDirectory as a backend enterprise directory?
A. Windows NT Connector
B. Generic (LDAP) Connector
C. Network Information Service Connector
D. Active Directory Service Interfaces Connector
Answer: B

8. What are two valid reasons for using IBM Tivoli Access Manager for Enterprise Single Sign-On Graphical Identification and Authentication (GINA)? (Choose two.)
A. The customer needs to implement a shared desktop or private desktop environment.
B. The customer's Active Directory passwords are synchronized with IBM Tivoli Access Manager for Enterprise Single Sign-On.
C. The customer's PCs have a Novell GINA, and IBM Tivoli Access Manager for Enterprise Single Sign-On does not support Novell GINA.
D. The customer wants to use the IBM Tivoli Access Manager for Enterprise Single Sign-On Self-Service Password Reset functionality from a locked machine.
E. If the customer decides to use IBM Tivoli Access Manager for Enterprise Single Sign-On GINA, they will not be able to bypass IBM Tivoli Access Manager for Enterprise Single Sign-On and log in directly to Windows in the event of an IBM Tivoli Access Manager for Enterprise Single Sign-On system failure.
Answer: AD

9. In the customer's environment, a group of five employees work within a room that has three PCs. The PCs have excellent hardware configurations, with considerable RAM and a fast CPU. The employees use these PCs only when they need to access an application, which is for a short duration of time. For the rest of the time, they work with their tools on their desks.

Which IBM Tivoli Access Manager for Enterprise Single Sign-On session management configuration should be used for these three PCs for optimum performance?
A. Citrix workstation
B. personal workstation
C. shared workstation, private desktop
D. shared workstation, shared desktop
Answer: C

10. Machine policy templates can be assigned based on certain attributes of a machine. A customer organizes their machines based on the following requirements:
The machines are all placed in specific Organizational Units in the Active Directory.
The customer has Citrix Servers, and they have a specific naming convention meant only for their Citrix Servers. The customer has DHCP enabled for all the client machines.
The customer has made it clear that they should not need to change anything in the existing infrastructure.
Given these requirements, which single assignment attribute would be chosen for assigning machine policy templates?
A. Hostnames
B. IP Addresses
C. Machine Group Tag
D. Active Directory Groups
Answer: C

11. Which two APIs are published by IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server? (Choose two.)
A. Data Mining API
B. Provisioning API
C. Cryptography API
D. API for Second Factors
E. SOAP API for Mobile ActiveCode
Answer: BE

12. Which two situations necessitate integration of external systems with IBM Tivoli Access Manager for Enterprise Single Sign-On using API published by IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server? (Choose two.)
A. to add second factor based authentication to a Web application
B. to pre-populate user wallets with all their application credentials in one go
C. to enhance out-of-the-box audit logging by creating custom audit log events
D. to create reports from audit log trails collected by IBM Tivoli Access Manager for Enterprise Single Sign-On
E. to configure automatic password change on expiry for an application so that the new password is a random string of specified strength
Answer: AB
13. Which statement is true about the database and database-user used during installation of IMS Server?

A. A preexisting database user may be used but a new database has to be created during installation.
B. A preexisting database may be used but a new database user has to be created during installation.
C. A preexisting database and user may be used or a new database and user are created during installation.
D. A preexisting database and user cannot be used; a new database and user are created during installation.
Answer: C

14. Which statement is true about a DB2 user that is to be used as the database user for IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server?
A. The database user must be created using DB2 Control Center.
B. The database user must be created using the DB2 Command Line Processor.
C. The database user may be created using DB2 Control Center or DB2 Command Line Processor.
D. The database user must be created by IBM Tivoli Access Manager for Enterprise Single Sign-On V8.0.1 IMS Installer.
Answer: C

15. How can it be determined if the IMS Server (below Version 8.0) is configured for "Active Directory (AD) deployment type 1" or "AD deployment type 2"?
A. Check the server.xml on the IMS Server.
B. Check the database table IMSSyncDataType.
C. Check the System policies in the AccessAdmin.
D. Check the IMS Server settings of the IMS Configuration Utility.
Answer: D

16. When upgrading the AccessAgent and IMS Server from V3.6.x or V8.0.0 to V8.0.1, which statement is true about the existing AccessAgent and IMS Server?
A. The AccessAgent DOES need to be uninstalled and the IMS Server software DOES need to be uninstalled.
B. The AccessAgent DOES need to be uninstalled and the IMS Server software DOES NOT need to be uninstalled.
C. The AccessAgent DOES NOT need to be uninstalled and the IMS Server software DOES need to be uninstalled.
D. The AccessAgent DOES NOT need to be uninstalled and the IMS Server software DOES NOT need to be uninstalled.
Answer: D

17. Which important factor is taken into account when determining an estimate for the maximum network bandwidth to be used by a customer?
A. the size of the hard drives for each PC connected to the client's network
B. the average size of the wallet based on the number of profiles and accounts
C. if any users will use IBM Tivoli Access Manager for Enterprise Single Sign-On during non-work hours
D. the number of users that will be connected using the wireless network, as opposed to a wired connection

Answer: B

18. By default what is the interval for synchronization of the wallet with the IMS Server?
A. once a day
B. once a week
C. every minute
D. every 30 minutes
Answer: D

19. The IBM Tivoli Access Manager for Enterprise Single Sign-On IMS is configured to cache user's wallets. The SLA for network reliability between the IMS Server and the desktop machines is 95%. The customer wants to use Graphical Identification and Authentication (GINA) replacement, and has enabled Active Directory (AD) password synchronization. The user has a cached wallet on their private desktop. Which statement is true when the network is unavailable?
A. The user would not be able to log in to the wallet.
B. The user is able to log in with their wallet password, but the wallet is not synchronized with the server.
C. A user must be re-assigned to another policy template in order to change any aspects of the applied policy.
D. The user experiences normal operation, but AccessAgent will be unable to store newly captured passwords.
Answer: B

20. Which Web-based administration tools are available in IBM Tivoli Access Manager for Enterprise Single Sign-On?
A. AccessAdmin, AccessAssistant, and IMS Configuration Utility
B. AccessStudio, AccessAdmin, AccessAssistant, and IMS Configuration Utility
C. AccessManager Console, AccessAdmin, AccessAssistant, and IMS Configuration Utility
D. AccessEnabler,AccessStudio, AccessAdmin, AccessAssistant, and IMS Configuration Utility
Answer: A