IBM 000-934

IBM 000-934 IBM Tivoli Identity Manager V5.0 Implementation

Practice Test

Version 1.1

QUESTION NO: 1

Which option would be included in the lifecycle management design?

A. Reconciliation schedule for all UNIX services
B. Approval requirements for the Active Directory accounts
C. e-mail notification to the service owner when accounts are provisioned
D. e-mail notification requirements when a new IBM Tivoli Identity Manager identity is created with an HR feed

Answer: D

QUESTION NO: 2

Which two attributes are required for an IBM Tivoli Identity Manager custom person entity? (Choose two.)

A. cn
B. sn
C. uid
D. mail
E. eraliases

Answer: A,B

QUESTION NO: 3

Which choice is relevant to creating the IBM Tivoli Identity Manager (ITIM) system architecture document?

A. Whether to perform ITIM database backup weekly or daily
B. Whether to allow the End User View holders to delete accounts or not delete accounts
C. Whether to implement the RBAC (role-based access control) model in ITIM or the DAC (discretionary access control) model in ITIM
D. Whether to install ITIM as an all-in-one installation or to separate the application server, directory server, and database server components

Answer: D

QUESTION NO: 4

A custom adapter can support which basic operations for user accounts on the target system?

A. Add, Delete, Suspend, Restore, Clone
B. Add, Delete, Suspend, Restore, Modify
C. Add, Delete, Suspend, Restore, Modify, Search
D. Add, Delete, Suspend, Restore, Reconcile, Purge

Answer: C

QUESTION NO: 5

When should recertification notification e-mails be sent out?

A. The first week of every month
B. During low production load hours
C. During system maintenance windows
D. During hours when users are reading e-mail

Answer: B

QUESTION NO: 6

Which information is stored in a certificate used to secure the connection between IBM Tivoli Identity Manager Server and its adapters?

A. Certificate expiration date
B. Certificate encryption type
C. Certificate requester name
D. Certificate encryption strength

Answer: A

QUESTION NO: 7

Identification of target platform business processes is essential to which IBM Tivoli Identity Manager configuration task?

A. Adoption policies
B. Account recertification
C. Organization administration
D. Provisioning policy join directives

Answer: B

QUESTION NO: 8

Which test phase should occur first in an IBM Tivoli Identity Manager (ITIM) acceptance plan?

A. System testing
B. Functional testing
C. Performance testing
D. User acceptance testing

Answer: B

QUESTION NO: 9

A new employee has been hired by Company A to fill a new function as a global LDAP administrator. This employee will also be responsible for performing tasks within the payroll system and performing updates in the sales system. Company A is using IBM Tivoli Identity Manager (ITIM) V5.0 to provision new users into the corporate information technology resources shortly after they have been hired. Some resources have restricted access and require specific approvals or other information before a new user account is created. User accounts will be provisioned for all new users appearing in the HR feed that IBM Tivoli Identity Manager V5.0 receives on these target systems:

-Active Directory
-Enterprise LDAP User
-Exchange

These target systems require the user first-line manager approval before the account is provisioned:

-Payroll
-Human Resources

These target systems require the system owner approval before the account is provisioned:

-Purchasing
-Sales

These account types for the Enterprise LDAP require approval from the Information Technology Risk group. The Information Technology Risk group is also required to submit additional

information regarding justification for the account:

-Account types
Administrator
Back Operator
Global Administrator
Superuser
-Justification
Replacement support role
New function # Business requirement
Other: Explain

Approvers are given 24 hours to take action on an approval request (either approve or reject). If no action is taken within 24 hours, the approval request is escalated to the Service Desk for manual intervention. The Service Desk will manually reassign the request to a peer approver (as designated in Company A's quarterly organizational chart), if available, or reject the request. Rejection by any one approver will affect only the account under that approver domain of approval.

What additional information will the Information Technology Risk group be required to provide?

A. Justification
B. Account Type
C. Account Attributes
D. First Line Manager

Answer: A

QUESTION NO: 10

Which two options describe components of the Self-Service User Interface that can be included in the customization design? (Choose two.)

A. Changing the button text
B. Changing the banner colors
C. Creating a custom workflow approval process
D. Changing the default lifecycle management flow
E. Creating new views for IBM Tivoli Identity Managergroups

Answer: A,B

QUESTION NO: 11

Which steps are needed to create the password policy design?

A. Define password policy scope, select password settings, document password policy design
B. Define password policy requirements, analyze password settings, document password policy design
C. Gather current passwordsettings, analyze password policy, define password scope, document password policy design
D. Gather password policy requirements, define password policy scope, define password settings,document password policy design

Answer: D

QUESTION NO: 12

The Business Continuity Review describes the system availability characteristics of the solution design. In a typical high availability (HA) configuration, a load balancer is configured in front of several peer masters for the directory server. Which statement is true regarding load balancing in an IBM Tivoli Identity Manager (ITIM) HA solution design?

A. If a primary master goes down, all traffic to that master is held until the master is available.
B. Load balancing of write traffic is unwise, because it leads to a possibility of an update conflict.
C. If the primary system goes down, the remaining systems do not need to be able to bear the work load.
D. The ITIM dataservices component will assist the load balancer in the redirecting of requests to one of the other replicated ITIM servers.

Answer: B

QUESTION NO: 13

What is the proper ordering of tasks during an IBM Tivoli Identity Manager V5.0 solution project?

A. solution design, installation, configuration, customization, testing, turn over
B. assessment, solution design, installation, customization, configuration, testing, turn over
C. assessment, solution design, installation, configuration, testing, customization, turn over
D. assessment, solution design, installation, configuration, customization, testing, turn over

Answer: D

QUESTION NO: 14

Which three options are valid membership types of a provisioning policy? (Choose three.)

A. All(*)
B. None
C. Others
D. All other users
E. Organizational role
F. All users in the organization

Answer: D,E,F

QUESTION NO: 15

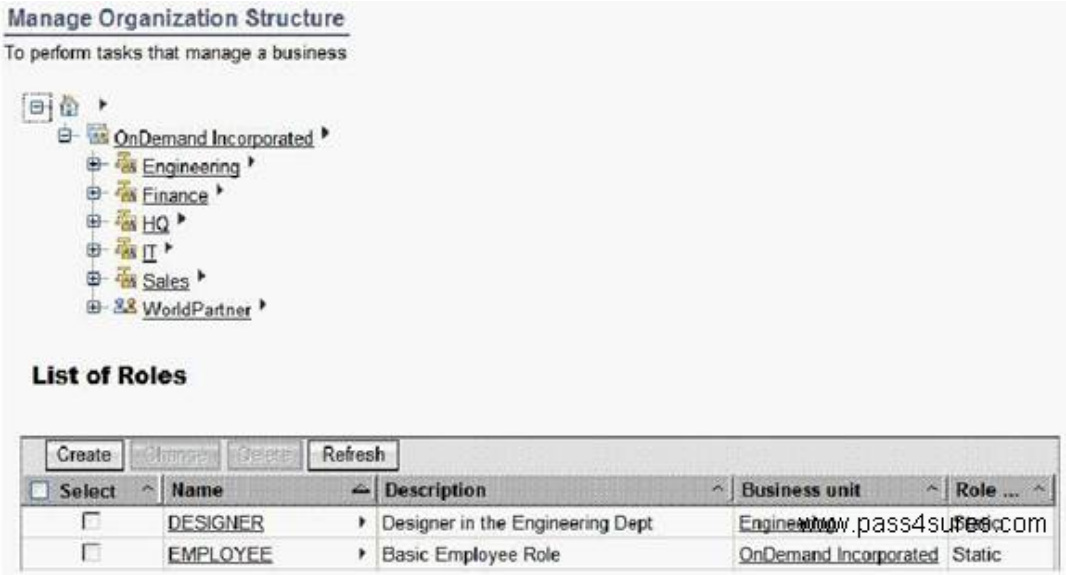
The account and password design document indicates that new accounts and passwords are initially set up by a designated security officer. Therefore, the notification is sent to the security officer and is not sent to each account owner. Which two options can be configured to meet this requirement? (Choose two.)

A. Modify the existing e-mail notification templates to add the custom recipient.
B. Configure a mail node in the operation workflow where the participant is a person with an e-mail account.
C. Design a new e-mail notification template and add to the list of available workflow notification templates.
D. The IBM Tivoli Identity Manager administrator would disable the New Account Notification template and the New Password template in Configuration > Properties > Notification Templates.
E. The IBM Tivoli Identity Manager administrator would disable the New Account Notification template and the New Password template in Configure System > Workflow Notification Properties.

Answer: B,E

QUESTION NO: 16

Click the Exhibit button.



Examine the organization chart and list of roles. Which option is correct for this IBM Tivoli Identity Manager (ITIM) V5.0 configuration?

A. A user in the OnDemandIncorporated business unit can be granted the DESIGNER organizational role.
B. Only users in the Engineering and any subtree business units can be granted the DESIGNER organizational role.
C. A provisioning policy with DESIGNER organizational role as membership can only be created in theEngineering business unit.
D. Users in the OnDemandIncorporated and subtree business units will automatically be granted the EMPLOYEE organizational role.

Answer: A

QUESTION NO: 17

Which two statements are true of groups and ACIs in a plain IBM Tivoli Identity Manager (ITIM) environment populated with some users and some basic services reconciled? (Choose two.)

A. The default HelpDesk Assistant group allows members of that group to manage entitlement workflows.
B. Groups define what tasks ITIM users will see on the administrative console through their group membership.
C. In the shipped product, default groups and default ACIs reflect the typical needs of administrative users in ITIM.
D. Members of the default Auditor group need additional ACIs only to manage their directly defined subordinates in ITIM.
E. Access owners can access the basic services relating to their defined target group Accesses without the need for additional ACIs.

Answer: C,E

QUESTION NO: 18

Which IBM Tivoli Identity Manager (ITIM) installation subdirectory would be inspected to verify that the logging properties were maintained after an upgrade?

A. {ITIM install}/cert
B. {ITIM install}/data
C. {ITIM install}/extensions
D. {ITIM install}/install_logs

Answer: B

QUESTION NO: 19

Which two options are part of the customization design process? (Choose two.)

A. Test the customization.
B. Create a customization prototype.
C. Document the customization code.
D. Determine the customization scope.
E. Determine the feasibility of the customization.

Answer: D,E

QUESTION NO: 20

Which three statements are valid regarding the IBM Tivoli Identity Manager organization tree? (Choose three.)

A. ACIs are attached to nodes in the organization tree.
B. After it is defined, an organization tree cannot be modified.
C. An organization tree can have multiple organizational units.
D. People are attached at a single point in the organization tree.
E. There can be only one organization at the top of the organization tree.
F. Locations, organizational units, and business partner organizations are technically different containers.

Answer: A,B,D

QUESTION NO: 21

Which sequence of actions best describes a secure practice for sensitive data in an IBM Tivoli Identity Manager (ITIM) database?

A. Enable security on the WebSphere Application Server and disallow running the WebSphere Application Server using a non-root account.
B. Store database backups at safe and secure retention locations and guard against leaks or exposure ofsensitive and confidential information.
C. Restrict network traffic to those ports or systems needed by the deployment only. If you write your own application and use a Tivoli Identity Manager API to retrieve sensitive data, encrypt the data before sending itover the network.
D. Restrict operating system access to database files. Limit the privileges of the operating system accounts (administrative, root-privileged, or DBA) to the least privileges needed, change the default passwords, and enforce periodic password changes.

Answer: D

QUESTION NO: 22

What are the primary sources for gathering identity policy requirements?

A. IBM Tivoli Identity Manager System Architecture and IT Security account creation procedures
B. IBM Tivoli Identity Manager Solution Design Document and IT Security account creation procedures
C. IBM Tivoli Identity Manager System Architecture and the access control policies for the customer Web space
D. IBM Tivoli Identity Manager Solution Design Document and the access control policies for the customer Web space

Answer: B

QUESTION NO: 23

Which users can run IBM Tivoli Identity Manager reports?

A. All users
B. Only administrators
C. Only users in the Auditor role
D. Any authenticated user with access granted by a reporting ACl

Answer: D