

IBM

Exam A2150-006

IBM Tivoli Identity Manager V5.1 Implementation

Version: 5.0

[Total Questions: 156]

Question No : 1

Which two join directives can be used when multiple provisioning policies affect the same account? (Choose two.)

- A. Xor
- B. Not
- C. And
- D. None
- E. Union

Answer: C,E

Question No : 2

Which two options should be included in a custom adapter design document? (Choose two.)

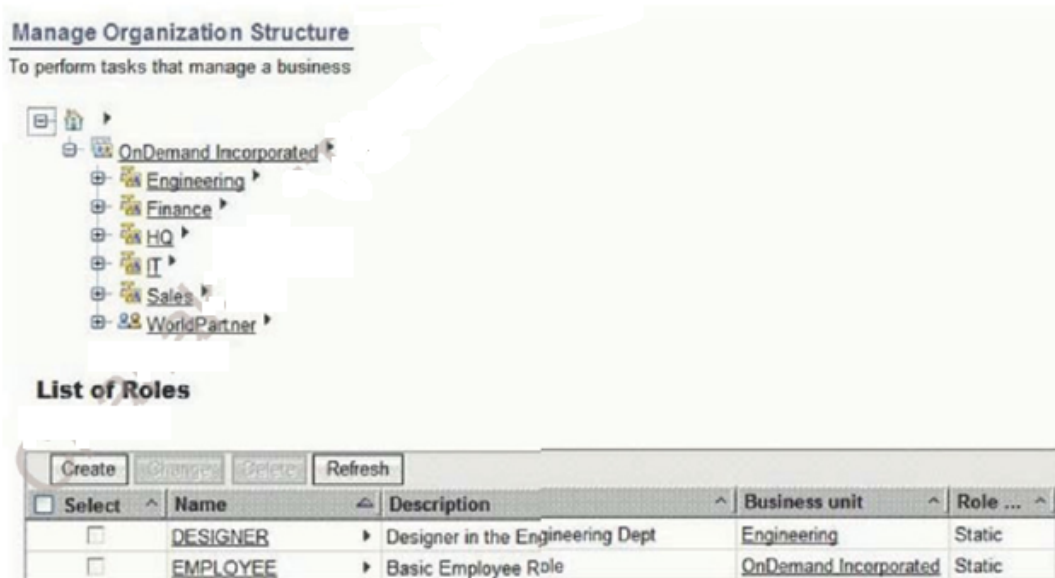
- A. supported platforms, Java version, log file locations
- B. input requirements, installation instructions, prerequisites
- C. process flow diagram, debugging information and log file information
- D. prerequisites, supported platforms, process flow diagrams, source code
- E. security certificate configuration, installation location, input requirements

Answer: B,C

Question No : 3

Click the Exhibit button.

Manage Organization Structure
To perform tasks that manage a business



List of Roles

<input type="checkbox"/> Select	Name	Description	Business unit	Role ...
<input type="checkbox"/>	DESIGNER	Designer in the Engineering Dept	Engineering	Static
<input type="checkbox"/>	EMPLOYEE	Basic Employee Role	OnDemand Incorporated	Static

Based on the organization chart and list of roles, which option is correct for this IBM Tivoli Identity Manager V5.1 configuration?

- A. A user in the On Demand Incorporated business unit can be granted the DESIGNER organizational role.
- B. Only users in the Engineering and any sub tree business units can be granted the DESIGNER organizational role.
- C. A provisioning policy with DESIGNER organizational role as membership can only be created in the Engineering business unit.
- D. Users in the On Demand Incorporated and sub tree business units will automatically be granted the EMPLOYEE organizational role

Answer: A

Question No : 4

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's name
- D. certificate encryption strength

Answer: A

Question No : 5

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 (Tivoli Identity Manager) 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 Tivoli Identity Manager data services component will assist the load balancer in redirecting requests to one of the other replicated Tivoli Identity Manager servers.

Answer: B

Question No : 6

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 password settings, 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 : 7

Which option is relevant to gathering requirements and creating an IBM Tivoli Identity Manager (Tivoli Identity Manager) system architecture document?

- A. formulate list of QUESTION NO:s, identify interviewees, identify timelines for project phases, and delegate responsibility
- B. formulate list of QUESTION NO:s, identify interviewees, identify network topology, and ensure businesscontinuity planning
- C. formulate list of QUESTION NO:s, identify interviewees, discuss organization chart structure, and discuss Tivoli Identity Manager ACI and group security model
- D. discuss firewall rules, discuss certificate installations for HTTPS communication, and discuss Tivoli Identity Manager Web application security and hijack-prevention features

Answer: B

Question No : 8

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

- A. Schedule periodic database backups regularly in order to prevent losing sensitive data.
- B. Enable security on the WebSphere Application Server and disallow running the WebSphere Application Server using a non-root account.
- C. Restrict network traffic to those ports and 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 it over 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 : 9

Given the desired services list and organization structure design, which two options are essential to create a service design? (Choose two.)

- A. Define reporting data.
- B. Validate human resource data.
- C. Define organization requirements.
- D. Gather platform/business processes.
- E. Gather IBM Tivoli Identity Manager access requirements

Answer: C,D

Question No : 10

In which formats can reports from the IBM Tivoli Identity Manager user interface be generated?

- A. PDF, CSV
- B. TXT, XML
- C. PDF, TXT
- D. HTML, PDF

Answer: A

Question No : 11

A simple IBM Tivoli Identity Manager (Tivoli Identity Manager) implementation running on a Windows-based server includes a single AIX platform with two adapters (UNIX and DB2). What are two necessary considerations when creating an upgrade planning document for this scenario?

- A. middleware versions and domain trust relationships
- B. secure FTP constraints and domain trust relationships
- C. middleware versions and operating system release levels
- D. secure FTP constraints and operating system release levels

Answer: C

Question No : 12

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 Manager groups

Answer: A,B

Question No : 13

When performing analysis for designing a global identity policy, which considerations are essential?

- A. UID constraints of each managed service type, and the erglobalid of the person object
- B. which managed service has the least restrictive UID constraints, and the erglobalid of the person objects
- C. UID constraints of eachmanaged service type, and which attributes are available from the person objects
- D. which managed service has the least restrictive UID constraints, and which attributes are available from the person object

Answer: C

Question No : 14

Given the informationIn the sample Organization Chart, which three pairs of roles are valid in a rule of a separation of duty policy? (Choose three.)

- A. Operations and Web Page design
- B. Development and Web page design
- C. Operations and Production Web Team
- D. Web page designand Production Web Team
- E. Engineering and Web Infrastructure Engineering
- F. Development and Web Infrastructure Engineering

Answer: A,D,F

Question No : 15

In preparation for an initial identity or Identity feed to I3M Tivoli Identity Manager (TivoliIdentity Manager) V5.1 ,, which two person attributes are required as a minimum in the feed? (Choose two.)

- A. Last Name (attribute sn)
- B. Common Name (attribute en)
- C. Organizational Unil (attribute ou)
- D. First Name (attribute givenname)
- E. EmployeeNumber (attribute employeeNumber)

Answer: A,B

Question No : 16

A customer has chosen to separate the administration in IBM Tivoli Identity Manager (Tivoli Identity Manager) of some target application services and provisioning parameters using Tivoli Identity Manager groups. Which two options will be required, as a minimum, to implement security in this instance? (Choose two.)

- A. group-based ACIs
- B. service-based ACIs for the application services
- C. account-based ACIs for the application targets
- D. provisioning policy ACIs for the provisioning policies
- E. organizational unit ACIs with services and policies defined at that level

Answer: B,D

Question No : 17

In a CSV identity feed, what is the definition of the name attribute?

- A. the attribute that uniquely identifies the person
- B. the attribute that contains the full name of the person
- C. the attribute that is used by IBM Tivoli Identity Manager to resolve account ownerships during reconciliations
- D. the attribute that contains the fully qualified DN of the person in the IBM Tivoli Identity Manager ou=person container

Answer: A

Question No : 18

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. Design a new e-mail notification template and add to the list of available workflow notification templates.
- C. Configure a mail node in the operation workflow where the participant is a person with an e-mail account.
- 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: C,E

Question No : 19

What is the proper ordering of tasks during an IBM Tivoli Identity Manager V5.1 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 : 20

When can an IBM Tivoli Identity Manager (Tivoli Identity Manager) functional test case be executed on a Tivoli Identity Manager adapter?

- A. after performance tests on the adapter have been completed
- B. after the adapter is installed and the corresponding service has been reconciled
- C. when a remediation procedure exists as part of the risk assessment if the test case fails

D. after test cases on the Tivoli Identity Managerserver configuration have been completed

Answer: D

Question No : 21

A backup design requiring backups of all IBM Tivoli Identity Manager (Tivoli Identity Manager)-related components (WebSphere, LDAP, database) to occur at midnight has been created. All Tivoli Identity Manager processes are quiesced for the duration of the backups. The backups run successfully, and Tivoli Identity Manager is restarted. During the night an identity feed runs, creating 1000 new employees. The identify feed specifies Use Workflow on the service definition and both a Tivoli Identity Manager account and an AD account are automatically provisioned for each person. Both services specify that noncompliance must be corrected. The related provisioning policies use UID from the person object for eruid on both services. An adoption policy exists for AD to search person objects for UIDs matching eruid during reconciliation. The identify feed and all of its provisioning operations are completed by 3 a.m. At 7 a.m., a catastrophic hardware failure occurs against the Tivoli Identity Manager LDAP and a restoration from the previous 12 a.m. backup must be performed.

Which actions must be taken to recover the updates to LDAP that occurred during the identity feed and related provisioning activities?

- A. Rerun the identify feed exactly as it was originally run.
- B. Rerun the identify feed with Use Workflow disabled. Then perform reconciliation against the Tivoli Identity Manager service specifying policy checking.
- C. Rerun the identify feed, disabling Use Workflow. Then perform reconciliation against the AD service specifying that policy checking not be performed during the reconciliation.
- D. Make the AD provisioning policy manual. Rerun the identify feed as it was originally run. Then perform reconciliation against the AD service specifying that policy checking be performed during the reconciliation. Make the AD provisioning policy automatic.

Answer: D

Question No : 22

Which two options would be included in a customization design? (Choose two.)

- A. definitions of e-mail content for all approval e-mails
- B. JavaScript for the Active Directory service identity policy