IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **IdentityIQ Engineer**

Title : SailPoint Certified IdentityIQ Engineer

Version : DEMO

1.For a user who wants to be able to enable an account for a subordinate or themselves through Manage Accounts, does this configuration need to be performed in Lifecycle Manager (LCM)?
Select the Rehire action under Manage Accounts Options in the LCM Configuration.
Solution: Select the Rehire action under Manage Accounts Options in the LCM Configuration.
A. Yes
B. No
Answer: B
Explanation:
In SailPoint IdentityIQ, the specific configuration that allows a user to enable an account for themselves or a subordinate through the "Manage Accounts" option does not necessarily need to be configured in Lifecycle Manager (LCM) alone. While LCM does provide extensive capabilities for account management actions like provisioning, rehire, and more, enabling an account is primarily tied to the permissions and entitlements granted to the user through their role, capabilities, and access profiles.
To address the specific functionality described:
Manage Accounts is typically a part of IdentityIQ's broader account management capabilities, which are not exclusively tied to LCM. The ability to enable or disable accounts can be governed by rules and workflows within IdentityIQ, and these may or may not be linked directly to LCM configurations.
Rehire Action in LCM: The "Rehire" action within LCM Configuration is specific to processes related to reactivating an employee's identity when they are rehired. This does not directly relate to enabling an account from the "Manage Accounts" screen. Rehire workflows typically involve reinstating the user's previous access, which could include enabling accounts, but this is a broader process.
Permissions and Roles: The ability to enable accounts is often governed by the permissions assigned to a user's role within IdentityIQ. These permissions may be granted outside of LCM configurations and handled by IdentityIQ's access governance framework.
Workflow Configurations: Enabling or disabling an account could also be tied to specific workflows, which can be configured separately from LCM, using IdentityIQ's workflow engine. These workflows determine the steps and approvals required to perform such actions.
Reference: SailPoint IdentityIQ Configuration Guide: Account Management SailPoint IdentityIQ Lifecycle Manager Configuration Guide
SailPoint IdentityIQ Administration Guide (Sections on Roles and Permissions, Workflow Configurations)

2.IdentityIQ has been installed and set up with the contents of IdentityExtended.hbm.xml as follows:

```
<property name="extended1" type="string" length="450"
          index="spt_identity_extended1_ci"/>
<property name="extended2" type="string" length="450"
          index="spt_identity_extended2_ci"/>
<property name="extended3" type="string" length="450"
          index="spt_identity_extended3_ci"/>
<property name="extended4" type="string" length="450"
          index="spt_identity_extended4_ci"/>
<property name="extended5" type="string" length="450"
          index="spt_identity_extended5_ci"/>```

<property name="extended6" type="string" length="450"
          index="spt_identity_extended6_ci"/>
<property name="extended7" type="string" length="450"
          index="spt_identity_extended7_ci"/>
<property name="extended8" type="string" length="450"
          index="spt_identity_extended8_ci"/>
<property name="extended9" type="string" length="450"
          index="spt_identity_extended9_ci"/>
<property name="extended10" type="string" length="450"
          index="spt_identity_extended10_ci"/>

<property name="employeeId" type="string" length="450"
          access="sailpoint.persistence.ExtendedPropertyAccessor"
          index="spt_identity_employeeId_ci"/>
<property name="status" type="string" length="450"
          access="sailpoint.persistence.ExtendedPropertyAccessor"
          index="spt_identity_status_ci"/>

<many-to-one name="extendedIdentity1" class="sailpoint.object.Identity"/>
<many-to-one name="extendedIdentity2" class="sailpoint.object.Identity"/>
<many-to-one name="extendedIdentity3" class="sailpoint.object.Identity"/>
<many-to-one name="extendedIdentity4" class="sailpoint.object.Identity"/>
<many-to-one name="extendedIdentity5" class="sailpoint.object.Identity"/>
```

Is this a correct statement about the installation?

Solution: There is a limitation in this installation: When defining the identity mappings using Global Settings > Identity Attributes, only 12 additional searchable attributes can be defined. Additional identity attributes and mappings can be defined, but they cannot be searchable.

A. Yes

B. No

Answer: A

Explanation:

In SailPoint IdentityIQ, the configuration in IdentityExtended.hbm.xml file as shown in the image indeed outlines the use of extended identity attributes. These attributes (extended1, extended2, etc.) are custom attributes that are appended to the standard identity object model to store additional identity-related data.

According to the official SailPoint IdentityIQ documentation, when defining identity mappings under Global Settings > Identity Attributes, only up to 12 additional attributes can be made searchable within the IdentityIQ system. This limitation is crucial because it directly impacts the efficiency of search operations in large environments, where making too many attributes searchable can significantly slow down performance.

Once you define these 12 searchable attributes, any additional attributes can still be added, but they will not be indexed for search operations. This means that while the data in these attributes can be used in workflows, reports, and other operations, they cannot be used in search filters in the IdentityIQ user interface.

This limitation is particularly important when planning the design of the identity schema, as it affects both performance and usability. Therefore, the statement in question is correct and accurately reflects the

constraints imposed by SailPoint IdentityIQ in terms of searchable identity attributes.
Reference: This explanation is derived from the SailPoint IdentityIQ Configuration Guide and official documentation on identity attributes and their limitations. Specifically, this is covered in sections related to extended attributes and searchable properties within the system.

3.Is this statement true about certifications? Solution: The staging period is required.
A. Yes
B. No
Answer: B
Explanation:
The statement that "the staging period is required" for certifications is not true. In SailPoint IdentityIQ, the staging period is an optional phase during the certification campaign configuration. The staging period is used to pre-generate certifications and allow for any preparatory actions or adjustments before the certifications are officially launched and sent to reviewers. However, it is not a mandatory component for all certification campaigns.
Administrators may choose to bypass the staging period entirely depending on the specific requirements of the certification process or the urgency of the certification campaign. Therefore, while the staging period can be beneficial for managing large or complex certifications, it is not a required step.
Reference: SailPoint IdentityIQ Certification Overview Guide
SailPoint IdentityIQ Administration Guide (Sections on Certification Configuration and Staging Period)

4.Is this statement true about certifications? Solution: All certifications include generation, the active period, sign-off, and the end period.
A. Yes
B. No
Answer: A
Explanation:
The statement that "All certifications include generation, the active period, sign-off, and the end period" is true. These stages are fundamental to the certification process in SailPoint IdentityIQ:
Generation: This is the initial stage where the certification campaign is created. During this phase, the system generates the list of items (such as access, roles, or entitlements) that need to be reviewed.
Active Period: Once the certification is generated, it enters the active period. During this time, the designated reviewers are responsible for examining the items in the certification, making decisions (such as approving or revoking access), and providing any necessary comments.
Sign-off: After the active period, the certification moves into the sign-off stage. Here, the final approver(s) review the decisions made during the active period and formally approve or reject the certification outcomes.
End Period: Finally, the end period marks the conclusion of the certification campaign. The certification is closed, and the results are archived. Any necessary actions, such as revoking access or triggering workflows based on the certification decisions, are implemented.
These stages are essential to the structured process that ensures all access rights are properly reviewed and either maintained or adjusted according to the organization's policies.
Reference: SailPoint IdentityIQ Certification Administrator's Guide
SailPoint IdentityIQ Certification Process Documentation

SailPoint IdentityIQ Administration Guide (Sections on Certification Lifecycle and Workflow)

5.Is this a default role type that is available in identityIQ? Solution: Entitlement Role
A. Yes
B. No
Answer: B
Explanation:
In SailPoint IdentityIQ, the concept of a "role" is fundamental to the identity governance framework. The platform supports several default role types that are pre-configured to help organizations manage access effectively. The default role types include:
Business Role: Represents a collection of entitlements necessary for a specific job function within the organization.
IT Role: Aggregates technical entitlements that are typically assigned together, often linked to specific applications or systems.
Application Role: Tied to a specific application, representing roles within that application's context.
Composite Role: A combination of other roles, either business or IT, to form a higher-level role.
The term "Entitlement Role" is not recognized as a default role type in SailPoint IdentityIQ. While entitlements can be components of roles, "Entitlement Role" itself is not a predefined role type in the platform. Therefore, the correct answer is B. No.
Reference: This answer is based on the SailPoint IdentityIQ Role Management Guide, which details the standard role types and their usage within the platform. The guide explicitly lists the supported default role types, and "Entitlement Role" is not among them.