

Increase Chances Of Success With SailPoint IdentityIQ-Associate Exam Dumps



Why do we need so many certifications? One thing has to admit, more and more certifications you own, it may bring you more opportunities to obtain a better job, earn more salary. This is the reason why we need to recognize the importance of getting the test IdentityIQ-Associate certification. Therefore, our IdentityIQ-Associate Study Tool can help users pass the qualifying examinations that they are required to participate in faster and more efficiently as our IdentityIQ-Associate exam questions have a pass rate of more than 98%. Just buy our IdentityIQ-Associate practice guide, then you will pass your IdentityIQ-Associate exam.

SailPoint IdentityIQ-Associate Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> • Applications: Focuses on how applications and connectors are configured in IdentityIQ, including schemas, correlation, aggregation tasks, and resolving uncorrelated accounts.
Topic 2	<ul style="list-style-type: none"> • Access Modeling: Covers how entitlements and roles are defined, cataloged, and assigned to identities within IdentityIQ.
Topic 3	<ul style="list-style-type: none"> • User-Driven Requests: Explains how users submit access requests, what request types are available, and how QuickLink Populations control who can request what for whom.
Topic 4	<ul style="list-style-type: none"> • Identity Modeling: Explains how identity data is structured and managed through IdentityCubes, identity attributes, groups, populations, and manager correlation.
Topic 5	<ul style="list-style-type: none"> • Foundational Concepts: Covers the core purpose of identity security, key IdentityIQ terminology, system components, and how rules, tasks, workflows, and business modeling fit into the platform.
Topic 6	<ul style="list-style-type: none"> • Governance: Addresses how access certifications are conducted and how policy violations are defined and detected across the organization.

>> Demo IdentityIQ-Associate Test <<

Top SailPoint IdentityIQ-Associate Questions | IdentityIQ-Associate Valid Exam Braindumps

If you buy our IdentityIQ-Associate study tool successfully, you will have the right to download our IdentityIQ-Associate exam torrent in several minutes, and then you just need to click on the link and log on to your website's forum, you can start to learn our IdentityIQ-Associate question torrent. We believe the operation is very convenient for you, and you can operate it quickly. At the same time, we believe that the convenient purchase process will help you save much time. More importantly, we provide all people with the trial demo for free before you buy our IdentityIQ-Associate Exam Torrent and it means that you have the chance to download from our web page for free; you do not need to spend any money.

SailPoint Certified IdentityIQ Associate Exam Sample Questions (Q36-Q41):

NEW QUESTION # 36

Is this displayed in the Identity Warehouse?

List of the user's direct reports (for manager identities)

- A. No
- B. Yes

Answer: B

Explanation:

Yes. In SailPoint IdentityIQ, the Identity Warehouse is used to review identity-centric information stored in the IdentityCube. For identities that are managers, IdentityIQ can display the list of identities that report to that manager. This information is derived from the manager relationship established during identity aggregation, correlation, and identity refresh processing.

The direct-report relationship is not an application account attribute by itself once modeled in IdentityIQ; it becomes part of the identity model. IdentityIQ uses manager correlation to associate each identity with its manager, and when those relationships are resolved, the manager identity can show its subordinate identities as direct reports. This is important for governance because managers are frequently used as certifiers, approvers, and reviewers in access review and request workflows.

The display of direct reports depends on the identity data being populated correctly and the viewer having permission to access the identity details. However, as a functional capability of the Identity Warehouse, direct reports for manager identities are part of the identity information that can be displayed.

Reference topics: Identity Modeling, IdentityCube contents, manager correlation, Identity Warehouse, identity refresh, and governance reviewer relationships.

NEW QUESTION # 37

Is this statement true about attributes in IdentityIQ?

Account attributes are updated through an identity refresh task.

- A. No
- B. Yes

Answer: A

Explanation:

The statement is false. In SailPoint IdentityIQ, account attributes are updated through application aggregation, not through the Identity Refresh task. Account attributes belong to account links for a specific application and are defined in that application's account schema. When an aggregation task runs, IdentityIQ connects to the target application using the application definition and connector configuration, reads account data, and updates the account/link attributes stored in IdentityIQ.

The Identity Refresh task performs a different function. It operates on IdentityCubes and recalculates identity-level information using data already present in the IdentityIQ repository. Identity Refresh can update identity attributes, refresh role assignments, evaluate policies, process lifecycle events, update manager relationships, and recalculate governance state. It does not directly re-read account attribute values from connected systems.

This distinction is central to IdentityIQ's data model: account attributes describe accounts on applications, while identity attributes describe the consolidated user identity. Therefore, account attribute updates come from aggregation, while identity attribute updates may occur during Identity Refresh.

Reference topics: Applications - application account schema and aggregation; Identity Modeling - identity attributes versus account attributes; Identity Refresh task options.

NEW QUESTION # 38

The purpose of marking an attribute as managed when defining the application account schema is to designate it as:

An attribute with values that are promoted to the Entitlement Catalog.

- A. No
- B. Yes

Answer: B

Explanation:

Yes. In SailPoint IdentityIQ, marking an application account schema attribute as managed designates that the values discovered for that attribute are treated as managed entitlement values and promoted into the Entitlement Catalog. This is typically used for attributes that represent access, such as groups, roles, permissions, profiles, or other application-specific entitlement assignments. During aggregation, IdentityIQ reads account data from the application. When a schema attribute is marked as managed, the distinct values of that attribute can become ManagedAttribute objects, allowing IdentityIQ to govern them as cataloged access items.

This catalog promotion is important because raw technical values often need business context before they can be reviewed, requested, approved, certified, or reported on. The Entitlement Catalog can store metadata such as display name, description, owner, requestability, classification, and other governance attributes. These values then become usable in access certifications, access requests, reports, policy evaluation, and role modeling.

Therefore, the statement accurately describes the managed attribute function. Reference topics: Applications

- account schema attribute properties; Access Modeling - entitlement catalog; Governance - certification content and entitlement review.

NEW QUESTION # 39

Is this a valid reason to grant an identity an IdentityIQ capability?

To give them elevated permissions on a connected application

- A. No
- B. Yes

Answer: A

Explanation:

No. IdentityIQ capabilities are used to control what a user can do inside SailPoint IdentityIQ, not to grant elevated permissions on a connected target application. A capability defines access to IdentityIQ functions such as administration, reporting, certification management, policy management, role management, access request functions, or other internal product features. Capabilities are part of IdentityIQ's internal authorization model and determine which menus, pages, actions, and administrative operations a logged-in IdentityIQ user may perform.

Elevated permissions on a connected application must be granted through governed access, such as requesting or provisioning an account, entitlement, role, or permission on that target system. That process is handled through access requests, approval workflows, provisioning plans, connector operations, and application-specific provisioning policies. For example, adding a privileged group in Active Directory or assigning an administrative application role would be modeled as target-system access, not as an IdentityIQ capability.

Therefore, granting an IdentityIQ capability is appropriate when the user needs additional permissions within IdentityIQ itself, not when they need elevated access on an external connected application. Reference topics:

Identity Modeling - how IdentityIQ access is granted to users; User-Driven Requests - access requests; Provisioning - target application access fulfillment.

NEW QUESTION # 40

Is this action an example of provisioning?

Reviewing an identity's access during a certification campaign

- A. No
- B. Yes

Answer: A

Explanation:

No. Reviewing an identity's access during a certification campaign is not provisioning. In SailPoint IdentityIQ, certification campaigns are part of governance and access review functionality. Their purpose is to allow designated reviewers, such as managers, application owners, role owners, or other certifiers, to examine existing access and decide whether it should be approved, revoked,

