PassQueen
a.k.a dumpsqueen.com

SailPoint Certified IdentityIQ Associate Exam

SailPoint IdentityIQ-Associate

Version Demo

Total Demo Questions: 9

Total Premium Questions: 91

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An organization must have each manager attest to the access held by their direct reports across all governed applications. The reviewers should receive review items based on the current manager hierarchy.

Which certification type best meets this requirement?

A. An application-owner certification

B. A manager certification

C. A role composition certification

D. An entitlement-owner certification

ANSWER: B

Explanation:

A manager certification assigns review responsibility through the manager relationship maintained on identities. It is designed for managers to review the access held by their direct reports.

An application-owner certification focuses on access associated with a particular application and its accountable owner. A role composition certification reviews role contents, while an entitlement-owner review focuses on the owner of a specific entitlement rather than the identity's manager.

QUESTION NO: 2

Is this statement true about Rapid Setup?

It will create the application definitions.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In SailPoint IdentityIQ, Rapid Setup provides a guided, streamlined method for onboarding common applications rather than requiring an administrator to complete every portion of the full application-configuration workflow manually. A central outcome of this setup process is creation of an IdentityIQ application definition. This object represents the connected source or target system within IdentityIQ and records the application type and connector along with the configuration IdentityIQ needs to communicate with and govern that system.

Once created, the application definition is the basis for the operational processes that make the connected system usable in IdentityIQ. Depending on the connector and selected configuration, it supports such activities as account and entitlement aggregation, schema discovery and management, identity correlation, and provisioning. Rapid Setup is therefore intended to accelerate initial onboarding while still producing the managed application object required by IdentityIQ's governance model.

Administrators should subsequently review and validate the generated configuration, especially correlation logic, schemas, aggregation settings, and any provisioning policies that apply to the environment. That validation does not change the fact that creating the application definition is a core function of Rapid Setup. See SailPoint's IdentityIQ Applications documentation and IdentityIQ product documentation.

QUESTION NO: 3

An identity has two accounts on the same managed application: a standard account and a separately administered account. Each account has different native attributes and entitlements.

Which IdentityIQ object represents each individual application account associated with the identity?

A. An IdentityCube

B. A Link

C. An application definition

D. A ManagedAttribute

ANSWER: B

Explanation:

A Link represents an individual account on an application that has been correlated to an IdentityCube. Each Link stores the account-specific attributes and entitlement values aggregated for that account.

The IdentityCube is the consolidated representation of the person and can contain multiple Links. An application definition represents the connected system, and a ManagedAttribute represents governed metadata for an entitlement value rather than an account.

QUESTION NO: 4

An access-request process allows users to request a new account on an application. The account must include a cost center value, and the organization wants IdentityIQ to control whether that value is entered by the requester or supplied automatically.

Which configuration is intended to define this account-creation behavior?

A. The application account schema

B. A provisioning policy

C. An account correlation rule

D. A lifecycle event

ANSWER: B

Explanation:

A provisioning policy defines the account attributes and field behavior used when IdentityIQ creates or modifies an account. It can determine which values are presented for input, required, or populated through configured logic during the provisioning process.

The application account schema describes the available account attributes, but it does not by itself define the user-facing provisioning form or account-creation policy. A correlation rule matches accounts to identities, while a lifecycle event determines when a workflow starts.

QUESTION NO: 5

Is this displayed in the Identity Warehouse?

Entitlements (identity’s permissions on native applications)

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In IdentityIQ, the Identity Warehouse provides an identity-centric view of the data held in an IdentityCube, including the accounts linked to an identity and the access represented on those accounts. Entitlements are the permissions, groups, roles, or other access-bearing values granted through native applications. After IdentityIQ aggregates account and entitlement information from connected applications, that access can be associated with identities and viewed as part of their overall access profile.

This visibility is fundamental to IdentityIQ governance processes. Entitlement data supports a reviewer's understanding of the access an identity has during certification campaigns, helps administrators investigate access and policy issues, and provides the access context used for lifecycle and role-management activities. In practice, the identity view can show application accounts and their entitlement values, while managed entitlement definitions can provide governance metadata such as owners, descriptions, classifications, and requestability. The Identity Warehouse therefore includes both identity attributes and access information, with entitlements forming a key part of the access information shown for an identity.

See SailPoint's IdentityIQ documentation portal and its entitlements documentation for IdentityIQ application and entitlement concepts.

QUESTION NO: 6

Is this statement true about Rapid Setup?

Rapid Setup birthright roles are requestable.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. A birthright role represents baseline access that IdentityIQ assigns automatically when an identity meets the role's membership criteria. In Rapid Setup, birthright access is designed to support common access patterns such as granting access based on identity attributes, organizational information, or lifecycle conditions. The role is evaluated as part of IdentityIQ's role and identity processing, so eligible identities receive the associated access without needing to initiate an access request.

This automated assignment behavior is the defining purpose of birthright access: it ensures that people who meet established business criteria consistently receive the access required for their role or status. IdentityIQ uses role assignment rules and identity refresh processing to evaluate those criteria and apply the resulting role assignments and provisioning changes. SailPoint's IdentityIQ documentation describes roles as mechanisms for aggregating and assigning access, including assignment through role membership criteria; see IdentityIQ Roles documentation. For the processing that evaluates identity data and role assignments, see Identity Refresh documentation.

QUESTION NO: 7

An account was removed directly from a target application. During the next account aggregation, the connector does not return that account, although IdentityIQ still has a Link for it.

Which aggregation option helps IdentityIQ recognize this source-side removal?

A. Enable Detect deleted accounts.

B. Enable account correlation.

C. Enable aggregation partitioning.

D. Disable rule processing.

ANSWER: A

Explanation:

Detect deleted accounts is correct. This option compares accounts returned by the current aggregation with existing Links for the application. When an existing Link is no longer represented by an account returned from the source, IdentityIQ can identify that the account was deleted from the target system.

Correlation configuration is used to associate returned accounts with identities. Aggregation partitioning distributes processing work, and disabling rule processing suppresses custom aggregation rules; none of these options detects that a previously known account is absent from the source result.

QUESTION NO: 8

Is this an example of a policy that can be defined in IdentityIQ?

An account policy to check whether an identity has requested the appropriate account

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. In IdentityIQ, an account policy evaluates account-related information that has been collected and correlated into the IdentityIQ identity model. Such policies are intended to identify governance violations involving an identity's actual accounts, including conditions such as having an account on a particular application, lacking a required account, or possessing account attributes that do not meet a defined rule. Policy evaluation therefore operates on the observed account and identity state maintained by IdentityIQ.

The stated condition is about whether an identity *requested* an appropriate account. Requesting access is part of IdentityIQ's access-request and provisioning process, where request forms, approval workflows, provisioning policies, and provisioning plans determine how requested access is evaluated and fulfilled. It is not an account-policy condition because it concerns the history or appropriateness of a request rather than an existing account condition subject to governance-policy detection.

SailPoint's IdentityIQ documentation describes policies as mechanisms for detecting violations in governed access data, while its access-request documentation covers the separate process of requesting and approving access. See SailPoint's IdentityIQ policy documentation and IdentityIQ access-request documentation.

QUESTION NO: 9

Is this a purpose of identity governance and administration (IGA)?

Defining corporate reporting hierarchies

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. The core purpose of identity governance and administration is to govern digital identities and access: establish appropriate access, automate identity lifecycle changes, enforce access policies, provide visibility into entitlements, and review or remediate access that is unnecessary or presents risk. SailPoint describes identity security as ensuring that the right people have the right access to the right resources at the right time, and IGA capabilities support that outcome through access requests, approvals, certifications, provisioning, and controls.

A corporate reporting hierarchy is ordinarily business and workforce data maintained by an authoritative source such as an HR information system. IdentityIQ can ingest manager and organizational attributes from that source and use them as identity context. For example, manager relationships can support approval routing, manager-based access reviews, escalations, and lifecycle events. That useful use of hierarchy data does not make defining or maintaining the organizational chart an IGA purpose. Rather, IGA consumes trusted organizational context to make access-governance decisions and demonstrate that access remains appropriate. See SailPoint's overview of identity governance and administration and its explanation of identity security.