# SailPoint.IdentityIQ-Associate.v2026-08-30.q37

| | |
|---|---|
| **Exam Code:** | IdentityIQ-Associate |
| **Exam Name:** | SailPoint Certified IdentityIQ Associate Exam |
| **Certification Provider:** | SailPoint |
| **Free Question Number:** | 37 |
| **Version:** | v2026-08-30 |
| **# of views:** | 108 |
| **# of Questions views:** | 370 |
| https://www.exam-tests.com/IdentityIQ-Associate-exam/SailPoint.IdentityIQ-Associate.v2026-08-30.q37.html | |

**NEW QUESTION: 1**
Is this a true statement about the provisioning process in IdentityIQ?
IdentityIQ determines if the account needs to be created before modification.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. In SailPoint IdentityIQ provisioning, the system evaluates the requested access change in the context of the identity's existing application accounts. When a provisioning request requires a modification on an application, IdentityIQ must determine whether the identity already has an account, represented by a Link, on that application. If no existing account is available and the requested change requires one, IdentityIQ can include account creation as part of the provisioning activity before applying attribute or entitlement modifications.
This behavior is central to request-based provisioning. For example, if a user requests an entitlement on an application where they do not yet have an account, IdentityIQ cannot simply add the entitlement to a nonexistent account. The provisioning process must first establish the account, collect required values through provisioning policies, and then apply the requested access. The provisioning plan may therefore be expanded or adjusted during compilation and fulfillment.
Therefore, the statement is true: IdentityIQ can determine whether an account must be created before modification. Reference topics: Provisioning, provisioning plan processing, account requests, provisioning policies, account creation, entitlement modification, and plan compilation.

**NEW QUESTION: 2**

Does this statement accurately describe how roles are acquired by users in the default role model configuration?
Business roles can only be requested by managers.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
No. This statement does not accurately describe role acquisition in IdentityIQ. Business roles are not restricted to being requested only by managers. In IdentityIQ, roles may be acquired through role assignment logic, role detection, access requests, or administrative action, depending on the role configuration and the organization's request model.
A business role commonly represents access associated with a business function, job, department, location, or organizational responsibility. Users may receive business roles automatically when their identity attributes satisfy configured role profiles or assignment rules, typically recalculated during Identity Refresh. Separately, roles may be made requestable through Lifecycle Manager and exposed through QuickLinks, where request eligibility is controlled by QuickLink Populations, request configuration, and workflow rules. Managers may be allowed to request roles for direct reports, but that is only one possible configuration. IdentityIQ can also allow users to request roles for themselves, allow delegated requesters to request for others, or restrict requests to specific populations. Therefore, "only requested by managers" is too narrow and incorrect. Reference topics: Access Modeling, business roles, role assignment, role detection, Identity Refresh, User-Driven Requests, QuickLink Populations, and role request configuration.

**NEW QUESTION: 3**
Is this statement true about group factories and/or populations?
New groups are created as a result of executing a task.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
The statement is true. In SailPoint IdentityIQ, group factories are used to generate identity groups dynamically based on identity attribute values or configured grouping logic. A group factory defines the rule or attribute basis for grouping identities, but the actual creation or refresh of the resulting groups occurs when the appropriate task is executed. For example, a group factory might be configured to create groups by department, location, cost center, or business unit. When the task runs, IdentityIQ evaluates identities against the factory definition and creates or updates the corresponding groups.
This differs from populations, which are typically defined sets of identities used for targeting, filtering, reporting, or governance scoping. Group factories are more generation-oriented because they can produce multiple group objects from identity data. The task execution step is important because it materializes the groups so they can be used in IdentityIQ operations.

Therefore, new groups can be created as a result of executing a task tied to group factory processing.
Reference topics: Identity Modeling - groups and populations, group factories, identity grouping, and task- driven group creation.

**NEW QUESTION: 4**
Is this statement true for the identity refresh task?
It can update an identity's attributes on their Identity Cube.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
The statement is true. In SailPoint IdentityIQ, the Identity Refresh task is used to recalculate and update identity-level data stored on IdentityCubes. One of its core functions is refreshing identity attributes, which are the normalized identity fields IdentityIQ uses for governance, correlation, lifecycle processing, certifications, policy evaluation, role assignment, and reporting. These attributes may originate from authoritative sources, account links, rules, mappings, or configured identity attribute definitions.
When the Identity Refresh task runs with the appropriate options selected, IdentityIQ evaluates the configured identity attribute mappings and updates the IdentityCube accordingly. This ensures that changes from authoritative data or aggregated account information are reflected at the identity level. For example, department, manager, location, job title, status, or lifecycle state may be recalculated and stored on the IdentityCube for downstream governance processes.
This task is different from aggregation. Aggregation collects account and entitlement data from applications, while Identity Refresh updates IdentityIQ's internal identity model using the data already stored in the repository.
Reference topics: Identity Modeling - IdentityCubes, identity attributes, manager correlation, and common Identity Refresh task options.

**NEW QUESTION: 5**
Is this displayed in the Identity Warehouse?
Entitlements (identity's permissions on native applications)
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. In SailPoint IdentityIQ, the Identity Warehouse presents identity-centered information collected and modeled inside the IdentityCube. Entitlements are part of that identity view because they represent the user's permissions or access rights on connected applications. During aggregation, IdentityIQ reads account data from applications, including entitlement-bearing attributes such as groups, roles, permissions, or other managed access values. These are stored on the identity's application accounts and surfaced in the Identity

Warehouse so reviewers, administrators, and governance users can understand what access the identity currently has.
This is distinct from identity attributes such as department, manager, location, or lifecycle state. Entitlements describe access on target systems and are central to access reviews, policy evaluation, role modeling, and access request decisions. Displaying entitlements in the Identity Warehouse allows IdentityIQ to provide a complete access profile for the identity, including accounts, assigned roles, detected roles, policy violations, and application permissions.
Therefore, entitlements are displayed as part of the Identity Warehouse identity details.
Reference topics: Identity Modeling, IdentityCube contents, Identity Warehouse, application accounts, entitlement aggregation, managed attributes, and access visibility.

**NEW QUESTION: 6**
Is this a function of QuickLink Populations?
They control which capabilities are granted to an identity.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
No. QuickLink Populations do not control which capabilities are granted to an identity. In SailPoint IdentityIQ, capabilities are administrative permission sets assigned to identities to determine what system- level functions they can perform, such as administration, certification management, report access, or other privileged IdentityIQ operations. Capabilities are part of the identity's authorization model and are managed separately from QuickLink Population configuration.
QuickLink Populations serve a different purpose. They determine which QuickLinks are visible and usable for a defined population of users, and they can also influence request behavior such as who may perform a request, what actions are available, and for whom the request may be submitted. For example, a QuickLink Population may allow certain users to request access for themselves, request access for others, edit identities, or initiate password-related actions, depending on configuration.
Therefore, QuickLink Populations control access to request actions and QuickLink availability, not the granting of IdentityIQ capabilities themselves. Reference topics: User-Driven Requests, QuickLink Populations, identity authorization, capabilities, access request configuration, and self-service request controls.

**NEW QUESTION: 7**
Is this statement about uncorrelated accounts true?
Uncorrelated Identity Cubes are removed from IdentityIQ after 30 days.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**

The statement is false. IdentityIQ does not apply a universal rule that removes uncorrelated IdentityCubes after 30 days. Uncorrelated accounts or uncorrelated identity records result from aggregation and correlation processing when IdentityIQ cannot confidently associate an account from an application with an existing IdentityCube. These records remain available for administrative review and remediation until they are resolved through correlation logic, manual correlation, re-aggregation, identity refresh activity, or configured cleanup processes.
The key point is that retention and removal behavior is configuration-driven, not controlled by a fixed 30-day product rule. Administrators may use tasks, aggregation settings, pruning behavior, or lifecycle processes to clean up stale identity or account data, but such actions depend on implementation choices and task configuration. IdentityIQ preserves uncorrelated data because it may represent a real account requiring governance, certification, policy evaluation, or investigation.
Therefore, the assertion that uncorrelated IdentityCubes are automatically removed after 30 days is incorrect.
Reference topics: Applications, uncorrelated account resolution, correlation configuration, aggregation results, IdentityCube association, identity refresh, and administrative cleanup tasks.

**NEW QUESTION: 8**
Is this statement true about group factories and/or populations?
New groups are created as a result of executing a task.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
The statement is true. In SailPoint IdentityIQ, group factories are used to generate identity groups dynamically based on identity attribute values or configured grouping logic. A group factory defines the rule or attribute basis for grouping identities, but the actual creation or refresh of the resulting groups occurs when the appropriate task is executed. For example, a group factory might be configured to create groups by department, location, cost center, or business unit. When the task runs, IdentityIQ evaluates identities against the factory definition and creates or updates the corresponding groups.
This differs from populations, which are typically defined sets of identities used for targeting, filtering, reporting, or governance scoping. Group factories are more generation-oriented because they can produce multiple group objects from identity data. The task execution step is important because it materializes the groups so they can be used in IdentityIQ operations.
Therefore, new groups can be created as a result of executing a task tied to group factory processing. Reference topics: Identity Modeling - groups and populations, group factories, identity grouping, and task-driven group creation.

**NEW QUESTION: 9**
Is this displayed in the Identity Warehouse?
List of objects the user owns
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. The Identity Warehouse in SailPoint IdentityIQ is used to display identity-centered information from the IdentityCube and related IdentityIQ object relationships. In addition to core identity attributes, accounts, roles, entitlements, manager relationships, and direct reports, IdentityIQ can show objects for which the identity is designated as the owner. Ownership is an important governance concept because owners may be responsible for approving access, maintaining roles, reviewing entitlements, managing applications, or participating in certification and remediation processes.
An object owner in IdentityIQ may be associated with configurable objects such as roles, applications, managed attributes, policies, or other governance-related items. Displaying owned objects from the identity view helps administrators and governance users understand the responsibilities assigned to that identity, not just the access held by the identity. This distinction matters because IdentityIQ models both "what access the identity has" and "what governance responsibilities the identity owns." Therefore, a list of objects the user owns is appropriately displayed in the Identity Warehouse when ownership relationships exist and the viewer has sufficient permission. Reference topics: Identity Modeling, IdentityCube contents, Identity Warehouse, object ownership, manager relationships, and governance responsibility modeling.

**NEW QUESTION: 10**
Is this statement true for the use of tasks?
They can be used to confirm that the correct access is included in a role.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
No. In SailPoint IdentityIQ, tasks are used to execute defined system operations, often as background or scheduled processes. Common task usage includes account aggregation, identity refresh, entitlement aggregation, maintenance activities, report execution, role processing, and other repeatable administrative operations. A task may calculate, update, import, refresh, or process data, but it does not itself perform the governance decision of confirming whether access in a role is correct.
Confirming that the correct access is included in a role is a governance review function, most closely associated with role certification, especially role composition certification. In that process, a role owner or designated certifier reviews the access profiles, entitlements, permissions, or requirements contained in a role and decides whether they are

appropriate. The confirmation requires business judgment and reviewer action, not merely task execution.
A task may support role governance indirectly by refreshing role data or generating background processing, but the validation of role contents belongs to certifications and access governance. Therefore, this statement is not accurate for the use of tasks.
Reference topics: Foundational Concepts, tasks versus workflows, Governance, role composition certification, Access Modeling, and role governance.

**NEW QUESTION: 11**
Is this statement about aggregation task options true?
Aggregation partitioning allows aggregation tasks to be split into smaller pieces so that data processing can be split across multiple hosts, as well as across multiple threads per host.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. Aggregation partitioning in SailPoint IdentityIQ is a performance and scalability option used to divide a large aggregation workload into smaller units of work. Instead of processing the entire aggregation as one continuous task on a single execution thread, IdentityIQ can partition the work so multiple task executors can process different portions of the aggregation workload concurrently.
This is especially useful in large environments where applications contain many accounts, groups, or entitlement records. Partitioning can improve throughput by distributing processing across multiple hosts in an IdentityIQ deployment and by allowing multiple threads per host to participate in the aggregation workload. The goal is to reduce total aggregation runtime while maintaining controlled processing of account and entitlement data.
Partitioning is not the same as connector-based delta processing. Delta processing depends on connector support for identifying changed records, while partitioning concerns how the aggregation workload is divided and executed. Therefore, the statement is accurate.
Reference topics: Applications, aggregation task options, aggregation partitioning, account aggregation, performance optimization, task execution, and multi-host processing.

**NEW QUESTION: 12**
Is this an accurate statement about the selection of a connector as part of an application definition?
Some connectors contain a predefined account schema.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**

Yes. In SailPoint IdentityIQ, some application connectors include predefined schema information because the structure of accounts and groups on those target systems is well known to the connector. When an application is created and a specific connector type is selected, IdentityIQ may automatically populate schema elements such as the account schema, native identity attribute, display attribute, common account attributes, and sometimes group or entitlement schema definitions. This is common for standard connectors where the managed system has a predictable object model.
However, predefined does not mean final or immutable. The application administrator must still review and adjust the schema to ensure it accurately represents the implementation, including which attributes are aggregated, which attributes are searchable, which attributes are entitlements, and which attributes are used for identity correlation. Other connector types, such as generic JDBC, delimited file, or custom connectors, may require more manual schema definition.
This statement is therefore accurate because connector selection can provide default schema structure. Reference topics: Applications, connector selection, account schema, group schema, schema attributes, aggregation configuration, and application definition.

**NEW QUESTION: 13**
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.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
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: 14**
Is this an accurate statement about preventive policy checking in IdentityIQ?
IdentityIQ can notify the requester when their access request will cause a policy violation.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
Yes. In SailPoint IdentityIQ, preventive policy checking evaluates proposed access changes before the request is completed or provisioned. When a user submits an access request, IdentityIQ can analyze the requested roles, entitlements, or account changes against configured policies, including separation-of-duty and other access-control policies. If the requested access would create a policy violation, IdentityIQ can present a notification or warning to the requester during the request process.
This notification allows the requester to understand that the requested access conflicts with defined governance rules before the request proceeds further. Depending on configuration, IdentityIQ may allow the request to continue with warning, require additional approval or mitigation, or prevent the request from being submitted. The behavior is controlled by policy configuration, request workflow, and preventive checking settings.
Therefore, the statement is accurate: IdentityIQ can notify the requester when an access request will cause a policy violation. Reference topics: Governance, policy detection, preventive policy checking, access request evaluation, policy violations, and User-Driven Requests.

**NEW QUESTION: 15**
Is this action an example of provisioning?
Defining access conditions that are in violation of the business policies
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
No. Defining access conditions that violate business policies is not provisioning. In SailPoint IdentityIQ, this activity belongs to governance and policy configuration. Policies define conditions that IdentityIQ should detect as violations, such as separation-of-duty conflicts, prohibited combinations of access, excessive privilege, or access that conflicts with organizational rules. These policies are evaluated against identities, roles, accounts, and entitlements to identify existing or potential violations.
Provisioning is the execution or fulfillment of access changes. Examples of provisioning include creating an account, modifying account attributes, adding or removing entitlements, disabling an account, deleting an account, or generating manual fulfillment work items. A policy violation may influence provisioning by blocking a request, warning the requester, requiring approval, or triggering remediation, but defining the violation condition itself is not a provisioning action.

Therefore, the described action is governance policy definition, not provisioning. Reference topics:
Governance, policy configuration, policy detection, preventive policy checking,
Provisioning, provisioning plans, remediation, and access-change fulfillment.

**NEW QUESTION: 16**
Is this statement accurate about the BeanShell rules used in the aggregation process?
The application ' s creation rule, if specified, will run when IdentityIQ is unable to correlate an account to an existing identity.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. In SailPoint IdentityIQ aggregation, correlation is attempted first to match an aggregated account to an existing IdentityCube. Correlation may use configured attribute mappings, correlation rules, or other application correlation logic. If IdentityIQ cannot correlate the account to an existing identity, the application' s creation rule, when configured, can be invoked to determine how IdentityIQ should handle identity creation for that uncorrelated account.
This is especially relevant for authoritative applications, where aggregated account records may represent people who should exist as identities in IdentityIQ. The creation rule can control identity creation behavior, populate required identity attributes, and apply implementation-specific logic when standard correlation does not find a match. Without appropriate creation behavior, the account may remain uncorrelated and require later remediation through corrected correlation logic, re-aggregation, or manual correlation.
Therefore, the statement is accurate: the creation rule is associated with the aggregation and correlation process and is used when an account cannot be matched to an existing IdentityCube. Reference topics:
Applications, BeanShell rules, account aggregation, correlation logic, identity creation rules, authoritative applications, and uncorrelated account handling.

**Valid IdentityIQ-Associate Dumps** shared by BraindumpsPass.com for Helping Passing IdentityIQ-Associate Exam! BraindumpsPass.com now offer the **newest IdentityIQ-Associate exam dumps**, the BraindumpsPass.com IdentityIQ-Associate exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com IdentityIQ-Associate dumps with Test Engine here: https://www.braindumpspass.com/SailPoint/IdentityIQ-Associate-practice-exam-dumps.html (**78** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

**NEW QUESTION: 17**

Is this statement true about group factories and/or populations?
Groups and populations can be assigned as object owners in IdentityIQ.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
The statement is false. In SailPoint IdentityIQ, groups and populations are used to classify, filter, and organize identities for governance, reporting, certifications, and targeted user experiences. A population is a defined collection of identities, and group factories can dynamically create identity groups based on configured identity attributes. These constructs are useful for segmentation, analysis, and campaign targeting, but they are not the standard objects assigned as owners of IdentityIQ objects.
Ownership in IdentityIQ is normally assigned to an identity or to a workgroup. A workgroup is used when ownership or responsibility must be shared by multiple users, such as application owners, certification owners, entitlement owners, or approval groups. This distinction matters because ownership drives accountability, work item assignment, approvals, escalations, and administrative responsibility. Populations and generated groups do not function as accountable owners in the same way workgroups do.
Therefore, while groups and populations can influence governance scope and visibility, they are not assigned as object owners. Reference topics: Identity Modeling - groups and populations; Foundational Concepts - common objects and usage; Governance - ownership, certifications, and work item responsibility.

**NEW QUESTION: 18**
Is this a use of the data provided by the entitlement catalog?
Provide entitlement descriptions for viewing on the application definition.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
The statement is not a correct use case for entitlement catalog data. In SailPoint IdentityIQ, the entitlement catalog is used to govern and enrich entitlement data after entitlements are discovered from application account/group schemas and aggregation. The catalog stores managed entitlement metadata such as display name, description, owner, classification, requestability, risk-related information, and other governance attributes. This information supports access reviews, access requests, approvals, role modeling, policy analysis, and decision-making by presenting business-readable information about technical access.
The application definition is primarily the configuration object for connecting to a target system. It contains connector settings, schemas, correlation configuration, aggregation options, provisioning settings, and related application-level controls. While entitlement-related configuration begins with the application schema, the entitlement catalog is not principally used to provide descriptions "for viewing on the application definition." Its

governed data is used in operational governance contexts, especially where reviewers, requesters, approvers, and administrators need understandable access context.
Therefore, entitlement descriptions are catalog governance metadata, not a feature whose purpose is simply display on the application definition. Reference topics: Access Modeling - purpose of the entitlement catalog; Applications - group/account schemas; Governance - certification decision support; User-Driven Requests - access request display and approval context.

**NEW QUESTION: 19**
Does this statement accurately describe how roles are acquired by users in the default role model configuration?
Business roles can only be requested by managers.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
No. This statement does not accurately describe role acquisition in IdentityIQ. Business roles are not restricted to being requested only by managers. In IdentityIQ, roles may be acquired through role assignment logic, role detection, access requests, or administrative action, depending on the role configuration and the organization's request model.
A business role commonly represents access associated with a business function, job, department, location, or organizational responsibility. Users may receive business roles automatically when their identity attributes satisfy configured role profiles or assignment rules, typically recalculated during Identity Refresh. Separately, roles may be made requestable through Lifecycle Manager and exposed through QuickLinks, where request eligibility is controlled by QuickLink Populations, request configuration, and workflow rules. Managers may be allowed to request roles for direct reports, but that is only one possible configuration.
IdentityIQ can also allow users to request roles for themselves, allow delegated requesters to request for others, or restrict requests to specific populations.
Therefore, "only requested by managers" is too narrow and incorrect. Reference topics: Access Modeling, business roles, role assignment, role detection, Identity Refresh, User-Driven Requests, QuickLink Populations, and role request configuration.

**NEW QUESTION: 20**
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: (SHOW ANSWER)**
This is not a correct example of an IdentityIQ policy as stated. IdentityIQ policies are used to detect governance violations based on identity, account, entitlement, role, risk, or activity

conditions. An account policy is concerned with whether an identity has an account, lacks a required account, or has an account that violates defined account-related criteria. It evaluates existing identity and account state after data is aggregated and correlated into IdentityIQ.
The phrase "has requested the appropriate account" describes an access request validation concept rather than a policy-detection use case. Requests are handled through the user-driven request and provisioning framework, including QuickLinks, request forms, approvals, workflows, provisioning policies, and provisioning plans. A request can be evaluated, approved, rejected, or fulfilled, but a governance policy is normally not defined to determine whether a request itself was "appropriate." IdentityIQ policies detect violations against current or observed access conditions. Therefore, an account policy may check whether an identity has an inappropriate account, but not whether the identity requested the appropriate account. Reference topics: Governance - common policy examples and policy detection; User- Driven Requests - access requests; Provisioning - provisioning process and provisioning policies.

**NEW QUESTION: 21**
Is this statement true for IdentityIQ application definitions?
Applications in IdentityIQ are named with the connector that is selected.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
No. In SailPoint IdentityIQ, the application name is a configurable label assigned to the application object and does not have to match the connector selected. The application definition represents an external system or source, while the connector defines the technical integration method used to communicate with that system. These are related configuration elements, but they are not the same field and one does not automatically name the other.
For example, an application could be named "Corporate Directory," "North America Active Directory," or "HR Source," while using an LDAP, Active Directory, JDBC, Delimited File, Web Services, or another connector type. The connector selection determines available configuration settings, supported schema behavior, aggregation options, and provisioning capabilities. The application name is used for identification within IdentityIQ, reporting, certifications, requests, policies, and administrative configuration.
Therefore, the statement is incorrect because IdentityIQ applications are not named by the selected connector. They are named by the administrator or implementer according to the business or system context. Reference topics: Applications, application definition, connector selection, connector-dependent settings, schemas, aggregation, and provisioning support.

**NEW QUESTION: 22**

Is this definition of entitlement accurate?
An access right on an application
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. In SailPoint IdentityIQ, an entitlement represents an access right, permission, privilege, group membership, role membership, or similar access-granting value on an application. Entitlements are discovered from application account data during aggregation and are commonly modeled in IdentityIQ through schema attributes marked as entitlement attributes. Once aggregated, these values may appear in the entitlement catalog as managed attributes, where they can be reviewed, requested, certified, governed by policies, and associated with roles.
The definition "an access right on an application" is accurate because entitlements describe what an identity's account is allowed to do or access within a connected system. Examples include Active Directory group membership, database roles, application permissions, cloud groups, or other system-specific access values.
IdentityIQ uses entitlements as core governance objects for certifications, access requests, policy checks, role modeling, and provisioning.
This definition is intentionally broad because different target systems represent access differently. IdentityIQ normalizes those application-specific access values into entitlement concepts for identity governance.
Reference topics: Access Modeling, entitlement catalog, managed attributes, application schema, entitlement aggregation, certifications, access requests, and provisioning.
'

**NEW QUESTION: 23**
Is this statement true about managers in IdentityIQ?
References to an identity's manager must be provided in the authoritative application.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
The statement is true in the context of IdentityIQ manager correlation. IdentityIQ does not infer an identity's manager relationship without source data that identifies the manager. The authoritative application, typically an HR or personnel source, provides the trusted identity records and should include a manager reference attribute, such as manager ID, employee number, username, distinguished name, or another value that can be correlated to an existing IdentityIQ identity.
During aggregation and identity refresh, IdentityIQ uses configured manager correlation logic to resolve that manager reference to an IdentityCube representing the manager. Once resolved, the manager relationship can support governance functions such as manager certifications, access request approvals, lifecycle approvals, escalations, and

reporting hierarchy-based controls. Without a manager reference from the authoritative source, IdentityIQ may still contain identities, accounts, and access, but it cannot reliably establish reporting relationships for those identities through standard manager correlation. This is distinct from manually assigning relationships or using custom logic; the standard governance model expects manager data to originate from the authoritative identity source. Reference topics: Identity Modeling
- manager correlation, IdentityCube attributes, authoritative identity data; Governance - manager-based certifications and approvals; User-Driven Requests - manager approval routing.

**NEW QUESTION: 24**
Is this statement true about attributes in IdentityIQ?
The value for a specific account attribute can be sourced from several applications.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
The statement is false. In IdentityIQ, an account attribute is defined within a specific application account schema and represents data stored on an account link for that application. Its value is obtained from the account data aggregated from that particular application connector. For example, an account attribute such asmemberOf,department,title, oraccountStatusbelongs to the account schema of a defined application and is populated from that application's aggregation results.
The concept of sourcing values from several applications applies more directly to identity attributes, not account attributes. Identity attributes reside on the IdentityCube and may be derived from authoritative sources, account links, rules, mappings, or precedence logic across multiple applications. IdentityIQ uses identity attribute configuration to normalize data such as department, location, manager, email, or lifecycle state at the identity level. Therefore, while multiple applications may contain similarly named account attributes, each account attribute value is tied to its own application account schema and account link. It is not a single shared account attribute sourced from several applications.
Reference topics: Applications - account schema attributes; Identity Modeling - identity attributes versus account attributes; Identity Refresh - updating IdentityCube attributes.

**NEW QUESTION: 25**
Is this action an example of provisioning?
Reviewing an identity's access during a certification campaign
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
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, delegated, or otherwise acted upon.
Provisioning is different. Provisioning refers to the fulfillment of access changes, such as creating accounts, modifying account attributes, adding or removing entitlements, disabling accounts, deleting accounts, or executing manual fulfillment work items when direct connector-based provisioning is unavailable. A certification decision may later trigger provisioning if a reviewer revokes access and IdentityIQ generates a remediation or deprovisioning action. However, the review activity itself is governance, not provisioning.
Therefore, "reviewing an identity's access during a certification campaign" is an access review action, not a provisioning action. Reference topics: Governance, certifications, access reviews, remediation, revocation decisions, Provisioning, provisioning plans, and deprovisioning fulfillment.

**NEW QUESTION: 26**
Is this statement true about group factories and/or populations?
Groups and populations are used to target operations to only a specific set of identities.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
The statement is true. In SailPoint IdentityIQ, groups and populations are identity-segmentation mechanisms used to define sets of identities that share specific characteristics. A population is typically a saved collection of identities based on search criteria or defined membership logic. A group factory can dynamically generate identity groups based on identity attributes, such as department, location, cost center, job title, or business unit.
These constructs are useful because many IdentityIQ operations should not apply to the entire identity population. They allow administrators to scope or target actions to the relevant identities only. For example, populations and groups can support targeted reporting, focused analysis, certification scoping, and other governance activities where only a defined subset of identities should be included. This improves accuracy, reduces review noise, and aligns governance activity with business structure.
They should not be confused with ownership objects such as workgroups. Their primary purpose is identity grouping and operational targeting, not shared ownership accountability.
Reference topics: Identity Modeling - groups and populations; Governance - certification targeting and reporting scope; Foundational Concepts - business modeling and identity segmentation.

**NEW QUESTION: 27**
Why would an organization define lifecycle events in IdentityIQ?

To prevent users from violating policies

**A.** Yes

**B.** No

**Answer: B (LEAVE A REPLY)**

No. Lifecycle Events in SailPoint IdentityIQ are not primarily defined to prevent users from violating policies. Lifecycle Events are configured to detect identity-related changes and trigger a business process or workflow in response. Typical examples include joiner, mover, leaver, rehire, or other lifecycle transitions based on changes to identity attributes such as lifecycle state, employment status, department, manager, location, or start and termination dates.

Preventing policy violations is handled through IdentityIQ's governance and policy framework, especially preventive policy checking during access request processing. Policies define prohibited access conditions, such as separation-of-duty conflicts, and IdentityIQ can warn, block, or route requests when a proposed access change would create a violation.

Lifecycle Events may indirectly support compliance by removing or adjusting access when a user changes status, but their purpose is event-driven lifecycle automation, not policy violation prevention itself. Therefore, this statement is not the correct reason for defining Lifecycle Events.

Reference topics: Provisioning, Lifecycle Events, joiner-mover-leaver processing, workflows, identity attribute changes, Governance, policy detection, and preventive policy checking.

**NEW QUESTION: 28**

Is this a true statement about Lifecycle Events?

Their configuration includes a business process that will be executed when a specified data change occurs on an identity.

**A.** Yes

**B.** No

**Answer: (SHOW ANSWER)**

Yes. In SailPoint IdentityIQ, a Lifecycle Event is configured to detect a defined change in identity data and then trigger a specified business process. Lifecycle Events are commonly used to automate identity lifecycle activities such as joiner, mover, leaver, rehire, or other status-driven events. The event definition identifies the condition to monitor, such as a change to an identity attribute, and associates that condition with a workflow or business process that IdentityIQ should execute when the event is detected.

For example, if an identity's lifecycle state changes from active to terminated, a Lifecycle Event can trigger a termination workflow that disables accounts, removes access, creates work items, or starts provisioning actions. The event itself does not perform all provisioning directly; rather, it initiates the configured process that carries out the required business logic.

Therefore, the statement is accurate because Lifecycle Event configuration includes both the triggering identity data change and the business process to execute in response. Reference topics: Provisioning, Lifecycle Events, identity attribute changes, business processes, workflows, identity refresh, and event-driven provisioning.

**NEW QUESTION: 29**
Is this statement accurate about the BeanShell rules used in the aggregation process?
The application's creation rule, if specified, will run when IdentityIQ is unable to correlate an account to an existing identity.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
Yes. In SailPoint IdentityIQ aggregation, correlation is attempted first to match an aggregated account to an existing IdentityCube. Correlation may use configured attribute mappings, correlation rules, or other application correlation logic. If IdentityIQ cannot correlate the account to an existing identity, the application's creation rule, when configured, can be invoked to determine how IdentityIQ should handle identity creation for that uncorrelated account.
This is especially relevant for authoritative applications, where aggregated account records may represent people who should exist as identities in IdentityIQ. The creation rule can control identity creation behavior, populate required identity attributes, and apply implementation-specific logic when standard correlation does not find a match. Without appropriate creation behavior, the account may remain uncorrelated and require later remediation through corrected correlation logic, re-aggregation, or manual correlation.
Therefore, the statement is accurate: the creation rule is associated with the aggregation and correlation process and is used when an account cannot be matched to an existing IdentityCube. Reference topics: Applications, BeanShell rules, account aggregation, correlation logic, identity creation rules, authoritative applications, and uncorrelated account handling.

**NEW QUESTION: 30**
Is this statement about uncorrelated accounts true?
If an application ' s correlation logic has changed, the aggregation task can change account correlations to match the new logic.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
The statement is true. In SailPoint IdentityIQ, account correlation is the process used to associate an application account, represented as a Link, with the appropriate IdentityCube. Correlation logic is configured on the application and may use account attributes, identity attributes, or correlation rules to determine ownership. When that logic is changed, a

subsequent account aggregation can evaluate account data against the updated correlation configuration and adjust account-to-identity associations where the aggregation process is configured to perform correlation.
This is important when accounts were previously uncorrelated, incorrectly correlated, or correlated under outdated matching criteria. For example, if an application originally correlated accounts by user name but is later changed to correlate by employee ID, aggregation can apply the new logic so that accounts align with the correct identities.
Manual correlation is therefore not the only remediation path; proper correlation configuration followed by aggregation is a standard way to resolve or correct account ownership.
The behavior depends on the aggregation and correlation configuration, but the principle is accurate:
aggregation can apply changed correlation logic to account correlations. Reference topics: Applications, correlation options, account aggregation, uncorrelated account resolution, Link-to-IdentityCube association, and Identity Modeling.

**NEW QUESTION: 31**
Is this action an example of provisioning?
Defining access conditions that are in violation of the business policies
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
No. Defining access conditions that violate business policies is not provisioning. In SailPoint IdentityIQ, this activity belongs to governance and policy configuration. Policies define conditions that IdentityIQ should detect as violations, such as separation-of-duty conflicts, prohibited combinations of access, excessive privilege, or access that conflicts with organizational rules. These policies are evaluated against identities, roles, accounts, and entitlements to identify existing or potential violations.
Provisioning is the execution or fulfillment of access changes. Examples of provisioning include creating an account, modifying account attributes, adding or removing entitlements, disabling an account, deleting an account, or generating manual fulfillment work items. A policy violation may influence provisioning by blocking a request, warning the requester, requiring approval, or triggering remediation, but defining the violation condition itself is not a provisioning action.
Therefore, the described action is governance policy definition, not provisioning. Reference topics: Governance, policy configuration, policy detection, preventive policy checking, Provisioning, provisioning plans, remediation, and access-change fulfillment.

**Valid IdentityIQ-Associate Dumps** shared by BraindumpsPass.com for Helping Passing IdentityIQ-Associate Exam! BraindumpsPass.com now offer the **newest IdentityIQ-Associate exam dumps**, the BraindumpsPass.com IdentityIQ-Associate exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com IdentityIQ-Associate dumps with Test Engine here: https://www.braindumpspass.com/SailPoint/IdentityIQ-Associate-practice-exam-dumps.html (**78** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

**NEW QUESTION: 32**
Is this a function of QuickLink Populations?
They control which identities can approve access requests.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
No. QuickLink Populations do not determine which identities can approve access requests.
In SailPoint IdentityIQ, QuickLink Populations control the availability and scope of QuickLinks for users. They define who can initiate a specific request action, what type of request can be launched, and in many cases who the request can be submitted for. For example, they may allow an employee to request access for themselves or allow a manager to request access for direct reports.
Approval authority is handled separately through request workflows, approval schemes, approval rules, work item assignment logic, application or role owners, managers, governance groups, or configured business processes. When an access request is submitted, IdentityIQ evaluates the configured approval path to determine which identities receive approval work items. That approval routing is not controlled by the QuickLink Population itself.
Therefore, the statement is inaccurate. QuickLink Populations govern request initiation and visibility, while approval routing is governed by workflow and approval configuration.
Reference topics: User-Driven Requests, QuickLink Populations, access request process, approval workflows, work items, and request authorization.

**NEW QUESTION: 33**
Is this statement true about attributes in IdentityIQ?
Account attributes are defined in the application account schema.
**A.** Yes
**B.** No
**Answer: A (LEAVE A REPLY)**
The statement is true. In SailPoint IdentityIQ, account attributes are defined on the application's account schema. The application definition tells IdentityIQ how to represent accounts from a connected source, and the account schema specifies which attributes

exist on those accounts. Examples may include account ID, display name, email, status, department, groups, roles, permissions, or other source-specific fields returned by the connector during aggregation.
This is distinct from identity attributes, which are stored on the IdentityCube and represent normalized identity-level data used across IdentityIQ. Account attributes belong to application account links, while identity attributes belong to the identity model. During aggregation, IdentityIQ reads account data according to the application schema and stores the discovered values as account/link attributes. Some account schema attributes may also be marked as managed when their values represent entitlement-like access that should be governed through the Entitlement Catalog.
Therefore, account attributes are correctly defined in the application account schema.
Reference topics:
Applications - application definitions, account schema attributes, schema attribute properties; Identity Modeling - identity attributes versus account attributes; Access Modeling - managed attributes and entitlement catalog.

**NEW QUESTION: 34**
Is this statement true about Rapid Setup?
Rapid Setup birthright roles are requestable.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
No. In IdentityIQ, a birthright role is intended to represent access that is automatically assigned to identities based on defined business criteria, such as lifecycle state, department, location, job function, or other identity attributes. The purpose of a birthright role is automatic access assignment, not user-driven request selection.
Rapid Setup can help configure common access-modeling and application-onboarding elements more efficiently, including birthright access patterns, but the birthright concept remains assignment-based rather than request-based.
Requestable access is handled through the access request model, where users select roles, entitlements, or other access items made available through request configuration and QuickLinks. Birthright access is different because it is granted when an identity satisfies the role assignment criteria and is recalculated through identity refresh and role evaluation. Making birthright roles requestable would undermine their purpose as standard baseline access automatically derived from identity data.
Therefore, the statement is inaccurate. Rapid Setup birthright roles are used for automated assignment and baseline access, not as requestable access items. Reference topics: Applications, Rapid Setup, Access Modeling, birthright roles, role assignment, identity refresh, and User-Driven Requests.

**NEW QUESTION: 35**

Does this statement accurately describe how roles are acquired by users in the default role model configuration?
Birthright role assignment may be processed during a mover lifecycle event.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
Yes. In SailPoint IdentityIQ, birthright roles represent access that is automatically granted based on identity context, such as job function, department, location, lifecycle state, or organizational assignment. A mover lifecycle event occurs when an identity undergoes a material change, such as transfer to a new department, change in manager, change in location, or change in business role eligibility. Because these changes can alter what baseline access the identity should have, birthright role assignment may be processed as part of the mover event.
The mover event can launch a configured business process that evaluates the identity's updated attributes and initiates access changes, including assignment of new birthright roles or removal of access no longer appropriate. This differs from requestable roles, where a user or manager explicitly asks for access through Lifecycle Manager. Birthright access is driven by identity state and business rules.
Therefore, the statement is accurate. Mover lifecycle processing can be used to keep baseline role-based access aligned with the user's changed business position. Reference topics: Access Modeling, birthright roles, role assignment, Identity Refresh, Lifecycle Events, mover processes, and Provisioning.

**NEW QUESTION: 36**
Is this an accurate statement about preventive policy checking in IdentityIQ?
Preventive policy checking can only stop self-service requests.
**A.** Yes
**B.** No
**Answer: B (LEAVE A REPLY)**
The statement is false. Preventive policy checking in SailPoint IdentityIQ is not limited only to self-service requests. Preventive policy evaluation is used to identify policy violations before access changes are completed. This can occur during access request processing, provisioning-related activity, or other configured request paths where IdentityIQ evaluates proposed changes against defined policies before allowing the transaction to proceed.
A self-service request is only one possible entry point. IdentityIQ access requests may be submitted by an end user, a manager, an administrator, or another authorized requester depending on QuickLink Population rules, request configuration, and access-request permissions. Preventive policy checking evaluates the requested access change itself, not merely the fact that the request was self-initiated. If the proposed access would violate a separation-of-duty, risk, or other governance policy, IdentityIQ can warn, require additional handling, or block the request depending on policy and workflow configuration.

Therefore, the word "only" makes the statement incorrect. Preventive policy checking is a governance control applied to configured access-change activity, not exclusively to self-service actions. Reference topics:
Governance, policy detection, preventive policy checking, access request policy evaluation, User-Driven Requests, and provisioning request control.

**NEW QUESTION: 37**
Is this statement true about attributes in IdentityIQ?
Account attributes are defined in the application account schema.
**A.** Yes
**B.** No
**Answer: (SHOW ANSWER)**
The statement is true. In SailPoint IdentityIQ, account attributes are defined on the application's account schema. The application definition tells IdentityIQ how to represent accounts from a connected source, and the account schema specifies which attributes exist on those accounts. Examples may include account ID, display name, email, status, department, groups, roles, permissions, or other source-specific fields returned by the connector during aggregation.
This is distinct from identity attributes, which are stored on the IdentityCube and represent normalized identity-level data used across IdentityIQ. Account attributes belong to application account links, while identity attributes belong to the identity model. During aggregation, IdentityIQ reads account data according to the application schema and stores the discovered values as account/link attributes. Some account schema attributes may also be marked as managed when their values represent entitlement-like access that should be governed through the Entitlement Catalog.
Therefore, account attributes are correctly defined in the application account schema.
Reference topics: Applications - application definitions, account schema attributes, schema attribute properties; Identity Modeling - identity attributes versus account attributes; Access Modeling - managed attributes and entitlement catalog.

**Valid IdentityIQ-Associate Dumps** shared by BraindumpsPass.com for Helping Passing IdentityIQ-Associate Exam! BraindumpsPass.com now offer the **newest IdentityIQ-Associate exam dumps**, the BraindumpsPass.com IdentityIQ-Associate exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com IdentityIQ-Associate dumps with Test Engine here: https://www.braindumpspass.com/SailPoint/IdentityIQ-Associate-practice-exam-dumps.html (**78** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)