PassQueen
a.k.a dumpsqueen.com

SailPoint Certified IdentityIQ Engineer

SailPoint IdentityIQ-Engineer

Version Demo

Total Demo Questions: 22

Total Premium Questions: 224

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Is this a default functionality of the Lifecycle Manager (LCM) module?

Proposed Solution:

Launch Certification Campaign

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. In IdentityIQ, Lifecycle Manager is designed to manage identity lifecycle events and user-driven access operations. Its standard capabilities include requesting access, managing accounts and access profiles, routing approvals, processing joiner/mover/leaver changes, and provisioning approved changes to connected applications. These functions enable an organization to make and fulfill access changes through governed lifecycle workflows.

Launching a certification campaign is instead part of IdentityIQ's certification and access-governance functionality. A certification campaign initiates a formal access-review process in which designated reviewers evaluate identities, accounts, roles, entitlements, or application access and make review decisions. Although a revocation decision produced during a certification can ultimately result in a provisioning action, the campaign's creation, scheduling, generation, and review workflow are certification capabilities rather than default LCM operations. Keeping this distinction clear is important when selecting IdentityIQ features and configuring governance processes: LCM handles lifecycle and access-request fulfillment, while certifications provide periodic or event-driven access attestation.

See SailPoint's Lifecycle Manager overview and Certification overview for the respective feature areas.

QUESTION NO: 2

Is this a benefit of using the Run Rule feature of the Debug-Object page?

Proposed Solution:

It can be used to display the return value of simple code.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In IdentityIQ, the Debug pages are administrative and development tools that let an authorized engineer inspect objects and test configuration behavior directly in the running application. The Run Rule capability is particularly useful for executing a selected rule and reviewing the value it returns. This makes it practical to validate a small piece of BeanShell logic before that logic is used by a larger feature such as a workflow, lifecycle event, task, or application-related configuration.

For example, an engineer can use a simple test rule to retrieve an Identity attribute, construct a string, evaluate a condition, or look up an IdentityIQ object, then use the displayed return value to confirm that the rule behaves as intended. This short feedback cycle helps with troubleshooting and iterative rule development because the engineer does not need to trigger the entire business process merely to see the result of the code. As with all Debug-page functionality, use should be limited to appropriately authorized administrators and performed carefully, since a rule can interact with live IdentityIQ data. SailPoint documents Debug pages as tools for examining and working with IdentityIQ objects; see the IdentityIQ Debug Pages documentation and SailPoint's IdentityIQ product documentation.

QUESTION NO: 3

An engineer is assigned to configure an account attribute. The requirements are:

Purpose: Flag privileged accounts

Read from: Financial application, privileged attribute

Calculate from: Keystore application, responsibility-code attribute

Usage 1: Display as option in Advanced Analytics

Usage 2: Use when writing rules

Usage 3: Include in policies

Does the engineer need to set this configuration option on the account attribute to meet the requirements?

Solution: Edit Mode: Read Only

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. The attribute is intended to represent a privileged-account flag whose value is obtained from authoritative account data and may be derived using the responsibility code from another application. It is therefore a system-populated attribute, rather than a value an administrator should manually alter through the IdentityIQ user interface. Setting *Edit Mode: Read Only* protects the integrity of the flag by preventing UI edits while still allowing IdentityIQ to populate and update the value through aggregation, attribute mapping, or configured calculation logic. Read-only edit mode controls user-interface modification; it does not prevent the platform's configured data-processing mechanisms from maintaining the attribute value.

Once populated, the account attribute remains available as account data for reporting and governance use cases. It can be exposed for Advanced Analytics when the relevant searchable/reporting configuration is also enabled, and it can be referenced by rules and policy logic. The read-only setting is appropriate because the privileged designation should consistently reflect its configured application sources and calculation rather than an ad hoc user-entered value. SailPoint's IdentityIQ documentation describes account and application-schema attribute configuration in the IdentityIQ documentation portal; implementation guidance is also available through the SailPoint Community.

QUESTION NO: 4

An engineer uses Run Rule on the Debug-Object page to test a rule configured as an application correlation rule. The rule depends on the account object supplied during account aggregation.

The rule fails in Run Rule because the expected account variable is null.

What is the most appropriate next step?

A. Test the rule through a controlled account aggregation that supplies the correlation-rule context.

B. Replace the account variable with a workflow variable and run the rule again.

C. Change the rule type to a task rule so that Run Rule supplies the account variable.

D. Map the account object to an Identity attribute before executing the rule.

ANSWER: A

Explanation:

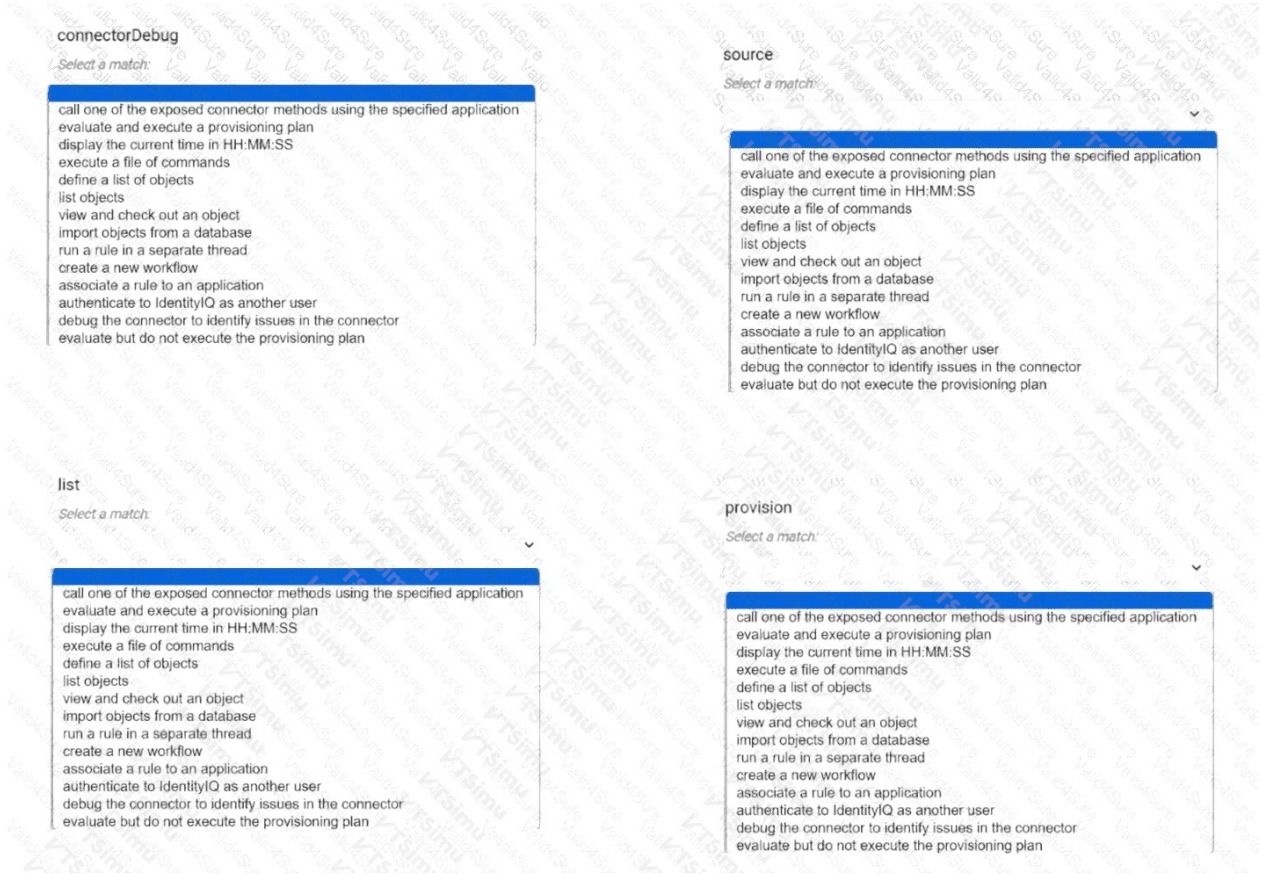
Run Rule is useful for testing simple logic and return values, but it does not automatically reproduce every runtime context supplied by a specific rule invocation. An application correlation rule receives its account-related context when IdentityIQ invokes it during aggregation. The engineer should test the rule through controlled application aggregation, using representative account data and reviewing the correlation result.

Changing the rule to use a workflow variable does not provide the aggregation account. Making the rule a task rule changes its invocation context. Adding the account as an Identity attribute does not establish the account object that the correlation-rule contract supplies.

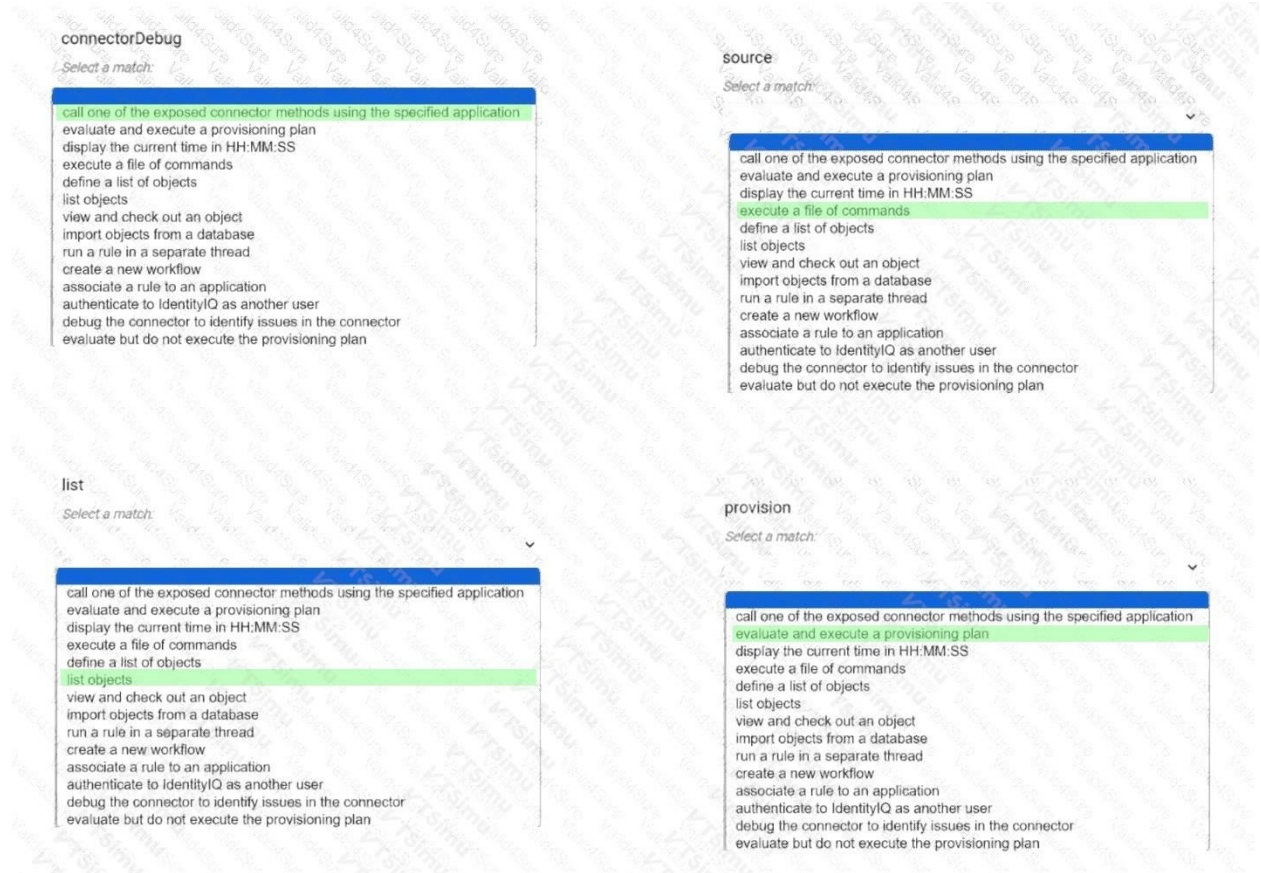
QUESTION NO: 5 - (HOTSPOT)

Match the following IdentityIQ console commands To their functions.

Use the drop-down menus to select your answers. Answer options from the drop-down menus may only be used once Some will not be used at all.



ANSWER:



Explanation:

IdentityIQ's console is designed to expose administrative, diagnostic, object-management, and provisioning operations through concise commands. The correct matching follows the purpose implied by each console command and the way it is used in IdentityIQ administration. **connectorDebug** is the connector-focused diagnostic command: it calls one of the exposed connector methods using the specified application. This lets an engineer directly exercise connector functionality and inspect behavior while troubleshooting an integration. **list** is the object-enumeration command, so it is used to list objects. That is useful when locating IdentityIQ objects in the repository for administration or follow-up console actions. **source** executes a file of commands. It supports repeatable console work by reading command lines from a prepared script rather than requiring an administrator to enter each command interactively. **provision** evaluates and executes a provisioning plan, making it the command associated with processing the requested account or entitlement changes represented by that plan. Together, these mappings distinguish direct connector invocation, object listing, command-file execution, and provisioning-plan processing. SailPoint documentation provides IdentityIQ product documentation through its IdentityIQ documentation portal, while SailPoint's Community is an additional official resource for implementation and troubleshooting guidance.

QUESTION NO: 6

Can the rule library named Common Rules Library" be included in a Rule by adding this code?

Solution:

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. IdentityIQ supports reusable rule-library logic, allowing a rule to declare a dependency on a named library and use the library's shared methods at runtime. The intended XML pattern places a reference inside the rule's `ReferencedRules` section and identifies the library object by its SailPoint object class and name, such as `Common Rules Library`. Once IdentityIQ resolves that reference, the library source is available to the referencing rule, which avoids duplicating common BeanShell helper functions across multiple rules.

Rule libraries are particularly appropriate for centrally maintained utility methods used by several implementations, including identity-attribute processing, account logic, and workflow-related calculations. The referenced library must exist in the IdentityIQ repository, be correctly named, and contain valid rule-library source before the dependent rule is executed. This mechanism is part of IdentityIQ's rule extensibility model; deployment should therefore include both the library object and the rule that references it. SailPoint's rule-development guidance is available in the SailPoint Developer documentation for rules, and IdentityIQ documentation resources are available through the SailPoint Documentation portal.

QUESTION NO: 7

An authoritative application has been aggregated successfully, and the source data now contains a revised department value for several identities.

The department identity attribute is populated by an IdentityIQ identity mapping. The engineer needs the changed source values to be reflected in the affected Identity Cubes.

Which action is most appropriate?

A. Run a Refresh Identity Cube task for the affected identities

B. Run a Role Mining task for the affected identities

C. Launch an identity certification for the affected identities

D. Delete the existing Links and aggregate the application again

ANSWER: A

Explanation:

The engineer should run identity refresh processing for the affected identities with identity-attribute refresh enabled. Identity mappings are evaluated as IdentityIQ refreshes the Identity Cube, allowing the mapped department value to be recalculated from the current authoritative account data.

Account aggregation collects and updates source-account information, but it does not by itself guarantee that every calculated identity attribute is recomputed in the required scope. Rebuilding roles or launching a certification does not refresh the mapped identity attribute.

QUESTION NO: 8

Assuming that the policy violation owner has the necessary permissions, is this a valid option for the policy violation owner to use when acting on a policy violation of type ' Account Policy ' ?

Proposed Solution:

Allow

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In IdentityIQ, an Account Policy violation can be handled through the policy-violation workflow by an authorized policy violation owner. *Allow* is a valid disposition for such a violation when the owner determines that the account condition is an acceptable business exception and therefore does not require corrective remediation. Using this action records the owner's decision in IdentityIQ and changes the violation's handling state accordingly, preserving governance visibility rather than silently ignoring the detected condition.

The permission assumption in the question is important: IdentityIQ uses ownership and delegated administrative capabilities to control who can act on policy violations. Once the designated owner has the applicable access, the owner can select the appropriate permitted action, including allowing an Account Policy violation. This supports exception-based governance, where a policy remains in force and continues to identify conditions that match it, while an authorized stakeholder can formally approve a particular instance based on business context. SailPoint's IdentityIQ documentation describes policy governance and the handling of policy violations in the product help: IdentityIQ Product Documentation. SailPoint also maintains IdentityIQ documentation resources through its customer community: IdentityIQ Documentation.

QUESTION NO: 9

Is this an example of a mover lifecycle event?

Solution: A contractor whose contract expired and accounts were disabled has a new contract with the company; the contractor needs all of their previous accounts enabled.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct because the contractor remains the same known identity but has undergone a change in workforce status: a new contract has been established after a prior contract ended. That status change requires IdentityIQ to update the identity's access state by restoring the accounts and access that are appropriate for the renewed engagement. In lifecycle-management terms, mover processing handles changes to an existing identity that require access adjustments rather than establishing an entirely unrelated identity record.

The important facts are that the contractor previously had accounts, those accounts were disabled as part of the earlier contract end, and the renewed contract creates a new business need for access. A mover lifecycle event can use identity attributes such as worker status, contract status, department, role, or other authoritative-source data to detect the change and initiate provisioning. The resulting workflow can enable the existing accounts and restore access according to the organization's lifecycle policy, while retaining the identity correlation and audit history associated with that person.

SailPoint IdentityIQ lifecycle events support automated provisioning actions when identity changes are detected. See SailPoint's Lifecycle Events documentation and Lifecycle Event Types documentation.

QUESTION NO: 10

Is this a true statement about localization support in IdentityIQ?

Solution: The default language can be changed from English by replacing the appropriate message files.

A. Yes

B. No

ANSWER: A

Explanation:

Yes. IdentityIQ's user-interface text is externalized into message-resource files, enabling the product to be localized without changing the application's Java source code. English message files provide the baseline text, and an implementation can replace or customize the appropriate message resources with translated content to establish another language as the effective default presentation language. This approach applies to labels, instructions, messages, and other UI strings resolved through IdentityIQ's localization framework. A careful implementation preserves the required message keys and resource-file naming and packaging conventions, while supplying translated values for the desired locale. This allows organizations to deliver a consistent user experience in their preferred language and to maintain custom translations as part of their IdentityIQ deployment artifacts. Localization should be performed using the documented message-catalog process so that translated resources can be managed appropriately through upgrades and deployment promotion. SailPoint's IdentityIQ documentation portal provides the product documentation, including administration and localization-related material: SailPoint IdentityIQ Documentation. SailPoint also provides customer documentation and support resources through SailPoint Community, where implementation teams can access version-specific guidance for message files and locale configuration.

QUESTION NO: 11

IdentityIQ is using emails to notify users about completion of steps within a process, or actions that need to be addressed. To ensure this notification is working, a main configuration must be set up in IdentityIQ to provide mail server and mail server authentication details.

Is this a required setting that an engineer must set up in IdentityIQ in order to ensure successful communication with the SMTP server?

Proposed Solution:

Mail Server Certificate

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. IdentityIQ email delivery is configured through its mail/SMTP settings, which provide the connection information IdentityIQ needs to send notifications, including the SMTP host and applicable port, authentication credentials

when the relay requires authentication, and relevant transport-security settings. A mail server certificate is not a universally required IdentityIQ configuration item for establishing SMTP communication. Its relevance depends on the SMTP server's TLS configuration and on whether the Java runtime hosting IdentityIQ trusts the certificate authority that issued the server certificate.

When an organization uses TLS and the SMTP endpoint presents a certificate that is not trusted by the application server JVM, an engineer may need to import the appropriate server or certificate-authority certificate into the JVM truststore. That is an environment-specific certificate-trust activity rather than a baseline mail-server field that must always be configured in IdentityIQ. Consequently, successful notification delivery is based on correct SMTP endpoint and authentication configuration, with certificate trust addressed only when the selected encrypted transport and trust chain require it. SailPoint's IdentityIQ documentation includes the application's system-configuration and email-related administration guidance at SailPoint IdentityIQ Documentation. Java's TLS certificate trust behavior is documented in the JSSE Reference Guide.

QUESTION NO: 12

Is this where email templates can be viewed after product installation?

Proposed Solution:

In the Debug page as an EmailTemplate object.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. IdentityIQ persists notification templates as `EmailTemplate` objects. Consequently, an authorized administrator or engineer can use the Debug pages to locate and inspect an email template object after IdentityIQ has been installed. This provides a direct way to verify that a template exists, identify its object name, and review the configured subject, body content, and variable references used when IdentityIQ generates notification messages.

Email templates support notifications generated by IdentityIQ features such as workflow processing, approval requests, lifecycle events, certification activities, and provisioning-related actions. Viewing the persisted object is particularly useful during troubleshooting when a notification is not being sent as expected, uses unexpected content, or references a template name supplied by a workflow or rule. The Debug interface is intended for administrative and diagnostic access to IdentityIQ objects, so access should be limited appropriately and changes should be managed through the organization's deployment and change-control process. SailPoint's documentation describes email-template configuration and its use in notifications, as well as the Debug pages used to inspect IdentityIQ data objects: IdentityIQ Email Templates and IdentityIQ Debug Pages.

QUESTION NO: 13

An identity's access is revoked during a certification. The affected application is currently unavailable, so IdentityIQ cannot complete the associated deprovisioning operation immediately.

Which statement is correct?

A. The revocation decision can remain recorded while its remediation remains incomplete until provisioning can be resolved.

B. The revocation decision is automatically changed to an approval when the target application is unavailable.

C. IdentityIQ removes the associated Link immediately, even though the target account still has the access.

D. The certification must be regenerated before remediation can be attempted again.

ANSWER: A

Explanation:

The certification decision and the remediation activity are separate parts of the process. IdentityIQ can retain the revocation decision and remediation work while the target-system operation remains incomplete. When the application becomes available, the remediation or provisioning processing can be retried or otherwise resolved according to the configured process.

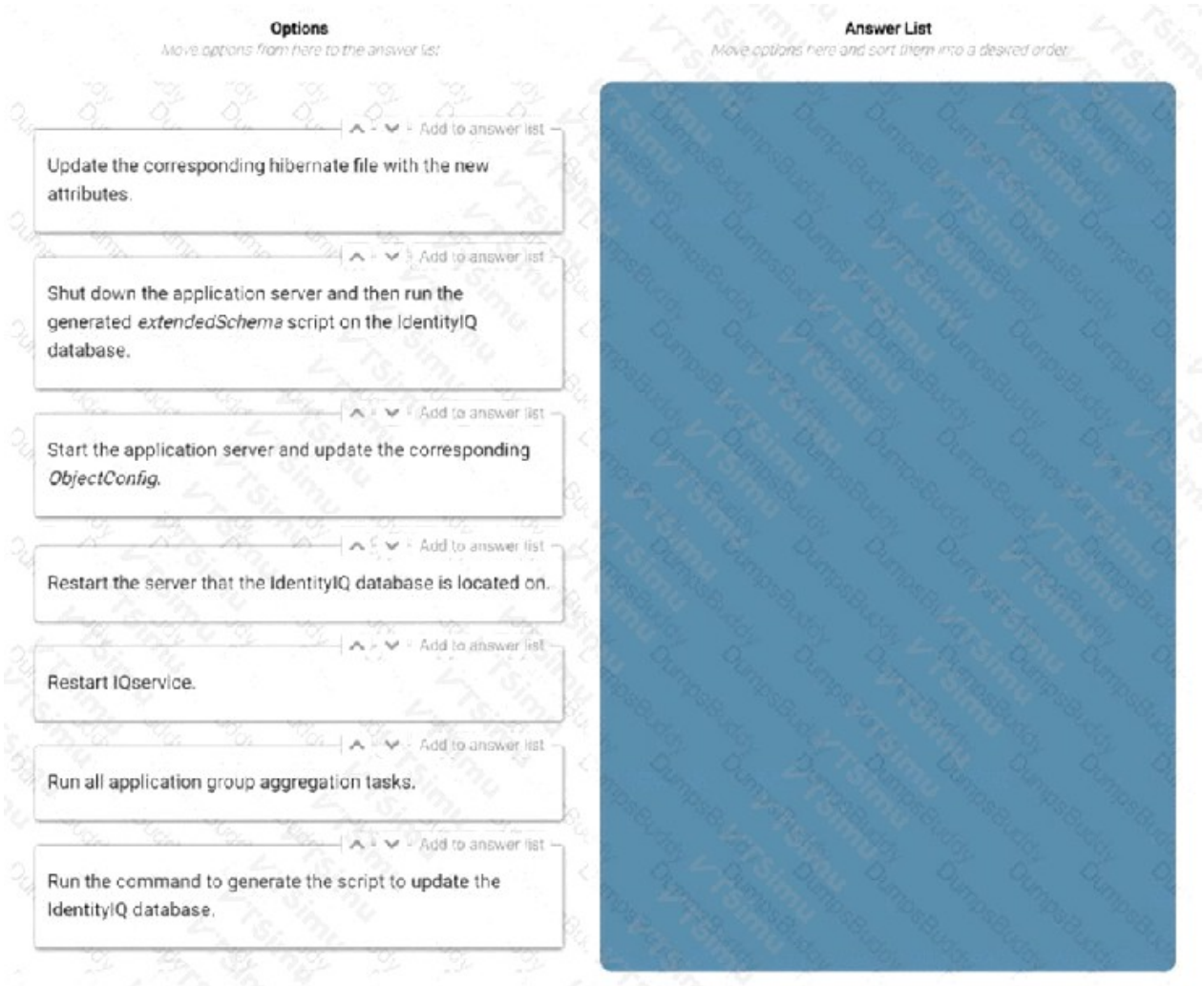
An approved certification decision is not automatically converted into an approval merely because a target application is unavailable. IdentityIQ should not silently remove the Link or entitlement data solely to make the Identity Cube appear compliant when the target access has not been changed. Restarting the certification is not required to preserve the decision.

QUESTION NO: 14 - (SIMULATION)

An IdentityIQ engineer needs to extend attributes in an IdentityIQ database after the database has been created.

What are the four minimum steps necessary to achieve this goal?

Drag four options from the left into the answer area on the right, and place them in the correct order.



ANSWER: Check the explanation for the answer

Explanation:

Place these four options in this order:

Update the corresponding hibernate file with the new attributes.

Run the command to generate the script to update the IdentityIQ database.

Shut down the application server and then run the generated `extendedSchema` script on the IdentityIQ database.

Start the application server and update the corresponding `ObjectConfig`.

The Hibernate mapping must define the new persisted attributes before the database-update script can be generated. Apply the generated schema changes while IdentityIQ is stopped, then restart IdentityIQ and update the applicable `ObjectConfig` so the new attributes are available to IdentityIQ.

QUESTION NO: 15

Can the following be achieved via configuration of control variables in the out-of-the-box Lifecycle Manager (LCM) workflows?

Proposed Solution:

Specify which applications support new account requests.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. Control variables in the out-of-the-box Lifecycle Manager workflows govern the execution of a request after the workflow has been launched. They can be used to control workflow behavior such as approval routing, policy evaluation, notification handling, provisioning execution, identity refresh behavior, and foreground or background processing. They are not the configuration layer that determines which target applications appear as eligible choices for a user requesting a new account.

The availability of a new-account request for a particular application is determined by the application's provisioning and account-request configuration. The application must be configured to support account creation, have the necessary schema and provisioning policy information, and be exposed through the relevant Lifecycle Manager request experience. This keeps application-specific capabilities and request eligibility in application configuration, while workflows remain reusable orchestration mechanisms for processing requests.

SailPoint's IdentityIQ documentation is organized around these separate administrative areas: application and provisioning setup versus Lifecycle Manager workflow configuration. See the SailPoint IdentityIQ documentation portal and SailPoint's IdentityIQ documentation resources for the applicable application configuration and Lifecycle Manager administration guidance.

QUESTION NO: 16

Can a Workgroup be used for the following scenario?

Solution: Providing a group of users with specific capabilities.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In IdentityIQ, a workgroup is an identity object used to represent a collection of users who share an administrative or business responsibility. Workgroups can be configured with capabilities, allowing IdentityIQ to grant the relevant functional privileges to the workgroup's members rather than requiring those capabilities to be administered separately for every individual. This makes workgroups appropriate when several users need the same IdentityIQ functions,

such as performing administrative activities, acting on assigned work items, or participating in governance processes appropriate to their responsibilities.

Using a workgroup centralizes capability administration: administrators maintain the membership and capability assignment at the workgroup level, and members receive the associated permissions through that membership. This supports consistent access for a team and reduces the effort and risk of managing equivalent capability assignments individually. Workgroups can also be used throughout IdentityIQ where a shared owner, recipient, or responsible party is needed, reinforcing their role as a reusable team-based administration construct. SailPoint's IdentityIQ documentation describes workgroups and their use in administration, including their membership and permission-related configuration: IdentityIQ Workgroups documentation. See also SailPoint's administrative reference for managing IdentityIQ capabilities: IdentityIQ Capabilities documentation.

QUESTION NO: 17

Can the search type in Identity be used to accomplish this result?

Proposed Solution:

Identifying details of a system error presented in the UI

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. In IdentityIQ, an Identity search is intended to locate and review identity objects and their associated business data, such as identity attributes, assigned roles, linked accounts, and lifecycle-related information. That scope can help an administrator identify the person affected by an issue, but it does not provide the diagnostic details needed to investigate an error rendered by the user interface. UI failures are application or server events and require the corresponding log information, including the error message, exception, stack trace, timestamp, and, where applicable, an incident identifier. IdentityIQ writes these details to its logging infrastructure, especially the syslog/application log output, where administrators can correlate a UI error with the underlying processing failure. This distinction is important during troubleshooting: first use the error or incident information displayed in the UI to locate the relevant log event, then review the server-side diagnostic context to determine the root cause. SailPoint's IdentityIQ documentation describes Identity search as a mechanism for working with identity data, while its system administration documentation covers logging and diagnostic configuration for operational errors. See SailPoint's Identity Search documentation and logging documentation.

QUESTION NO: 18

Is the following statement true about out-of-the-box reporting?

Solution: In the Reporting user interface, instances of reports are located on the ' My Reports ' tab, and templates are located on the ' Reports ' tab.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. IdentityIQ reporting distinguishes between report definitions (templates) and report results (instances). The *Reports* tab is the catalog of report templates available to the user. A template defines what a report can retrieve and display, including its report logic, columns, filters, and any runtime parameters that a user may be prompted to supply when running it. Running or scheduling a template creates a report instance: a particular execution of that definition with its selected parameters and generated output.

The *My Reports* tab is intended for the current user's report instances. It provides access to reports that the user has generated or that are available to that user, including their execution status and resulting output. This separation allows administrators and authorized users to manage reusable report definitions independently from the individual report runs created from those definitions. Therefore, the statement accurately describes the standard IdentityIQ Reporting user-interface organization. See SailPoint's IdentityIQ Reporting documentation and the report-template documentation for the reporting model and template management details.

QUESTION NO: 19

Is this what should be performed in order to generate the database script to extend Application attributes in the IdentityIQ database on the initial installation?

Solution: Run the command iiq extendedSchema in the IIQ_Home/WEB-INF/bin directory.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. IdentityIQ supports extending persistent object schemas, including the Application object, through its extended-schema mechanism. On an initial installation, after the required extended-attribute definitions have been added to the applicable IdentityIQ configuration, the `iiq extendedSchema` command is run from `IIQ_HOME/WEB-INF/bin`. This command evaluates the configured extended-schema definitions and generates the database-specific DDL script needed to create or alter the corresponding database columns and supporting schema objects. The generated script should be reviewed under the organization's database-change procedures and then executed against the IdentityIQ database so that the physical database schema matches the configured Application attributes. Performing this generation step is important because defining an attribute in IdentityIQ configuration alone does not create the required persistent database storage. SailPoint documents IdentityIQ product documentation and installation/configuration resources through its documentation portal; access requires the appropriate customer or partner entitlement. See the SailPoint Documentation portal and SailPoint's Compass Community for IdentityIQ documentation and implementation guidance.

QUESTION NO: 20

Can the Provisioning tab under " Administrator Console ' be used to do the following task?

Solution: Manually retry the provisioning attempt for pending transactions.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. In IdentityIQ, the Administrator Console's Provisioning tab provides operational controls for monitoring and managing provisioning activity, including transactions that have not completed successfully. A provisioning transaction can remain pending when IdentityIQ is awaiting processing, a connector response, or completion of a request sent to a target application. Administrators can use the provisioning administration views to locate the relevant pending transaction, review its state and associated details, and initiate a retry when it is appropriate to submit the provisioning work again. This capability supports recovery from temporary issues—such as target-system availability or transient connector communication problems—without requiring the administrator to recreate the original access request or manually construct a new provisioning plan. Before retrying, the administrator should verify that the underlying issue has been addressed and confirm that reprocessing will not create an unintended duplicate change in the connected system. SailPoint's IdentityIQ documentation describes the administrative and provisioning features used to oversee request processing and provisioning operations. See the IdentityIQ product documentation and SailPoint's IdentityIQ product documentation resources for the version-specific Administrator Console guidance.

QUESTION NO: 21 - (SIMULATION)

An implementation engineer needs to perform an initial installation of identityIQ.

Drag the options from the left into the answer area on the right, and place them in the correct order.

ANSWER: Check the explanation for the answer

Explanation:

Place the installation steps in this order:

1. Ensure all of the application servers are stopped.
2. Un-jar the IdentityIQ WAR file in the desired directory of each application server.
3. Configure `iiq.properties` file with database credentials and datasource.
4. Create the IdentityIQ database.
5. Update all necessary Hibernate XML files to include custom attributes.
6. Generate database schema to include custom attributes by executing `iiq schema`.
7. Initialize default IdentityIQ system objects from `iiq console` using the `import` command.
8. Start all of the application servers.
9. Apply the latest patch.

The Hibernate mappings must be updated before generating the schema so the required custom-attribute database structures are included. The default IdentityIQ objects are then imported only after the database schema exists.

QUESTION NO: 22

A customer wants to make changes in their IdentityIQ user interface.

Consider branding and other IdentityIQ UI changes. Is this statement valid?

Proposed Solution:

If SailPoint is removed from the header bar, “Powered by SailPoint IdentityIQ” must be added to the copyright footer.

A. Yes

B. No

ANSWER: A

Explanation:

Yes. The proposed solution preserves required SailPoint product attribution while permitting customer-specific branding of the IdentityIQ interface. IdentityIQ supports controlled user-interface customization, including changes to visual presentation and branding elements. However, removing SailPoint identification from a prominent location such as the header does not remove the obligation to identify the product. Placing the text “Powered by SailPoint IdentityIQ” in the copyright footer maintains clear attribution for the software while allowing the customer to use its own branding in the header area.

This approach is also consistent with good implementation practice: branding customizations should be isolated, documented, and reviewed during upgrades because customized UI resources can require validation after an IdentityIQ patch or version upgrade. The attribution text should remain visible and unmodified so that the deployed application continues to identify IdentityIQ as the underlying SailPoint product. SailPoint’s IdentityIQ documentation portal is available at SailPoint IdentityIQ Documentation, and SailPoint’s legal and intellectual-property information is available at SailPoint Legal.