Free Questions for IdentityIQ-Engineer

Shared by Clarke on 04-10-2024

Question 1

A client wants users who belong to an IdentitylQ workgroup named Management to be able to request entitlements and roles, but only for other users whose location attribute is the same as theirs.

Is this a population that will achieve the goal?

Solution: Create a quicklink population, set the membership match list to "All," and set "Who can members request for?'' as share attributes with the requester, with the attribute set to location.'

Options:

A- Yes

B- No

Answer:

A

Explanation:

This solution correctly addresses the client's requirement. By setting the membership match list to 'All' and configuring 'Who can members request for?' as 'share attributes with the requester,' with the attribute set to location, the system ensures that users in the 'Management' workgroup can only request roles and entitlements for other users who share the same location. This setup effectively filters based on the location attribute, aligning with the client's needs.

SailPoint IdentityIQ Quicklink Population Configuration Guide

SailPoint IdentityIQ Attribute-Based Access Control Guide

Question 2

Question Type: **MultipleChoice**

A client wants users who belong to an IdentityIQ workgroup named Management to be able to request entitlements and roles, but only for other users whose location attribute is the same as theirs.

Is this a population that will achieve the goal?

Solution: Create a quicklink population, set the membership match list to the IdentityIQ workgroup "Management," and set "Who can members request for?" as report to the requester.

Options:

A- Yes

B- No

Answer:

B

Explanation:

The provided solution does not fulfill the client's requirement. Setting 'Who can members request for?' to 'report to the requester' only limits the request scope to users who directly report to the requester, which does not account for the location attribute. The goal is to restrict requests based on the location attribute, and this specific configuration does not consider that attribute. To achieve the desired behavior, the configuration should include logic that filters users based on the same location as the requester.

SailPoint IdentityIQ Quicklink Population Configuration Guide

SailPoint IdentityIQ Advanced Population Management Guide

Question 3

Question Type: **MultipleChoice**

Can the following IdentityIQ object be extended to store client-specific data by updating the corresponding .HBM file?

Solution: WorkItem

Options:

A- Yes

B- No

Answer:

B

Explanation:

In SailPoint IdentityIQ, certain objects are designed to be extended by updating their corresponding Hibernate Mapping (.HBM) files. However, the WorkItem object is not one of these extendable objects. The WorkItem is a system object that primarily represents tasks or actions that need to be processed within the workflow. It is not intended to store client-specific data through direct modification of its .HBM file. Instead, client-specific data should be handled using other mechanisms, such as custom attributes or the extension of Identity or Account objects. Attempting to modify the WorkItem object's HBM file could lead to unexpected behavior and is not supported by SailPoint's best practices.

SailPoint IdentityIQ Customization Guide

SailPoint IdentityIQ Object Model Documentation

Question 4

Question Type: MultipleChoice

Can the following IdentityIQ object be extended to store client-specific data by updating the corresponding .HBM file?

Solution: Link

Options:

A- Yes

B- No

Answer:

B

Explanation:

In SailPoint IdentityIQ, certain objects, such as the Link object, cannot be directly extended by updating the corresponding .HBM (Hibernate Mapping) file. Modifying or extending core IdentityIQ objects typically requires a deeper level of customization involving the extension of the application schema and possibly custom Java code. The .HBM files are part of IdentityIQ's internal persistence framework, and altering them is not a supported or recommended method for extending objects in a production environment. Customization should instead be done using SailPoint's supported extension points, such as using ManagedAttributes or CustomAttributes within the IdentityIQ application framework. For guidelines on extending IdentityIQ objects, refer to the SailPoint IdentityIQ Customization Guide and best practices documentation.

Top of Form

Bottom of Form

Question 5

Question Type: **MultipleChoice**

An engineer needs to first create a custom audit event and then set up an associated report. What are four steps to accomplish this goal?

Solution: Create and load a Custom Audit Report TaskDefinition XML and corresponding Custom Audit Report Form XML.
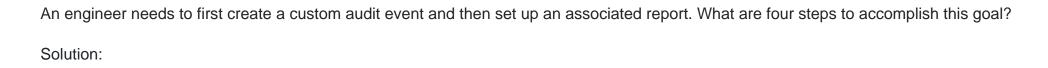
Options:

A- Yes

B- No

Answer:

A

Explanation:

Creating and loading a Custom Audit Report TaskDefinition XML and corresponding Custom Audit Report Form XML is indeed part of the process for setting up a custom audit report in SailPoint IdentityIQ. The TaskDefinition XML defines the report task, and the Form XML defines the user interface for running the report. These steps are essential to creating a custom audit report, and the solution correctly outlines a valid approach. Refer to the SailPoint IdentityIQ Reporting Guide, particularly the section on creating custom reports and forms, for more detailed instructions.

Question 6

Question Type: **MultipleChoice**

An engineer needs to first create a custom audit event and then set up an associated report. What are four steps to accomplish this goal?

Solution:

Set up a new AuditAction in the AuditConfig object XML:

`<ObjectAttribute displayName="User Type" editMode="Permanent" extendedNumber="2" name="userType" type="string"/>`

Options:

A- Yes

B- No

Answer:

B

Explanation:

The solution provided is incomplete. To create a custom audit event and set up an associated report, the process involves several steps, including defining the custom audit event in the Audit Configuration object, updating or creating relevant audit triggers in the system, and defining the custom report using XML or the IdentityIQ report editor. The steps mentioned in the solution do not cover the necessary configuration and implementation details required for this task. For a complete process, consult the SailPoint IdentityIQ Reporting Guide and the Audit Framework documentation.

Question 7

An engineer needs to first create a custom audit event and then set up an associated report. What are four steps to accomplish this goal?

Solution: Create a Data Export task.

Options:

A- Yes

B- No

Answer:

B

Explanation:

Creating a custom audit event and setting up an associated report involves steps such as defining the audit event, modifying the audit configuration, and creating a custom report using the SailPoint IdentityIQ reporting framework. Simply creating a Data Export task does not fulfill these requirements. A Data Export task is used for exporting data from IdentityIQ and is unrelated to the creation of custom audit events or custom reports. Refer to the SailPoint IdentityIQ Reporting Guide and the IdentityIQ Audit Framework documentation for more information on correctly creating and configuring custom audit events and reports.

Question 8

Is this a valid statement about connector rules?

Solution: A Post-Iterate Rule, if configured, is run after reading accounts from a SQL Loader application.

Options:

A- Yes

B- No

Answer:

A

Explanation:

A Post-Iterate Rule in SailPoint IdentityIQ is a type of connector rule that is executed after each account from the source system (e.g., SQL Loader application) has been read during the aggregation process. This rule allows for additional processing or customization of the data after the account has been iterated over. According to SailPoint IdentityIQ documentation, configuring a Post-Iterate Rule enables the execution of logic after each account's data has been processed, confirming that the given statement is valid. Refer to the SailPoint IdentityIQ Connector Development Guide for detailed information on rule execution during aggregation.