Quiz High Hit-Rate SCAIP - Saviynt Certified Advanced IGA Professional (Level 200) Passguide

For your convenience, TestInsides has prepared authentic Saviynt SCAIP Exam study material based on a real exam syllabus to help candidates go through their exams. Candidates who are preparing for the Saviynt exam suffer greatly in their search for preparation material.

Saviynt SCAIP Exam Syllabus Topics:

Topic	Details
Topic 1	• Access Request System: This section focuses on configuring and managing the end-to-end access request process, including workflows, approvals, and provisioning for both connected and disconnected applications.
Topic 2	• Rules Engineering: This section covers creating and managing automated access policies and rules that handle joiner, mover, and leaver scenarios through technical and user update rules.

Topic 3	• Building Identity Warehouse: This section covers setting up the foundation of Saviynt by importing users, onboarding applications, and managing roles and access within the identity warehouse.
Topic 4	• Analytics: This section focuses on building, configuring, and delivering reports, analytic controls, and dashboards to support data-driven identity governance decisions.
Topic 5	• Segregation of Duties: This section addresses identifying, preventing, and remediating SOD conflicts using rulesets, mitigating controls, and both preventative and detective analysis methods.

New SCAIP Dumps Pdf & New SCAIP Exam Book

As a customer you will want to choose low-price and high-passing rate products. Sometime it seems paradoxical. But now our Saviynt SCAIP exam questions vce will be a nice choice. If you care about price, there are many companies lower than us, if you care about passing rate I am sure there is little companies higher than us. Our SCAIP Exam Questions Vce highlight the quality and value for money; it is really worth to buy in this field.

Saviynt Certified Advanced IGA Professional (Level 200) Sample Questions (Q25-Q30):

NEW QUESTION # 25
An EIC Administrator has created a workflow containing hidden dynamic attributes; however, the administrator is unable to fetch the value of the hidden Dynamic Attributes in the request. How can this issue be resolved?

- A. Enable the "Expose hidden dynamic attributes in workflow" setting in Global Config
- B. Enable the "Expose hidden dynamic attributes in workflow" setting in Endpoint
- C. Enable the "Enable use for default attributes in workflow" setting in Global Config
- D. Enable the "Save Hidden Dynamic Attribute Default Value" setting in Global Config

Answer: A

Explanation:
In Saviynt EIC,Dynamic Attributesare often used in request forms to capture additional information, and some of these attributes may be configured ashidden fieldsfor backend processing. By default, hidden dynamic attributes are not exposed in workflows, which can prevent administrators from accessing their values during request processing.
To resolve this issue, Saviynt provides a specific configuration inGlobal Configurationscalled"Expose hidden dynamic attributes in workflow". Enabling this setting (Option A) ensures that even if the dynamic attributes are hidden in the UI, their values are still accessible within workflows for processing, approvals, and provisioning logic.
Option B is incorrect because this setting is not configured at the endpoint level. Option C relates to saving default values but does not ensure visibility in workflows. Option D is unrelated to hidden attribute exposure.
Thus, enabling theGlobal Config setting to expose hidden dynamic attributesis the correct solution to ensure their values are available within workflow execution.

NEW QUESTION # 26
In Saviynt App for ServiceNow, the manager is submitting a request for his subordinate, who is a valid SNOW user. However, when searching for the user, they are not appearing in the request form. What could be the potential issue?

- A. user already has access to the selected application
- B. user does not have the selected application account
- C. SNOW user is not linked to imported Saviynt user
- D. The logged in manager requires additional access to submit request

Answer: C

Explanation:

In Saviynt-ServiceNow integration, user visibility in request forms depends on properidentity correlation between ServiceNow users and Saviynt identities. The most common reason a valid ServiceNow (SNOW) user does not appear in the request form is that theSNOW user record is not linked or mapped to an imported Saviynt user(Option B).
Saviynt relies on its internal identity repository to populate requestable users. Even if a user exists in ServiceNow, they must also exist in Saviynt and be properly correlated (typically via attributes like username, email, or employee ID). Without this linkage, Saviynt cannot recognize the user during request submission, and therefore the user will not appear in the search results.
Option A is incorrect because even if the user already has access, they would still appear in search results (though requests may be restricted). Option C is unrelated to user visibility. Option D is incorrect because lack of an account does not prevent user selection-it only affects provisioning outcomes.
Thus, properuser correlation between SNOW and Saviyntis essential for request visibility.

NEW QUESTION # 27
For which of the following options duplicate identities can be identified in EIC?

- A. All of the above
- B. By running Duplicate Identity Detection Job
- C. While Importing Users
- D. While Updating Users through Admin > Identity Repository

Answer: A

Explanation:
In Saviynt EIC,Duplicate Identity Management (DIM)supports multiple mechanisms to detect duplicate identities across the identity lifecycle, makingOption D (All of the above)the correct answer.
Firstly, duplicate identities can be detectedduring user import (Option A)when data is ingested from authoritative sources like HR systems. Saviynt can apply matching rules and prevent or flag duplicates at the ingestion stage. Secondly, duplicates can be identified by executing theDuplicate Identity Detection Job (Option B), which is a detective control that scans existing identities in the repository and identifies potential duplicates based on configured correlation rules such as email, username, or employee ID.
Additionally, duplicates may also be identifiedduring manual updates in the Identity Repository (Option C) when administrators modify user attributes. If updated values match existing identities based on defined criteria, Saviynt can flag potential duplicates.
These multiple detection points ensure both proactive and reactive duplicate management, helping maintain identity data accuracy and preventing access risks associated with duplicate identities.

NEW QUESTION # 28
Which option can be used in the REST Connector to perform attribute mapping between target application and EIC?

- A. UpdateAccountJSON
- B. CreateAccountEntJSON
- C. ImportAccountEntJSON
- D. CreateAccountJSON

Answer: D

Explanation:
In Saviynt EIC REST connector configurations,attribute mapping between Saviynt and the target applicationis primarily handled during provisioning operations such as account creation and updates. Among the given options,CreateAccountJSONis the correct configuration where attribute mapping is explicitly defined for provisioning new accounts in the target system.
CreateAccountJSON (Option C)contains the payload structure and field mappings that determine how Saviynt attributes (such as username, email, department, etc.) are translated into the target application's API request format. Administrators define mappings using placeholders and transformation logic to ensure correct data flow from Saviynt to the external system.
OptionA (ImportAccountEntJSON)is used for reconciliation (importing accounts and entitlements), not provisioning. OptionB (CreateAccountEntJSON)is not a standard REST connector configuration in Saviynt.
OptionD (UpdateAccountJSON)is used for modifying existing accounts, but the primary and most commonly referenced mapping configuration for attribute mapping is defined in CreateAccountJSON during initial provisioning.
Thus,CreateAccountJSONis the correct answer for attribute mapping between EIC and the target application.

NEW QUESTION # 29

A customer requires provisioning of time-bound access through roles that should be revoked automatically after certain days from the day of assignment. What option in EIC will help the customer achieve this requirement?

- A. Enable Time-bound for Roles in Global Configurations > Roles
- B. Configure an Emergency Access Role
- C. Configure an Enterprise Role and enable timestamp under Role Details
- D. Configure Dynamic Attributes for Roles

Answer: A

NEW QUESTION # 30

.....

These Saviynt Certified Advanced IGA Professional (Level 200) (SCAIP) exam questions are a one-time investment to clear the SCAIP test in a short time. These SCAIP exam questions eliminate the need for candidates to study extra or irrelevant content, allowing them to complete their Saviynt test preparation quickly. By avoiding unnecessary information, you can save time and crack the Saviynt Certified Advanced IGA Professional (Level 200) (SCAIP) certification exam in one go. Check out the features of the three formats.