DUMPSARENA

Saviynt Certified Advanced IGA Professional (Level 200)

Saviynt SCAIP

Version Demo

Total Demo Questions: 6

Total Premium Questions: 69

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which campaign type should be used when managers must review and certify access for their direct reportees?

A. User Manager Campaign

B. Entitlement Owner Campaign

C. Role Owner Campaign

D. Service Account Campaign

ANSWER: A

Explanation:

User Manager Campaign is the appropriate campaign type because it assigns the access-certification review to each user's manager, using the organizational reporting relationship. This supports a manager-led access review in which managers evaluate whether their direct reportees still need the accounts, roles, and entitlements they hold. The manager is normally best positioned to validate the user's current job responsibilities, team assignment, and business need for access, which makes this campaign type suitable when the review population is defined by direct-report hierarchy.

In Saviynt Enterprise Identity Cloud, certifications are generated and routed according to the campaign configuration and the selected certifier model. A User Manager Campaign operationalizes the principle of periodic access recertification by sending the relevant review items to the manager responsible for each employee. Managers can then certify, revoke, or otherwise take the configured remediation actions for their reportees' access. This provides an auditable review process aligned to managerial accountability and least-privilege governance. Saviynt's access-governance and certification capabilities are described on the Saviynt Identity Governance and Administration page and in the Saviynt Resources portal.

QUESTION NO: 2

In the Saviynt App for ServiceNow, what options are available to refresh the RITM status in the ServiceNow app based on the respective Saviynt's status? (Multi-Select)

A. Make a Postman API call

B. Click Refresh button on the RITM page in ServiceNow

C. It will be automatically updated in 1 minute via Request item history job in ServiceNow

D. Regenerate application catalog item

ANSWER: B C

Explanation:

The available RITM-status refresh mechanisms are **Click Refresh button on the RITM page in ServiceNow** and **It will be automatically updated in 1 minute via Request item history job in ServiceNow**. The Refresh action on an individual Request Item provides an on-demand synchronization path: when a ServiceNow user needs the most current fulfillment state, the app can retrieve the corresponding request status from Saviynt and update the RITM without waiting for the scheduled process. This is particularly useful when an approver, requester, or fulfiller is actively tracking a request.

The Request Item History Job provides the complementary background synchronization mechanism. It periodically evaluates request-item history and updates ServiceNow RITM records to reflect the current Saviynt request status. With the job running at its configured short interval, ServiceNow remains aligned with Saviynt even when no user manually opens or refreshes a particular RITM. Together, these capabilities support both immediate, user-initiated status verification and ongoing automated reconciliation of request progress. Saviynt product documentation and integration guidance are available through the Saviynt Documentation portal; ServiceNow's platform documentation is available at ServiceNow Docs.

QUESTION NO: 3

An organization is planning its Saviynt and ServiceNow architecture. It needs to govern ServiceNow accounts as a target application, allow users to submit access requests from ServiceNow, and use ServiceNow tickets for disconnected-application fulfillment. Which integration options support these requirements? (Choose 3 options)

A. ServiceNow as a Managed Application

B. ServiceNow as a Request Form

C. ServiceNow as a Ticketing System

D. ServiceNow as a Role Mining engine

ANSWER: A B C

Explanation:

ServiceNow can be integrated with Saviynt as a Managed Application, as a Request Form, and as a Ticketing System. In the managed-application model, Saviynt can import and govern ServiceNow accounts and access. In the request-form model, ServiceNow provides the requester-facing experience while Saviynt applies approval, policy, and fulfillment processing. In the ticketing-system model, ServiceNow manages fulfillment tickets, including for disconnected applications.

Role Mining is a Saviynt access-analysis capability and is not a ServiceNow integration option.

QUESTION NO: 4

An EIC Administrator has a requirement to execute provisioning as soon as the user import is completed, what type of job can be configured to achieve this?

A. Multi threading job

B. Trigger chain job

C. Single Threaded Job

D. WSRetry job

ANSWER: B

Explanation:

Trigger chain job is the appropriate configuration because it orchestrates dependent Saviynt jobs based on the completion of a preceding job. An administrator can configure the user-import process as the initiating job and configure provisioning as the subsequent job in the chain. When the import completes successfully, Saviynt launches the next configured process without requiring an administrator to wait for a separate schedule or manually start provisioning. This is useful where imported identity data must be available before access-related changes are evaluated and provisioned, preserving the intended lifecycle sequence and reducing delay between ingestion and fulfillment. Trigger chains therefore provide event-driven job sequencing rather than simply controlling parallelism or an individual job's execution behavior. Saviynt's documentation resources describe the platform's job and task automation capabilities, while its product documentation portal provides the detailed configuration guidance available to customers: Saviynt Documentation and Saviynt Identity Cloud.

QUESTION NO: 5

Choose the correct SQL query from the below options to populate an attribute with the logged-in user's Display Name

A. select DISPLAYNAME as ID from Users u where u.userkey=${loggedInUser}

B. select DISPLAYNAME as ID from Users u where u.userkey=${user.id}

C. select DISPLAYNAME as ID from Users u where u.userkey=${requestor}

D. All the above

ANSWER: A

Explanation:

The query `select DISPLAYNAME as ID from Users u where u.userkey=${loggedInUser}` is the appropriate choice because it uses Saviynt's logged-in-user context variable to identify the user who is currently authenticated in the active session. The `Users` table is then filtered by that user's internal key, and the query returns the corresponding `DISPLAYNAME`. Aliasing the selected value as `ID` follows the common Saviynt query-based attribute/list pattern, in which the returned value is consumed to populate the configured attribute at runtime.

This approach is context-aware: the result changes automatically according to the current session user rather than requiring a fixed identity or manually supplied value. It is therefore suitable when a form, dynamic attribute, or request-related configuration must show the active user's display name. Saviynt's documentation portal provides product documentation and configuration guidance for Identity Cloud, including request and form configuration concepts: Saviynt Documentation. Saviynt's product overview also describes the Identity Cloud platform and its identity-governance capabilities: Saviynt Identity Cloud.

QUESTION NO: 6

Which capabilities are supported for Active Directory groups through Saviynt group management? (Multi-Select)

A. Create groups

B. Update groups

C. Delete groups

D. Only launch certification campaigns

ANSWER: A B C

Explanation:

Create groups, **Update groups**, and **Delete groups** are supported capabilities for Active Directory group management in Saviynt when the Active Directory or ADSI connection and its group-management operations are appropriately configured. Saviynt Group Management provides lifecycle administration for group objects, rather than merely displaying group data. This includes provisioning a new group in the connected directory, modifying supported group properties after creation, and removing a group when it is no longer required. The group-management lifecycle can also encompass maintaining associated data such as memberships, owners, and configured group attributes, subject to the connector configuration and the permissions of the account used by the connection.

These lifecycle operations are important in an IGA implementation because they allow governed group administration to occur through Saviynt workflows and controls while changes are executed in Active Directory. In practice, the exact attributes and operations available depend on the AD connector configuration, endpoint definitions, and delegated directory permissions, but create, update, and delete are the core supported group-object actions. Saviynt's product documentation portal contains the connector and group-management guidance used to configure these functions: Saviynt Documentation. Additional product and identity-governance resources are available from Saviynt.