Saviynt SAVIGA-C01 Practice Questions

Shared by Bonner on 08-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An Application Owner Campaign can have multiple primary Certifiers and a single secondary Certifier.

Options:

A- True
B- False

Answer:

B

Explanation:

The statement 'An Application Owner Campaign can have multiple primary Certifiers and a single secondary Certifier' is generally False in Saviynt. Here's why:

Saviynt's Application Owner Campaign: This campaign type is designed for Application Owners to review and certify access to their applications.

Primary Certifier: There is usually a single designated Application Owner for each application. This is because application ownership is typically a single point of accountability. While it is technically possible to assign multiple owners, it is not considered a best practice.

Secondary Certifiers (Backup/Delegates): Application Owner Campaigns can have multiple secondary certifiers. These are often used as:

Backup: To ensure the campaign can proceed if the primary certifier is unavailable.

Delegates: To allow the primary certifier to delegate some of the certification tasks.

Consultants: Other stakeholders, such as security or compliance teams, who can be consulted during the decision-making process.

Why the Statement Is Generally False: The core principle of application ownership implies a single point of accountability. While multiple secondary certifiers can assist, having multiple primary certifiers can lead to confusion and conflicting decisions.

Possible Exceptions (Less Common):

Highly Customized Configurations: In some very specific scenarios, organizations might customize Saviynt to allow multiple primary certifiers for an application, but this is not a standard or recommended practice.

Question 2

Question Type: MultipleChoice

Which option best aspects in EIC is regarded as a unique identity of a person?

Options:

A- Endpoint
B- Employee
C- Account
D- User

Answer:

D

Explanation:

In Saviynt, a User represents the unique identity of a person. It's the central object that ties together all the information about an individual, including their accounts, entitlements, roles, and attributes.

Why other options are incorrect:

Endpoint: Represents a system or application, not a person.

Employee: While many users might be employees, the term 'user' is more general and can include contractors, partners, etc.

Account: Represents a user's access to a specific system, not their overall identity.

Saviynt IGA Reference:

Saviynt Documentation: Throughout the documentation, 'User' consistently refers to the individual's identity within the system.

Saviynt User Interface: The User Management section in Saviynt focuses on managing the lifecycle and access of individual users.

Question 3

Question Type: MultipleChoice

_____ filters the requestable applications under "Request New Access."

Options:

A- Access Add Workflow
B- Access Query
C- Provisioning Connection
D- Whom to Request

Answer:

B

Explanation:

The component that filters the requestable applications under 'Request New Access' in Saviynt is the Access Query. Here's a detailed explanation:

Saviynt's Access Request System (ARS): As the front end for requesting access, the ARS needs a mechanism to determine which applications (and entitlements) should be displayed to a user as requestable.

Access Query: This is a powerful feature within Saviynt that allows administrators to define specific criteria to control the visibility of applications and entitlements in the ARS. Think of it as a filter that determines what a user can see and request.

How Access Queries Work:

Defined on Applications/Entitlements: Access Queries are configured on individual applications or entitlements within Saviynt.

Based on User Attributes: They use user attributes (e.g., department, location, job title, group memberships) and other criteria (e.g., risk level) to determine if a user should see a particular application or entitlement.

Dynamic Filtering: When a user accesses the 'Request New Access' section, Saviynt evaluates the Access Queries associated with each application and entitlement in real-time. Based on the user's attributes, the system dynamically filters the list, showing only the applications and entitlements that match the query conditions.

Saviynt's Security Model: Access Queries are a fundamental part of Saviynt's security model. They ensure that users are only presented with access options that are relevant and appropriate for their role and context, preventing accidental over-provisioning and reducing the attack

surface.

Other Options:

Access Add Workflow: While essential for processing access requests, the workflow itself doesn't filter which applications are initially displayed.

Provisioning Connection: This relates to how Saviynt connects to target systems for automated provisioning. It doesn't control the initial visibility of applications in the ARS.

Whom to Request: This setting might determine the available approvers, but it doesn't filter the list of requestable applications.

In essence: Access Queries act as a dynamic filter, leveraging user attributes and defined criteria to determine which applications and entitlements are presented to a user within Saviynt's 'Request New Access' interface, ensuring a personalized and secure access request experience.

Question 4

Question Type: MultipleChoice

John, who recently joined an organization as a full-time employee, is required to work from the Sydney office. He was assigned birthright entitlements as part of the new joiner provisioning. Which of the following Enterprise Roles will be assigned to John from the Birthright Rule?

Options:

A- Birthright - Sydney
B- Birthright - Permanent - Full-time
C- Birthright - All
D- Birthright - Employee

Answer:

A

Explanation:

In this scenario, where John is a new full-time employee required to work from the Sydney office, the most specific and appropriate Enterprise Role assigned from the Birthright Rule would likely be A. Birthright - Sydney. Here's the reasoning:

Saviynt's Birthright Roles and Rules: Birthright roles are designed to automatically provision

access based on specific criteria like location, job role, or employment type. Birthright rules define the conditions for assigning these roles.

Specificity of Role Assignment: The goal is to assign the most relevant and granular role based on the available information. In this case, John's location (Sydney) is the most specific criterion mentioned.

Why Other Options Are Less Likely:

B . Birthright - Permanent - Full-time: While John is a full-time employee, this role might be too broad if there are other location-specific roles.

C . Birthright - All: This role is likely too generic and would grant excessive access. It's generally not good practice to have an 'all-encompassing' birthright role.

D . Birthright - Employee: Similar to the 'Full-time' role, this might be too broad if location-specific roles are available.

Best Practices: It's a best practice in identity governance to use the most specific criteria possible when assigning birthright access. This helps enforce the principle of least privilege.

In summary: The 'Birthright - Sydney' role is the most appropriate choice because it aligns with John's specific work location, ensuring he receives the necessary access for his role while adhering to the principle of least privilege.

Question 5

Question Type: MultipleChoice

Single Sign-On is enabled in EIC using Azure Identity Provider. In this scenario, can the user log in using Azure and EIC native authentication?

Options:

A- True
B- False

Answer:

B

Explanation:

When Single Sign-On (SSO) is enabled in Saviynt EIC using an external Identity Provider (IdP)

like Azure AD, it generally becomes the exclusive authentication method. This means users cannot use Saviynt's native authentication (i.e., logging in with a username/password stored directly within Saviynt).

Reasons for this:

Security and Centralized Control: SSO with an IdP enhances security by centralizing authentication and enforcing stronger password policies. Allowing native logins would create a potential bypass of these security measures.

User Experience: SSO provides a seamless login experience, eliminating the need for users to remember multiple credentials. Offering both SSO and native logins could lead to confusion and a less streamlined process.

Administrative Efficiency: SSO simplifies user management by delegating authentication to the IdP. Administrators don't need to manage separate user accounts and passwords within Saviynt.

Saviynt IGA Reference:

Saviynt Documentation: Saviynt's documentation on SSO configurations emphasizes that enabling SSO typically disables native authentication methods.

Saviynt Best Practices: Saviynt's best practices for SSO recommend enforcing SSO as the sole authentication method for improved security and user experience.

Saviynt Implementation Guides: Implementation guides for setting up SSO with various IdPs, including Azure AD, often highlight the exclusive nature of SSO authentication.

Question 6

Question Type: MultipleChoice

Which of the following connection types is best suited to expose Workday reports as a data service?

Options:

A- Workday-RAAS
B- Workday-REST
C- Workday-OAuth
D- Workday-SOAP

Answer:

A

Explanation:

The connection type best suited to expose Workday reports as a data service in Saviynt is A. Workday-RAAS (Report as a Service). Here's why:

Workday-RAAS: This connection type is specifically designed to integrate with Workday's RaaS functionality. Workday RaaS allows you to expose custom reports created within Workday as web services that can be consumed by external applications like Saviynt.

Data Service for Reports: RaaS essentially turns a Workday report into a data service, making it easy to retrieve the report's data in a structured format (typically XML or JSON).

Saviynt's Integration: Saviynt's Workday-RAAS connection type is built to leverage this capability, allowing you to:

Select Workday Reports: Choose the specific Workday reports you want to integrate with.

Import Data: Import the data from those reports into Saviynt for various purposes (e.g., identity governance, access certification, analytics).

Schedule Imports: Schedule regular data imports to keep Saviynt's data synchronized with Workday.

Why Other Options Are Less Suitable:

B . Workday-REST: While Workday has a REST API, it's more general-purpose and not specifically tailored for exposing reports as data services in the same way as RaaS.

C . Workday-OAuth: OAuth is an authorization protocol, not a connection type for retrieving report data.

D . Workday-SOAP: Workday's SOAP API is being gradually replaced by the REST API and is less focused on report data retrieval than RaaS.

Question 7

Question Type: MultipleChoice

Which of the following options can a Campaign Owner use to view the Entitlements Query that was used in a previously launched Campaign?

Options:

A- Reconfigure option
B- Campaign Export

C- Campaign Summary
D- Export option at the top right corner of the page, next to the Refresh Progress option

Answer:

C

Explanation:

To view the Entitlements Query used in a previously launched Campaign in Saviynt, a Campaign Owner can use the C. Campaign Summary. Here's why:

Saviynt's Campaign Summary: The Campaign Summary provides a detailed overview of a campaign's configuration, including:

Campaign Scope: The users, applications, or entitlements included in the campaign.

Filters and Queries: Any filters or queries used to define the campaign scope, including the Entitlements Query.

Certifier Information: Details about the assigned certifiers.

Schedule: The campaign's start and end dates.

Status: The current status of the campaign (e.g., Active, Completed, Expired).

Accessing the Entitlements Query: The Campaign Summary typically includes a section that displays the exact query used to select the entitlements included in the campaign.

Why Other Options Are Less Suitable:

A . Reconfigure option: While you might be able to see the query by going into the reconfiguration, it's not the most direct way. The Campaign Summary is designed to provide this information readily.

B . Campaign Export: Exporting the campaign data might include the list of entitlements but not necessarily the original query used to select them.

D . Export option at the top right corner of the page, next to the Refresh Progress option: This option typically exports the current view of the campaign data, not the underlying configuration details like the Entitlements Query.

In conclusion: The Campaign Summary in Saviynt is the most direct and convenient place for a Campaign Owner to review the detailed configuration of a campaign, including the Entitlements Query used to define the campaign's scope.

Question 8

Question Type: MultipleChoice

A Campaign Owner can create various types of a User Manager Campaign to save different settings for various categories of Manager Access Reviews.

Options:

A- Global Configurations
B- Campaign Types
C- Campaign Templates
D- Campaign Previews

P2P exams

Answer:

C

Explanation:

To save different settings for various categories of Manager Access Reviews within User Manager Campaigns, a Campaign Owner can create C. Campaign Templates. Here's why:

Saviynt's Campaign Templates: Templates allow you to pre-configure various settings for a campaign and save them as a reusable template. This includes settings related to:

Campaign Scope: Defining which users, applications, or entitlements are included.

Certifier Selection: Specifying the type of certifiers (e.g., Managers, Application Owners).

Scheduling and Notifications: Setting up the campaign schedule and email notifications.

Advanced Configurations: Including filters, risk scores, and other advanced settings.

Multiple Templates for Different Categories: A Campaign Owner can create multiple templates, each tailored to a specific category of Manager Access Review. For example:

Template 1: For high-risk applications, with stricter filters and more frequent reviews.

Template 2: For low-risk applications, with broader scope and less frequent reviews.

Template 3: For specific departments or business units, with customized certifier selection.

Benefits of Using Templates:

Consistency: Ensures that similar types of reviews are conducted consistently.

Efficiency: Saves time by eliminating the need to configure each campaign from scratch.

Reduced Errors: Minimizes the risk of manual configuration errors.

Why Other Options Are Less Suitable:

A . Global Configurations: Global configurations apply to all campaigns, not to specific categories of reviews.

B . Campaign Types: Campaign types (e.g., User Manager, Entitlement Owner) define the overall purpose of the campaign, not the specific settings for different categories within a campaign type.

D . Campaign Previews: Previews are for reviewing the campaign data before launch, not for saving different configurations.

In conclusion: Campaign Templates in Saviynt provide a powerful way to save and reuse different configurations for various categories of Manager Access Reviews, promoting consistency, efficiency, and accuracy in the certification process.

Question 9

Question Type: MultipleChoice

The following USER_IMPORT_MAPPING attribute is set up in Workday RAAS connection:

USER_IMPORT_MAPPING

{

"ImportType": "RAAS",

"ResponsePath": "wd:Report_Data.wd:Report_Entry",

"ImportMapping": {

"USERNAME": "wd:User_Name~#~string",

"SYSTEMUSERNAME": "wd:User_Name~#~string",

"FIRSTNAME": "wd:First_Name~#~string",

"CITY": "wd:Location.wd:Descriptor~#~string"

}

}

As per the above mapping, USERNAME is the user attribute defined in Workday, and User_Name is the attribute defined in EIC.

Options:

A- True
B- False

Answer:

B

Explanation:

The statement is False. In the provided USER_IMPORT_MAPPING, USERNAME is the user attribute defined in EIC (Enterprise Identity Cloud), and wd:User_Name is the attribute defined in Workday. Here's a breakdown:

Saviynt's USER_IMPORT_MAPPING: This configuration within a connection (in this case, Workday RAAS) defines how data from the connected system (Workday) should be mapped to attributes within Saviynt's EIC.

ImportMapping: This section specifies the mapping between source attributes (Workday) and target attributes (EIC).

USERNAME: In the provided mapping, USERNAME (without the wd: prefix) is the target attribute, meaning it's an attribute within Saviynt's EIC.

wd:User_Name: The wd: prefix typically indicates a Workday attribute. Therefore, wd:User_Name is the source attribute from Workday.

~#~string: This likely indicates the data type of the attribute (string in this case).

Correct Interpretation: The mapping is saying: 'Take the value of the wd:User_Name attribute from Workday and map it to the USERNAME attribute in EIC.'

In essence: The USER_IMPORT_MAPPING defines how data from Workday is translated into Saviynt's internal data model, and in this case, USERNAME belongs to Saviynt (EIC), while wd:User_Name belongs to Workday.

Question 10

Question Type: MultipleChoice

There is a requirement to have multiple users as Campaign Owners for a User Manager Campaign.

Which of the following configurations would be appropriate to achieve this?

Options:

A- Create a user Query and add users
B- Create a user group and choose the user group as the Campaign Owner
C- Create a Roles Query and add Roles of various users
D- Create an Organization Query and add users

Answer:

B

Explanation:

To have multiple users as Campaign Owners for a User Manager Campaign in Saviynt, the appropriate configuration is to B. Create a user group and choose the user group as the Campaign Owner. Here's the explanation:

Saviynt's User Groups: User groups are collections of users that can be used for various purposes, including assigning roles, permissions, and ownership.

Campaign Owner as a User Group: Saviynt allows you to specify a user group as the owner of a campaign. This means that all members of the group will have the same campaign ownership permissions.

Benefits of Using a User Group:

Simplified Management: It's easier to manage a group of users than to assign individual users as campaign owners.

Flexibility: You can easily add or remove users from the group to adjust campaign ownership as needed.

Shared Responsibility: All members of the group share responsibility for managing the campaign.

Why Other Options Are Less Suitable:

A . Create a user Query and add users: While you can use queries to select users, directly using a user group is a more standard and manageable approach for assigning multiple campaign owners.

C . Create a Roles Query and add Roles of various users: Roles are typically used for granting access rights, not for defining campaign ownership.

D . Create an Organization Query and add users: Organization queries are related to the organizational structure and are not the best way to define a group of campaign owners.

In conclusion: Using a user group as the Campaign Owner in Saviynt provides a flexible and manageable way to assign multiple users as owners, simplifying administration and promoting

shared responsibility for campaign management.

P2P exams

P2P exams

To Get Premium Files for SAVIGA-C01 Visit

https://www.p2pexams.com/products/saviga-c01

For More Free Questions Visit

https://www.p2pexams.com/saviynt/pdf/saviga-c01

